UNIVERSITÁ DEGLI STUDI DI CAMERINO

SCIENZE E TECNOLOGIE INFORMATICHE

Corso di Laurea in Informatica

Classe 26

Scansione ed Analisi Di Vulnerabilità

Case study: Burp Suite

Tesi di Laurea in

Reti di Elaboratori

Relatore

Prof. Fausto Marcantoni

Studente

Koliou Georgios

Ai miei genitori e a Niki

INDICE

Abstract

Il problema della sicurezza informatica è un tema che tutti riconoscono come importante ma a cui ben pochi prestano attenzione. Questo è particolarmente vero se parliamo di dispositivi sempre più ricchi di funzionalità di uso quotidiano e di conseguenza di scambio di dati sensibili che spesso sono di grande valore per un malintenzionato. Purtroppo, alla rapidissima evoluzione tecnologica dei nostri dispositivi non è corrisposta una nostra evoluzione in termini di consapevolezza dei rischi che corriamo e delle buone abitudini di utilizzo del dispositivo. Spesso succede invece che continuiamo a usare il nostro dispositivo con la stessa leggerezza di quando era uno strumento in grado soltanto di effettuare e ricevere chiamate, o di semplice elaborazione di documenti.

La Sicurezza informatica è il ramo dell'informatica che si occupa dell'analisi delle vulnerabilità, del rischio, delle minacce e della successiva protezione dell'integrità logico-funzionale. In particolare, nella sicurezza delle reti si valutano l'eventuale presenza di vulnerabilità dei singoli nodi che compongono la rete, la sicurezza dello scambio di informazioni tra i nodi e tutto quello che riguarda l'interfacciarsi di un nodo in una rete. Negli ultimi anni ha acquisito progressivamente maggiore interesse a causa della crescente informatizzazione della società e dei servizi, in particolare per i settori dove le informazioni conservate, scambiate o create sono di importanza critica. La problematica della sicurezza delle reti consiste nel compromesso tra le misure di sicurezza da adottare per proteggere la rete da accessi indesiderati e la versatilità con cui essa opera. Particolarmente critica è la problematica legata alla presenza di vulnerabilità che può compromettere l'intero funzionamento della rete stessa e l'integrità dei nodi da cui è composta.

Introduzione

Scopo della tesi

La sicurezza informatica è un argomento vasto, che copre una moltitudine di problemi. Nella forma più semplice, riguarda come fare in modo che intrusi non riescano a leggere (o modificare di nascosto) i messaggi destinati a terzi. Si occupa inoltre, di impedire che determinate persone possano accedere a servizi remoti che non sono autorizzati ad usare. La sicurezza si occupa anche di come accertarsi dell'identità dei mittenti dei messaggi, di come impedire l'intercettazione e la ripetizione di messaggi legittimi catturati sulla rete e di come perseguire chi afferma di non aver mai spedito certi messaggi.

Alternative di Burp Suite

Mitmproxy

Mitmproxy si usa per il debug, i test, le misurazioni della privacy e i test di penetrazione. Può essere utilizzato per intercettare, ispezionare, modificare e riprodurre nuovamente il traffico Web come HTTP / 1, HTTP / 2, WebSocket o qualsiasi altro protocollo protetto da SSL / TLS. È possibile preimpostare e decodificare una varietà di tipi di messaggi che vanno da HTML a Protobuf, intercettare al volo messaggi specifici, modificarli prima che raggiungano la loro destinazione e riprodurli successivamente su un client o un server.

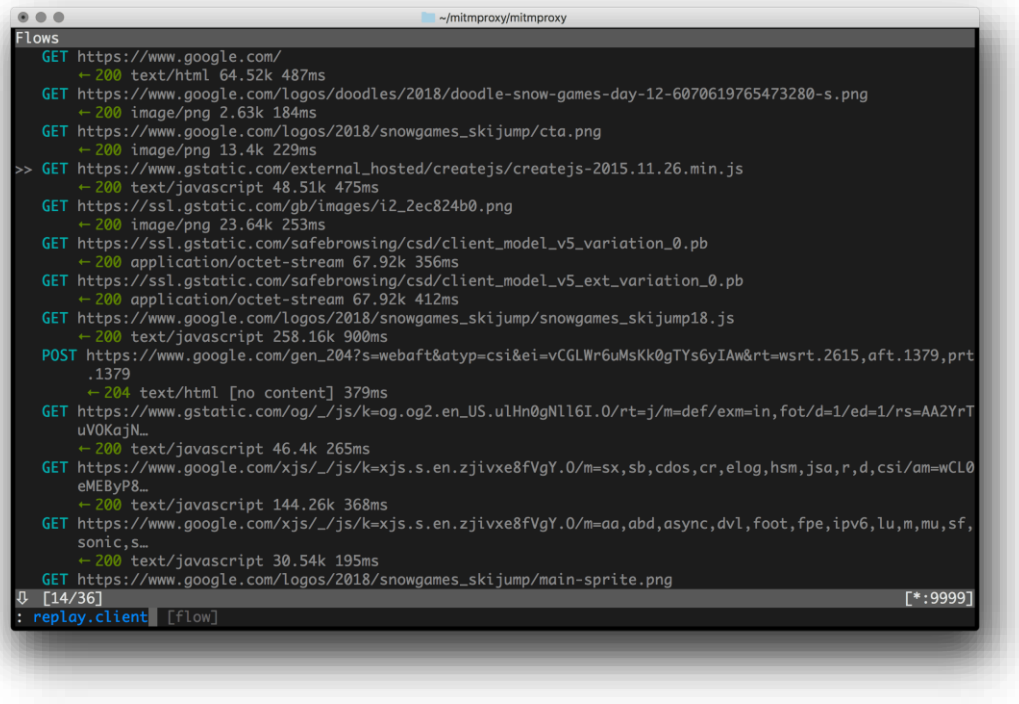


Immagine presa da mitmproxy.org

Interfaccia Web

Usa le funzionalità principali di mitmproxy in un'interfaccia grafica con mitmweb. mitmweb ti offre un'esperienza simile per qualsiasi altra applicazione o dispositivo, oltre a funzionalità aggiuntive come l'intercettazione e la riproduzione delle richieste.

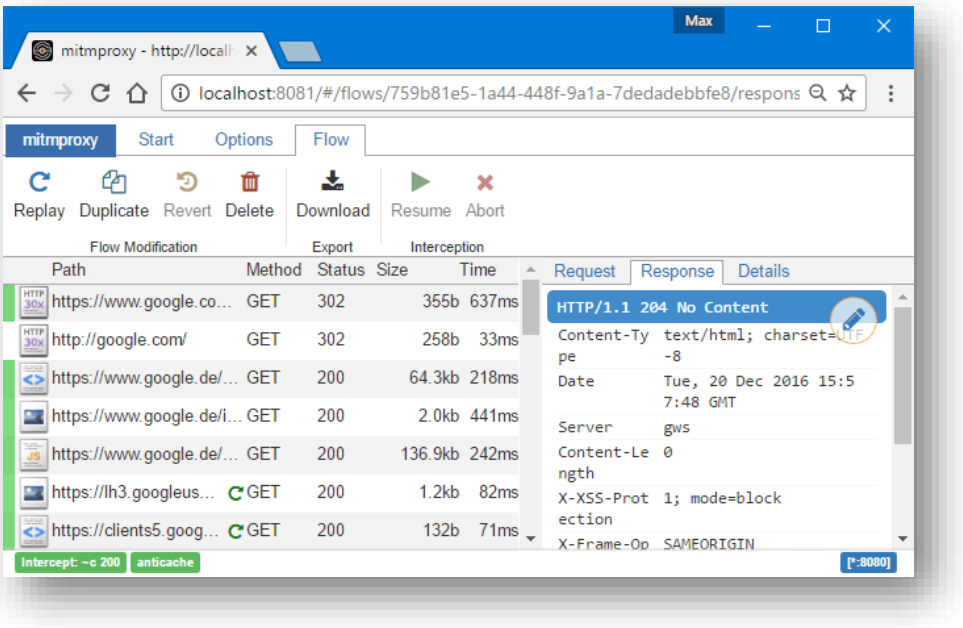


Immagine pressa da mitmproxy.org mitmproxy con interfaccia di Chrome.

Caratteristiche

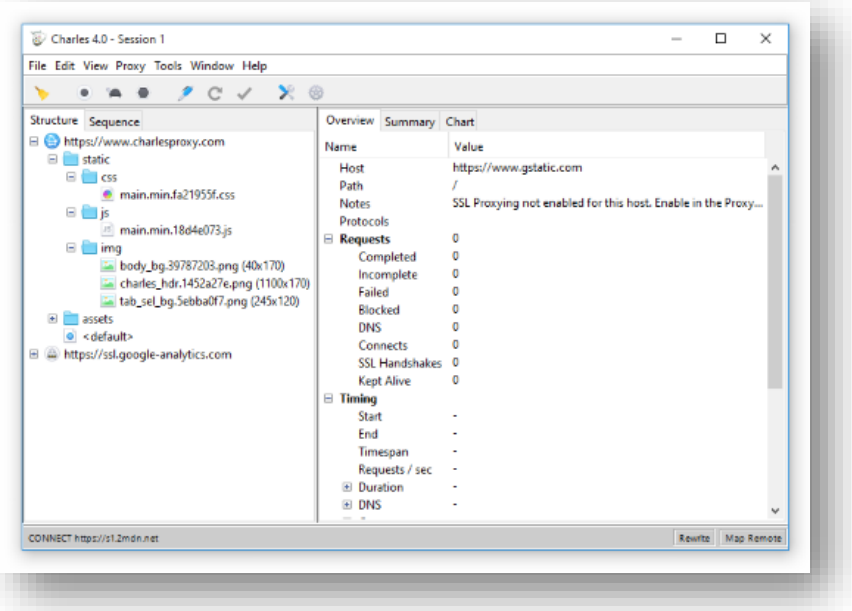
- Intercetta le richieste e le risposte HTTP e HTTPS e modificale al volo
- Salva conversazioni HTTP complete per la riproduzione e l'analisi successive
- Riproduci il lato client delle conversazioni HTTP
- Riproduci le risposte HTTP di un server precedentemente registrato
- Modalità proxy inversa per inoltrare il traffico a un server specificato
- Modalità proxy trasparente su macOS e Linux
- Apporta modifiche tramite script al traffico HTTP utilizzando Python
- I certificati SSL / TLS per l'intercettazione vengono generati al volo

Charles

Charles è un proxy Web (proxy HTTP / HTTP Monitor) che viene eseguito sul tuo computer. Il tuo browser web (o qualsiasi altra applicazione Internet) è quindi configurato per accedere a Internet tramite Charles e Charles è quindi in grado di registrare e visualizzare per te tutti i dati inviati e ricevuti. Nello sviluppo Web e Internet non è possibile vedere cosa viene inviato e ricevuto tra il browser / client Web e il server. Senza questa visibilità è difficile e richiede tempo determinare esattamente dove si trova l'errore. Charles rende facile vedere cosa sta succedendo, in modo da poter diagnosticare e risolvere rapidamente i problemi. Charles rende il debug rapido, affidabile e avanzato; risparmiando tempo e frustrazione!

Funzionalità chiave

- Proxy SSL: visualizza le richieste e le risposte SSL in testo semplice
- Larghezza di banda Limitazione per simulare connessioni Internet più lente, inclusa la latenza
- Debug AJAX: visualizza le richieste e le risposte XML e JSON come albero o testo
- AMF: visualizza i contenuti dei messaggi Flash Remoting / Flex Remoting come una struttura ad albero
- Ripetere le richieste per testare le modifiche del back-end
- Modifica le richieste per testare diversi input
- Punti di interruzione per intercettare e modificare richieste o risposte
- Convalida delle risposte HTML, CSS e RSS / atom registrate utilizzando il validatore W3C



Zap

Zed Attack Proxy (ZAP) è uno strumento gratuito di test di penetrazione open source gestito sotto l'egida dell'Open Web Application Security Project (OWASP). ZAP è progettato specificamente per il test di applicazioni Web ed è sia flessibile che estensibile.

Alla base, ZAP è ciò che è noto come "proxy man-in-the-middle". Si trova tra il browser del tester e l'applicazione Web in modo da poter intercettare e ispezionare i messaggi inviati tra il browser e l'applicazione Web, modificare i contenuti se necessario, quindi inoltrare tali pacchetti alla destinazione. Può essere usato come applicazione autonoma e come processo daemon.

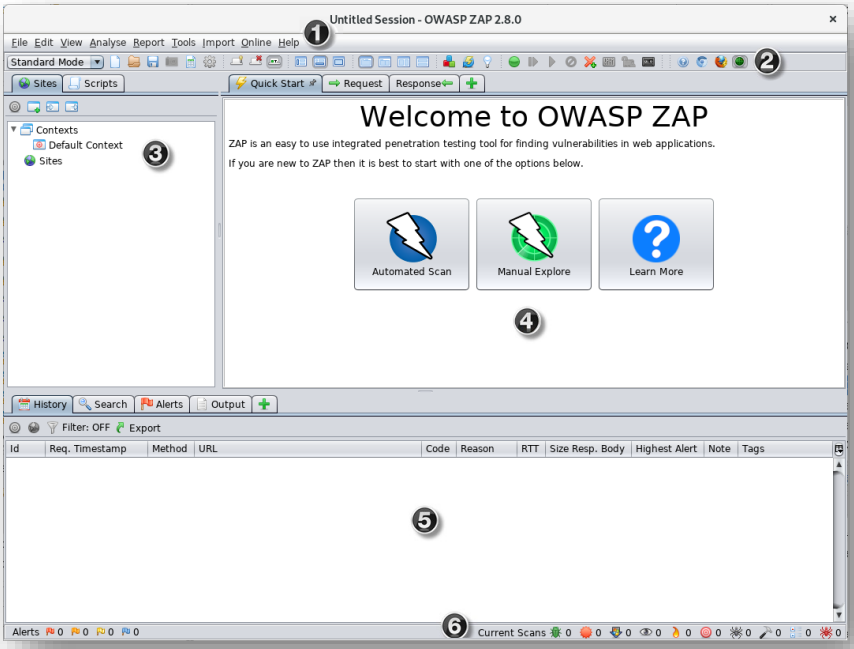


Immagine pressa da zaproxy.org

Il ZAP Desktop UI è compost dai seguenti elementi:

1. Menu Bar – Fornisce l'accesso a molti strumenti automatici e manuali.
2. Toolbar – Include pulsanti che consentono di accedere facilmente alle funzioni più comunemente utilizzate.
3. Tree Window – Visualizza I siti ‘tree’ e gli Scripts ‘tree’.
4. Workspace Window – Visualizza richieste, risposte e script e consente di modificarli.
5. Information Window – Visualizza i dettagli degli strumenti automatici e manuali.
6. Footer – Visualizza un riepilogo degli avvisi rilevati e lo stato dei principali strumenti automatizzati.

	Windows	Linux	Integrabile con Meta-sploit	report	Interfaccia (web – GUI – Command line)	Costo
Burb Suite	Sì	Sì	Sì	Sì	Sì	€349 - €3.499
ZAP	Sì	Sì	Sì	Sì	Sì	Gratis per 100 attività
Mitmproxy	Sì	Sì	Sì	Sì	Sì	
Charles	Sì	Sì	No	Sì	Sì	$50 - $700

Perché ho scelto Burp suite?

Ho scelto Burp Suite perché è una piattaforma integrata per l'esecuzione di test di sicurezza delle applicazioni Web. I suoi vari strumenti collaborano perfettamente per supportare l'intero processo di test, dalla mappatura iniziale e dall'analisi della superficie di attacco di un'applicazione, fino alla ricerca e allo sfruttamento delle vulnerabilità di sicurezza.
Burp Suite ti dà il pieno controllo, permettendoti di combinare tecniche manuali avanzate con automazione all'avanguardia, per rendere il tuo lavoro più veloce, più efficace e più divertente.

Damn Vulnerable Web App

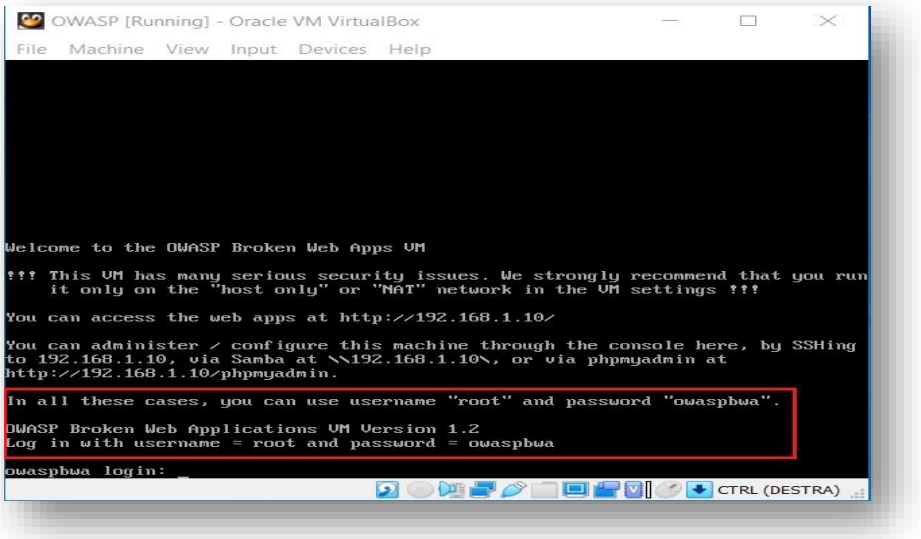
Cos'è Damn Vulnerable Web App?

Damn Vulnerable Web App (DVWA) è un'applicazione Web PHP / MySQL che è dannatamente vulnerabile. I suoi obiettivi principali sono di aiutare i professionisti della sicurezza a testare le proprie competenze e strumenti in un ambiente legale, aiutare gli sviluppatori Web a comprendere meglio i processi di protezione delle applicazioni Web e aiutare insegnanti e studenti apprendere la sicurezza delle applicazioni Web in un ambiente isolato.

Configurare DVWA

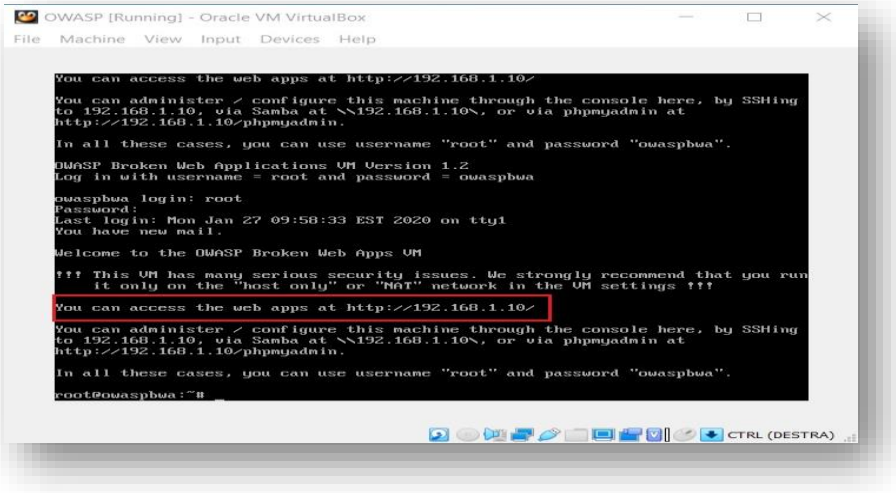
Una volta scaricato ed estratto DVWA, dalla cartella dei suoi contenuti si sceglie il file 'OWASP Broken Web Apps-cl1' per installarlo su VirtualBox.

Dopo aver installato DVWA su ambiente virtuale viene avviato e si visualizza il seguente

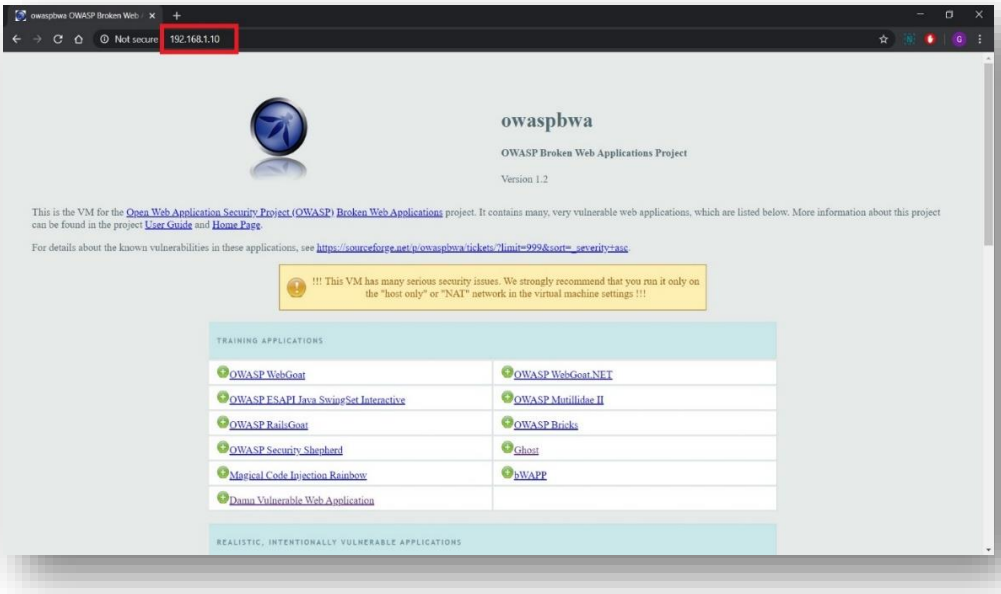


Si fa login con username: root e password: owaspbwa

Inserendo le credenziali indicate il sistema ci indica l'indirizzo IP della sottorete per collegarsi al browser che si ha precedentemente configurato per iniziare I test.



Inserendo http://192.168.1.10 su Firefox si vedrà l'ambiente virtuale su qui si fa tutti I test.



Burp Suite

Cos'è Burp Suite?

Burp Suite è un framework per penetration test Web scritto in Java. È diventata una suite di strumenti standard del settore, utilizzata dai professionisti della sicurezza delle informazioni. Burp Suite aiuta a identificare le vulnerabilità e verificare i vettori di attacco che interessano le applicazioni web.

Nella sua forma più semplice, Burp Suite può essere classificato come proxy di intercettazione. Durante la navigazione della applicazione di destinazione, un tester di penetrazione può configurare il proprio browser Internet per instradare il traffico attraverso il server proxy Burp Suite. Burp Suite agisce quindi come una sorta di Man In The Middle acquisendo e analizzando ogni richiesta da e verso l'applicazione Web di destinazione in modo che possano essere analizzati. I tester di penetrazione possono mettere in pausa, manipolare e riprodurre singole richieste HTTP al fine di analizzare potenziali parametri o punti di iniezione. I punti di iniezione possono essere specificati per attacchi di fuzzing manuali e automatici per scoprire comportamenti, arrestare anomalie e messaggi di errore potenzialmente indesiderati.

Strumenti

- **Proxy HTTP** - Funziona come un server proxy Web e si pone come un intermediario tra il browser e i server Web di destinazione. Ciò consente l'intercettazione, l'ispezione e la modifica del traffico non elaborato che passa in entrambe le direzioni.

- **Scanner**: È uno scanner di sicurezza delle applicazioni Web, utilizzato per eseguire scansioni automatizzate di vulnerabilità delle applicazioni Web.

- **Intruder**: Questo strumento può eseguire attacchi automatici alle applicazioni Web. Offre un algoritmo configurabile in grado di generare richieste HTTP dannose. Lo strumento antitrusione può testare e rilevare SQL injection, scripting cross-site, manipolazione dei parametri e vulnerabilità suscettibili agli attacchi di brute-force.

- **Repeater**: È uno strumento semplice che può essere utilizzato per testare manualmente un'applicazione. Può essere utilizzato per modificare le richieste al server, inviarle nuovamente e osservare i risultati.

- **Decoder**: È uno strumento per trasformare i dati codificati nella loro forma canonica o per trasformare i dati in varie forme codificate e con hash. È in grado di riconoscere in modo intelligente diversi formati di codifica mediante tecniche euristiche.

- **Comparer**: È uno strumento per eseguire un confronto (una "diffchecker" visiva) tra due elementi di dati qualsiasi.

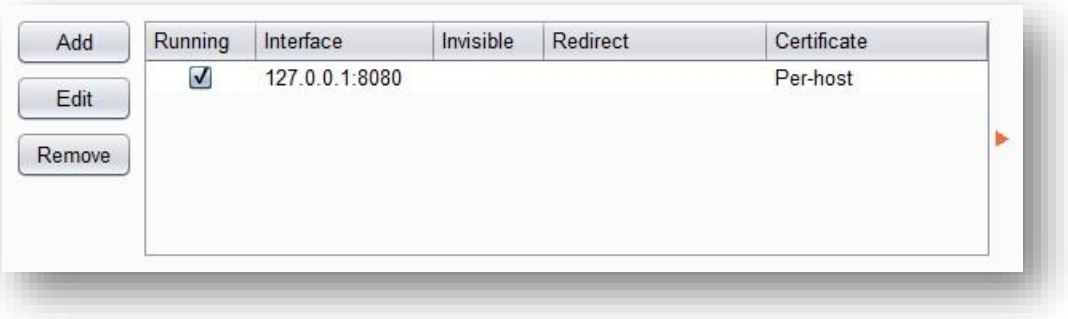
- **Extender**: Consente ai tester di sicurezza di caricare le estensioni Burp Suite, di estendere le funzionalità di Burp Suite utilizzando il codice proprietario o di terze parti dei tester di sicurezza.

- **Sequencer** – È uno strumento per analizzare la qualità della casualità in un campione di elementi di dati. Può essere utilizzato per testare token di sessione di un'applicazione o altri elementi di dati importanti che sono destinati a essere imprevedibili, come token anti-CSRF, token di reimpostazione password, etc.

Configurare e impostare Burp Suite Proxy Listeners.

Dobbiamo configurare il browser (ho scelto mozila) per ricevere le richieste HTTP.

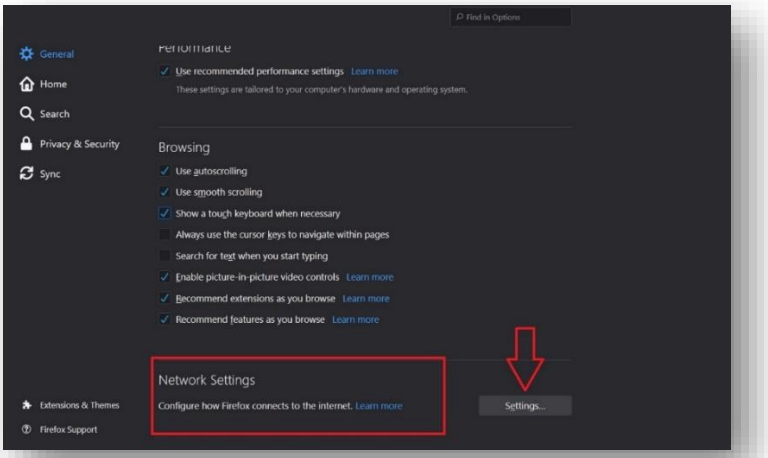
Devo inserire la seguente interfaccia



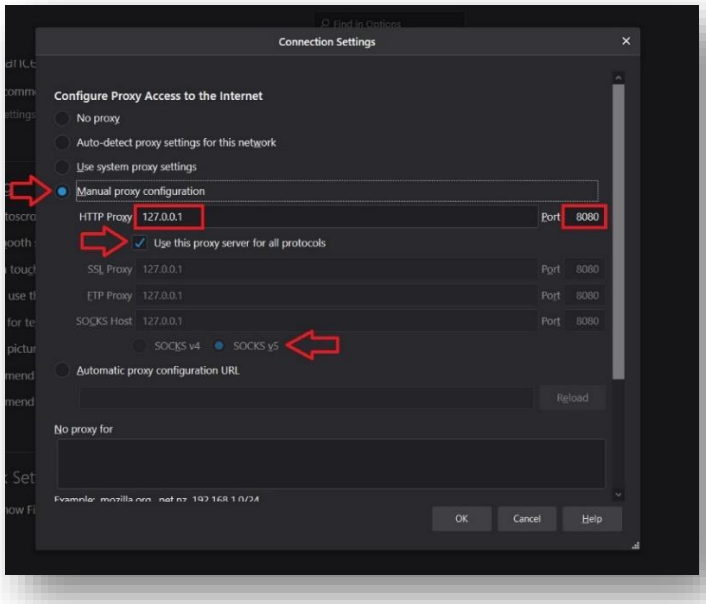

```
HTTP Proxy: 127.0.0.1
Port: 8080
```

Configurazione Mozila Firefox.

Dalle opzioni di Firefox scelgo ‘Network Settings’. Menu -> Options -> Network Settings -> Settings



Scegliere ‘Manual proxy configuration’.



HTTP Proxy: 127.0.0.1

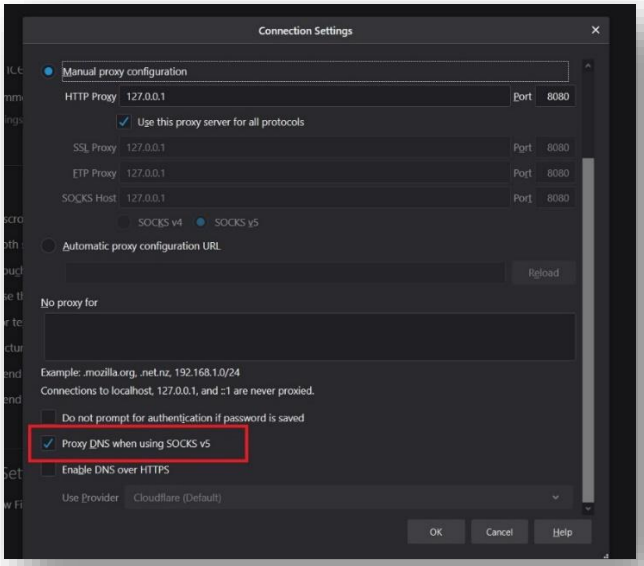
Port: 8080

Scegliere: ‘Use this proxy server for all protocols’

E da SOCKS Host:

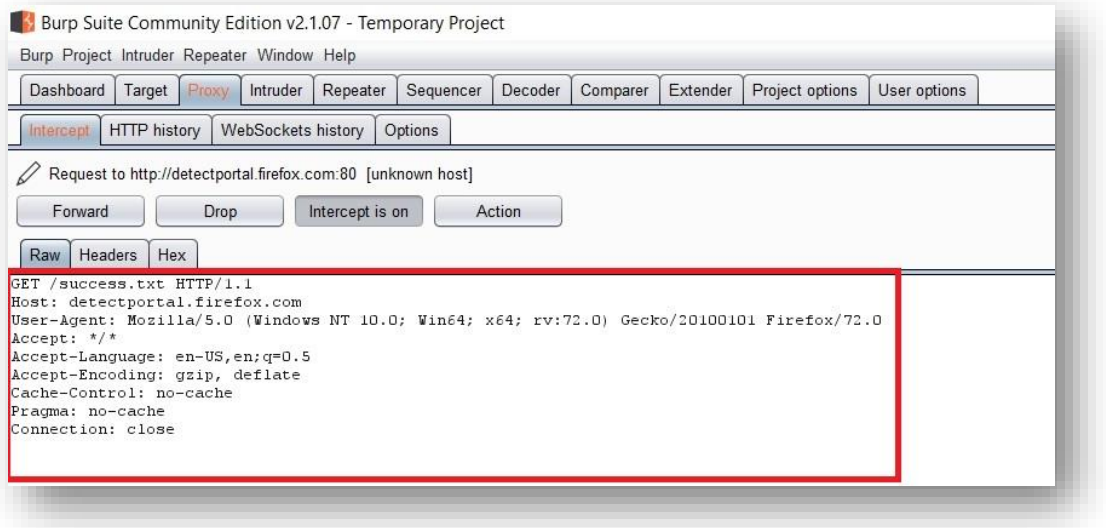
SOCKS v5

Per concludere, scegliere ‘Proxy DNS when using SOCKS v5’

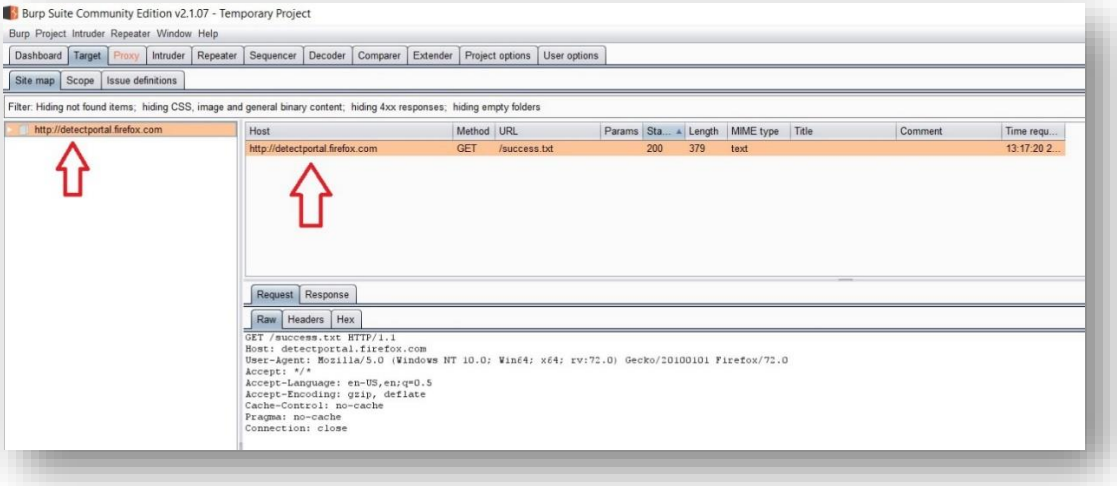


Premere ‘ok’ per salvare la configurazione.

Su Burp Suite dovrebbe visualizzare il seguente messaggio

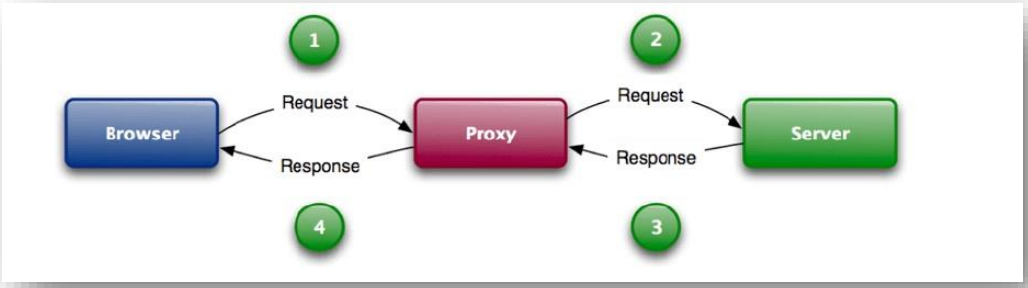


Quando ‘Intercept is on’ viene scelto, scegliendo ‘Forward’ si visualizza Firefox su ‘Site map’.



Lo strumento Proxy

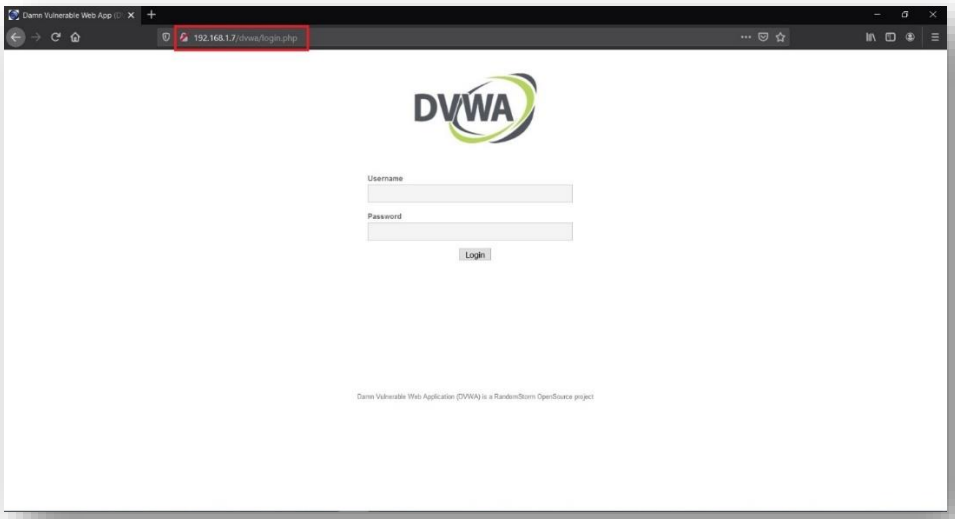
Lo strumento proxy di Burp Suite funziona come intermediario (man-in-the-middle), cioè è una terminologia impiegata nella crittografia e nella sicurezza informatica per indicare un attacco informatico in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.



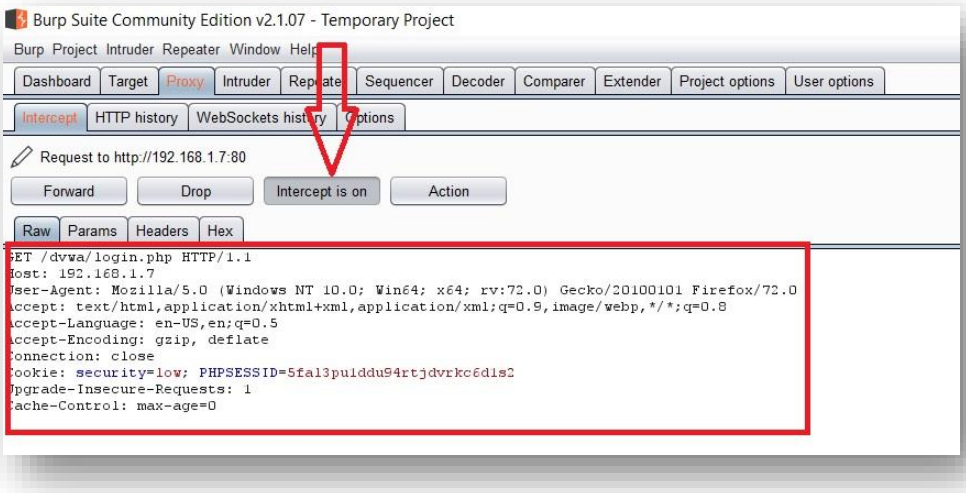
Lo strumento Proxy è al centro del flusso di lavoro guidato dagli utenti di Burp e offre una visione diretta di come l'applicazione di destinazione funziona "sotto il cofano" (under the hood). Funziona come un server proxy Web e si pone come un intermediario tra il browser e i server Web di destinazione. Ciò consente di intercettare, ispezionare e modificare il traffico non elaborato che passa in entrambe le direzioni.

Se l'applicazione utilizza HTTPS, Burp interrompe la connessione TLS tra il browser e il server, in modo che anche i dati crittografati possano essere visualizzati e modificati all'interno del proxy.

Esempio

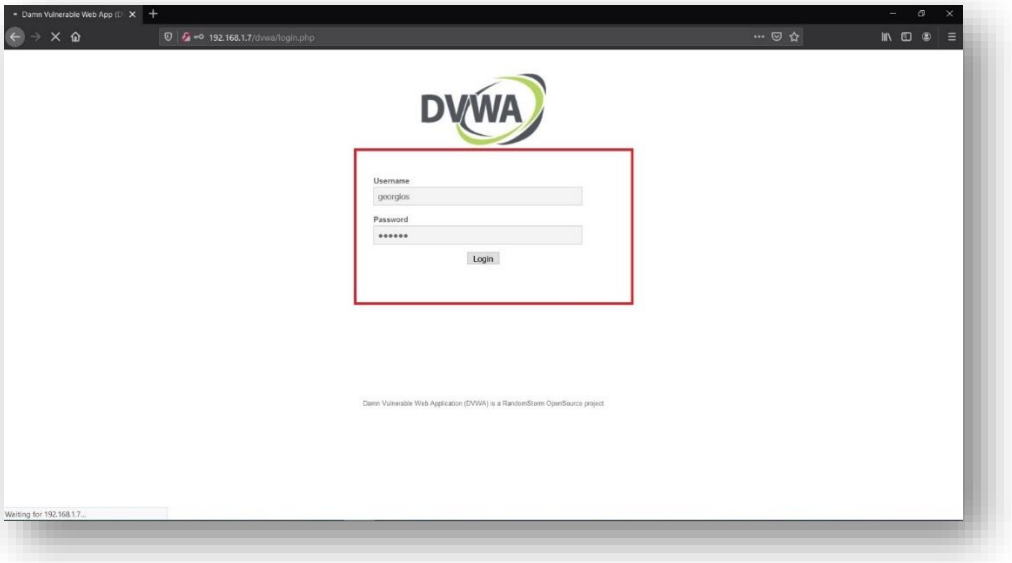


Per prima accendo dal browser configurato (firefox) in una pagina di login sul server configurato OWASP.

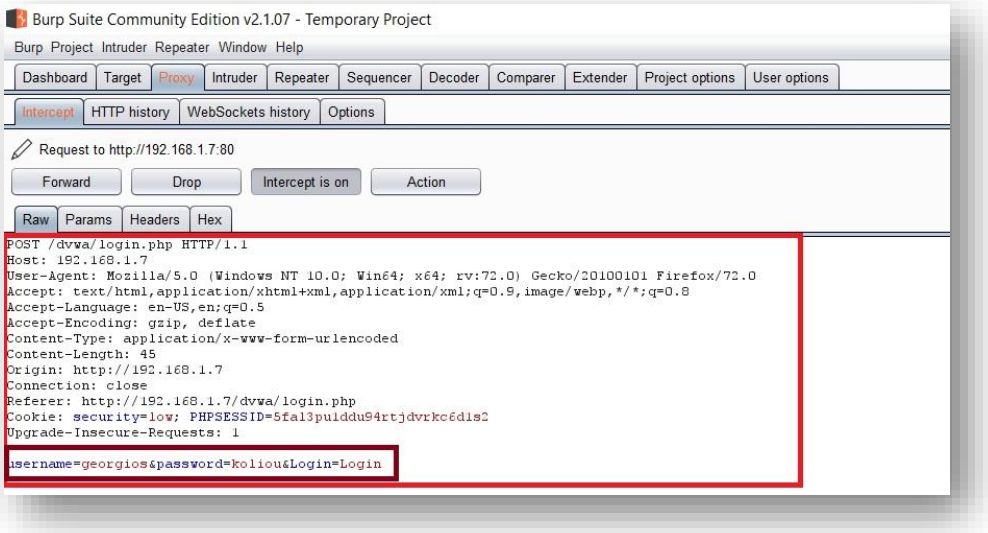


Sulla piataforma Burp Suite avendo l'intersept accesso (on), si può vedere in dettaglio il pacchetto presso (GET) dal Burp Suite. Cioè, che il browser è connesso in una

pagina login, il browser usato è Firefox, il sistema operativo è Windows 10 con architettura da 64 bit etc.



Provando di mettere dei credenziali su questa pagina login Username: georgios Password: koliou, su Burp Suite viene visualizzato il seguente

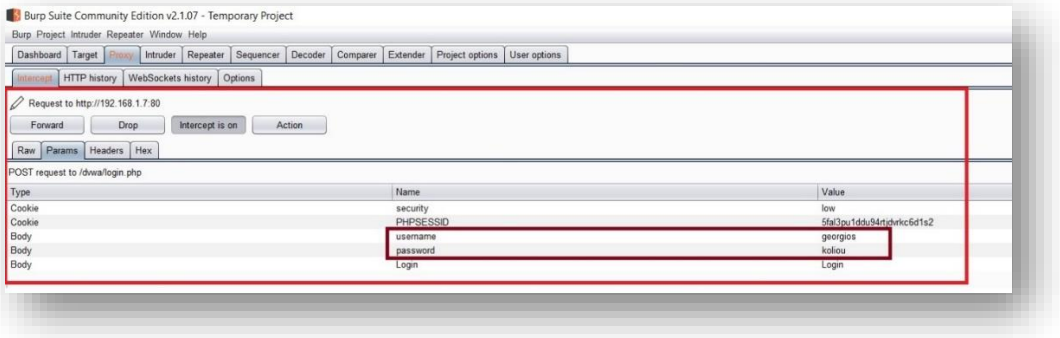


È una richiesta POST, nell'informatica la richiesta POST è un metodo supportato da HTTP utilizzato dal World Wide Web. In base alla progettazione, il metodo di richiesta POST richiede che un server Web accetti i dati racchiusi nel corpo del messaggio

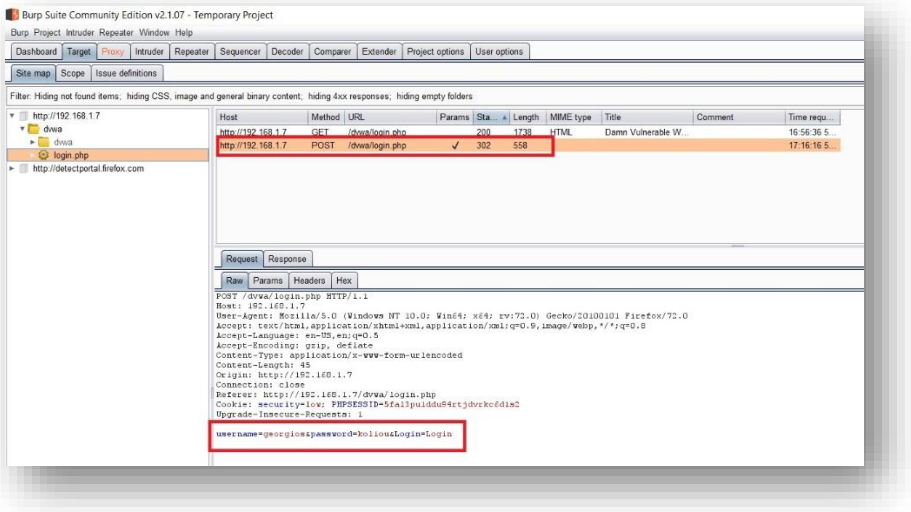
di richiesta, molto probabilmente per memorizzarli. Viene spesso utilizzato quando si carica un file o quando si invia un modulo Web completo.

Anche qui si può vedere I dettagli dell'utente e alla fine I suoi credenziali.

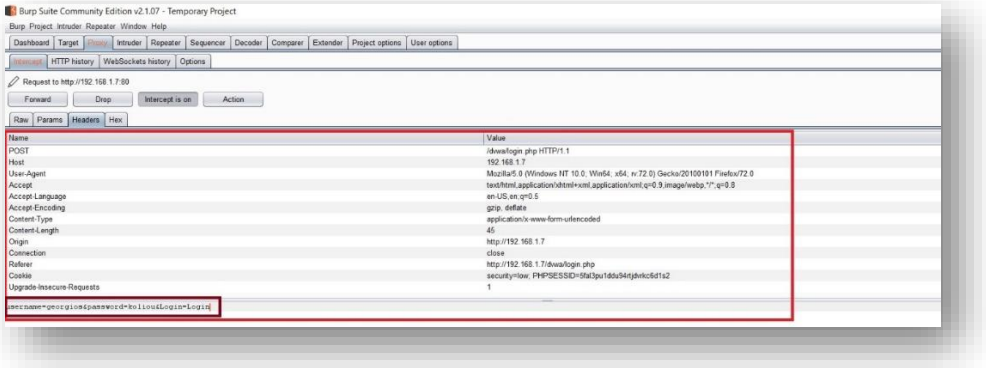
Nella cartella 'Params' si può vedere in chiaro I credenziali dell'utente, I coockies e la configurazione della sicurezza.



Nella cartella ‘Target’ / ‘Site map’ anche visualizzano le richieste GET e POST e anche I credenziali dell’utente.



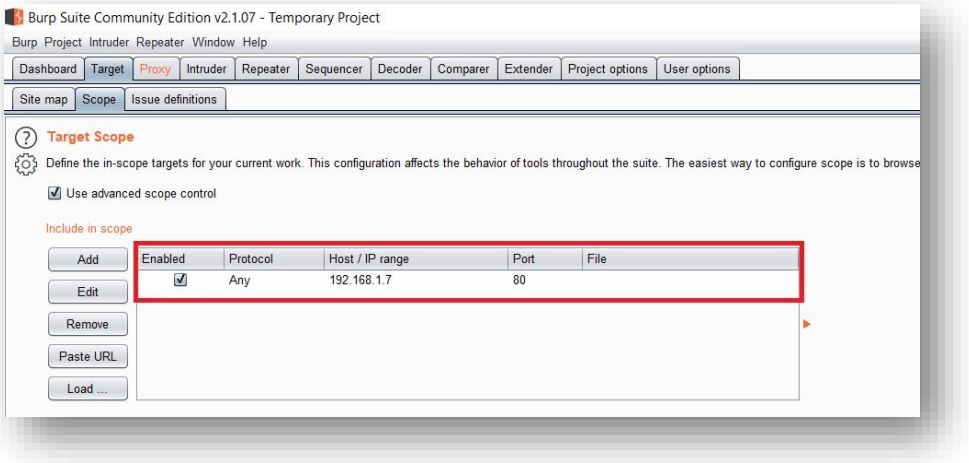
Nella cartella ‘Proxy’/ ‘Intersept’/ ‘Headers’ si visualizza il seguente



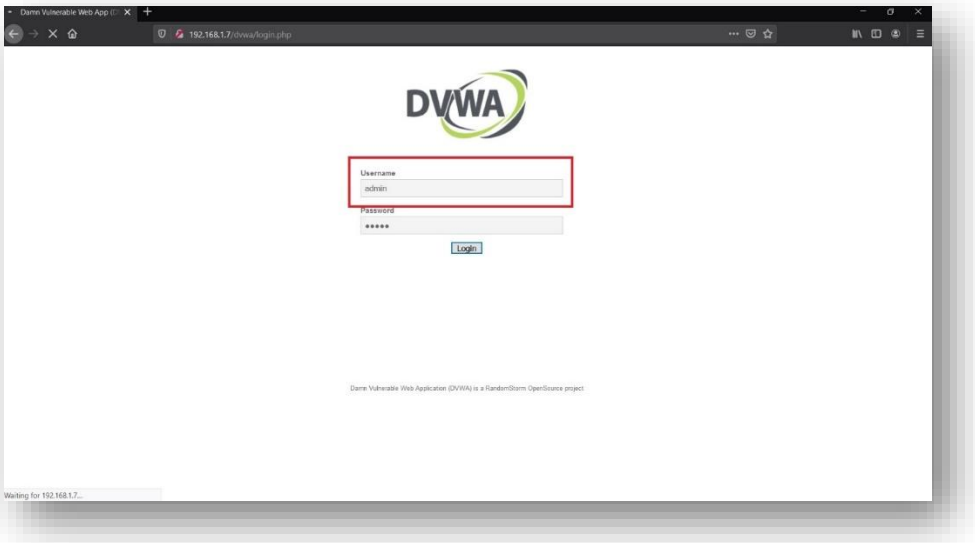
Dove è stata seguita una richiesta POST, dove si visualizzano anche l’host, il browser e il sistema operativo usato dall’utente. In fondo appaiono I credenziali dell’utente.

Cambiare I credenziali dalla piattaforma di BurpSuite

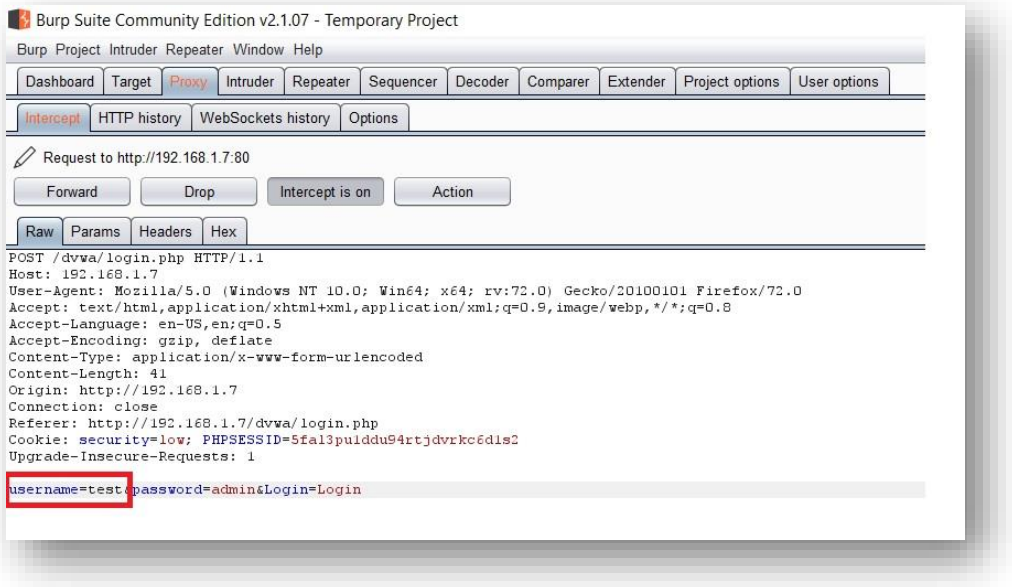
Prima si deve inserire la particolare IP allo ‘Scope’



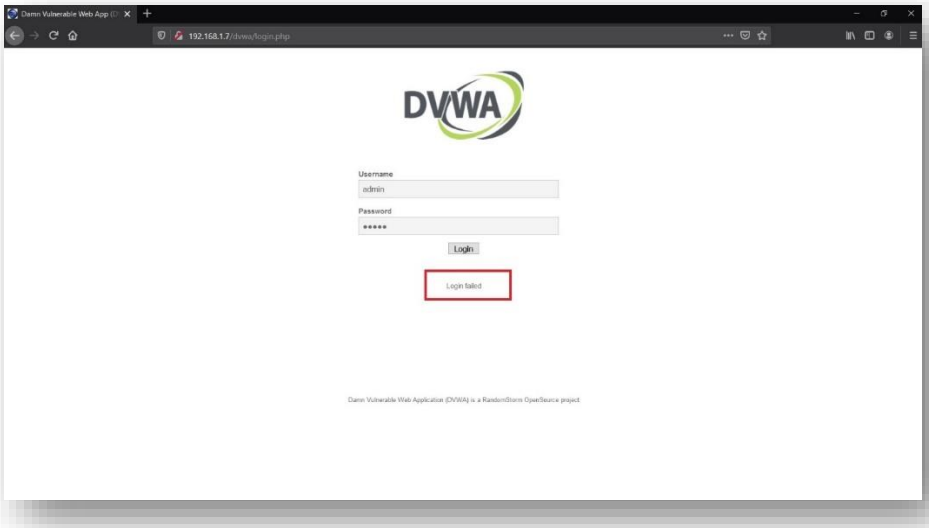
Successivamente provando l’utente di fare login si può manipolare i suoi credenziali e cambiarli.



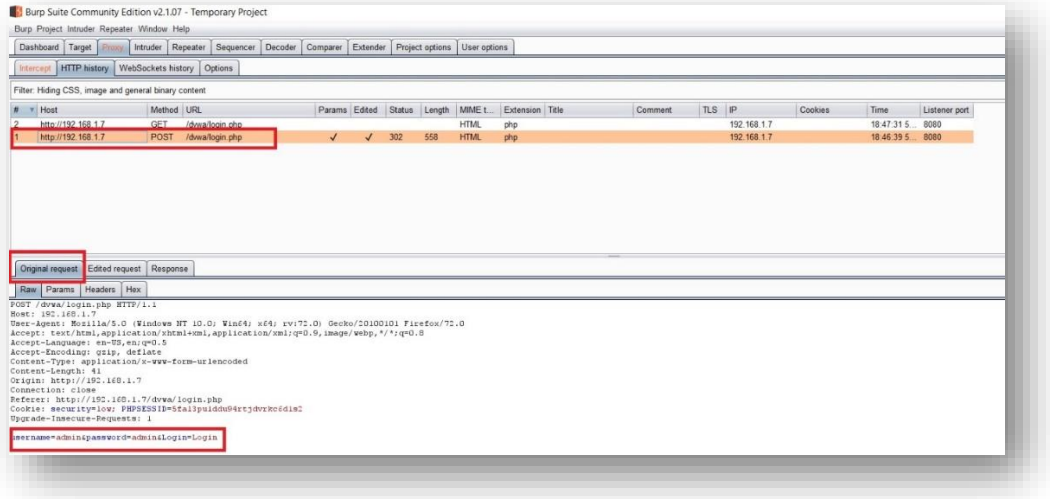
Ho sostituito l'useraname utente 'admin' con 'test'.



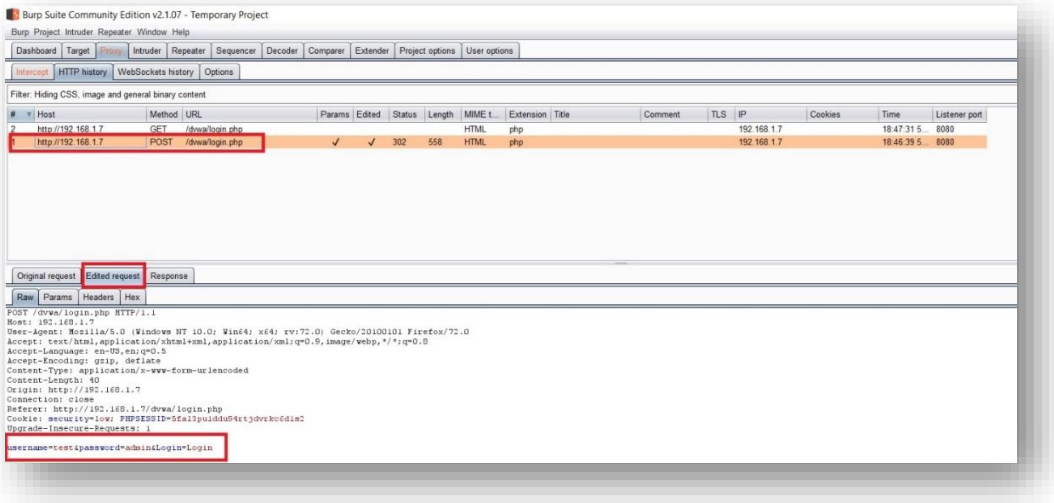
Premendo 'Forward' vedremo che il login fallisce



Nella cartella 'Proxy'/'HTTP history'/'Original request' si può vedere la richiesta originale dall'utente di browser



Invece nella cartella 'Proxy'/'HTTP history'/Edited request'



Si può vedere la richiesta dell'utente di Burpe Suite dopo aver sostituito il nome utente.

Utilizzo di Burp Suite con siti web abilitati per SSL

Cosa sono le autorità di certificazione e le gerarchie di fiducia?

Le autorità di certificazione o CAs sono piccoli file di dati verificabili che contengono credenziali di identità per aiutare i siti Web, le persone e i dispositivi a rappresentare la loro identità online autentica (autentica perché la CA ha verificato l'identità). Le autorità di certificazione svolgono un ruolo fondamentale nel modo in cui Internet funziona e in che modo è possibile effettuare transazioni online affidabili. Le autorità di certificazione rilasciano milioni di certificati digitali ogni anno e questi certificati vengono utilizzati per proteggere le informazioni, crittografare miliardi di transazioni e consentire comunicazioni sicure.
Un certificato SSL è un tipo popolare di certificato digitale che lega i dettagli di proprietà di un server Web (e sito Web) a chiavi crittografiche. Queste chiavi sono utilizzate nel protocollo SSL / TLS per attivare una sessione sicura tra un browser e il server Web che ospita il certificato SSL. Affinché un browser si fidi di un certificato SSL e stabilisca una sessione SSL / TLS senza avvisi di sicurezza, il certificato SSL deve contenere il nome di dominio del sito Web che lo utilizza, essere rilasciato da un'autorità di certificazione attendibile e non scaduto.

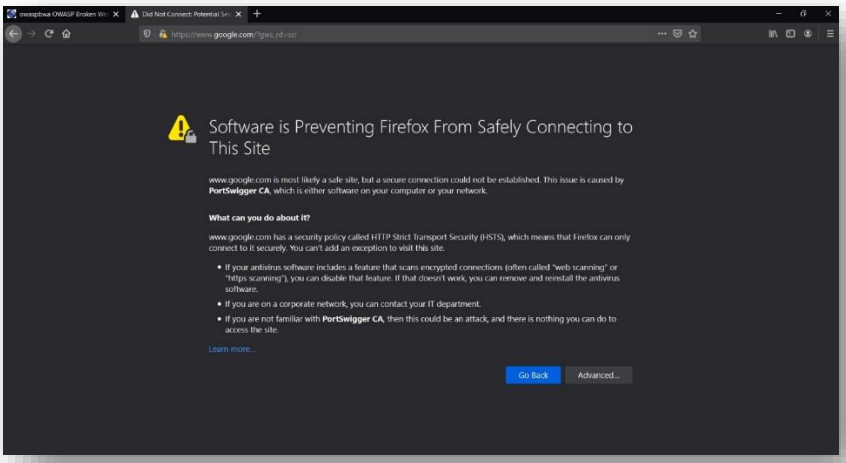
Per impostazione predefinita, quando si visita un sito Web HTTPS tramite Burp, il proxy genera un certificato TLS per ciascun host, firmato dal proprio certificato dell'autorità di certificazione (CA). Questo certificato CA viene generato la prima volta che Burp viene eseguito e archiviato localmente. Per utilizzare Burp Proxy nel modo più efficace con i siti Web HTTPS, è necessario installare il certificato CA di Burp come radice attendibile (root) nel browser.

l'HyperText Transfer Protocol over Secure Socket Layer (HTTPS), (anche noto come HTTP over TLS, HTTP over SSL e HTTP Secure) è un protocollo per la comunicazione sicura attraverso una rete di computer utilizzato su Internet. La porta utilizzata generalmente (ma non necessariamente) è la 443. Consiste nella comunicazione tramite il protocollo HTTP (Hypertext Transfer Protocol) all'interno di una connessione criptata, tramite crittografia asimmetrica, dal Transport Layer Security (*TLS*) o dal suo predecessore, Secure Sockets Layer (*SSL*) fornendo come requisiti chiave:

1. un'autenticazione del sito web visitato
2. protezione della privacy (riservatezza o confidenzialità)
3. integrità dei dati scambiati tra le parti comunicanti.

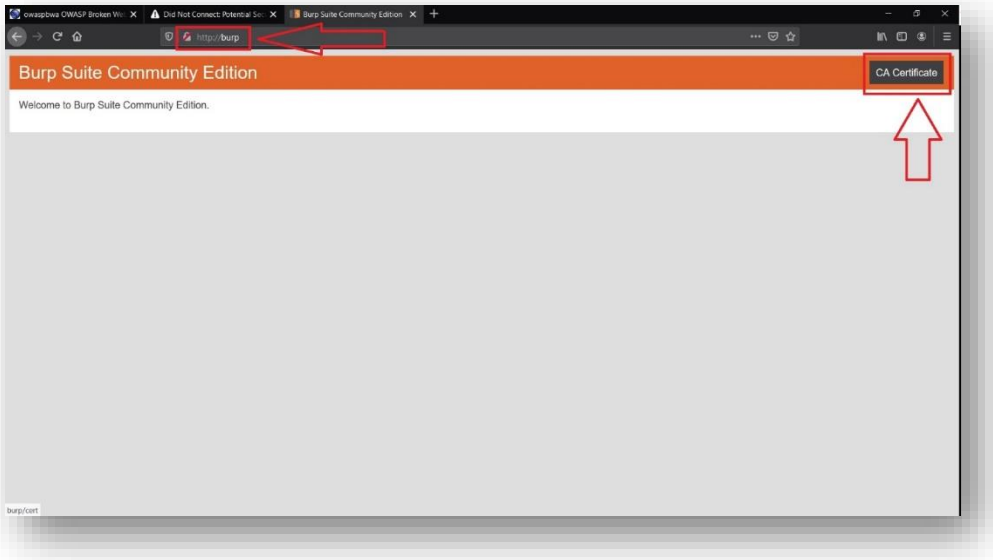
Configurazione Burp Suite con protocollo SSL

Inizialmente provando di connettersi tramite il proxy di Burp Suite in un sito abilitato con protocollo SSL, il risultato sarà il seguente.

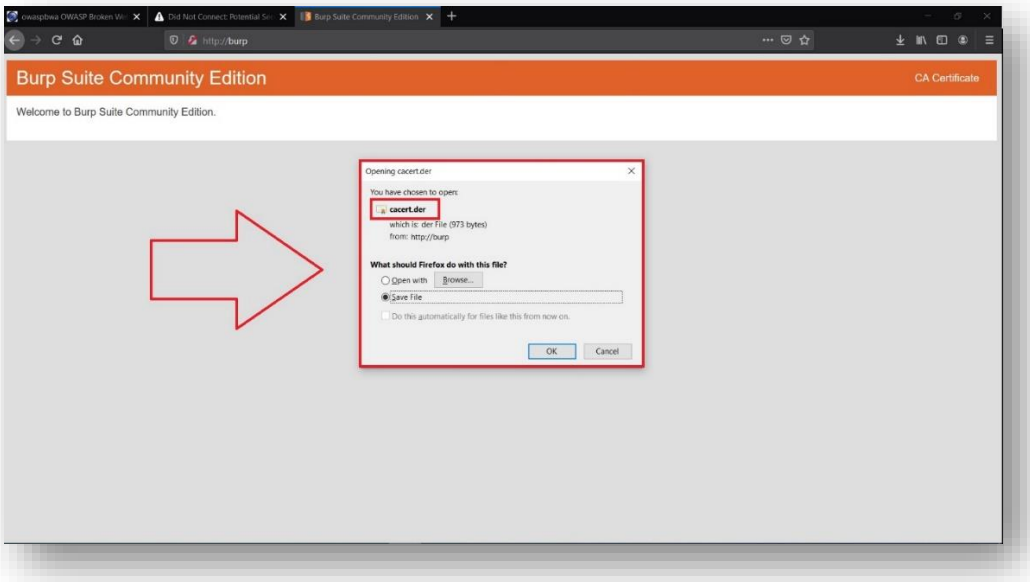


Per risolvere questo problema, PortSwigger ci fornisce con un certificato che si può installare sul browser (Firefox al nostro caso).

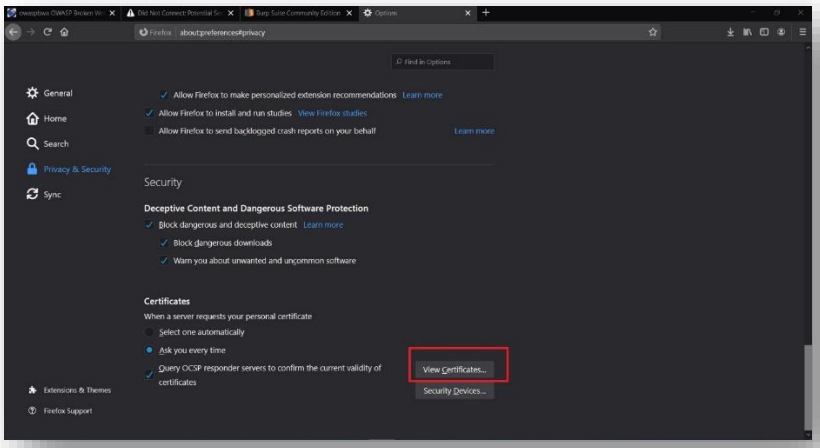
Prima per scaricare il certificato si deve collegare su http://burp dal browser configurato.



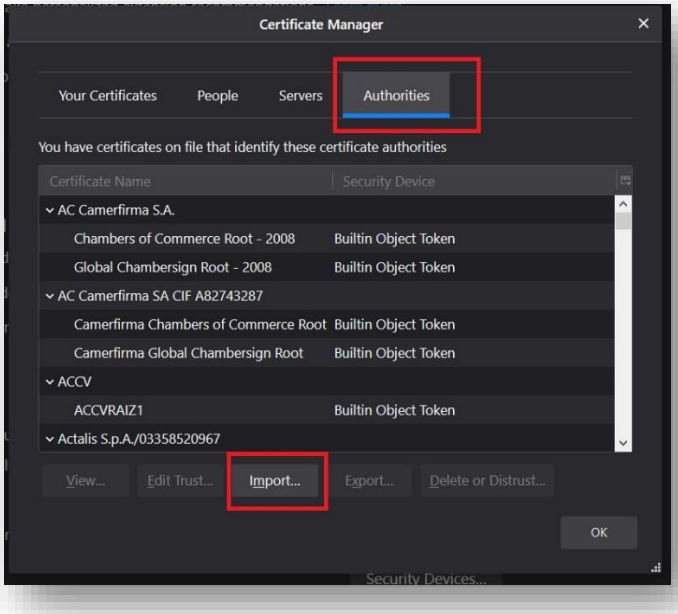
E scaricare il certificato '*casert.der*'



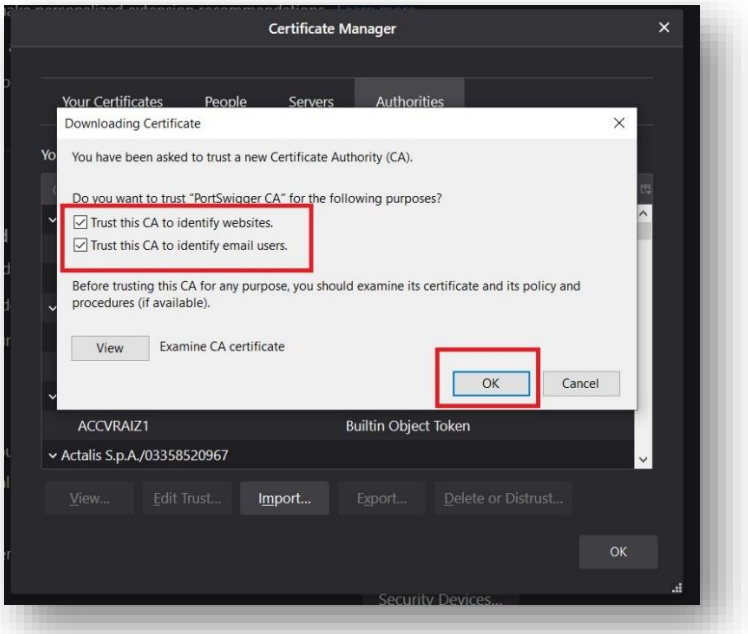
Una volta salvato, da *Options -> Privacy & Security -> Certificates -> View Certificates*, si può installare il certificato come si vede nelle immagini in seguito.



Si visualizza la cartella '*Certificate Manager*'. Nella sessione '*Authorities*' si preme '*Import*'.

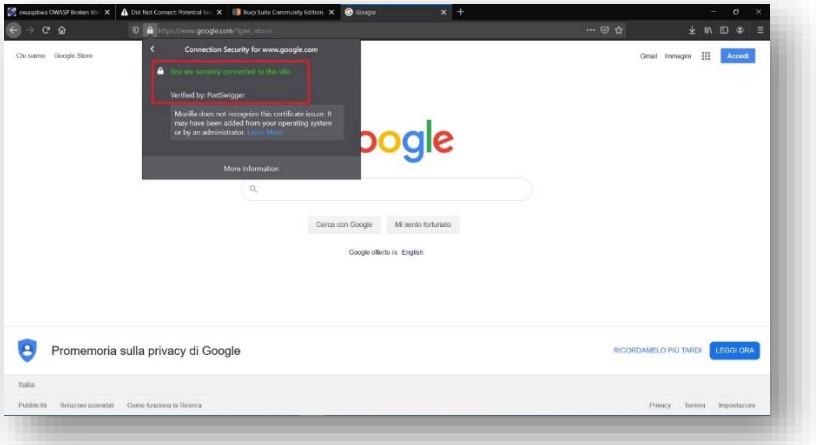


poi si sceglie il certificato salvato e premi '*open*'.



Si sceglie sia '*Trust this CA to identity website*', sia '*Trust this CA to identity email users*' e si preme '*OK*'.

Riprovando di collegarsi su Google il risultato questa volta è il seguente



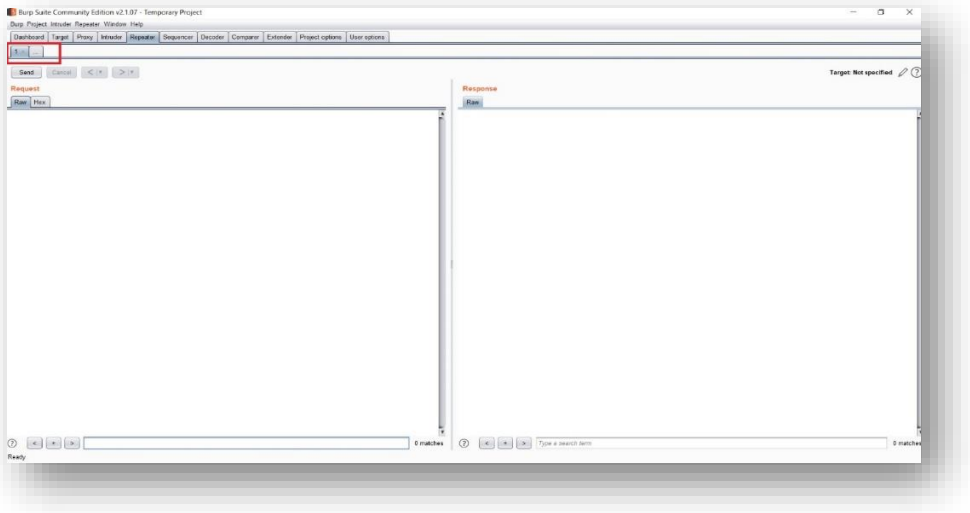
Burp Suite Repeater

Burp Repeater è un semplice strumento per manipolare e riemettere manualmente le singole richieste HTTP e analizzare le risposte dell'applicazione. Puoi inviare una richiesta a Repeater da qualsiasi luogo all'interno di Burp, modificare la richiesta ed emetterla più e più volte.

Usando Burp Suite Repeater

È possibile utilizzare Repeater per tutti gli scopi, come la modifica dei valori e dei parametri, per verificare le vulnerabilità basate sull'input (input-based), l'emissione di richieste in una sequenza specifica, per verificare i difetti logici e la remissione delle richieste dai problemi di Burp Scanner e per verificare manualmente i problemi segnalati.

L'interfaccia utente principale di Repeater ti consente di lavorare su più messaggi diversi contemporaneamente, ciascuno nella sua scheda. Quando invii messaggi a Repeater, ognuno viene aperto nella sua scheda numerata. È possibile rinominare le schede facendo doppio clic sull'intestazione della scheda.



Message editor

L'editor dei messaggi viene utilizzato in Burp per visualizzare e modificare richieste e risposte HTTP e messaggi WebSocket. I contenuti JavaScript, JSON e CSS vengono visualizzati utilizzando la colorazione della sintassi, che viene aggiornata in modo dinamico durante la digitazione. Oltre a visualizzare i messaggi grezzi stessi, l'editor include un gran numero di funzioni che consentono di analizzare rapidamente i messaggi, guidare il flusso di lavoro principale di Burp ed eseguire altre attività utili.

Schede di analisi dei messaggi

L'editor utilizza varie schede per visualizzare e analizzare diversi tipi di messaggi. Le schede visualizzate dipendono dal tipo e dal contenuto del messaggio attualmente visualizzato.

Params

Questa scheda si applica solo alle richieste HTTP e visualizza i parametri della richiesta in forma tabellare. Se il messaggio è modificabile, è possibile modificare il nome e il valore di ciascun parametro direttamente nella tabella e anche cambiare il tipo di parametro. È inoltre possibile aggiungere, spostare e riordinare i parametri.

Laddove applicabile, i nomi e i valori dei parametri vengono visualizzati nella tabella nel loro formato con decodifica URL, per una visualizzazione più semplice. Quando fai doppio clic su un elemento per la modifica, questo verrà mostrato nella sua forma originale. Se, durante la modifica, inserisci tutti i metacaratteri pertinenti nella loro forma letterale (come una e commerciale o un carattere uguale), questi verranno automaticamente codificati in URL al termine della modifica.

Puoi selezionare una singola cella e usare Ctrl + C per copiarne il valore. Selezionano più righe, vengono copiati tutti i valori selezionati, con delimitatori di tabulazione / nuova riga, che consente di incollare facilmente il contenuto in altri software, ad esempio un foglio di calcolo.

Per i messaggi HTTP, ogni scheda Ripetitore contiene i seguenti elementi:

- Controlla l'emissione delle richieste e naviga nella cronologia delle richieste.
- Viene visualizzato il server di destinazione a cui verrà inviata la richiesta: è possibile fare clic sui dettagli di destinazione per modificarli.
- Un editor di messaggi HTTP contenente la richiesta da emettere. È possibile modificare la richiesta ed emetterla più e più volte.
- Un editor di messaggi HTTP che mostra la risposta ricevuta dall'ultima richiesta emessa.
-

Headers

Questa scheda si applica a qualsiasi messaggio HTTP contenente intestazioni dopo la prima riga. Visualizza i nomi e i valori delle intestazioni in forma tabellare. Se il messaggio è modificabile, è possibile modificare il nome e il valore di ciascuna intestazione direttamente nella tabella. Puoi anche aggiungere, spostare e riordinare le intestazioni.

Se il messaggio ha un corpo non vuoto, questo verrà visualizzato nella metà inferiore della scheda delle intestazioni, nel suo editor di testo.

Hex

Questa scheda visualizza il messaggio in forma grezza in un editor esadecimale. È possibile modificare i singoli byte direttamente facendo doppio clic sui valori nella tabella. I valori devono essere indicati in forma esadecimale a due cifre, da 00 a FF.

Il menu di scelta rapida per questa scheda contiene inoltre i seguenti elementi:

- Insert byte - inserisce un singolo nuovo byte prima del byte selezionato.
- Insert bytes - inserisce il numero richiesto di nuovi byte prima del byte selezionato.
- Insert string - inserisce la stringa specificata prima del byte selezionato.
- Delete byte - elimina il byte selezionato.
- Delete bytes - elimina il numero richiesto di byte a partire dal byte selezionato.

HTML

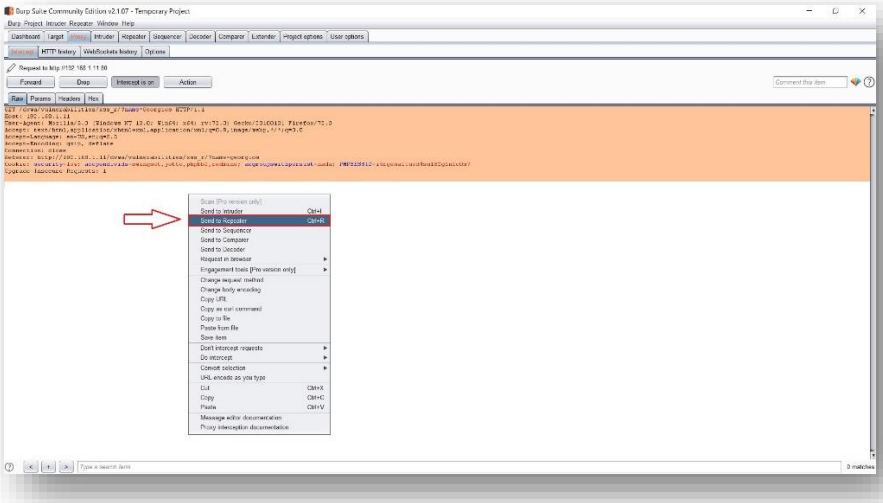
Questa scheda si applica alle risposte HTTP contenenti contenuto HTML nel corpo del messaggio. La scheda mostra solo l'HTML (senza intestazioni) e lo mostra in una forma predefinita, con il contenuto esposto e rientrato secondo la gerarchia dei tag HTML. L'uso principale di questa scheda è di rendere più facilmente leggibile l'HTML formattato in modo errato (come mostrato nella scheda Raw).

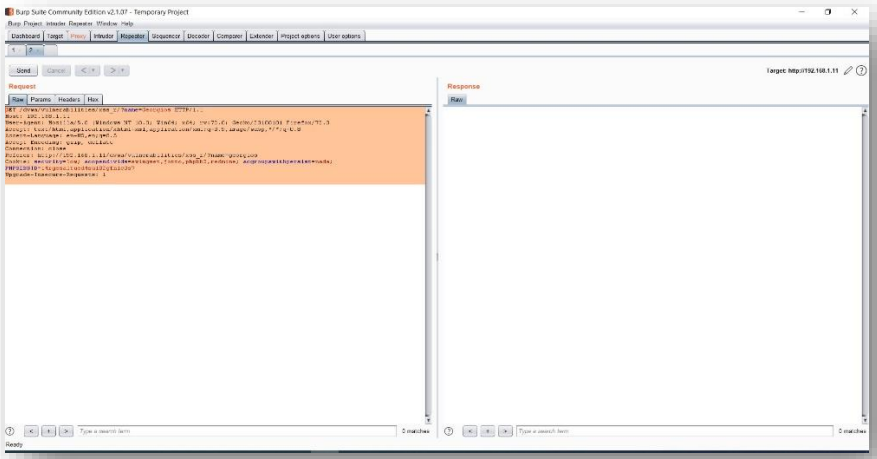
Render

Questa scheda si applica alle risposte HTTP contenenti contenuto HTML o di immagine. Tenta di eseguire il rendering del contenuto del corpo del messaggio nella forma in cui apparirebbe quando visualizzato in un browser.

Utilizzo di Burp Repeater con messaggi HTTP

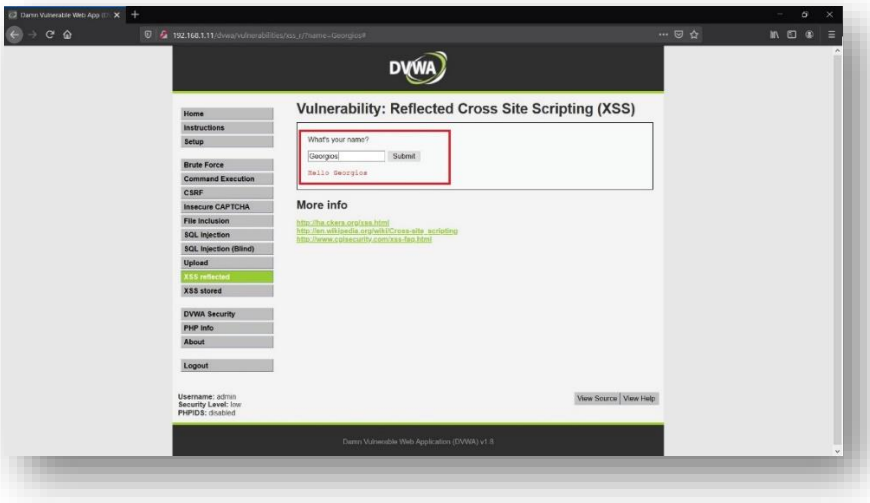
Per usare Burp Repeater con i messaggi HTTP, puoi selezionare un messaggio HTTP ovunque in Burp e scegliere "Invia a Repeater" dal menu contestuale. Ciò creerà una nuova scheda di richiesta in Repeater, popolerà automaticamente i dettagli di destinazione e richiederà all'editor dei messaggi i dettagli pertinenti. In alternativa, puoi aprire manualmente una nuova scheda Ripetitore e selezionare l'opzione "HTTP".

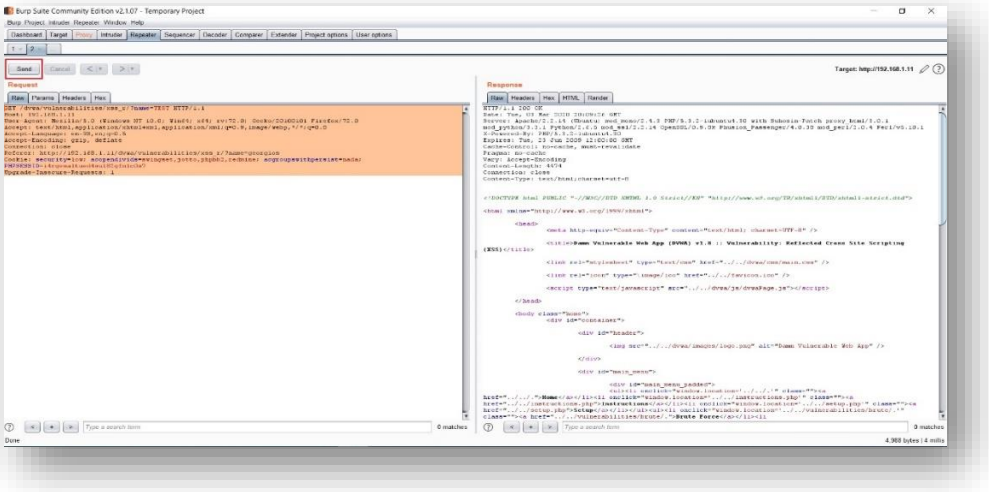

Burp Suite Community Edition v2.1.07 - Temporary Project
Send to Intruder
Send to Repeater
Send to Sequencer
Send to Comparer
Send to Decoder

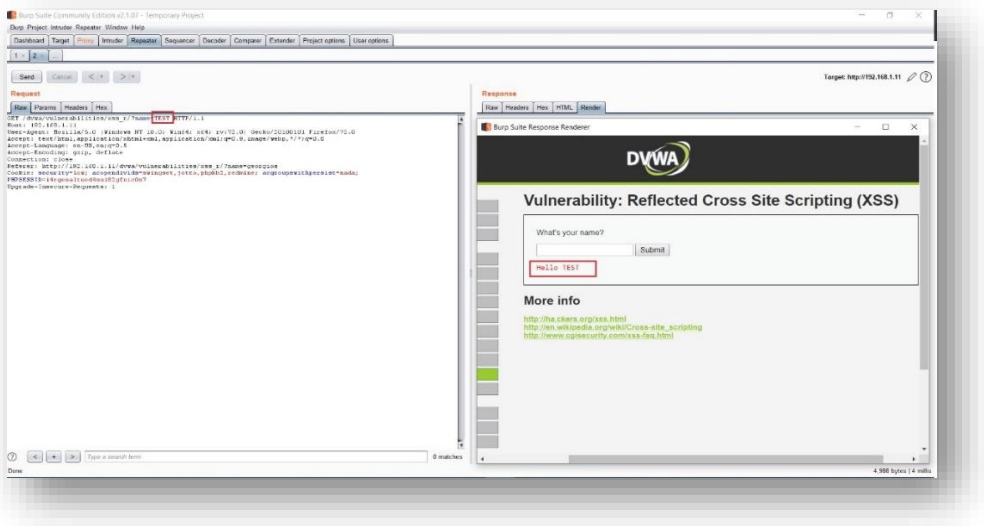

Burp Suite Community Edition v2.1.07 - Temporary Project
Request
Response

Invio di richieste HTTP

Quando la richiesta è pronta per l'invio, si clicca sul pulsante "Invia" per inviarla al server. La risposta viene visualizzata quando viene ricevuta, insieme alla lunghezza della risposta e un timer (in millisecondi). È possibile utilizzare le consuete funzioni dell'editor dei messaggi HTTP per analizzare i messaggi di richiesta e risposta ed eseguire ulteriori azioni.







Opzioni di Burp Repeater

Il menu Ripetitore controlla gli aspetti del comportamento di Burp Repeater. Sono disponibili le seguenti opzioni:

- Aggiorna lunghezza contenuto - questa opzione controlla se Burp aggiorna automaticamente l'intestazione Lunghezza contenuto della richiesta, se necessario. L'uso di questa opzione è normalmente essenziale quando il messaggio di richiesta contiene un corpo.
- Decomprimi GZIP / deflate - questa opzione controlla se Burp decomprime automaticamente i contenuti compressi di GZIP e deflate ricevuti nelle risposte.
- Segui reindirizzamenti - questa impostazione controlla se le risposte di reindirizzamento vengono seguite automaticamente. Nota: se Repeater riceve una risposta di reindirizzamento che non è configurata per seguire automaticamente, verrà visualizzato un pulsante "Segui reindirizzamento" vicino alla parte superiore dell'interfaccia utente. Ciò consente di seguire manualmente il reindirizzamento dopo averlo visualizzato. Questa funzione è utile per esaminare ogni richiesta e risposta in una sequenza di reindirizzamento. I nuovi cookie verranno elaborati in questi reindirizzamenti manuali se questa opzione è stata impostata nell'opzione "Elabora cookie nei reindirizzamenti" descritta di seguito.

- Elaborazione dei cookie nei reindirizzamenti - se questa opzione è selezionata, tutti i cookie impostati nella risposta al reindirizzamento verranno reinviati quando viene seguito l'obiettivo di reindirizzamento.
- Visualizza - questo sottomenu consente di configurare il layout del pannello richiesta / risposta. È possibile visualizzare i messaggi HTTP in una divisione superiore / inferiore, una divisione sinistra / destra o in schede.
- Azione - questo sottomenu contiene le stesse opzioni disponibili nel menu contestuale degli editor dei messaggi di richiesta e risposta.

Burp Decoder

Burp Decoder è un semplice strumento per trasformare i dati codificati nella sua forma canonica o per trasformare i dati grezzi in varie forme codificate e con hash. È in grado di riconoscere in modo intelligente diversi formati di codifica mediante tecniche euristiche.

Caricamento dei dati nel Decoder

È possibile caricare i dati in Decoder in due modi:

- Digitando o incollando direttamente nel pannello dell'editor superiore.
- Selezionando i dati ovunque all'interno di Burp e scegliendo "Invia a Decoder" dal menu contestuale.

Puoi utilizzare i pulsanti "Text" e "Hex" per attivare o disattivare il tipo di editor da utilizzare sui tuoi dati.

Trasformazioni

Possono essere applicate diverse trasformazioni a diverse parti dei dati. Sono disponibili le seguenti operazioni di decodifica e codifica:

- URL
- HTML
- Base64
- ASCII hex
- Hex
- Octal
- Binary
- GZIP

Inoltre, sono disponibili varie funzioni hash comuni, a seconda delle capacità della piattaforma Java.

Quando viene applicata una trasformazione a una parte dei dati, si verificano le seguenti:

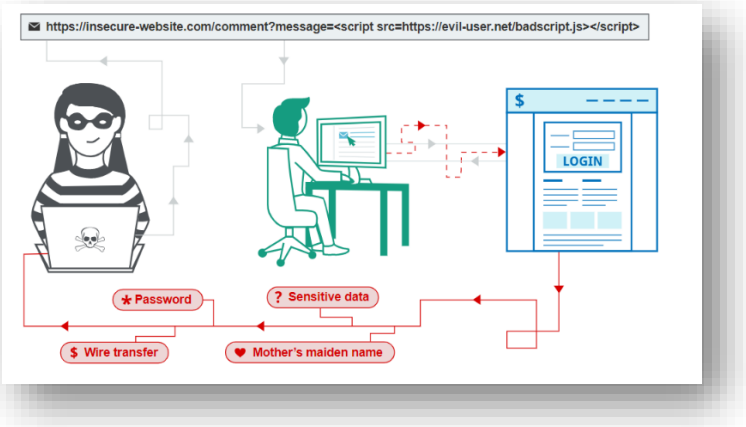
- La parte dei dati da trasformare viene colorata.
- Viene aperto un nuovo editor che mostra i risultati di tutte le trasformazioni applicate. Tutte le parti dei dati che non sono state trasformate vengono copiate nel nuovo pannello nella loro forma grezza.

Il nuovo editor consente di lavorare in modo ricorsivo, applicando più livelli di trasformazioni agli stessi dati, per decomprimere o applicare schemi di codifica complessi. Inoltre, puoi modificare i dati trasformati in qualsiasi pannello dell'editor, non solo nel pannello superiore. Quindi, ad esempio, puoi prendere una struttura di dati complessa, eseguire la decodifica URL e HTML su di essa, modificare i dati decodificati e quindi riapplicare la codifica HTML e URL (in ordine inverso), per generare dati modificati ma validamente formattati da utilizzare in un attacco.

Utilizzo di Burp Scanner per trovare problemi di cross-site scripting (XSS)

Come funziona XSS?

Gli script tra siti funzionano manipolando un sito Web vulnerabile in modo da restituire agli utenti JavaScript dannoso. Quando il codice dannoso viene eseguito all'interno del browser di una vittima, l'utente malintenzionato può compromettere completamente la loro interazione con l'applicazione.



Quali sono i tipi di attacchi XSS?

Esistono tre tipi principali di attacchi XSS. Questi sono:

- Reflected XSS, in cui lo script dannoso proviene dalla richiesta HTTP corrente.
- Stored XSS, in cui lo script dannoso proviene dal database del sito Web.
- DOM-based XSS, in cui esiste la vulnerabilità nel codice lato client anziché nel codice lato server.

Reflected XSS

Reflected XSS è la più semplice varietà di scripting cross-site. Si verifica quando un'applicazione riceve i dati in una richiesta HTTP e li include nella risposta immediata in modo non sicuro.

Ecco un semplice esempio di vulnerabilità XSS riflessa:

https://insecure-website.com/status?message=All+is+well.

Status: All is well.

L'applicazione non esegue nessun'altra elaborazione dei dati, quindi un attaccante può facilmente costruire un attacco come questo:

https://insecure-website.com/status?message=<script>/*+Bad+stuff+here...+*/</script>

Status: <script>/* Bad stuff here... */</script>

Se l'utente visita l'URL creato dall'autore dell'attacco, lo script dell'attaccante viene eseguito nel browser dell'utente, nel contesto della sessione dell'utente con l'applicazione. A quel punto, lo script può eseguire qualsiasi azione e recuperare tutti i dati a cui l'utente ha accesso.

Stored XSS

L'XSS memorizzato (noto anche come XSS persistente o di secondo ordine) sorge quando un'applicazione riceve dati da una fonte non attendibile e li include in una risposta non sicura successiva.

I dati in questione potrebbero essere inviati all'applicazione tramite richieste HTTP; ad esempio commenti su un post di blog, nickname dell'utente in una chat room o dettagli di contatto su un ordine cliente. In altri casi, i dati potrebbero arrivare da altre fonti non attendibili; ad esempio, un'applicazione webmail che visualizza i messaggi ricevuti tramite SMTP, un'applicazione di marketing che visualizza post sui social media o un'applicazione di monitoraggio della rete che visualizza i dati dei pacchetti dal traffico di rete.

Ecco un semplice esempio di vulnerabilità XSS memorizzata. Un'applicazione bacheca consente agli utenti di inviare messaggi, che vengono visualizzati ad altri utenti:

```
<p>Hello, this is my message!</p>
```

L'applicazione non esegue nessun'altra elaborazione dei dati, quindi un utente malintenzionato può facilmente inviare un messaggio che attacca altri utenti:

```
<p><script>/* Bad stuff here... */</script></p>
```

DOM – based XSS

XSS basato su DOM (noto anche come DOM XSS) sorge quando un'applicazione contiene alcuni JavaScript lato client che elaborano i dati da una fonte non attendibile in modo non sicuro, in genere riscrivendoli nel DOM.

Nell'esempio seguente, un'applicazione utilizza JavaScript per leggere il valore da un campo di input e scrivere quel valore su un elemento all'interno dell'HTML:

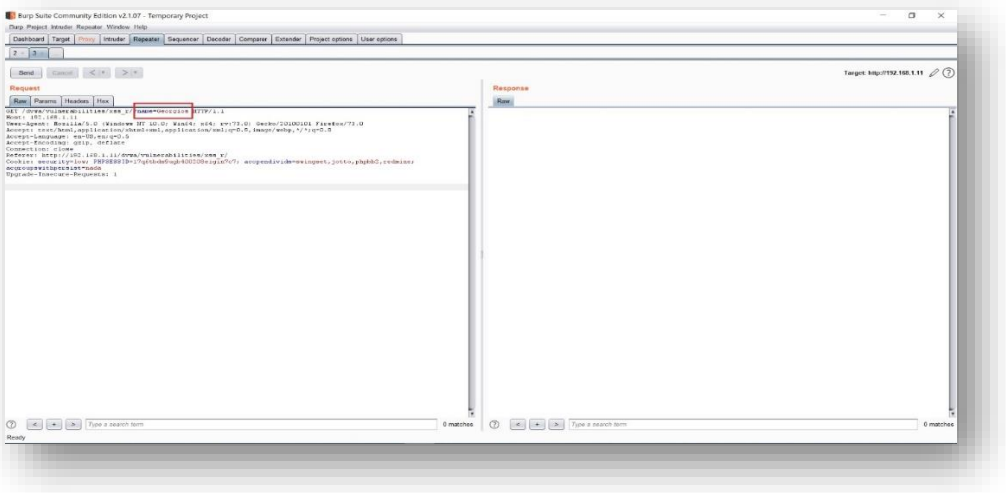
```
var search = document.getElementById('search').value;
var results = document.getElementById('results');
results.innerHTML = 'You searched for: ' + search;
```

Se l'attaccante può controllare il valore del campo di input, può facilmente costruire un valore dannoso che causa l'esecuzione del proprio script:

You searched for: <img src=1 onerror='/* Bad stuff here... */'>

In un caso tipico, il campo di input verrebbe popolato da parte della richiesta HTTP, ad esempio un parametro della stringa di query URL, consentendo all'autore dell'attacco di inviare un attacco utilizzando un URL dannoso, allo stesso modo dell'XSS riflesso.

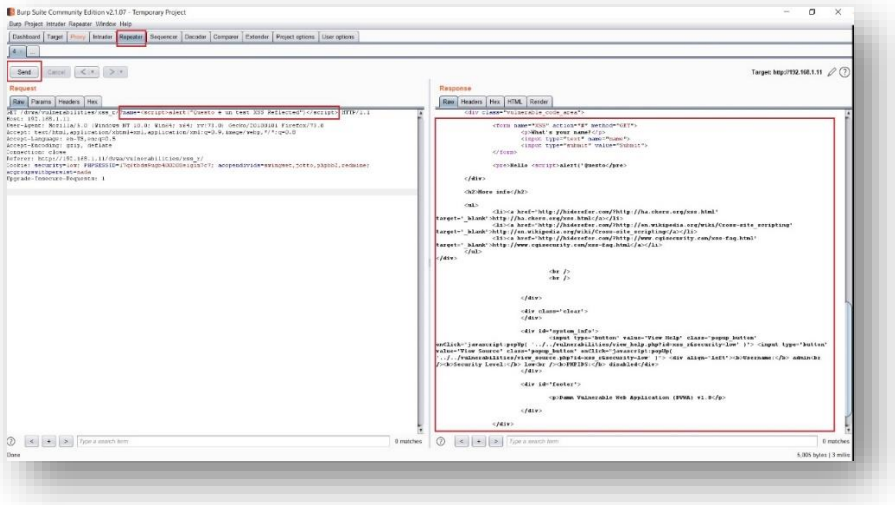
Esempio di XSS Reflected usando Repeater e Decoder



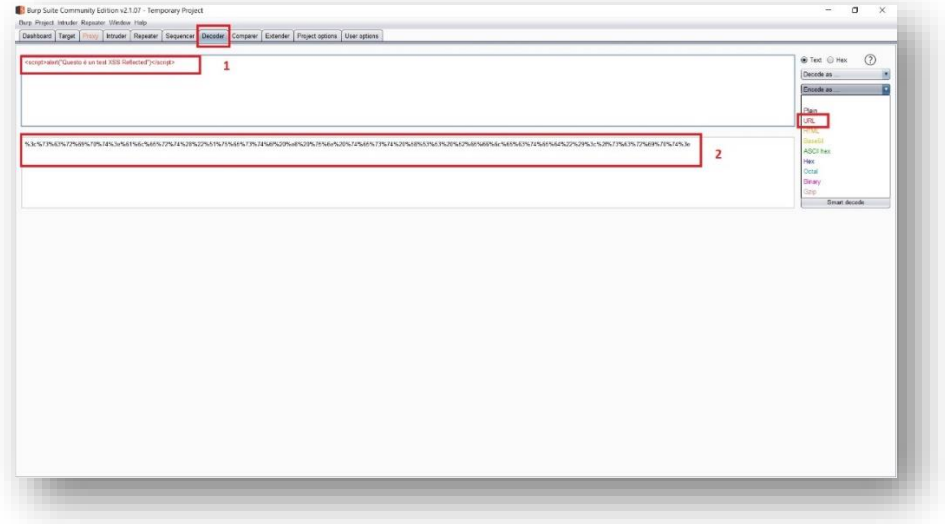
Poi si cambia il nome ‘Georgios’ con il codice Javascript

<script> alert(“Questo è un test XSS Reflected”)</script>

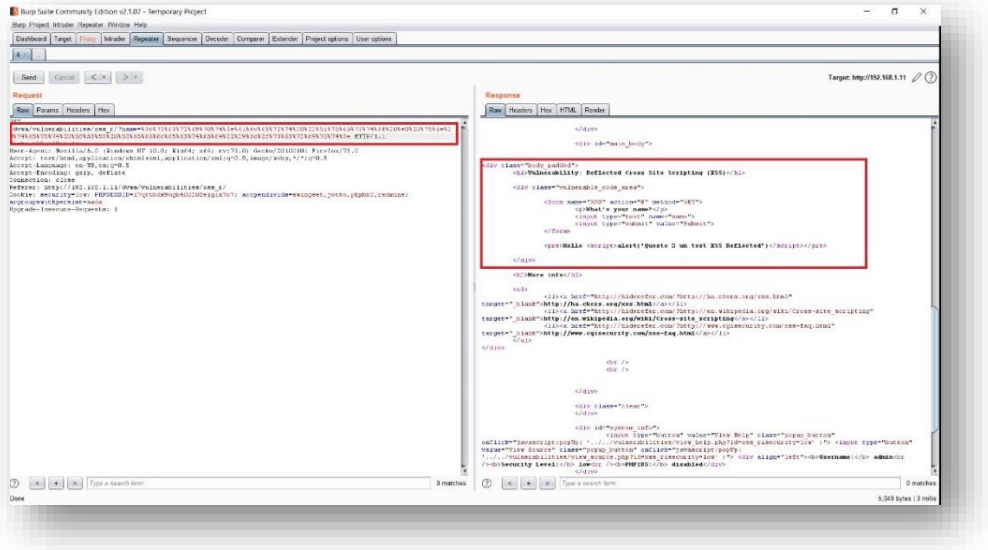
Premendo “Send” il risultato sarà il seguente



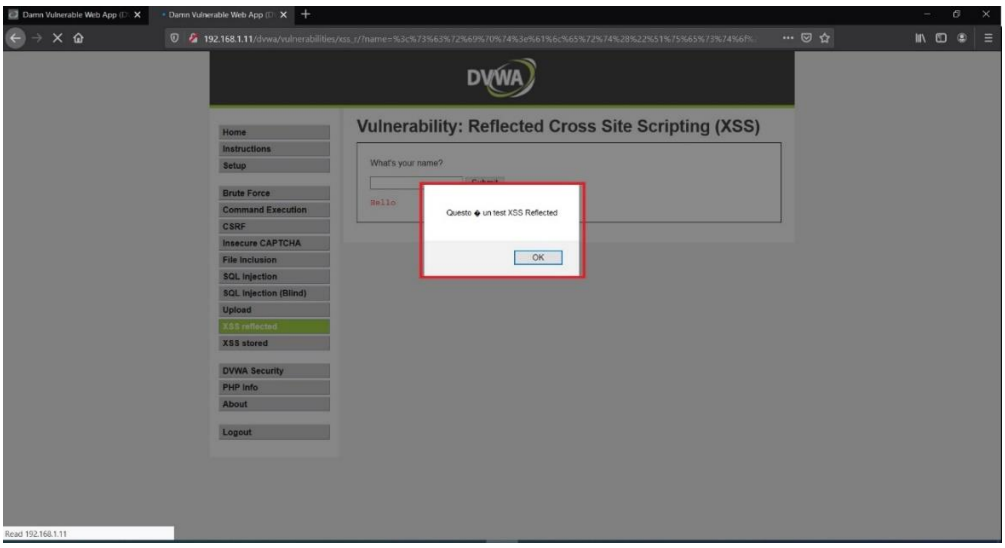
Lo script non è stato eseguito. Il problema si può risolvere con il modo seguente



Nella tabella ‘Decoder’ copio lo script Javascript e scelgo ‘Encode as URL’ come si vede nell’immagine. Poi viene creata la stringa n.2. Sostituisco il nome ‘Georgios’ con la stringa creata da Decoder come si vede sull’immagine seguente, si vede che il problema è stato risolto



Poi eseguendo lo script sul browser il risultato è il seguente



*Per le seguenti funzioni ho installato Burp Suite Pro.

Scansione di siti Web

Burp Scanner automatizza l'attività di scansione di siti Web alla ricerca di contenuti e vulnerabilità. A seconda della configurazione, lo scanner può eseguire la scansione dell'applicazione per scoprirne il contenuto e le funzionalità e controllare l'applicazione per rilevare le vulnerabilità.

Avvio delle scansioni

Le scansioni possono essere avviate in vari modi:

- Scansione da URL specifici. Ciò esegue una scansione eseguendo la scansione del contenuto all'interno di uno o più URL forniti e controllando facoltativamente il contenuto sottoposto a scansione. Per fare ciò, si va alla Dashboard Burp e fai clic sul pulsante "*New scan*". Ciò aprirà il programma di avvio della scansione che consente di configurare i dettagli della scansione.
- Scansiona gli oggetti selezionati. Ciò consente di eseguire una scansione di solo controllo (senza ricerca per indicizzazione) di richieste HTTP specifiche. Per fare ciò, selezionare una o più richieste ovunque all'interno di Burp e selezionare "*Scan*" dal menu contestuale. Ciò aprirà il programma di avvio della scansione che consente di configurare i dettagli della scansione.
- Scansione dal vivo. È possibile utilizzare le scansioni in tempo reale per scansionare automaticamente le richieste elaborate da altri strumenti Burp, come gli strumenti Proxy o Repeater. È possibile configurare con precisione quali richieste vengono elaborate e se devono essere analizzate per identificare il contenuto o controllare le vulnerabilità. Per fare ciò, si va alla Dashboard Burp e fai clic sul pulsante "*New live task*". Ciò aprirà il programma di avvio della scansione in tempo reale che consente di configurare i dettagli dell'attività.

Configurazione delle scansioni

È possibile avviare più scansioni in parallelo e ogni scansione ha le proprie opzioni di configurazione che determinano esattamente come viene eseguita la scansione. Esistono due aree chiave di configurazione:

- Opzioni di scansione. Queste opzioni controllano il comportamento come la massima profondità del collegamento, il modo in cui il crawler ottimizza per la velocità rispetto alla copertura e i limiti sull'estensione della scansione.
- Opzioni di controllo. Queste opzioni controllano comportamenti come la gestione dei punti di inserimento e quali metodi di rilevamento sono impiegati. Queste opzioni sono molto importanti nel controllo del tipo di attività di audit che verrà svolta, da un'analisi puramente passiva leggera a una scansione invasiva dei pesi massimi.

Monitoraggio dell'attività di scansione

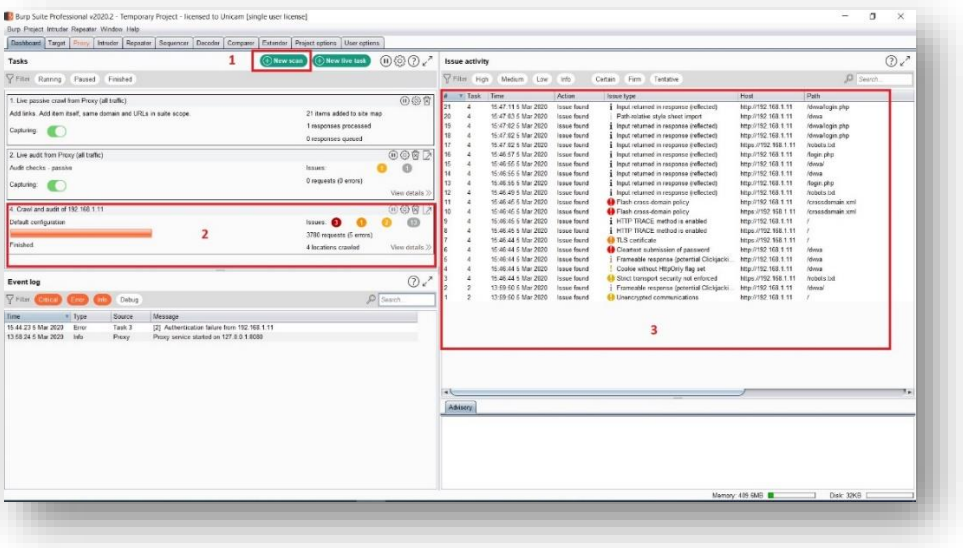
È possibile monitorare l'avanzamento e i risultati di una scansione in vari modi:

- La dashboard Burp mostra le metriche sullo stato di avanzamento di ciascuna attività e il registro delle attività relative ai problemi riporta i problemi segnalati da tutte le attività di scansione.
- È possibile aprire la finestra dei dettagli dell'attività per una singola scansione, per visualizzare il registro delle attività del problema solo per quella scansione e una vista dettagliata degli elementi di controllo per le attività applicabili.
- La mappa del sito di destinazione mostra tutti i contenuti e i problemi che sono stati identificati, organizzati per dominio e URL.

Reporting

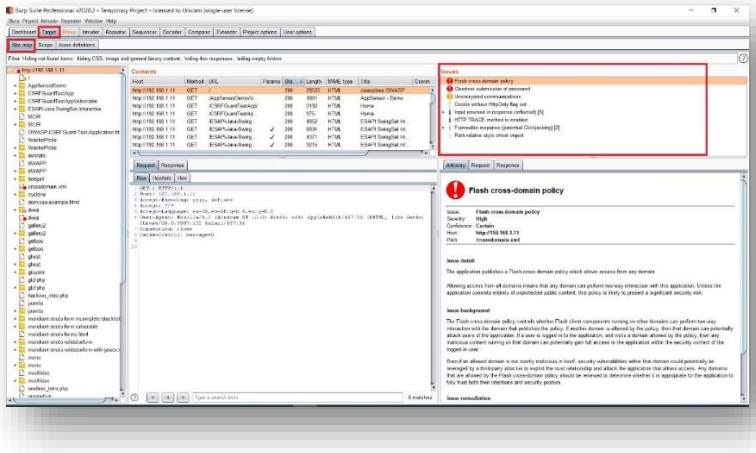
È possibile generare report di problemi rilevati tramite Burp Scanner in formato HTML. Puoi anche esportare problemi in formato XML adatti all'importazione in altri strumenti.

Esempio di scansione su Burp Suite

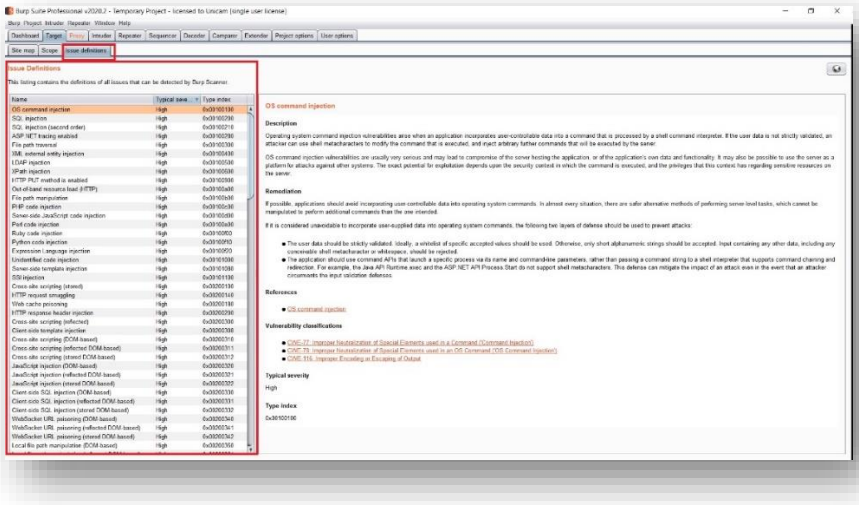


1. Si preme “New scan” per effettuare una nuova scansione
2. Panoramica delle vulnerabilità trovate
3. Vulnerabilità trovate in dettaglio

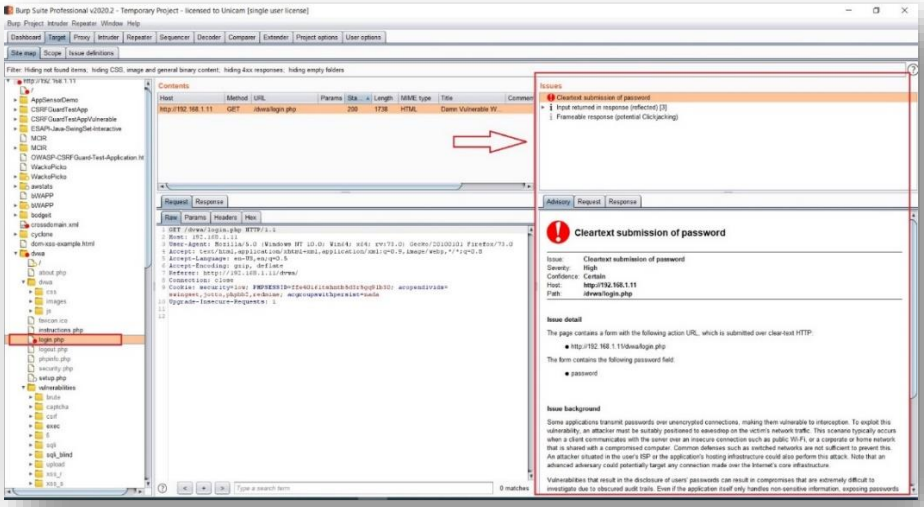
Sulla tabella ‘Target – Site map’ si può vedere l’analisi completa delle vulnerabilità trovate.



Sulla tabella ‘Target – Issue definitions’ si può leggere la definizione completa di ogni problema trovato.



Per esempio, lo scanner di Burp Suite ci informa che esiste una vulnerabilità di ‘Cleartext submission of password’ cioè alcune applicazioni trasmettono le password su connessioni non crittografate, rendendole vulnerabili all'intercettazione.


Cleartext submission of password
Issue: Cleartext submission of password
Severity: High
Confidence: Certain
Host: http://192.168.1.11
Path: /dvwa/login.php
Issue detail
The page contains a form with the following action URL, which is submitted over clear-text HTTP:
http://192.168.1.11/dvwa/login.php
The form contains the following password field:
password
Issue background
Some applications transmit passwords over unencrypted connections, making them vulnerable to interception. To exploit this vulnerability, an attacker must be suitably positioned to eavesdrop on the victim's network traffic. This scenario typically occurs when a client communicates with the server over an insecure connection such as public Wi-Fi, or a corporate or home network that is shared with a compromised computer. Common defenses such as switched networks are not sufficient to prevent this. An attacker situated in the user's ISP or the application's hosting infrastructure could also perform this attack. Note that an advanced adversary could potentially target any connection made over the Internet's core infrastructure.
Vulnerabilities that result in the disclosure of users' passwords can result in compromises that are extremely difficult to investigate due to obscured audit trails. Even if the application itself only handles non-sensitive information, exposing passwords

Burp Extender

Burp Extender si trova sia alla versione Professional sia alla Communoty. Consente di utilizzare le estensioni Burp, per estendere le funzionalità di Burp usando il tuo codice proprio o di terze parti. Puoi caricare e gestire estensioni, visualizzare i dettagli sulle estensioni installate, installare estensioni dal BApp Store, visualizzare l'API Burp Extender corrente e configurare le opzioni per la gestione delle estensioni.

Le estensioni Burp possono personalizzare il comportamento di Burp in numerosi modi, come la modifica delle richieste e delle risposte HTTP, la personalizzazione dell'interfaccia utente, l'aggiunta di controlli personalizzati dello scanner e l'accesso alle informazioni chiave di runtime, tra cui la cronologia proxy, la mappa del sito di destinazione e i problemi dello scanner.

Per assistenza sulla creazione di estensioni Burp personalizzate, consultare la documentazione di estensibilità principale.

Caricamento e gestione delle estensioni

La tabella mostra un elenco di tutte le estensioni installate. È possibile aggiungere, rimuovere e riordinare le estensioni utilizzando i pulsanti della tabella delle estensioni.

Notare che:

- L'ordine in cui vengono visualizzate le estensioni è l'ordine in cui verranno richiamati eventuali listener registrati e altre risorse di estensione.
- Le estensioni possono essere scaricate ma conservate nella tabella per consentire un facile ricaricamento in un secondo momento. Per attivare o disattivare lo stato di un'estensione senza rimuoverlo dall'elenco, fare clic sulla casella di controllo nella colonna "Loaded" o nel pannello dei dettagli dell'estensione. **Nota**: è possibile ricaricare rapidamente un'estensione premendo Ctrl + facendo clic sulla casella di controllo "Loaded". Questo scaricherà e ricaricherà l'estensione senza mostrare una finestra di conferma.
- Per eseguire le estensioni scritte in Python, devi prima configurare la posizione del JAR autonomo Jython, nelle opzioni dell'ambiente Python.

Dettagli dell'estensione

La selezione di un elemento nella tabella delle estensioni mostra le informazioni su tale estensione nel pannello inferiore.

La scheda *'Details'* mostra le seguenti informazioni:

- Se l'estensione è attualmente caricata. È possibile fare clic sulla casella di controllo per caricare o scaricare l'estensione selezionata.
- Il nome dell'estensione. Le estensioni possono impostare a livello di programmazione il loro nome preferito che appare nell'interfaccia utente. È possibile modificare manualmente questo nome, se necessario.
- Il tipo di estensione (Java o Python).
- Il file da cui è stata caricata l'estensione.
- Dettagli su metodi, *'listener'* e altre risorse in uso dall'estensione.

La scheda *'Output'* contiene i dettagli del flusso di output standard dell'estensione e la scheda *'Error'* contiene le stesse informazioni sul flusso di errori standard. Per ogni flusso, è possibile configurare se l'output dell'applicazione deve essere indirizzato alla console di sistema, o salvato su file o visualizzato nell'interfaccia utente.

Notare che:

- La finestra di output basata sull'interfaccia utente ha dimensioni limitate e non è progettata per la registrazione pesante.
- Le estensioni sono responsabili di indirizzare i loro messaggi di output e di errore ai flussi corretti che Burp Suite ha assegnato loro e che sono disponibili a livello di programmazione tramite l'API di estensibilità. Le estensioni che non rispettano questo aspetto possono indirizzare l'output direttamente alla consola di sistema indipendentemente dalle impostazioni specificate qui.

BApp Store

BApp Store contiene estensioni Burp che sono state scritte dagli utenti di Burp Suite, per estendere le capacità di Burp.

È possibile visualizzare l'elenco dei BApp disponibili, installare BApp specifici e inviare valutazioni degli utenti per quelli installati

Se non si dispone dell'accesso a Internet dal computer che esegue Burp, è possibile scaricare i file BApp dal sito Web di BApp Store e installarli manualmente in Burp.

Alcuni BApp sono scritti in Python o Ruby e richiedono il download di Jython o JRuby e la configurazione di Burp con la posizione dei relativi interpreti linguistici. Alcuni BApp potrebbero richiedere una versione più recente di Burp o una diversa edizione di Burp.

Burp Extender API

Questa scheda contiene i dettagli delle API disponibili per la creazione di estensioni Burp. L'elenco mostra le API disponibili nella versione di Burp in esecuzione. Seleziona il nome di un'interfaccia dall'elenco per mostrare il codice dell'interfaccia per intero.

È inoltre possibile utilizzare i pulsanti "Salva file di interfaccia" e "Salva file Javadoc" per salvare copie locali di questi file, da utilizzare durante lo sviluppo di estensioni.

Extender Options

Questa scheda contiene opzioni per le impostazioni dell'estensione, l'ambiente Java, l'ambiente Python e l'ambiente Ruby.

Settings

Sono disponibili le seguenti impostazioni:

- Ricaricare automaticamente le estensioni all'avvio. Se Burp è stato chiuso con questa impostazione selezionata e si desidera comunque riavviare Burp senza ricaricare automaticamente alcuna estensione, è possibile avviare Burp con il flag della riga di comando `--disable-extensions`. Ciò impedirà a Burp di ricaricare automaticamente eventuali estensioni.
- Aggiornare automaticamente i BApp installati all'avvio.

Ambiente Java

Queste impostazioni consentono di configurare l'ambiente per l'esecuzione di estensioni scritte in Java. Se le estensioni utilizzano librerie, puoi specificare una cartella da cui verranno caricate le librerie. Burp Suite cercherà i file JAR in questa cartella e in qualsiasi sottocartella e li includerà nel percorso di classe del classloader utilizzato per caricare le estensioni Java.

Ambiente Python

Queste impostazioni consentono di configurare l'ambiente per l'esecuzione di estensioni scritte in Python. Per utilizzare le estensioni Python, si deve scaricare Jython, che è un interprete Python implementato in Java. Sono disponibili le seguenti opzioni:

- Posizione del file JAR autonomo di Jython: questa è la posizione in cui è stato scaricato Jython. Devi scaricare la versione standalone di Jython.
- Cartella per il caricamento dei moduli: questa impostazione è facoltativa e può essere utilizzata per specificare una cartella da cui l'interprete Python dovrebbe tentare di caricare i moduli necessari per le estensioni. Se configurata, questa opzione fa sì che Burp aggiorni la variabile sys.path di Python con la posizione specificata. L'uso di questa opzione è utile se hai creato il tuo set di librerie Python per l'uso in più estensioni separate.

Nota: a causa del modo in cui Jython genera dinamicamente le classi Java, potresti riscontrare problemi di memoria se carichi diverse estensioni Python o se scarichi e ricarichi un'estensione Python più volte. In questo caso, si vedrà un errore come:

java.lang.OutOfMemoryError: PermGen space

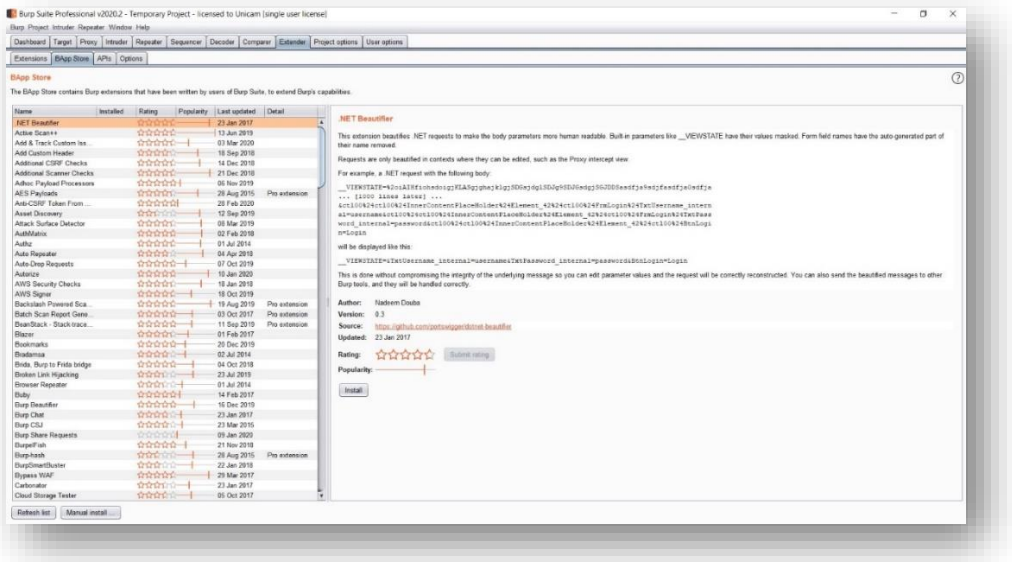
È possibile evitare questo problema configurando Java per allocare più spazio di archiviazione PermGen, aggiungendo un'opzione -XX: MaxPermSize alla riga di comando all'avvio di Burp. Per esempio:

java -XX:MaxPermSize=1G -jar burp.jar

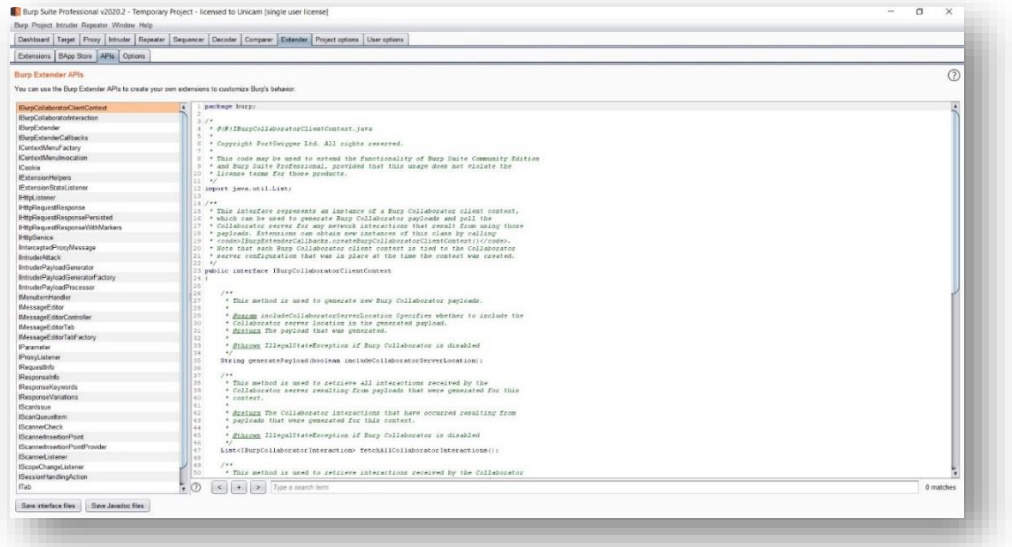
Ambiente Ruby

Queste impostazioni consentono di configurare l'ambiente per l'esecuzione delle estensioni scritte in Ruby. Per usare le estensioni di Ruby, si deve scaricare JRuby, che è un interprete di Ruby implementato in Java. Si noti che è possibile configurare qui la posizione del file JAR JRuby oppure caricare il file JAR all'avvio tramite il percorso di classe Java.

Nota: se si caricano più estensioni Ruby, lo stesso problema può verificarsi con l'archiviazione PermGen come descritto per l'ambiente Python e il problema può essere risolto allo stesso modo.



Burp Extender BApp store



Burp Extender APIs

Burp Suite Sequencer

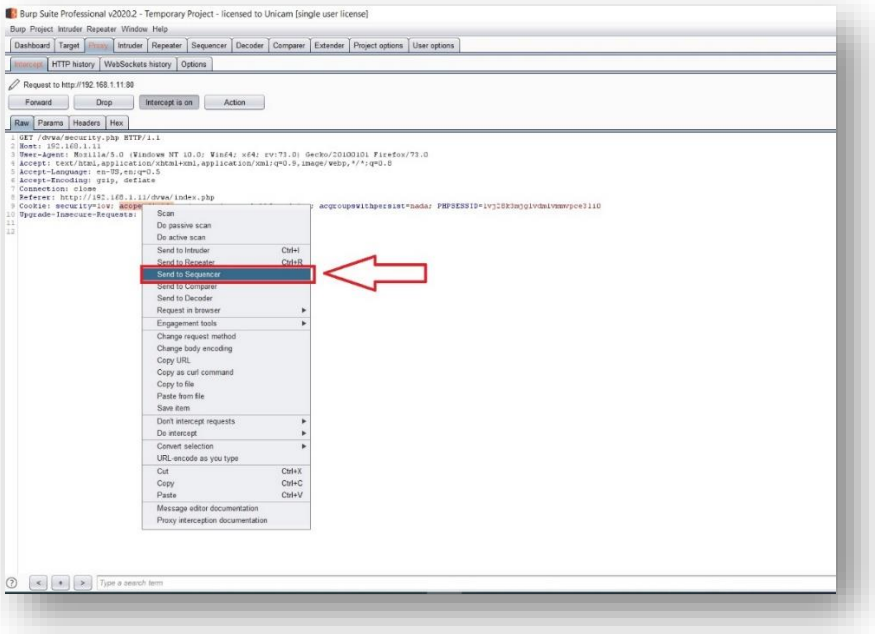
Ottenere un campione

Per eseguire i test di casualità sui token di un'applicazione, è innanzitutto necessario ottenere un campione adeguato di tali token. Questo può essere fatto in due modi: eseguendo un'acquisizione automatica in tempo reale di token direttamente dalla destinazione o caricando manualmente un campione di token che hai già acquisito.

Nota: ovviamente, una dimensione del campione più grande consente un'analisi più affidabile. Burp ti consentirà di eseguire un'analisi iniziale con un campione di soli 100 token, anche se questo non dovrebbe essere considerato affidabile per scopi seri. Un campione di 5.000 token è sufficiente per eseguire un'analisi affidabile per la maggior parte degli scopi, sebbene ciò possa dipendere dalle caratteristiche del campione. La dimensione massima supportata del campione è di 20.000 token, che è sufficiente per eseguire test statistici conformi a FIPS.

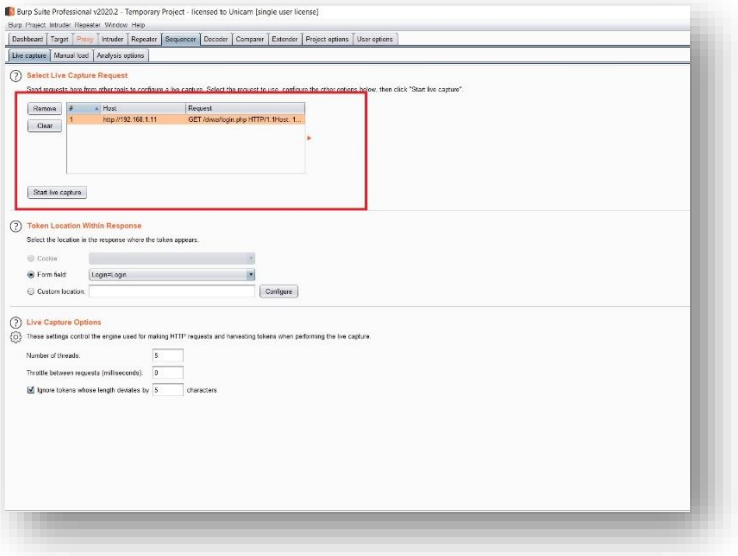
Live Capture

Per eseguire un'acquisizione live, è necessario individuare una richiesta all'interno dell'applicazione di destinazione che restituisce da qualche parte nella sua risposta il token di sessione o un altro elemento che si desidera analizzare. Puoi farlo selezionando una richiesta ovunque all'interno di Burp e selezionando l'opzione "Send to Sequencer" dal menu contestuale. I passaggi necessari per configurare l'acquisizione live su questa richiesta sono descritti di seguito.



Live Capture Request

L'elenco delle richieste di acquisizione live mostra le richieste che hai inviato a Sequencer da altri strumenti Burp. Seleziona la richiesta che restituisce il token o un altro elemento che desideri analizzare.



Posizione del token nella risposta

Seleziona la posizione all'interno della risposta dell'applicazione in cui appare il token. Sono disponibili le seguenti opzioni:

- Cookie: se la risposta imposta cookie, questa opzione consente di selezionare un cookie da analizzare. Questo è il metodo più comune per passare i token di sessione ai client.
- Campo modulo: se la risposta contiene campi modulo HTML, questa opzione consente di selezionare un valore del campo modulo da analizzare. Questo metodo viene spesso utilizzato per trasmettere ai client token anti-CSRF e altri token per pagina.
- Posizione personalizzata: è possibile utilizzare questa opzione per specificare una posizione personalizzata specifica all'interno della risposta contenente i dati che si desidera analizzare. Questo viene fatto usando la finestra di dialogo della regola di estrazione della risposta.

Opzioni Live Capture

Queste impostazioni controllano il motore utilizzato per effettuare richieste HTTP e raccogliere token quando si esegue l'acquisizione live. Sono disponibili le seguenti opzioni:

- Numero di thread: questa opzione controlla il numero di richieste simultanee che l'acquisizione live è in grado di effettuare.
- Limitazione tra le richieste: facoltativamente, l'acquisizione live può attendere un ritardo specificato (in millisecondi) prima di ogni richiesta. Questa opzione è utile per evitare di sovraccaricare l'applicazione o per essere più invisibile.
- Ignora token la cui lunghezza si discosta di X caratteri: è possibile facoltativamente configurare l'acquisizione live per ignorare i token la cui lunghezza si discosta di una determinata soglia dalla lunghezza media del token. Ciò può essere utile se l'applicazione restituisce occasionalmente una risposta

anomala contenente un elemento diverso nella posizione in cui viene normalmente visualizzato il token.

Esecuzione del Live Capture

Dopo aver configurato completamente l'acquisizione live, fare clic sul pulsante "Start live capture" per iniziare l'acquisizione live. Burp Sequencer emetterà ripetutamente la tua richiesta ed estrarrà il token pertinente dalle risposte dell'applicazione.

Durante l'acquisizione live, viene visualizzata una barra di avanzamento, con contatori del numero di token, richieste ed errori di rete. Sono disponibili le seguenti opzioni:

- Pause / Resume: sospende temporaneamente e riprende l'acquisizione.
- Stop: interrompe definitivamente l'acquisizione.
- Copy token: copia negli appunti i token attualmente acquisiti, da utilizzare in altri attacchi Burp (come nei payload Intruder) o in strumenti.
- Save token: salva i token attualmente acquisiti su file.
- Auto - analyze: se questa opzione è abilitata, Burp eseguirà automaticamente l'analisi dei token e aggiornerà periodicamente i risultati durante l'acquisizione live.
- Analyze now: è disponibile quando sono stati acquisiti almeno 100 token e provoca Burp di analizzare il campione corrente e aggiornare i risultati.

Risultati dell'analisi

La finestra dei risultati contiene tutti i dettagli di tutti i test eseguiti.

Sommario

La scheda Summary è il primo posto in cui cercare una conclusione generale sul grado di casualità nel campione. Include un grafico che mostra il numero di bit di entropia effettiva pari o superiore a ciascun livello di significatività. Ciò fornisce un verdetto intuitivo sul numero di bit che superano i test di casualità per diversi possibili livelli di significatività.

La scheda riporta anche una stima dell'affidabilità dei risultati, in base al numero di campioni.

Character-level analysis

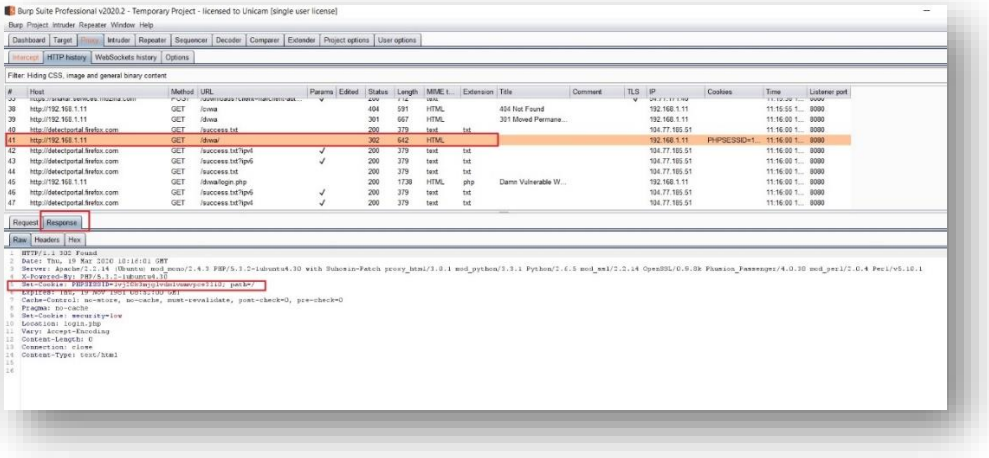
La scheda Character-level analysis di carattere mostra i risultati di riepilogo di tutti i test a livello di carattere e ti consente di approfondire i dettagli di ciascun test a livello di personaggio. Contiene inoltre grafici che mostrano la dimensione del set di caratteri in ciascuna posizione e il numero massimo di bit di entropia che possono essere forniti da ciascuna posizione del carattere.

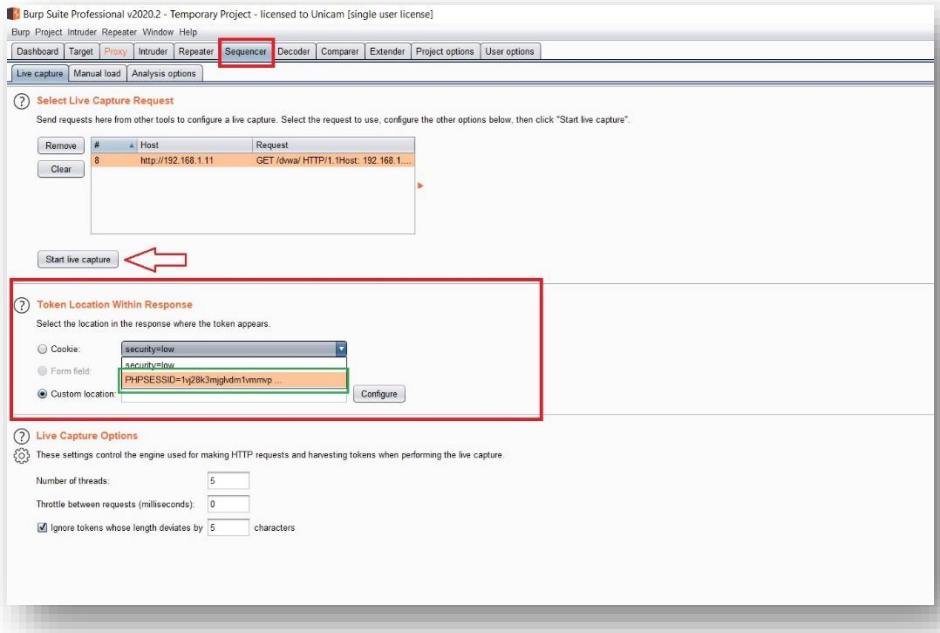
Si noti che i test a livello di carattere non sono affidabili se la dimensione dei set di caratteri utilizzati è troppo grande rispetto al numero di campioni. Ad esempio, se un token impiega 64 caratteri diversi in ciascuna posizione e si acquisiscono solo 100 campioni, non vi è alcun dato di campione sufficiente per trarre conclusioni attendibili sulla distribuzione dei caratteri. Per questo motivo, quando sussiste il rischio di risultati inaffidabili, Burp Sequencer disabiliterà automaticamente i test a livello di personaggio, per evitare che i risultati a livello di personaggio minino i risultati complessivi combinati dall'analisi.

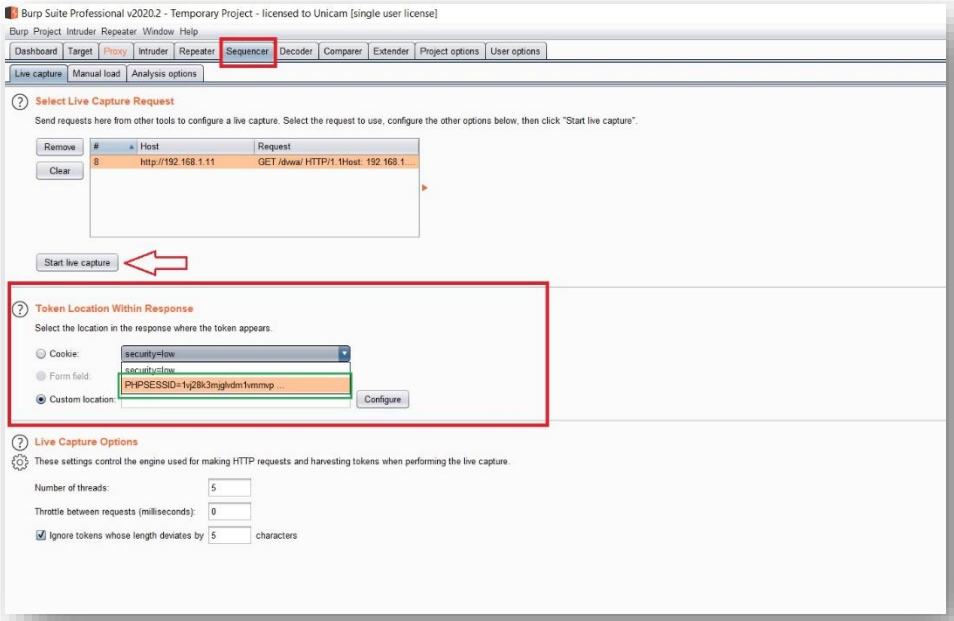
Bit-level analysis

The Bit-level analysis tab shows the summary results from all bit-level tests, and lets you drill down into the detail of each bit-level test. This can let you gain a deeper understanding of the properties of the sample, to identify the causes of any anomalies, and to assess the possibilities for token prediction.

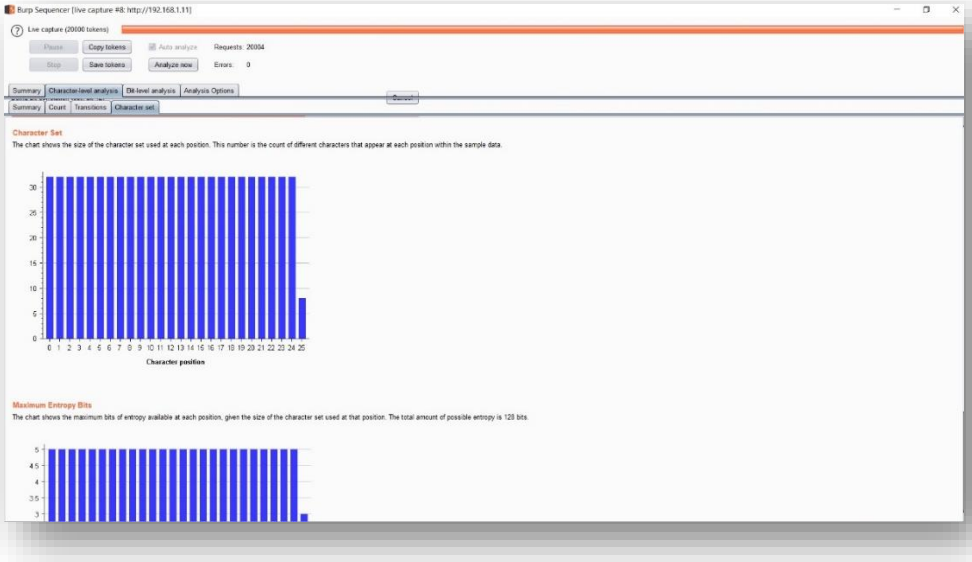
There is also a chart showing the number of bits contributed by each character position in the token. This will enable you cross-reference individual bits within the token back to the original character positions, if you need to.

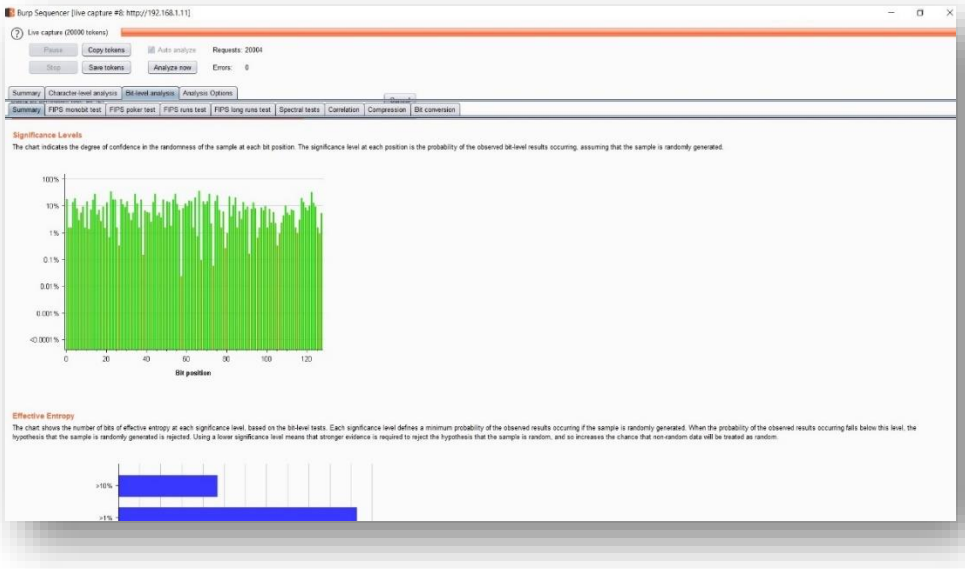



Burp Suite Professional v2020.2 - Temporary Project - licensed to Unicam [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Live capture Manual load Analysis options
Select Live Capture Request
Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".
Remove
Clear
Host Request
8 http://192.168.1.11 GET /dvwa/ HTTP/1.1Host: 192.168.1....
Start live capture
Token Location Within Response
Select the location in the response where the token appears.
Cookie:
security=low
Form field:
PHPSESSID=1vj28k3mjglvdm1vmmvp ...
Custom location:
Configure
Live Capture Options
These settings control the engine used for making HTTP requests and harvesting tokens when performing the live capture.
Number of threads: 5
Throttle between requests (milliseconds): 0
Ignore tokens whose length deviates by 5 characters


Burp Suite Professional v2020.2 - Temporary Project - licensed to Unicam [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Live capture Manual load Analysis options
Select Live Capture Request
Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".
Remove
Clear
Host Request
8 http://192.168.1.11 GET /dvwa/ HTTP/1.1Host: 192.168.1....
Start live capture
Token Location Within Response
Select the location in the response where the token appears.
Cookie:
security=low
Form field:
PHPSESSID=1vj28k3mjglvdm1vmmvp ...
Custom location:
Configure
Live Capture Options
These settings control the engine used for making HTTP requests and harvesting tokens when performing the live capture.
Number of threads: 5
Throttle between requests (milliseconds): 0
Ignore tokens whose length deviates by 5 characters


Burp Sequencer [live capture #8: http://192.168.1.11]
Live capture (20000 tokens)
Pause
Copy tokens
Auto analyze
Requests: 20004
Stop
Save tokens
Analyze now
Errors: 0
Summary
Character-level analysis
Bit-level analysis
Analysis Options
At a significance level of 1%, the amount of effective entropy is estimated to be: 113 bits.
Effective Entropy
The chart shows the number of bits of effective entropy at each significance level, based on all tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.
Significance level
>10%
>1%
>0.1%
>0.01%
>0.001%
0
10
20
30
40
50
60
70
80
90
100
110
120
Number of bits of entropy
Reliability
The analysis is based on a sample of 20000 tokens. Based on the sample size, the reliability of the results is: FIPS-compliant.
Note that statistical tests provide only an indicative guide to the randomness of the sampled data. Results obtained may contain false positives and negatives, and may not correspond to the practical predictability of the tokens sampled.
Sample
Sample size: 20000
Token length: 26

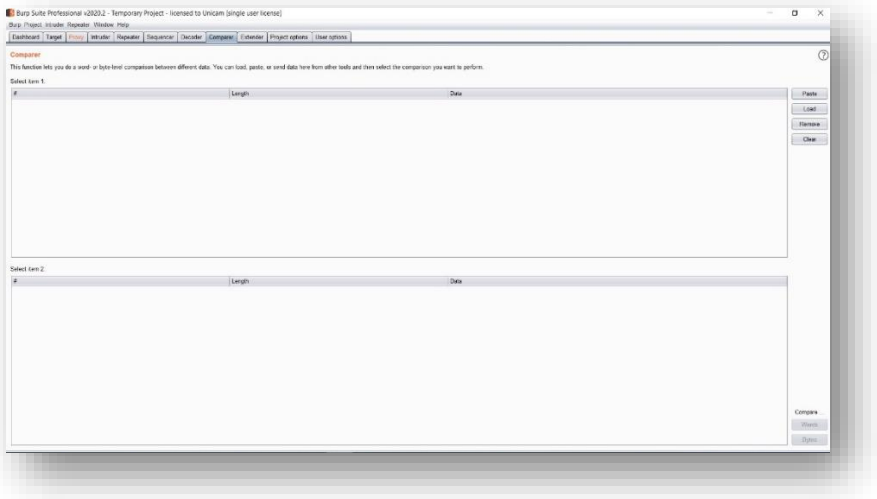

Burp Sequencer [live capture #8: http://192.168.1.11]
Live capture (20000 tokens)
Pause
Copy tokens
Auto analyze
Requests: 20004
Stop
Save tokens
Analyze now
Errors: 0
Summary
Character-level analysis
Bit-level analysis
Analysis Options
Summary
Count
Transitions
Character set
Character Set
The chart shows the size of the character set used at each position. This number is the count of different characters that appear at each position within the sample data.
30
25
20
15
10
5
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
Character position
Maximum Entropy Bits
The chart shows the maximum bits of entropy available at each position, given the size of the character set used at that position. The total amount of possible entropy is 128 bits.
5
4.5
4
3.5
3


Burp Sequencer [live capture #8: http://192.168.1.11]
Live capture (20000 tokens)
Pause
Copy tokens
Auto analyze
Requests: 20304
Stop
Save tokens
Analyze now
Errors: 0
Summary
Character-level analysis
Bit-level analysis
Analysis Options
Summary
FIPS monobit test
FIPS poker test
FIPS runs test
FIPS long runs test
Spectral tests
Correlation
Compression
Bit conversion
Significance Levels
The chart indicates the degree of confidence in the randomness of the sample at each bit position. The significance level at each position is the probability of the observed bit-level results occurring, assuming that the sample is randomly generated.
100%
10%
1%
0.1%
0.01%
0.001%
<0.0001%
0
20
40
60
80
100
120
Bit position
Effective Entropy
The chart shows the number of bits of effective entropy at each significance level, based on the bit-level tests. Each significance level defines a minimum probability of the observed results occurring if the sample is randomly generated. When the probability of the observed results occurring falls below this level, the hypothesis that the sample is randomly generated is rejected. Using a lower significance level means that stronger evidence is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.
>10%
>1%

Burp Suite Comparer

Burp Comparer è un semplice strumento per eseguire un confronto (un "diff" visivo) tra due elementi di dati qualsiasi. Alcuni usi comuni di Burp Comparer sono i seguenti:

- Quando cerchi le condizioni di enumerazione dei nomi utente, puoi confrontare le risposte con accessi non riusciti utilizzando nomi utente validi e non validi, cercando sottili differenze nelle risposte.
- Quando un attacco Intruso ha prodotto risposte molto grandi con lunghezze diverse rispetto alla risposta di base, puoi confrontarle per vedere rapidamente dove si trovano le differenze.
- Quando si confrontano le mappe del sito o le voci della cronologia proxy generate da diversi tipi di utenti, è possibile confrontare coppie di richieste simili per vedere dove si trovano le differenze che danno origine al diverso comportamento dell'applicazione.
- Quando si eseguono test per bug di SQL injection cieca utilizzando l'iniezione di condizioni booleane e altri test simili, è possibile confrontare due risposte per vedere se l'iniezione di condizioni diverse ha comportato una differenza rilevante nelle risposte.



Caricamento dei dati in Comparer

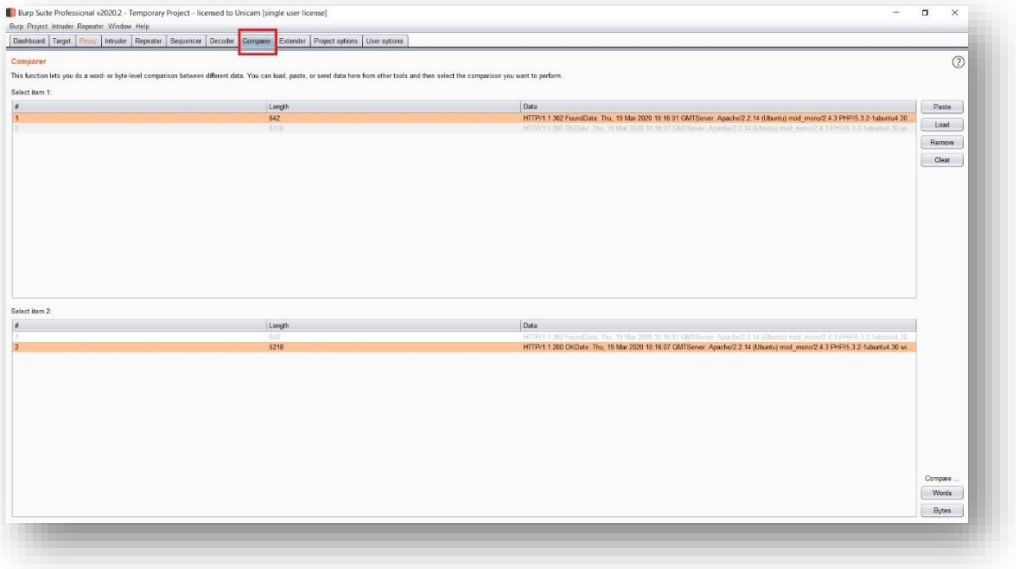
È possibile caricare i dati in Comparer nei seguenti modi:

- Incollando direttamente dagli appunti.
- Caricando dal file.
- Selezionando i dati ovunque all'interno di Burp e scegli "Send to comparer" dal menu contestuale.

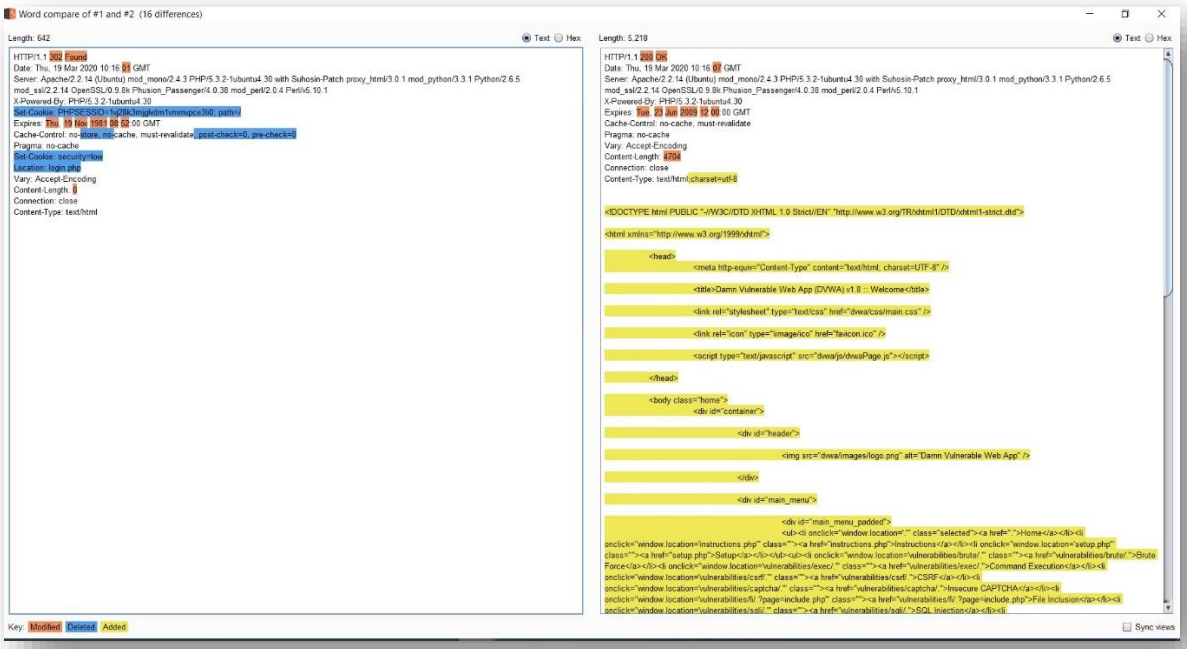
Esecuzione di confronti

Ogni elemento di dati caricati viene mostrato in due elenchi identici. Per eseguire un confronto, selezionare un elemento diverso da ciascun elenco e fare clic su uno dei pulsanti "Confronta":

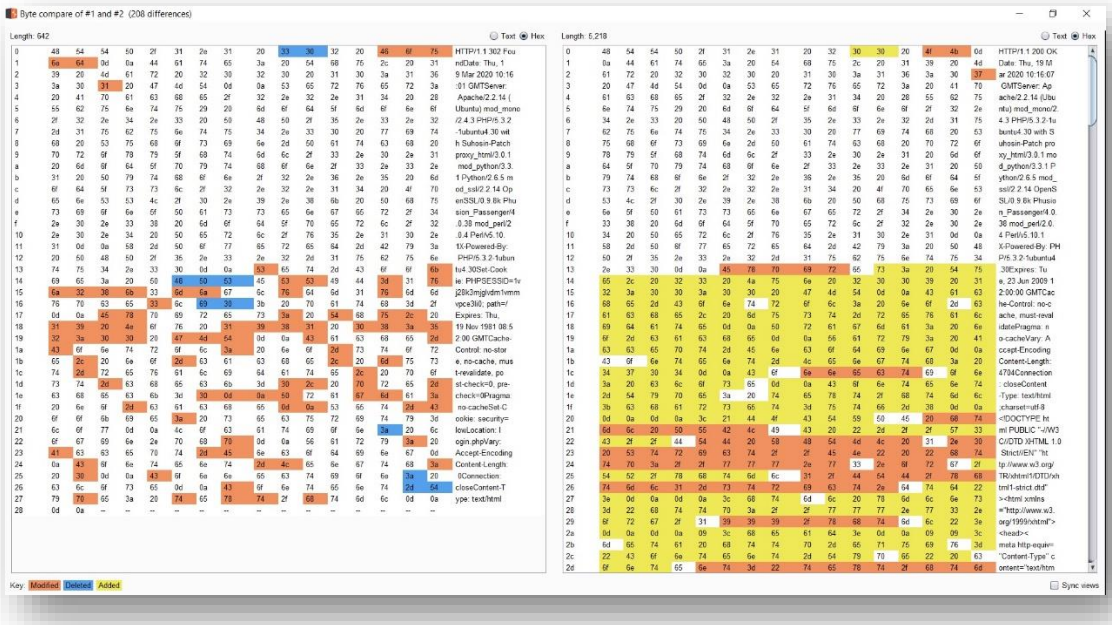
- Confronto di parole: questo confronto tokenizza ogni elemento di dati in base a delimitatori di spazi bianchi e identifica le modifiche a livello di token richieste per trasformare il primo elemento nel secondo. È molto utile quando esistono differenze interessanti tra gli elementi confrontati a livello di parola, ad esempio nei documenti HTML con contenuto diverso.
- Confronto byte: questo confronto identifica le modifiche a livello di byte necessarie per trasformare il primo elemento nel secondo. È molto utile quando esistono interessanti differenze tra gli elementi confrontati a livello di byte, ad esempio nelle richieste HTTP che contengono valori leggermente diversi in un determinato parametro o valore del cookie.



Inserire dati in Comparer



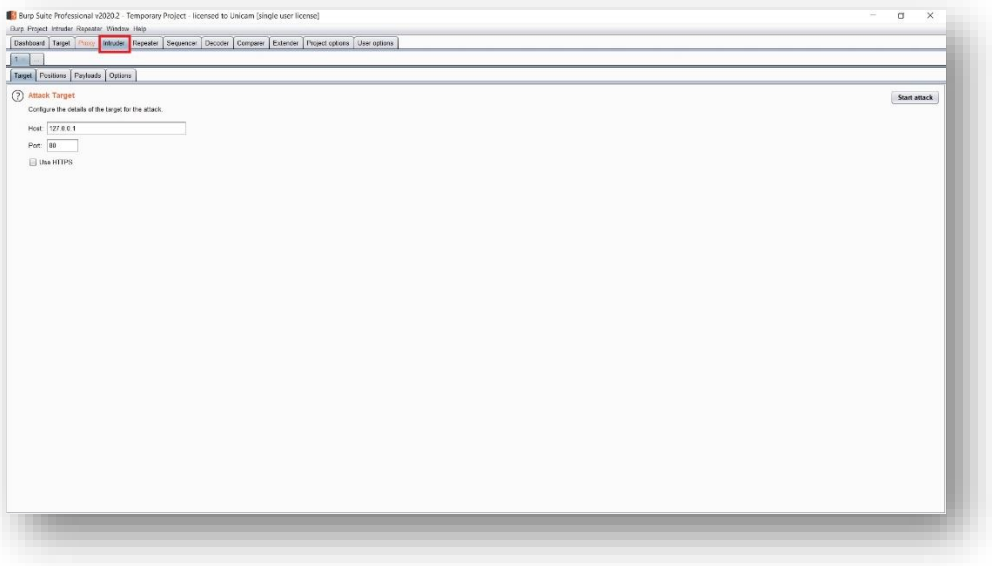
Words compare



Bytes compare

Burp Suite Intruder

Burp Intruder è uno strumento per automatizzare gli attacchi personalizzati contro le applicazioni web. È estremamente potente e configurabile e può essere utilizzato per eseguire una vasta gamma di attività, dalla semplice ipotesi bruta di directory Web allo sfruttamento attivo di vulnerabilità complesse di blind SQL injection.



Cos’è blind SQL injection?

Blind SQL injection sorge quando un'applicazione è vulnerabile a SQL injection, ma le sue risposte HTTP non contengono i risultati della relativa query SQL o i dettagli di eventuali errori del database.

Con vulnerabilità di blind SQL injection, molte tecniche come gli attacchi UNION non sono efficaci, poiché si basano sulla capacità di vedere i risultati della query iniettata nelle risposte dell'applicazione. È ancora possibile sfruttare la blind SQL injection per accedere a dati non autorizzati, ma è necessario utilizzare diverse tecniche.

Come funzione l'intruder

Burp Intruder funziona prendendo una richiesta HTTP (chiamata " base request"), modificando la richiesta in vari modi sistematici, emettendo ogni versione modificata della richiesta e analizzando le risposte dell'applicazione per identificare caratteristiche interessanti.

Per ogni attacco, è necessario specificare uno o più set di payload e le posizioni nella richiesta di base in cui devono essere posizionati i payload. Sono disponibili numerosi metodi per generare payload (inclusi semplici elenchi di stringhe, numeri, date, brute force, bit flipping e molti altri). I payload possono essere inseriti in posizioni di payload utilizzando diversi algoritmi. Sono disponibili vari strumenti per aiutare ad analizzare i risultati e identificare elementi interessanti per ulteriori indagini.

Tipi di attacco

Burp Intruder supporta vari tipi di attacco: determinano il modo in cui i payload sono assegnati alle posizioni del payload. Il tipo di attacco può essere selezionato usando il menu a discesa sopra l'editor del modello di richiesta. Sono disponibili i seguenti tipi di attacco:

- Sniper: utilizza un singolo set di payload. Si rivolge a turno a ciascuna posizione del carico utile e posiziona a turno ciascun carico utile in quella posizione. Le posizioni non targetizzate per una determinata richiesta non sono interessate: i marker di posizione vengono rimossi e qualsiasi testo racchiuso tra loro che appare nel modello rimane invariato. Questo tipo di attacco è utile per confondere individualmente una serie di parametri di richiesta per vulnerabilità comuni. Il numero totale di richieste generate nell'attacco è il prodotto del numero di posizioni e del numero di payload nel set di payload.
- Battering ram: utilizza un unico set di payload. Esegue l'iterazione dei payload e posiziona lo stesso payload in tutte le posizioni definite del payload contemporaneamente. Questo tipo di attacco è utile quando un attacco

richiede l'inserimento dello stesso input in più punti all'interno della richiesta (ad es. Un nome utente all'interno di un cookie e un parametro body). Il numero totale di richieste generate nell'attacco è il numero di payload nel set di payload.

- Pitchfork: utilizza più set di payload. Esiste un set di payload diverso per ciascuna posizione definita (fino a un massimo di 20). L'attacco scorre simultaneamente tutti i set di payload e posiziona un payload in ciascuna posizione definita. In altre parole, la prima richiesta posizionerà il primo payload dal set di payload 1 nella posizione 1 e il primo payload dal set di payload 2 nella posizione 2; la seconda richiesta posizionerà il secondo payload dal set di payload 1 in posizione 1 e il secondo payload dal set di payload 2 in posizione 2, ecc. Questo tipo di attacco è utile quando un attacco richiede input diversi ma correlati da inserire in più punti all'interno del richiesta (ad es. un nome utente in un parametro e un numero ID noto corrispondente a quel nome utente in un altro parametro). Il numero totale di richieste generate nell'attacco è il numero di payload nel set di payload più piccolo.
- Cluster bomb: utilizza più set di payload. Esiste un set di payload diverso per ciascuna posizione definita (fino a un massimo di 20). L'attacco scorre a turno ogni serie di payload, in modo da testare tutte le permutazioni delle combinazioni di payload. Ad esempio, se ci sono due posizioni di payload, l'attacco posizionerà il primo payload dal set di payload 2 in posizione 2 e scorrerà attraverso tutti i payload nel set di carichi utili 1 in posizione 1; posizionerà quindi il secondo payload dal set di payload 2 in posizione 2 e ripeterà tutti i payload nel set di payload 1 in posizione 1. Questo tipo di attacco è utile quando un attacco richiede input diversi e non correlati o sconosciuti da inserire in più punti all'interno della richiesta (ad es. quando si indovinano le credenziali, un nome utente in un parametro e una password in un altro parametro). Il numero totale di richieste generate nell'attacco è il prodotto del numero di payload in tutti i set di payload definiti - questo può essere estremamente elevato.

Usi tipici

Burp Intruder è uno strumento molto flessibile e può aiutare ad automatizzare tutti i tipi di attività durante il test delle applicazioni web. I casi d'uso più comuni per Intruder rientrano nelle seguenti categorie:

- Enumerazione degli identificatori
- Raccolta di dati utili
- Fuzzing per le vulnerabilità

Enumerazione degli identificatori

Le applicazioni Web utilizzano frequentemente identificatori per fare riferimento a elementi di dati e risorse; ad esempio nomi utente, ID documento e numeri di conto. Spesso, sarà necessario scorrere un gran numero di potenziali identificatori per elencare quali sono validi o meritevoli di ulteriori indagini. Per fare ciò in Burp Intruder, devi eseguire i seguenti passi:

- Trova una richiesta di applicazione che contiene l'identificatore in un parametro e dove la risposta indica se l'identificatore è valido.
- Configurare una singola posizione di payload al valore del parametro.
- Utilizzare un tipo di payload adatto per generare potenziali identificatori da testare, utilizzando il formato o lo schema corretti.
- Identificare una caratteristica della risposta da cui si possano dedurre in modo affidabile identificatori validi e configurare Burp di conseguenza. Ad esempio, se un identificatore valido restituisce un diverso codice di stato HTTP o lunghezza di risposta, è possibile ordinare i risultati dell'attacco su questo attributo. Oppure se un identificatore valido restituisce una risposta contenente un'espressione specifica, è possibile definire un elemento grep di corrispondenza per selezionare le risposte che corrispondono a questa espressione.

Alcuni esempi di attacchi del mondo reale di questo tipo sono i seguenti:

- Se i messaggi di errore di accesso dell'applicazione consentono di enumerare nomi utente validi, utilizzare il tipo di payload del generatore di nomi utente

per scorrere un lungo elenco di possibili nomi utente e identificare quelli validi.
- Dopo aver identificato un elenco di nomi utente validi, è possibile utilizzare il semplice tipo di payload dell'elenco con un set di password comuni per tentare di indovinare le password dell'utente.
- Se una funzione dell'applicazione consente di visualizzare i dettagli di qualsiasi ordine, inviando un ID ordine valido, è possibile utilizzare il tipo di payload iteratore personalizzato per generare potenziali ID ordine nel formato corretto e eseguire il trawl per gli ordini di altri utenti.
- Se un'applicazione utilizza token di sessione strutturati significativi che sono crittografati utilizzando un codice CBC, è possibile utilizzare il tipo di payload bit flipper per modificare sistematicamente un token valido per tentare di alterare in modo significativo il suo valore decrittografato.

Raccolta di dati utili

In molte situazioni, anziché semplicemente identificare identificativi validi, è necessario estrarre alcuni dati interessanti su ciascun oggetto, per aiutarti a concentrare i tuoi sforzi sugli oggetti più critici o per alimentare altri attacchi. Per fare ciò in Burp Intruder, devi eseguire i seguenti passi:

- Trova una richiesta di applicazione che contiene un identificatore in un parametro e in cui la risposta contiene i dati interessanti sull'elemento richiesto.
- Configurare una singola posizione di payload al valore del parametro.
- Utilizzare un tipo di payload adatto per generare potenziali identificatori da testare, utilizzando il formato o lo schema corretti.
- Configurare un elemento grep di estrazione per recuperare i dati rilevanti da ciascuna risposta ed elencarli nei risultati dell'attacco.

Alcuni esempi di attacchi del mondo reale di questo tipo sono i seguenti:

- Se l'applicazione dispone di una funzione "Password dimenticata" che accetta un nome utente come parametro e visualizza un suggerimento password impostato dall'utente, è possibile scorrere un semplice elenco di nomi utente comuni ed estrarre il suggerimento password per ciascun utente

valido. È quindi possibile scansionare rapidamente l'elenco dei suggerimenti recuperati per individuare quelli che possono essere facilmente indovinati.

- Se l'applicazione restituisce dinamicamente alcuni contenuti, tramite un singolo URL che contiene un parametro ID pagina numerico, è possibile utilizzare il tipo di payload dei numeri per scorrere tutti i possibili identificatori e recuperare il tag del titolo HTML per ogni pagina. È quindi possibile rivedere rapidamente l'elenco delle pagine disponibili per identificare quelli che sono particolarmente interessanti o ai quali non si dovrebbe consentire l'accesso.
- Se l'applicazione ha una pagina "Profilo utente" che contiene informazioni su ciascun utente, incluso il ruolo nell'applicazione, è possibile scorrere un elenco di nomi utente già estratti e recuperare il ruolo per ciascun utente, consentendo di identificare rapidamente gli account amministrativi per ulteriori attacchi mirati.

Fuzzing per le vulnerabilità

Molte vulnerabilità basate sull'input, come iniezione SQL, script tra siti e attraversamento di percorsi di file possono essere rilevate inviando varie stringhe di test nei parametri di richiesta e analizzando le risposte dell'applicazione per messaggi di errore e altre anomalie. Date le dimensioni e la complessità delle applicazioni odierne, eseguire questi test manualmente è un processo che richiede tempo e noioso.

È possibile automatizzare il fuzzing delle applicazioni Web con Burp Intruder, attenendosi alla seguente procedura:

- Configurare le posizioni del payload ai valori di tutti i parametri della richiesta.
- Utilizzare il tipo di payload dell'elenco semplice.
- Configura l'elenco dei payload utilizzando uno degli elenchi di payload predefiniti di Burp contenenti stringhe fuzz comuni o il tuo elenco di stringhe di attacco.
- Configurare gli elementi grep di corrispondenza con varie stringhe comuni di messaggi di errore. Le opzioni predefinite nell'interfaccia utente grep della partita includono un elenco di stringhe utili a questo scopo.

- Dopo aver lanciato l'attacco, rivedi i risultati dell'attacco per identificare errori interessanti e altre anomalie. È necessario ordinare la tabella dei risultati su ciascuna delle colonne grep di corrispondenza e anche su altre colonne pertinenti come lunghezza della risposta, codice di stato HTTP, timer di risposta, ecc.

Configurare un attacco

L'interfaccia utente principale di Intruder consente di configurare più attacchi contemporaneamente, ciascuno nella propria scheda. Quando si inviano richieste a Intruder, ognuna viene aperta nella propria scheda numerata. Ogni scheda di configurazione dell'attacco contiene diverse sottoschede utilizzate per configurare l'attacco. Utilizzare i collegamenti seguenti per assistenza sui dettagli di ciascuna scheda:

- Target: utilizzato per configurare i dettagli del server target per l'attacco.
- Positions: viene utilizzato per configurare il modello di richiesta per l'attacco, insieme alle posizioni del payload e al tipo di attacco (determina il modo in cui i payload sono assegnati alle posizioni del payload).
- Payload: viene utilizzato per configurare uno o più set di payload, che verranno posizionati in posizioni di payload durante l'attacco.
- Options: consente di configurare numerose altre opzioni che incidono sull'attacco.

Il modo più semplice per creare un nuovo attacco Intruso è selezionare la richiesta di base pertinente all'interno di un altro strumento Burp (come la cronologia proxy o il site map) e utilizzare l'opzione "Send to Intruder" nel menu di scelta rapida. Ciò creerà una nuova scheda di attacco e popolerà automaticamente le schede Target e Posizioni con i dettagli rilevanti sulla richiesta di base. È quindi possibile modificare le posizioni di payload automatico, se necessario, e configurare payload adeguati e altre opzioni di attacco.

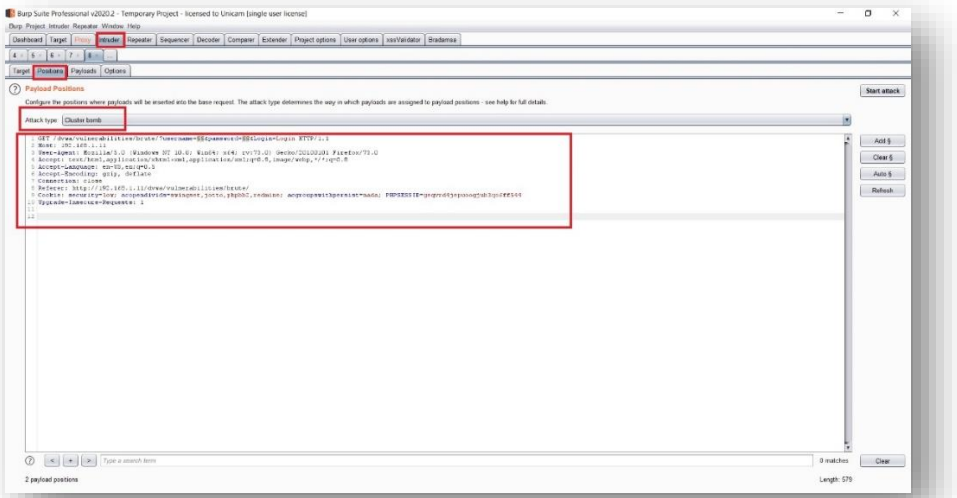
Burp Intruder ha una serie di funzioni che ti aiutano a gestire le configurazioni di attacco. Queste funzioni sono disponibili tramite il menu Intruder:

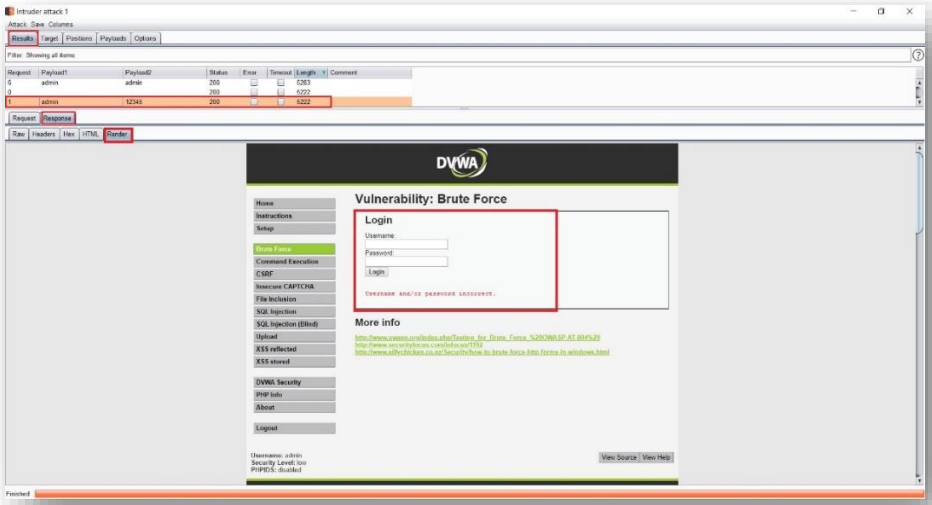
- È possibile salvare la configurazione dell'attacco per la scheda corrente e ricaricarla in un secondo momento. Durante il caricamento o il salvataggio, è possibile includere o escludere facoltativamente le impostazioni delle posizioni del payload. L'inclusione delle impostazioni delle posizioni del payload consente di salvare la configurazione completa per un attacco specifico. Escludendo le impostazioni delle posizioni di payload, è possibile salvare una configurazione di attacco generica che può essere riutilizzata per un altro modello di richiesta di base e posizioni di payload, ad esempio la configurazione preferita per il fuzzing di un particolare tipo di richiesta.
- È possibile copiare le configurazioni di attacco tra due schede esistenti o in una nuova scheda. Ancora una volta, puoi facoltativamente includere o escludere le impostazioni delle posizioni del payload.
- Puoi controllare come Intruder gestisce le configurazioni di attacco quando apri una nuova scheda di attacco (facendo clic sulla scheda "..." all'estrema destra o inviando una nuova richiesta a Intruder). È possibile facoltativamente utilizzare la configurazione di attacco predefinita, copiare la configurazione dalla prima scheda aperta o copiare la configurazione dall'ultima scheda aperta. L'uso di queste ultime opzioni ti consente di creare una configurazione di attacco generica (ad es. Per fuzzing) e di applicarla automaticamente a ogni nuova richiesta che invii a Intruder.

Le schede di attacco stesse sono facili da gestire. Si può:

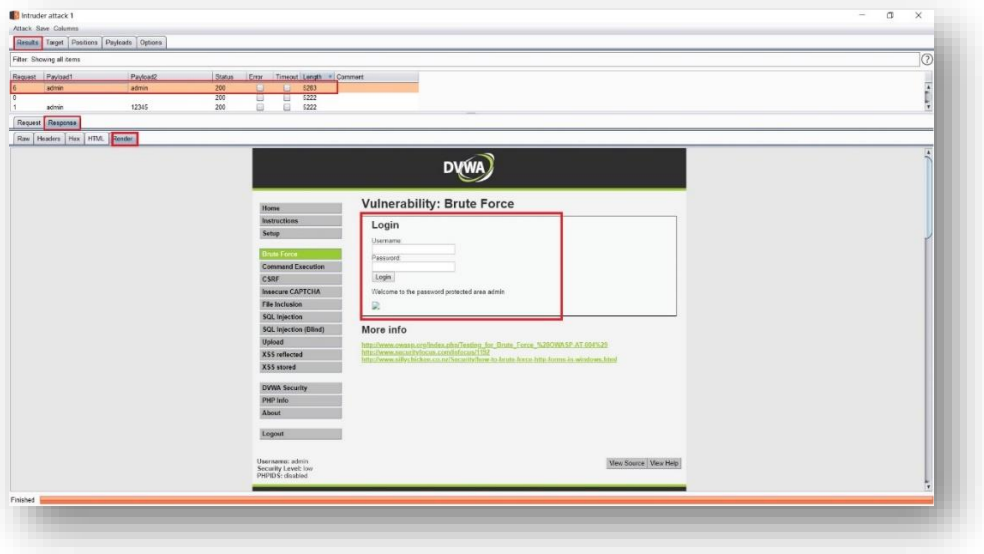
- Rinominare le schede facendo doppio clic sull'intestazione della scheda.
- Riordinare le schede trascinandole.
- Aprire una nuova scheda facendo clic sulla scheda "..." più a destra.
- Chiudere le schede facendo clic sul pulsante X nell'intestazione della scheda.

Esempio di Cluster Bomb

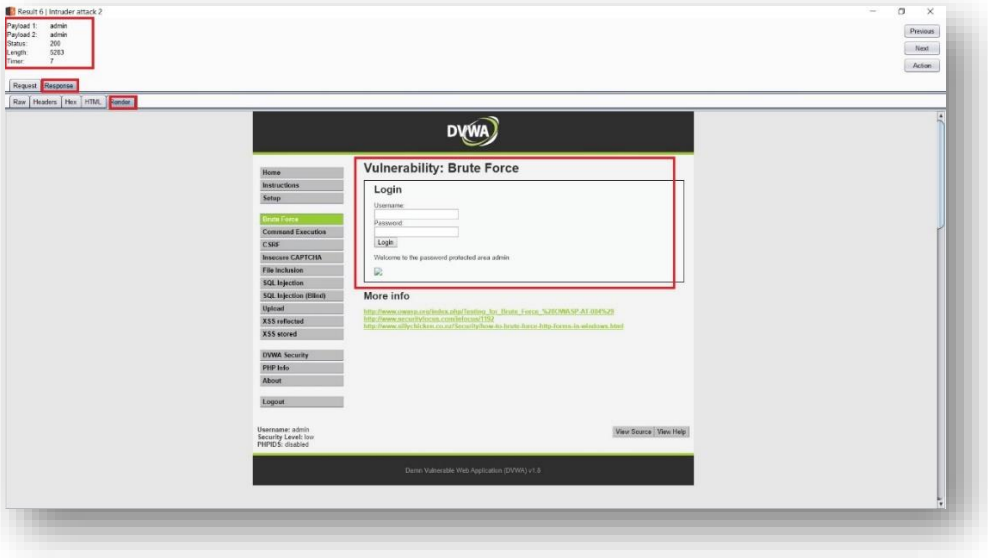




Brute Force che ha fallito



Brute force con successo



Conclusioni

Concludendo, ogni suite di test contiene diversi strumenti complementari che condividono informazioni sull'applicazione di destinazione. In genere, l'attaccante si impegna normalmente con l'applicazione tramite il suo browser. Gli strumenti monitorano le richieste e le risposte risultanti, memorizzando tutti i dettagli rilevanti sull'applicazione di destinazione e forniscono numerose funzioni utili. Occasionalmente, potresti trovare te stesso a testare delle applicazioni che utilizzano un client spesso che viene eseguito al di fuori del browser. Molti di questi client non offrono alcuna impostazione per configurare un proxy HTTP e tentano semplicemente di connettersi direttamente al server Web che ospita l'applicazione. Questo comportamento ti impedisce di utilizzare semplicemente un proxy di intercettazione per visualizzare e modificare il traffico dell'applicazione. La suite tipica contiene i seguenti toolkit principali:

- Un proxy
- Un fuzzer di applicazioni Web personalizzabile
- Uno scanner di vulnerabilità
- Uno strumento di richiesta manuale
- Funzioni per l'analisi dei cookie e di altri token
- Varie funzioni e utilità condivise

Fortunatamente, Burp Suite offre alcune funzionalità che ti consentono di continuare a lavorare in questa situazione.

- Modifica il file ‘host’ del tuo sistema operativo per risolvere i nomi host utilizzati dall'applicazione nel tuo indirizzo di loopback (127.0.0.1).
  Ciò causa il reindirizzamento delle richieste del cliente al proprio computer.
- Per ciascuna porta di destinazione utilizzata dall'applicazione (in genere 80 e 443), configurare un ‘listener proxy Burp’ su questa porta dell'interfaccia di ‘loopback’ e impostare il ‘listener’ in modo che supporti il proxy invisibile. La funzione di proxy invisibile indica che l'ascoltatore accetterà le richieste di tipo non proxy inviate dal client, che sono state reindirizzate al tuo indirizzo di ‘loopback’.
- Il proxy in modalità invisibile supporta richieste HTTP e HTTPS. Per evitare errori irreversibili nei certificati con SSL, potrebbe essere necessario

configurare il ‘listener’ proxy invisibile per presentare un certificato SSL con un nome ‘host’ specifico che corrisponda a ciò che si aspetta il client thick.

- Per ogni nome ‘host’ reindirizzato utilizzando il file ‘hosts’, configurare Burp per risolvere il nome ‘host’ al suo indirizzo IP originale. Ti consentono di specificare mappature personalizzate di nomi di dominio su indirizzi IP per sovrascrivere la risoluzione DNS del tuo computer. Questo fa sì che le richieste in uscita da Burp vengano indirizzate al server di destinazione corretto. (Senza questo passaggio, le richieste verrebbero reindirizzate sul proprio computer in un ciclo infinito.)

Questi toolkit differiscono ampiamente nelle loro capacità e alcuni sono più recenti e più sperimentali di altri. In termini di pura funzionalità, Burp Suite è la più sofisticata e attualmente è l'unica Suite che contiene tutte le funzionalità descritte. In una certa misura, quali strumenti usi sono una questione di preferenza personale.

Sviluppi futuri di Burp Suite

In programma ci sono grandi piani per Burp Suite durante il 2020, con l'obiettivo di migliorare il suo valore per tester professionisti, team di sviluppo software e aziende con risorse Web da proteggere. Qui condivido alcuni dettagli chiave per ciascuno dei prodotti.

Burp Suite Enterprise Edition

Burp Suite Enterprise Edition è quella di offrire alle squadre di sicurezza e sviluppo un nuovo livello di difesa per i loro siti web in espansione. Pianifica e ridimensiona le scansioni su decine, centinaia o migliaia di siti per evidenziare le vulnerabilità in precedenza, dare la priorità alle minacce e accelerare il tempo per affrontare i problemi critici.

Esistono due grandi aree di interesse per Burp Suite Enterprise Edition nel 2020. Continueremo ad aggiungere nuove funzionalità rivolte all'utente in base alle priorità dei clienti. E miglioreremo il supporto per una vasta gamma di casi d'uso e scenari di distribuzione diversi.

I punti salienti per il 2020 includono:

- API migliorate: forniremo API più ricche per l'integrazione con sistemi esterni e altri casi d'uso automatizzati.
- Compatibile con il cloud: supporteremo una facile installazione in ambienti cloud, il ridimensionamento automatico delle risorse per supportare i carichi di lavoro di scansione e le licenze con misurazione oraria.
- Integrazioni aziendali: ci integreremo con piattaforme popolari per la gestione degli utenti (incluso Active Directory) e il monitoraggio dei problemi (inclusi GitHub e Team Foundation Server).

Burp Suite Professional

Ci impegnano a mantenere Burp Suite Pro come il migliore toolkit per i test pratici sulla penetrazione del web. Sarà priorità della Portswigger alle varie nuove funzionalità rivolte agli utenti tecnici avanzati, oltre a migliorare il nucleo del prodotto, rendendolo più affidabile, stabile e utilizzabile da tutti.

I punti salienti per il 2020 includono:

- Interfaccia utente: apporteranno vari miglioramenti all'interfaccia utente e all'usabilità, a partire dall'editor dei messaggi HTTP. Supporteranno la colorazione e la prettificazione di JSON e altri tipi di contenuto e forniremo flussi di lavoro migliorati per codifica, analisi e altre attività comuni sul posto.
- HTTP / 2: supporterà le funzionalità di base di HTTP / 2, prima in Burp Proxy e poi in altri strumenti applicabili. Oltre ad esporre una superficie di attacco aggiuntiva, ciò consentirà a strumenti automatizzati come Burp Intruder e Scanner di funzionare molto più velocemente con alcuni obiettivi.
- Burp Intruder: apporterà vari miglioramenti, tra cui nuovi tipi di payload, nuove opzioni per il posizionamento del payload, analisi più complete dei risultati degli attacchi e salvataggio incrementale dei dati.

Burp Scanner

La loro ambizione è che Burp Scanner si occupi di tutte le tecnologie e funzionalità dell'applicazione comuni, mantenendo al contempo la copertura e le prestazioni della scansione.

I punti salienti per il 2020 includono:

- Scansione basata su browser: partendo dalle basi della nuova funzione sperimentale, continueranno a migliorare le prestazioni e la copertura dei moderni modelli di navigazione. Forniremo un'eccellente copertura di obiettivi tradizionalmente difficili come applicazioni a pagina singola pesanti AJAX. Se del caso, abiliteranno la scansione guidata dal browser per impostazione predefinita.
- Sequenze di accesso registrate: Burp consentirà all'utente di registrare sequenze di accesso utilizzando il proprio browser. Ciò fornirà una copertura e un'accuratezza migliorate rispetto alle semplici credenziali configurate, funzionerà con funzioni di accesso ricche di JavaScript e Single Sign-On e sarà molto più facile da configurare rispetto alle regole di gestione delle sessioni.
- Segnala librerie JavaScript vulnerabili - Burp Scanner eseguirà l'analisi della composizione software (SCA) del codice visibile dal client e segnalerà le librerie JavaScript in uso contenenti vulnerabilità note.

Installazioni necessarie per le dimostrazioni

1. Java
2. Burp Suite (.jar)
3. Burp Suite Pro (.jar)
4. Mozilla Firefox
5. DVWA
6. Oracle VirtualBox
7. BApp Store

Sitografia

1. mitmproxy
2. Charles
3. https://en.wikipedia.org/wiki/Burp_Suite
4. https://portswigger.net/burp/documentation/desktop/getting-started
5. https://support.portswigger.net/customer/portal/articles/1783055-configuring-your-browser-to-work-with-burp
6. https://www.pentestgeek.com/what-is-burpsuite
7. https://www.pentestgeek.com/web-applications/burp-suite-tutorial-1
8. https://www.pentestgeek.com/penetration-testing/credential-harvesting-via-mitm-burp-suite-tutorial
9. https://www.academia.edu/30941407/Burp_Suite
10. https://it.wikipedia.org/wiki/Attacco_man_in_the_middle
11. https://portswigger.net/burp/documentation/desktop/tools/proxy/using
12. https://portswigger.net/burp/documentation/desktop/tools/proxy/options#proxy-listeners
13. https://en.wikipedia.org/wiki/POST_(HTTP)
14. https://it.wikipedia.org/wiki/HTTPS
15. https://portswigger.net/support/installing-burp-suites-ca-certificate-in-firefox
16. https://portswigger.net/burp/documentation/desktop/tools/repeater
17. https://portswigger.net/burp/documentation/desktop/tools/repeater/using
18. https://portswigger.net/support/using-burp-scanner-to-find-cross-site-scripting-(xss)-issues
19. https://portswigger.net/web-security/cross-site-scripting
20. https://portswigger.net/burp/documentation/desktop/scanning
21. https://portswigger.net/burp/documentation/desktop/tools/extender
22. https://portswigger.net/burp/documentation/desktop/tools/sequencer
23. https://portswigger.net/burp/documentation/desktop/tools/comparer
24. https://portswigger.net/burp/documentation/desktop/tools/intruder/using
25. https://tools.kali.org/web-applications/burpsuite

Bibliografia

1. The Web Application Hacker's Handbook Second Edition Finding and Eploiting Security Flaws Dafydd Stuttard Marcus Pinto ISBN: 978-1-118-02647-2

2. Burp Suite Essentials Discover the secrets of web application pentesting using Burp Suite, the best book for the job. Akash Mahajan. ISBN 978-1-78355-011-1