

# Burp Suite



# PERCHÉ BURP SUITE

Burp Suite è uno strumento molto popolare tra gli ethical hacker, utilizzato per testare la sicurezza delle applicazioni web.

Di seguito alcune cose da sapere su Burp Suite:

**Interception Proxy:** Burp Suite include un proxy di intercettazione che permette all'utente di intercettare e modificare le richieste e le risposte HTTP tra il browser web e il server. Questo è utile per esaminare e manipolare il traffico tra il client e il server per individuare vulnerabilità come le vulnerabilità di injection.

**Scanner di sicurezza:** Burp Suite include uno scanner di sicurezza automatico che può individuare automaticamente vulnerabilità comuni nelle applicazioni web, come injection (SQL, NoSQL, OS, ecc.), XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), Broken Authentication, Security Misconfiguration, Insecure Direct Object References, Broken Access Control, Sensitive Data Exposure, XML External Entity (XXE), Insecure Deserialization.

**Estensioni personalizzate:** Burp Suite supporta estensioni personalizzate scritte in Java. Questo consente agli utenti di estendere le funzionalità di Burp Suite per adattarsi alle loro esigenze specifiche o per automatizzare compiti ripetitivi.

**Collaborazione:** Burp Suite offre funzionalità di collaborazione che consentono a più utenti di lavorare insieme su un progetto di test della sicurezza delle applicazioni web. Ciò è particolarmente utile per team di sicurezza informatica o per collaborazioni tra ricercatori di sicurezza.

**Analisi dei cookies:** Burp Suite consente agli utenti di analizzare i cookies inviati tra il client e il server. Questo è importante per individuare e comprendere le vulnerabilità legate alla gestione delle sessioni e all'autenticazione.

**Ricerca e sviluppo costante:** Burp Suite è continuamente aggiornato e migliorato dagli sviluppatori di PortSwigger, l'azienda che lo produce. È importante che un ethical hacker sia aggiornato sulle nuove funzionalità e sulle best practice nell'uso di questo strumento.

**Suite di strumenti:** Burp Suite è una suite completa di strumenti per il test della sicurezza delle applicazioni web. Include funzionalità come scanner di vulnerabilità, strumenti per l'intrusione, spidering (per l'analisi automatica dei siti web), repeater (per ripetere richieste HTTP), sequencer (per l'analisi dell'entropia di token di sessione), e molto altro ancora.

In conclusione, Burp Suite è uno strumento potente e versatile per il test della sicurezza delle applicazioni web, e un ethical hacker dovrebbe avere una conoscenza approfondita delle sue funzionalità e capacità per sfruttarlo al massimo nel suo lavoro di individuazione e risoluzione di vulnerabilità.

# Perché abbiamo installato MySQL E APACHE

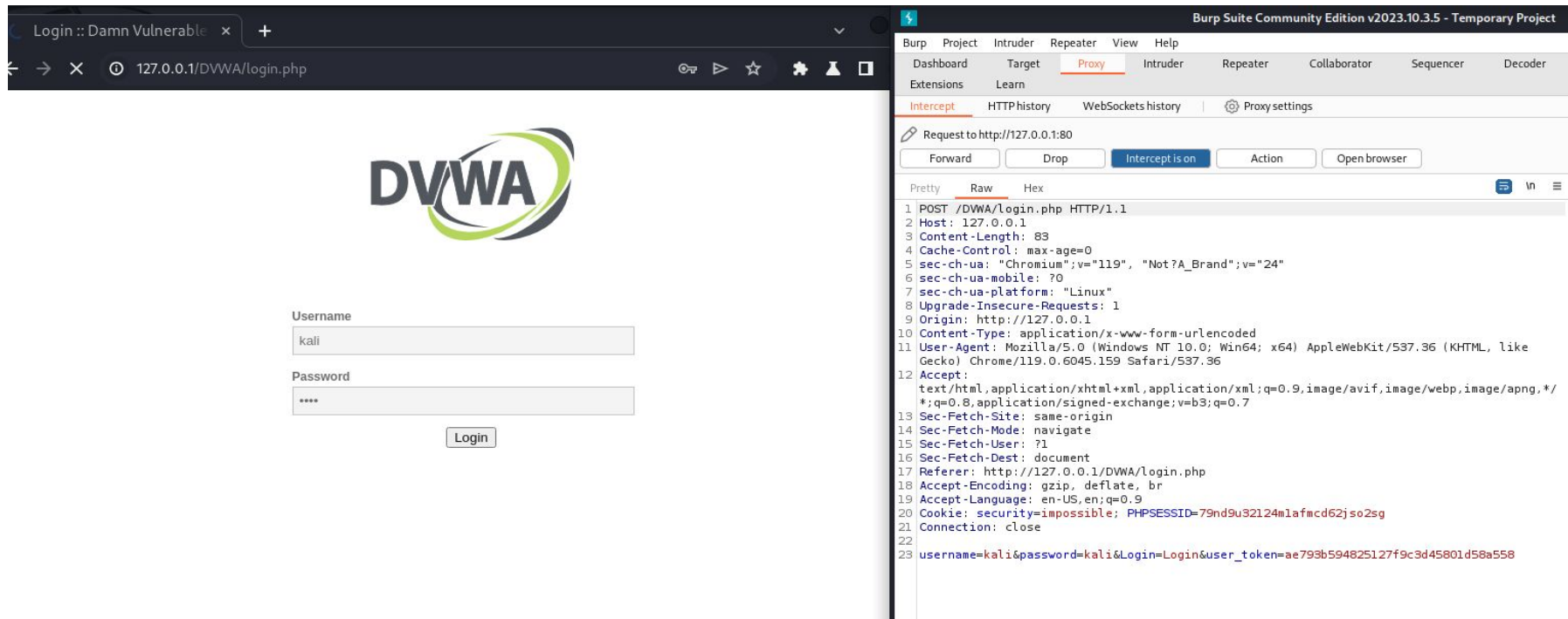
Burp Suite è molto utilizzato per testare la sicurezza delle applicazioni web, inclusi gli aspetti legati al database e al server web.

Avere MySQL e Apache installati ci consente di effettuare test più approfonditi su come l'applicazione interagisce con il database e con il server web, individuando eventuali vulnerabilità legate a queste componenti.

Come detto in precedenza Burp Suite consente di intercettare e analizzare il traffico HTTP tra il browser web e il server. Se Apache è installato sulla stessa macchina, è più semplice configurare il browser per inviare il traffico HTTP tramite il proxy di Burp Suite. Inoltre, è possibile configurare Apache per registrare il traffico di accesso, consentendo un'analisi più approfondita del comportamento dell'applicazione web.

Avere un ambiente completo con MySQL e Apache installati consente di simulare più accuratamente attacchi e test di penetrazione contro l'applicazione web. Ciò può essere utile per valutare la reale esposizione dell'applicazione a diverse minacce e per sviluppare e testare contromisure appropriate.

# Svolgimento dell'esercizio



The image shows a web browser window on the left and the Burp Suite interface on the right. The browser window displays the DVWA (Damn Vulnerable Web Application) login page. The URL bar shows `127.0.0.1/DVWA/login.php`. The login form has a "Username" field containing "kali" and a "Password" field containing "\*\*\*\*". A "Login" button is visible below the fields.

The Burp Suite interface on the right shows the "Proxy" tab selected. The "Intercept" button is highlighted, and the "Intercept is on" status is displayed. The "Request to http://127.0.0.1:80" is shown in the "Raw" tab. The request details are as follows:

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 83
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
12 Gecko) Chrome/119.0.6045.159 Safari/537.36
13 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://127.0.0.1/DVWA/login.php
19 Accept-Encoding: gzip, deflate, br
20 Accept-Language: en-US,en;q=0.9
21 Cookie: security=impossible; PHPSESSID=79nd9u32l24mlafmcd62js02sg
22 Connection: close
23 username=kali&password=kali&Login=Login&user_token=ae793b594825127f9c3d45801d58a558
```

# NOTA

La homepage di DVWA è stata accessibile solo dopo ripetuti tentativi e controlli dei singoli passaggi.

In particolare, il fattore critico per superare il blocco è stato il reinserimento del parametro "low", seguito dal salvataggio e ricaricamento della pagina con il livello di "security level". È da notare che ho mantenuto aperta la finestra delle impostazioni di sicurezza per tenere sotto controllo che i cookie non modificassero il livello di sicurezza, che è rimasto invariato. Tuttavia, il riavvio della pagina DVWA è stato comunque necessario ed efficace.



## Request

Pretty Raw Hex

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/119.0.6045.159 Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
  /*;q=0.8,application/signed-exchange;v=b3;q=0.7
6 Sec-Fetch-Site: none
7 Sec-Fetch-Mode: navigate
8 Sec-Fetch-User: ?1
9 Sec-Fetch-Dest: document
10 sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
11 sec-ch-ua-mobile: ?0
12 sec-ch-ua-platform: "Linux"
13 Accept-Encoding: gzip, deflate, br
14 Accept-Language: en-US,en;q=0.9
15 Cookie: security=impossible; PHPSESSID=79nd9u32124n1afncd62jso2sg
16 Connection: close
```

## Response

Pretty Raw Hex Render

```
50
51 <br />
52
53 <p class="submit">
54   <input type="submit" value="Login" name="Login">
55 </p>
56
57 </fieldset>
58
59 <input type="hidden" name="user_token" value="ae798b594825127f9c3d45801d58a558"
60   />
61 </form>
62
63 <br />
64
65 <br />
66 <br />
67 <br />
68 <br />
69 <br />
70 <br />
71 <br />
72 <br />
73
74 </div>
75 <!--<div id="content">...>
76
77 <div id="footer">
78
79 <p>
80   <a href="https://github.com/digininja/DVWA/" target="_blank">
81     Dawn Vulnerable Web Application (DVWA)
```