

## Burpsuite & DVWA

Completata l'installazione di DVWA e avendo Burpsuite già preinstallato ho iniziato a startare i servizi necessari: **apache2** e **mysql**. Ho verificato poi la loro attivazione:

```
└# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
  Active: active (running) since Sat 2025-11-22 07:19:51 EST; 2s ago
    ● mariadb.service - MariaDB 11.8.3 database server
      Loaded: loaded (/usr/lib/systemd/system/mariadb.service; disabled; preset: disabled)
      Active: active (running) since Sat 2025-11-22 07:20:18 EST; 7s ago
```

La DVWA presente nella directory /var/www/html sarà ospitata da apache2, raggiungibile da browser all'indirizzo //127.0.0.1/DVWA, previa configurazione su setup.php e creazione del Database, ho iniziato l'intercettazione del web server con Burpsuite:

| Time                 | Type | Direction | Method | URL                    |
|----------------------|------|-----------|--------|------------------------|
| 07:47:06 22 Nov 2025 | HTTP | → Request | GET    | http://127.0.0.1/DVWA/ |

Facendo click su Forward è possibile andare avanti con la navigazione nel mentre che si analizzano le request e response http, arrivando alla login ho inserito credenziali errate. Controllando la request su burpsuite ho notato la presenza delle credenziali da me inserite:

```
20 | Cookie: PHPSESSID=1639a3693e09220fbb9f1769cad46171; security=low
21 | Connection: keep-alive
22 |
23 | username=ethical&password=hacker Login=Login&user_token=49079060f52a06e6cdc9590f4442879b
```

Vicino sono presenti cookie di sicurezza da me precedentemente settati, la sessione php e la connessione stabilita (keep-alive), evidentemente perché deve ancora chiudersi non avendo clickato su forward dopo la login. Facendo click destro e inviando la request al repeater ho potuto modificare la request prima di inviarla.

Inviando la mia request e selezionando 'follow redirection' ho potuto leggere la response, in cui:

```
64 |     <div class="message">
       Login failed
     </div>
```

**N.B:** nella riga 64 dentro lo 'stato'  
<div class="message"> si legge '**Login failed**'

Ripetendo i passaggi con i diversi livelli di sicurezza ho notato alcune differenze sulla request:

### Medium Level

```
20 | Cookie: PHPSESSID=1639a3693e09220fbb9f1769cad46171; security=medium
21 | Connection: keep-alive
22 |
23 | username=medium&password=test&Login=Login&user_token=6861c1d950fb54f73014ac25eb94dc70
```

## *High Level*

```
20 | Cookie: PHPSESSID=1b67289badccac61d840b6dbf1719058; security=high
21 | Connection: keep-alive
22 |
23 | username=high&password=test&Login=Login&user_token=d2bea1508642f6d8b6adcc483b703007
```

## *Impossible Level*

```
20 | Cookie: security=impossible; PHPSESSID=348cc3d7d2eed960ccd3c7ffa009e5ad
21 | Connection: keep-alive
22 |
23 | username=impossible&password=test&Login=Login&user_token=b72af8fec2da58e336e9e5c2c8c647d
```

Mentre sulla response l'unica differenza è al livello Impossible:

```
62 | <br />          dove prima c'era Login failed adesso non c'è più
63 | <br />          uno stato <div class="message">
64 |
65 |
66 | <br />
```