```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 87
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="119", "Not?A_Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: application/x-www-form-urlencoded
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
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/login.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: security=impossible; PHPSESSID=q6tqjpj15orpdp9n50eep9q4v4
Connection: close

username=stefano&password=12345&Login=Login&user_token=7dbf98b6e85c81e89c173f7bb467a0c4
```

Nell’esercizio di oggi vediamo cos'è e come funziona burp suite. Burp suite è un software utilizzato per il penetration testing di web application ed è definito come un proxy di intercettazione. Possiede molti tool tra cui scanner, repeater, proxy, ecc. e può catturare il traffico di rete, modificarlo e reinoltrarlo. Come possiamo vedere dall’immagine sopra abbiamo intercettato una richiesta di login a DVWA, poi ho provato a inserire delle credenziali non valide e ho inoltrato la richiesta con il repeater.

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

Come possiamo vedere il login non è andato a buon fine. Poi ho provato a inserire le credenziali corrette.

```
1  POST /DVWA/login.php HTTP/1.1
2  Host: 127.0.0.1
3  Content-Length: 87
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 Gecko) Chrome/119.0.6045.159 Safari/537.36
12 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b
   3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://127.0.0.1/DVWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: PHPSESSID=q6tqjpj15orpdp9n50eep9q4v4; security=impossible
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=8a795643e07cdb77e40ebfdc91fd79eb
```

E sono riuscito ad entrare.

```
<br />
<div class="body_padded">
  <div class="message">
    You have logged in as 'admin'
  </div>
```

In sostanza burp suite fa da tramite fra noi e l’applicazione, inoltre può anche modificare i coockie. Può essere usato, per esempio, per attacchi man in the middle, oltre che per attacchi di intercettazione e replica.