

BurpSuite

Traccia: Lanciamo Burpsuite, scegliamo un progetto temporaneo ed apriamo un browser, inserendo l'indirizzo della nostra DVWA: 127.0.1/DVWA e inseriamo nei campi login e password i valori «admin» e «password» rispettivamente. Intercettiamo la richiesta con burp e vediamo come possiamo modificarla. Guardate i parametri di login, possiamo modificarli a nostro piacimento prima di inviare la richiesta all'app.

Credenziali corrette:

The image displays two screenshots of the Burp Suite Community Edition v2023.10.3.5 interface, illustrating a successful login attempt on the DVWA (Damn Vulnerable Web Application).

Top Screenshot: Intercepted Request

The interface shows the "Proxy" tab with "Intercept" selected. A request to `http://127.0.0.1:80` is intercepted. The "Request" tab displays the raw HTTP request:

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 88
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=b3;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: security=impossible; PHPSESSID=ddhi4qsmifpb00ct8hdsuutd
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=5889c11316ad195f87e0415ea9c049a7
```

The "Inspector" tab on the right shows the request attributes, including the request body parameters:

```
username=admin&password=password&Login=Login&user_token=5889c11316ad195f87e0415ea9c049a7
```

Bottom Screenshot: Intercepted Response

The interface shows the "Repeater" tab with "Send" selected. The "Response" tab displays the raw HTTP response:

```
1 HTTP/1.1 200 OK
2 Date: Wed, 06 Dec 2023 14:03:56 GMT
3 Server: Apache/2.4.58 (Debian)
4 Expires: Tue, 23 Jun 2009 12:00:00 GMT
5 Cache-Control: no-cache, must-revalidate
6 Pragma: no-cache
7 Vary: Accept-Encoding
8 Content-Length: 6103
9 Connection: close
10 Content-Type: text/html; charset=utf-8
11
12 <!DOCTYPE html>
13
14 <html lang="en-GB">
15
16 <head>
17 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
18
19 <title>
20 Welcome :: Damn Vulnerable Web Application (DVWA)
21 </title>
22
23 <link rel="stylesheet" type="text/css" href="
24 dvwa/css/main.css" />
25
26 <link rel="icon" type="image/ico" href="favicon.ico" />
27
28 <script type="text/javascript" src="dvwa/js/dvwaPage.js">
29 </script>
30
31 </head>
32
33 <body class="home">
34 <div id="container">
35
36 <div id="header">
37
38 
40
41 </div>
```

The "Inspector" tab on the right shows the response attributes, including the response body parameters:

```
1 HTTP/1.1 200 OK
```

Traccia: Proviamo a modificare i campi, ed inviare la richiesta inserendo delle credenziali sicuramente errate. Prima di inviare la richiesta, clicchiamo con il tasto destro e selezioniamo «send to repeater» Clicchiamo su send per inviare la richiesta di login ed e poi su follow redirection.

Come ci aspettavamo con le credenziali errate non riusciamo ad entrare. Ne abbiamo evidenza nel body della http response dove leggiamo «Login failed».

Credenziali sbagliate:

The image displays two screenshots of the Burp Suite Community Edition v2023.10.3.5 interface, showing an HTTP request and its corresponding response.

Top Screenshot (Request):

- Target:** http://127.0.0.1
- Request:** POST /DWA/login.php HTTP/1.1
- Host:** 127.0.0.1
- Content-Length:** 88
- 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/DWA/login.php
- Accept-Encoding:** gzip, deflate, br
- Accept-Language:** en-US,en;q=0.9
- Cookie:** security=impossible; PHPSESSID=ddhi4qsmifpb00ct8hdsumutd
- Connection:** close
- Body:** username=gigi&password=gigi&Login=Login&user_token=5889c11316ad195f87e0415ea9c049a7

Bottom Screenshot (Response):

- Target:** http://127.0.0.1
- Response:** GET /DWA/login.php HTTP/1.1
- Host:** 127.0.0.1
- 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
- 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/DWA/login.php
- Accept-Encoding:** gzip, deflate, br
- Accept-Language:** en-US,en;q=0.9
- Cookie:** security=impossible; PHPSESSID=ddhi4qsmifpb00ct8hdsumutd
- Connection:** close
- Body:** </label>
<input type="password" class="loginInput" AUTOCOMPLETE="off" size="20" name="password">

<p class="submit"><input type="submit" value="Login" name="Login"></p></fieldset><input type="hidden" name="user_token" value="837cf2f469928082b59e6a894b0ade5f" /></form>
<div class="message">Login failed</div>

</div><!--<div id="content">--><div id="footer">Damn Vulnerable Web Application (DWA)