DVWA

Username
user

Password
••••••••

Login

Damn Vulnerable Web Application (DVWA)

Burp Suite — Proxy Intercept

Request to http://127.0.0.1:80

Forward | Drop | Intercept is on | Action | Open browser

Pretty | Raw | Hex

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 87
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
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/126.0.6478.127 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
Cookie: security=impossible; PHPSESSID=j20gpaig619hpau7jkf8tbshu5
Connection: keep-alive

username=ciao&password=ciao&Login=Login&user_token=8c542c143f5aea824ff67f9c87480860
```

Burp Suite — Repeater (Request)

```
POST /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Content-Length: 87
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
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/126.0.6478.127 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
Cookie: security=impossible; PHPSESSID=j20gpaig619hpau7jkf8tbshu5
Connection: keep-alive

username=ciao&password=ciao&Login=Login&user_token=8c542c143f5aea824ff67f9c87480860
```

Burp Suite — Repeater (Request / Response)

Request:
```
GET /DVWA/login.php HTTP/1.1
Host: 127.0.0.1
Cache-Control: max-age=0
sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Accept-Language: en-US
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/126.0.6478.127 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
Cookie: security=impossible; PHPSESSID=j20gpaig619hpau7jkf8tbshu5
Connection: keep-alive
```

Response:
```
HTTP/1.1 200 OK
Date: Thu, 17 Oct 2024 13:34:54 GMT
Server: Apache/2.4.62 (Debian)
Expires: Tue, 23 Jun 2009 12:00:00 GMT
Cache-Control: no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Length: 1342
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html;charset=utf-8

<!DOCTYPE html>

<html lang="en-GB">

  <head>

    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>
      Login :: Damn Vulnerable Web Application (DVWA)
    </title>

    <link rel="stylesheet" type="text/css" href="dvwa/css/login.css" />

  </head>

  <body>

    <div id="wrapper">

      <div id="header">

        <br />

        <p>
          <img src="dvwa/images/login_logo.png" />
        </p>

        <br />
```

1,670 bytes | 1,025 mil...

DVWA

Username

Password

Login

CSRF token is incorrect