

[Home](#)[Instructions](#)[Setup / Reset DB](#)[Brute Force](#)[Command Injection](#)[CSRF](#)[File Inclusion](#)[File Upload](#)[Insecure CAPTCHA](#)[SQL Injection](#)[SQL Injection \(Blind\)](#)[Weak Session IDs](#)[XSS \(DOM\)](#)[XSS \(Reflected\)](#)[XSS \(Stored\)](#)[CSP Bypass](#)[JavaScript](#)[Authorisation Bypass](#)[Open HTTP Redirect](#)[DVWA Security](#)[PHP Info](#)[About](#)[Logout](#)

# Welcome to Damn Vuln

Damn Vulnerable Web Application (DVWA) is a PHP and MySQL web application. Its goal is to be an aid for security professionals to test their skills and for developers better understand the processes of secure coding. It is a controlled environment to learn about web application security in a controlled manner.

The aim of DVWA is to **practice some of the more common vulnerabilities**, with a simple straightforward interface.

## General Instructions

It is up to the user how they approach DVWA. Either by selecting any module and working up to reach the goal, or by trying to break the system is not a fixed object to complete a module; however, the goal is to break the system as best as they possible could by using the available tools.

Please note, there are **both documented and undocumented** vulnerabilities. You are encouraged to try and discover the undocumented ones.

There is a help button at the bottom of each page. There are also additional links for further background information.

## WARNING!

Damn Vulnerable Web Application is damn vulnerable. It should not be installed on **any html folder or any Internet facing servers**, as it is a security tool. It should be installed on a test machine (such as [VirtualBox](#) or [VMware](#)), which can download and install [XAMPP](#) for the web server and database.

## Disclaimer

We do not take responsibility for the way in which the application is used. The purposes of the application are clear and it should not be used for anything other than its intended purpose. Measures to prevent users from installing DVWA on production servers are not our responsibility. It is not our responsibility if you install DVWA on a production server.

## More Training Resources

Pretty   **Raw**   Hex

```
1 POST /DWA/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
Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,
ge;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/DWA/login.php
18 Accept-Encoding: gzip, deflate, br
19 Accept-Language: en-US,en;q=0.9
20 Cookie: security=impossible; PHPSESSID=d5vhe27a417dcipefmqnbmorje
21 Connection: close
22
23 username=admin&password=password&Login=Login&user_token=e93fled961132168c9a0
```

**Response**

Pretty   **Raw**   Hex   Render

```
1 HTTP/1.1 302 Found
2 Date: Wed, 07 Feb 2024 15:14:02 GMT
3 Server: Apache/2.4.58 (Debian)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache,
must-revalidate
6 Pragma: no-cache
7 Set-Cookie: PHPSESSID=
69rhcmu2th7g6r3n447dm7cqo5; expires=Thu,
08 Feb 2024 15:14:02 GMT; Max-Age=86400;
path=/; HttpOnly; SameSite=Strict
8 Location: login.php
9 Content-Length: 0
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
```