

Burp Suite Community Edition v2024.1.1.6 - Temporary Project

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger

Intercept HTTP history WebSockets history Proxy settings

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action Open browser


Pretty Raw Hex

1 GET /DVWA/index.php HTTP/1.1  
2 Host: 127.0.0.1  
3 User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:109.0) Gecko/20100101 Firefox/115.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Referer: http://127.0.0.1/DVWA/login.php  
8 Connection: close  
9 Cookie: PHPSESSID=nhstdqimvlf8ul8k39ifr99td1; security=impossible  
10 Upgrade-Insecure-Requests: 1  
11 Sec-Fetch-Dest: document  
12 Sec-Fetch-Mode: navigate  
13 Sec-Fetch-Site: same-origin  
14 Sec-Fetch-User: ?1  
15  
16

Welcome :: Damn Vulnerable Web Application

127.0.0.1/DVWA/index.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



HomeInstructionsSetup / Reset DB

Brute ForceCommand InjectionCSRFFile InclusionFile UploadInsecure CAPTCHASQL InjectionSQL Injection (Blind)Weak Session IDSXSS (DOM)SXSS (Reflected)SXSS (Stored)CSP BypassJavaScriptAuthorisation BypassOpen HTTP Redirect

## Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

### General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

### WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

### Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the