

Editor: Internet [Running] - Google VM VirtualBox

Burp Suite Community Edition v2022.3.6 - Temporary Project

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser options

Learn

SendCancel<>>>

Target: <http://127.0.0.1> HTTP/1.1

Request

Raw

Hex

Text

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="102", "Not;A=Brand";v="24"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 User-Agent: Mozilla/5.0 (X11; Linux x86_64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.120 Safari/537.36
9 Origin: http://127.0.0.1
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (X11; Linux x86_64; AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.120 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,*/*;q=0.8
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Referer: http://127.0.0.1/DVWA/login.php
17 Accept-Encoding: gzip, deflate
18 Accept-Language: fr-FR;q=0.9,en-US;q=0.8,en;q=0.7
19 Cookie: security=impossible; PHPSESSID=urs083rs9z08l5j5q9406t1p
20 Connection: close
21 username=admin&password=admin&login=Login&security_token=ef7c6c10897e53fed3c1b70f438f056c

0 matches

Response

Ready

Welcome :: Damn Vulnerable Web Application

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)

CSRF Bypass

JavaScript

Authorization Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Login

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 possibly 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 recommended using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Install 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 purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility & is the responsibility of the person(s) who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

Burp Suite Community Edition v2022.3.6 - Temporary Project

DashboardTargetProxyIntruderRepeaterSequencerDecoderComparerLoggerExtenderProject optionsUser options

Learn

InterceptHTTP historyWebSockets historyOptions

ForwardStopIntercept & LogActionOpen browser

Login :: Damn Vulnerable

Username

Password

Login

Login failed

[Damn Vulnerable Web Application \(DVWA\)](#)

Qui ho provato a modificare il metodo in POST al posto di GET su una qualsiasi dei prompt laterali e vedere cosa usciva

The image displays two screenshots of a web security testing environment. The top screenshot shows the Burp Suite interface with the 'Intercept' tab selected, displaying a list of intercepted HTTP requests. The bottom screenshot shows the same interface with the 'HTTP history' tab selected, showing a list of intercepted requests. The right side of both screenshots shows the DVWA (Damn Vulnerable Web Application) interface, specifically the 'Vulnerability: Cross Site Request Forgery (CSRF)' page. The page includes a sidebar with navigation links (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, Authentication Bypass, Open HTTP Redirect, DVWA Security, PHP Info, About, Logout) and a main content area with a form titled 'Change your admin password:'. The form has fields for 'Current password:', 'New password:', and 'Confirm new password:', along with a 'Test Credentials' button. The bottom screenshot shows the 'Intercept' tab selected, displaying a list of intercepted HTTP requests, including a POST request to the DVWA 'change_password.php' endpoint.

Questo invece è il normale continuo dell'esercizio in cui vedo le password immesse e le modifico per non far entrare l'utente

The image displays two screenshots of a web application security exercise using Burp Suite and a web browser.

Top Screenshot: The Burp Suite interface shows a request to `http://127.0.0.1:80`. The request details include the following headers:

```
1 POST /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 80
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chrome"
6 sec-ch-ua-platform: "Linux"
7 sec-ch-ua-version: "107"
8 Origin: http://127.0.0.1
9 Content-Type: application/x-www-form-urlencoded
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.127 Safari/537.36
11 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=0.9
12 Accept-Encoding: gzip, deflate
13 Accept-Language: it-IT,it,en-US;q=0.9,en-US;q=0.8,en-US;q=0.7
14 Connection: close
15 Cookie: securitytoken=PPPS3G2DursB89K2b89J9q9H8iip
16 Connection: close
17 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.127 Safari/537.36
18 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=0.9
19 Accept-Encoding: gzip, deflate
20 Accept-Language: it-IT,it,en-US;q=0.9,en-US;q=0.8,en-US;q=0.7
21 Connection: close
22 Cookie: securitytoken=PPPS3G2DursB89K2b89J9q9H8iip
23 Connection: close
```

The browser window shows the DVWA login page with the username `admin` and password `admin` entered. The "Login" button is clicked, and the message "You have logged out" is displayed.

Bottom Screenshot: The Burp Suite interface shows a request to `http://127.0.0.1:80`. The request details include the following headers:

```
1 GET /DVWA/login.php HTTP/1.1
2 Host: 127.0.0.1
3 Content-Length: 80
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chrome"
6 sec-ch-ua-platform: "Linux"
7 sec-ch-ua-version: "107"
8 Origin: http://127.0.0.1
9 Content-Type: application/x-www-form-urlencoded
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.127 Safari/537.36
11 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=0.9
12 Accept-Encoding: gzip, deflate
13 Accept-Language: it-IT,it,en-US;q=0.9,en-US;q=0.8,en-US;q=0.7
14 Connection: close
15 Cookie: securitytoken=PPPS3G2DursB89K2b89J9q9H8iip
16 Connection: close
```

The browser window shows the DVWA login page with the username `admin` and password `admin` entered. The "Login" button is clicked, and the message "Login failed" is displayed.