

localhost/dvwa/security.php

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

Cryptography

DVWA Security

PHP Info

About

DVWA

DVWA Security

Security Level

Security level is currently: low

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA.

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.

3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.

4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low

Submit

77°F

Clear

Search

ENG

10:35 PM

11/20/2024

7.txt7.txt7.txtNew Text Document.txtconfig.inc.phpphp.inicsrf.html

FileEditView

```
<form action="#" method="GET">
  New password:<br />
  <input type="password" AUTOCOMPLETE="off" name="password_new" value="hacker"><br />
  Confirm new password:<br />
  <input type="password" AUTOCOMPLETE="off" name="password_conf" value="hacker"><br />
  <br />
  <input type="submit" value="Change" name="Change">

</form>
```

Ln 5, Col 81332 characters100%Windows (CRLF)UTF-8

77°F
Clear

Search

10:39 PM
11/20/2024

Test Credentials

Confirm new password:

Change

Password Changed:

Announcements

- Chromium
- Edge
- Firefox

More Information

- <https://owasp.org/www-community/attacks/csrf>
- <https://www.cgisecurity.com/csrf-faq.html>
- https://en.wikipedia.org/wiki/Cross-site_request_forgery



