

**№4**

---

21 . .  
2025

‘ ‘



- 

- 

- 

-03-23



- nikto



nikto.






- , . DVWA. apache2 ( .  
(fig:001?)).

```
udnazarmamadov@udnazarmamadov: ~  
Session Actions Edit View Help  
(udnazarmamadov@udnazarmamadov)-[~]  
$ sudo systemctl start mysql  
[sudo] password for udnazarmamadov:  
(udnazarmamadov@udnazarmamadov)-[~]  
$ sudo systemctl start apache2
```

. 1: apache2

## DVWA ( . (fig:002?)).



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

## DVWA Security

### Security Level

Security level is currently: **Impossible**.

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

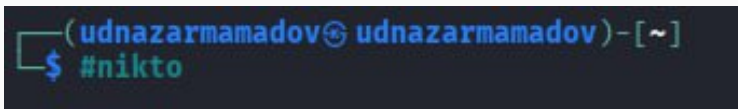
1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting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

nikto ( . (fig:003?)).

A terminal window with a dark background. The prompt is a green square followed by the text "(udnazarmamadov@udnazarmamadov)~". Below the prompt, the command "#nikto" is entered in green text.

```
(udnazarmamadov@udnazarmamadov)~  
$ #nikto
```

. 3: nikto

- , URL ( . (fig:004?)).

```
(udnazarmamadov@udnazarmamadov)-[~]
$ nikto -h http://127.0.0.1/DVWA/
- Nikto v2.5.0

-
+ Target IP:          127.0.0.1
+ Target Hostname:    127.0.0.1
+ Target Port:        80
+ Start Time:         2025-09-21 18:42:42 (GMT-4)

-
+ Server: Apache/2.4.65 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See
: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DVWA/: The X-Content-Type-Options header is not set. This could allow t
he user agent to render the content of the site in a different fashion to
the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/v
ulnerabilities/missing-content-type-header/
+ Root page /DVWA redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
```

( . (fig:005?)).

```
(udnazarmamadov@udnazarmamadov)-[~]
$ nikto -h 127.0.0.1 -p 80
- Nikto v2.5.0

-
+ Target IP:          127.0.0.1
+ Target Hostname:    127.0.0.1
+ Target Port:        80
+ Start Time:         2025-09-21 18:44:19 (GMT-4)

-
+ Server: Apache/2.4.65 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cf, size: 63f4e67c3a417, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
```

- , :

: Apache/2.4.58 (Debian) + /DVWA/: X-Frame-Options,

, . :

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

- /DVWA/: X-Content-Type-Options .

, MIME- . :

<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>

- /DVWA : login.php

- CGI ( '-C all', )

- : HTTP- : GET, POST, OPTIONS, HEAD .



nikto

-