

Индивидуальный проект. Этап 4

Основы информационной безопасности

Иванов Сергей Владимирович, НПИбд-01-23

10 апреля 2025

Российский университет дружбы народов, Москва, Россия

Просканировать веб-приложение используя сканер nikto.

1. Использовать nikto

Выполнение работы

Запуск DVWA

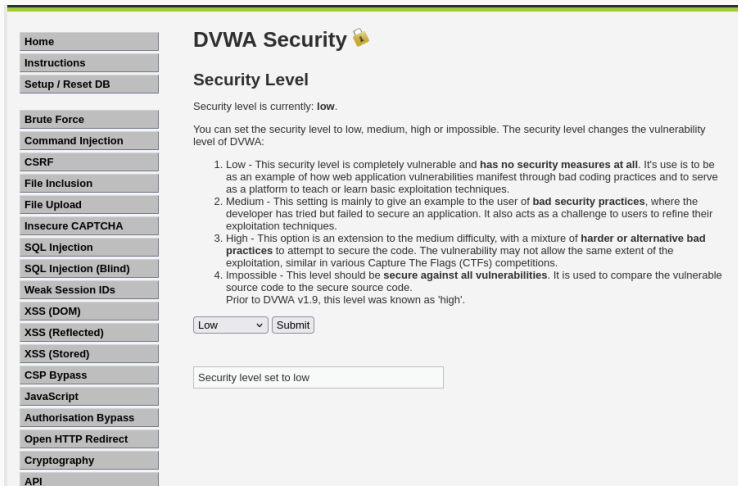
Для начала запустим веб приложение DVWA. Для этого необходимо запустить mysql и apache2. (рис. 1).

```
(svivanov@svivanov)-[~]  
$ sudo systemctl start mysql  
[sudo] пароль для svivanov:  
^[A  
  
(svivanov@svivanov)-[~]  
$ sudo systemctl start apache2
```

Рис. 1: Запуск DVWA

Выбор уровня безопасности

Захожу на сайт DVWA и перехожу во вкладку DWVA Security. Выбираю низкий уровень безопасности. (рис. 2)



The screenshot shows the DVWA Security page. On the left is a sidebar with a list of vulnerability categories: 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, and API. The main content area is titled 'DVWA Security' with a lock icon. Below the title is the 'Security Level' section. It states 'Security level is currently: low.' and 'You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:'. There are four numbered points explaining the levels: 1. Low - completely vulnerable with no security measures; 2. Medium - bad security practices; 3. High - harder or alternative bad practices; 4. Impossible - secure against all vulnerabilities. At the bottom of this section is a dropdown menu currently set to 'Low' and a 'Submit' button. Below the dropdown is a text box that says 'Security level set to low'.

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

API

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:

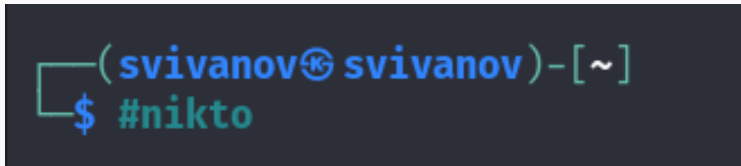
1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting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

Security level set to low

Запуск nikto

Запускаю сканер nikto. (рис. 3)

A terminal window with a dark background. The prompt is '(svivanov@svivanov)~'. The command '\$ #nikto' has been entered.

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

Рис. 3: Запуск nikto

Запускаю сканирование веб приложения вводя URL адрес. (рис. 4)

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

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2025-04-10 13:44:58 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /DWVA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /DWVA/: 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)
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET .
+ /DWVA///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /DWVA/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /DWVA/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /DWVA/login.cgi?cli=aaa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
```


Запускаю сканирование вводя номер порта и адрес порта. (рис. 5)

```
(svivanov@svivanov)-[~]
$ 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:     2025-04-10 13:46:35 (GMT3)

+ Server: Apache/2.4.62 (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: 62fac5ae956b8, mt ime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
```

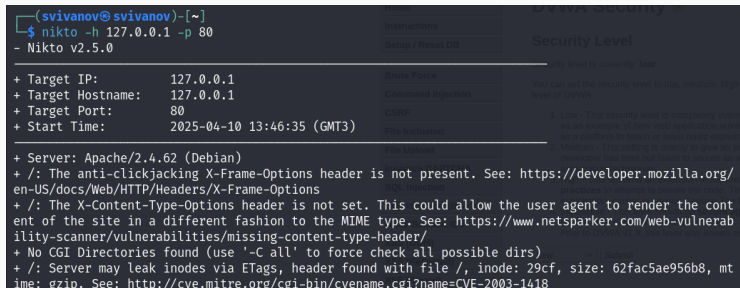
The image shows a terminal window on the left with the command 'nikto -h 127.0.0.1 -p 80' and its output. On the right is a graphical user interface for Nikto, featuring a dark theme. It includes sections for 'Instructions', 'Setup / Reset DB', and 'Security Level'. The 'Security Level' section indicates the current level is 'low' and provides a detailed explanation of what this means for the user, including examples of how security levels are determined and the implications of a 'low' rating.

Рис. 5: Сканирование

Вывод

Получены практические навыки по использованию nikto для сканирования веб приложений.