

Индивидуальный проект этап №4

Основы информационной безопасности

Павлюченков С.В.

07 сентября 25

Российский университет дружбы народов, Москва, Россия

- Павлюченков Сергей Витальевич
- Студент ФФМиЕН
- Российский университет дружбы народов
- 1132237372@pfur.ru
- <https://serapshi.github.io/svpavliuchenkov.github.io/>



Использование `nikto` — базовый сканер безопасности веб-сервера. Он сканирует и обнаруживает уязвимости в веб-приложениях, обычно вызванные неправильной конфигурацией на самом сервере, файлами, установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями.

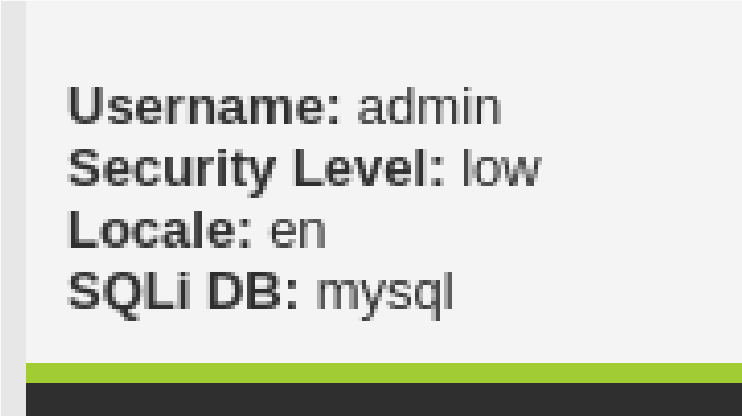
Выполнение лабораторной работы

Проверка факта установки nikto

```
(sipa@tuchemkov ~)$ nikto -h
Option host requires an argument

Options:
  -ask+          Whether to ask about submitting updates
                  yes   Ask about each (default)
                  no    Don't ask, don't send
                  auto   Don't ask, just send
  -check6        Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -Cgидirs+      Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1     Show redirects
                  2     Show cookies received
                  3     Show all 200/OK responses
                  4     Show URLs which require authentication
                  D     Debug output
                  E     Display all HTTP errors
                  P     Print progress to STDOUT
```

Рис. 1: Параметры nikto

A screenshot of the DVWA (Damn Vulnerable Web Application) security settings page. The page has a light gray background with a vertical gray bar on the left. The settings are displayed in a large, bold, black font. Below the text, there are two horizontal bars: a green one and a dark gray one.

Username: admin
Security Level: low
Locale: en
SQLi DB: mysql

Рис. 2: Меняю защиту на слабую

```
(sepatluchenkov@sepatluchenkov) ~  
$ 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:     2025-09-14 09:45:52 (GMT-4)  
+-----+  
  
+ Server: Apache/2.4.63 (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 the user agent to render the content of the site in a different fashion to the MIME type.  
+ /missing-content-type-header/  
+ Root page /dvwa redirects to: login.php  
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Рис. 3: Поиск уязвимостей DVWA

Результат работы

```
svpavluchenkov@svpavluchenkov:~$  
$ 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: 2025-09-14 09:49:36 (GMT-4)  
  
+ Server: Apache/2.4.63 (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/blog/web-security/x-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: 63ec0152ac979, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418  
+ OPTIONS: Allowed HTTP Methods: GET, POST, OPTIONS, HEAD .  
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.  
+ /server-status: This reveals Apache information. Comment out appropriate line in the Apache conf file or restrict access to allowed sources. See: OSVDB-561  
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wp-includes/Requests/utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wordpress/wp-includes/Requests/utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wp-includes/js/tinymce/themes/modern/Menuehy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /wordpress/wp-includes/js/tinymce/themes/modern/Menuehy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /assets/mobileise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.  
+ /login.cgi?ll=aa2baa27cat20/etc/hosts: Some D-Link router remote command execution.  
+ /shell?cat=/etc/hosts: A backdoor was identified.  
+ 8074 requests: 0 error(s) and 15 item(s) reported on remote host  
+ End Time: 2025-09-14 09:50:44 (GMT-4) (68 seconds)  
  
+ 1 host(s) tested  
  
*****  
Portions of the server's headers (Apache/2.4.63) are not in  
the Nikto 2.5.0 database or are newer than the known string. Would you like  
to submit this information (w/o server specific data) to CIRT.net  
for a Nikto update (or you may email to sully@cirt.net) (y/n)? n  
  
svpavluchenkov@svpavluchenkov:~$
```

Рис. 4: Список уязвимостей

Изменение настроек безопасности DVWA на высокие

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

PHP Info

About

Logout

Username: admin
Security Level: high
Locale: en
SQLI DB: mysql

as an example of how web application vulnerabilities manifest themselves as a platform to teach or learn basic exploitation techniques.

2. Medium - This setting is mainly to give an example to the user (developer has tried but failed to secure an application. It also as exploitation techniques.
3. High - This option is an extension to the medium difficulty, with **practices** to attempt to secure the code. The vulnerability may exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities** source code to the secure source code.

Prior to DVWA v1.9, this level was known as 'high'.

High

Security level set to high

Результат работы

```
(svpavliuchenkov@svpavliuchenkov)-[~]
$ 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:     2025-09-14 09:51:58 (GMT-4)

+ Server: Apache/2.4.63 (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 the user agent to render the content of the site in a different fashion to what was intended.
+ /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: GET, POST, OPTIONS, HEAD .
+ /dvwa///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ /dvwa/config/: Directory indexing found.
+ /dvwa/config/: Configuration information may be available remotely.
+ /dvwa/tests/: Directory indexing found.
+ /dvwa/tests/: This might be interesting.
+ /dvwa/database/: Directory indexing found.
+ /dvwa/database/: Database directory found.
+ /dvwa/docs/: Directory indexing found.
+ /dvwa/login.php: Admin login page/section found.
+ /dvwa/.git/index: Git Index file may contain directory listing information.
+ /dvwa/.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /dvwa/.git/config: Git config file found. Infos about repo details may be present.
+ /dvwa/.gitignore: .gitignore file found. It is possible to grasp the directory structure.
+ /dvwa/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /dvwa/wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /dvwa/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /dvwa/wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /dvwa/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /dvwa/wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /dvwa/assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /dvwa/login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /dvwa/shell?cat=/etc/hosts: A backdoor was identified.
+ /dvwa/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 8074 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time:      2025-09-14 09:53:38 (GMT-4) (100 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.63) are not in the Nikto 2.5.0 database or are newer than the known string. Would you like to submit this information (*no server specific data*) to CIRT.net for a Nikto update (or you may email to sullo@cirt.net) (y/n)? n
```

Рис. 6: Список уязвимостей

В этом этапе я научился пользоваться `nikto` вместе с `dvwa` для нахождения уязвимостей с примерами из `dvwa`.