

Четвертый этап индивидуального проекта

Использование nikto

Беличева Д. М.

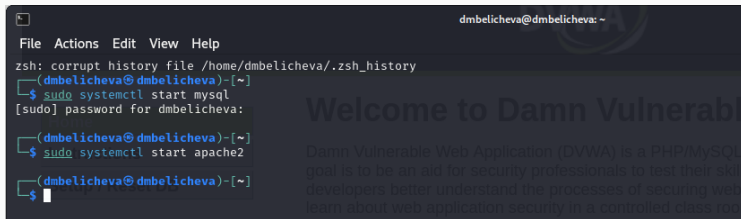
Российский университет дружбы народов, Москва, Россия

Информация

- Беличева Дарья Михайловна
- студентка
- Российский университет дружбы народов
- 1032216453@pfur.ru
- <https://dmbelicheva.github.io/ru/>



Целью данной работы является использование Nikto для сканирования уязвимостей веб-приложения.



```
dmbelicheva@dmbelicheva: ~
File Actions Edit View Help
zsh: corrupt history file /home/dmbelicheva/.zsh_history
(dmbelicheva@dmbelicheva)-[~]
$ sudo systemctl start mysql
[sudo] password for dmbelicheva:
(dmbelicheva@dmbelicheva)-[~]
$ sudo systemctl start apache2
(dmbelicheva@dmbelicheva)-[~]
$
```

Welcome to Damn Vulnerable

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL goal is to be an aid for security professionals to test their skills developers better understand the processes of securing web learn about web application security in a controlled class room

Рис. 1: Запуск mysql и apache2

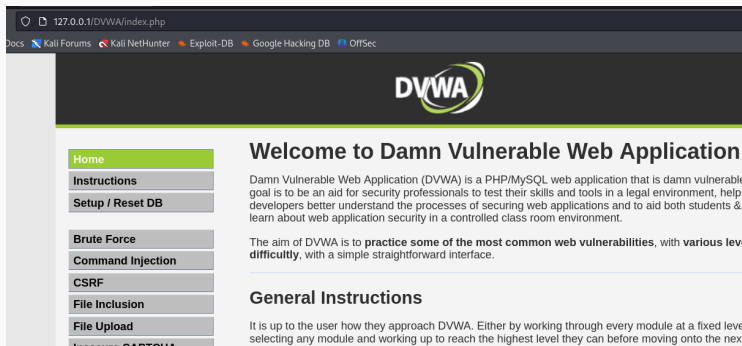


Рис. 2: Страница DVWA

```
(dmbelicheva@dmbelicheva)-[~]
$ nikto
- Nikto v2.5.0

+ ERROR: No host (-host) specified

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
  -Cgidirs+      Scan these CGI dirs: "none", "all", or values like "/cgi
  -config+       Use this config file
  -Display+      Turn on/off display outputs:
                  1     Show redirects
```

Рис. 3: Проверка наличия nikto

Выполнение лабораторной работы

```
(dmbelicheva@dmbelicheva)~$ nikto -h http://127.0.0.1/DVWA -o report.html -Format htm
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-10-05 21:32:55 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /DVWA/: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/
+ /DVWA/: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
ee: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/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: HEAD, GET, POST, OPTIONS .
+ /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.
```

Рис. 4: Проверка уязвимостей по доменному имени

Выполнение лабораторной работы

127.0.0.1 / 127.0.0.1 port 80	
Target IP	127.0.0.1
Target hostname	127.0.0.1
Target Port	80
HTTP Server	Apache/2.4.62 (Debian)
Site Link (Name)	http://127.0.0.1:80/DVWA/
Site Link (IP)	http://127.0.0.1:80/DVWA/
URI	/DVWA/
HTTP Method	GET
Description	/DVWA/: The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://127.0.0.1:80/DVWA/ http://127.0.0.1:80/DVWA/
References	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
URI	/DVWA/
HTTP Method	GET
Description	/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 fa
Test Links	http://127.0.0.1:80/DVWA/ http://127.0.0.1:80/DVWA/
References	https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
URI	/DVWA/
HTTP Method	OPTIONS
Description	OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS

Рис. 5: Отчет об уязвимостях в формате htm

Выполнение лабораторной работы

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

+ Target IP: 127.0.0.1 header is not present.
+ Target Hostname: 127.0.0.1
+ Target Port: 80
+ Start Time: 2024-10-05 21:42:29 (GMT3)

+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ as in a document
+ 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: 6221461e4b1d3, mtime: g
VE-2003-1418
+ OPTIONS: Allowed HTTP Methods: HEAD, GET, POST, OPTIONS
+ /etc/passwd: 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
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor file manager
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/passwd: A PHP backdoor fi
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/Requests/Utility/content-post.php?filesrc=/etc/passwd: A PHP backdoor file manager
+ /wp-includes/js/tinymce/themes/modern/Meuby.php?filesrc=/etc/passwd: A PHP backdoor file manager was found
```

Рис. 6: Проверка уязвимостей с указанием порта

В результате выполнения работы был использован сканер Nikto для сканирования уязвимостей веб-приложения.

1. Обзор сканера Nikto для поиска уязвимостей в веб-серверах [Электрон- ный ресурс]. 2023. URL: <https://habr.com/ru/companies/first/articles/731696/>.