

Основы информационной безопасности. Индивидуальный проект

Этап № 4. Использование Nikto

Демидова Е.А.

09.09.2023

Российский Университет дружбы народов

Информация

- Демидова Екатерина Алексеевна
- студентка группы НКНбд-01-21
- Российский университет дружбы народов
- <https://github.com/eademidova>



Вводная часть

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

Задачи:

- Проанализировать уязвимости веб-приложения DVWA с помощью сканера Nikto.

Инструмент: DVWA, Nikto

Выполнение лабораторной работы

```
(eademidova@eademidova)~[~]
$ perl -v
This is perl 5, version 38, subversion 2 (v5.38.2) built for x86_64-linux-gnu-thread-multi
(with 44 registered patches, see perl -V for more detail)

Copyright 1987-2023, Larry Wall

Perl may be copied only under the terms of either the Artistic License or the
GNU General Public License, which may be found in the Perl 5 source kit.

Complete documentation for Perl, including FAQ lists, should be found on
this system using "man perl" or "perldoc perl". If you have access to the
Internet, point your browser at https://www.perl.org/, the Perl Home Page.

(eademidova@eademidova)~[~]
$ 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 value set in nikto.conf)
  -Cgkdirs+      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 redirects and status codes
                  3     Show redirects, status codes, and content
                  4     Show redirects, status codes, content, and headers
                  5     Show redirects, status codes, content, headers, and cookies
                  6     Show redirects, status codes, content, headers, cookies, and IP addresses
                  7     Show redirects, status codes, content, headers, cookies, IP addresses, and user-agent
                  8     Show redirects, status codes, content, headers, cookies, IP addresses, user-agent, and
                        user-agent IP address
```

Рис. 1: Проверка установки ПО

```
(eademidova@eademidova)~$ nikto -h http://localhost/DVWA/ -o report.html -format htm
- Nikto v2.5.0

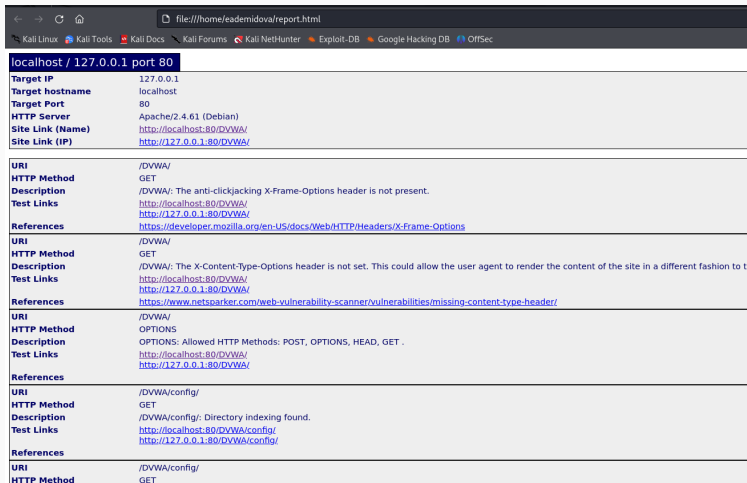
+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-07-31 09:29:18 (GMT-4)

+ Server: Apache/2.4.61 (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.
+ /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.
+ /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.
+ 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 .
+ /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/.dockerignore: .dockerignore file found. It may be possible to grasp the directory structure and learn more about the site.
+ 7850 requests: 0 error(s) and 16 item(s) reported on remote host
+ End Time: 2024-07-31 09:29:33 (GMT-4) (15 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.61) 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)? ^C
```

Рис. 2: Проверка уязвимостей по доменному имени



localhost / 127.0.0.1 port 80	
Target IP	127.0.0.1
Target hostname	localhost
Target Port	80
HTTP Server	Apache/2.4.61 (Debian)
Site Link (Name)	http://localhost: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://localhost: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 fashion to t
Test Links	http://localhost: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: POST, OPTIONS, HEAD, GET .
Test Links	http://localhost:80/DVWA/ http://127.0.0.1:80/DVWA/
References	
URI	/DVWA/config/
HTTP Method	GET
Description	/DVWA/config/: Directory indexing found.
Test Links	http://localhost:80/DVWA/config/ http://127.0.0.1:80/DVWA/config/
References	
URI	/DVWA/config/
HTTP Method	GET

Рис. 3: Отчет об уязвимостях в формате html

Сканирование и анализ

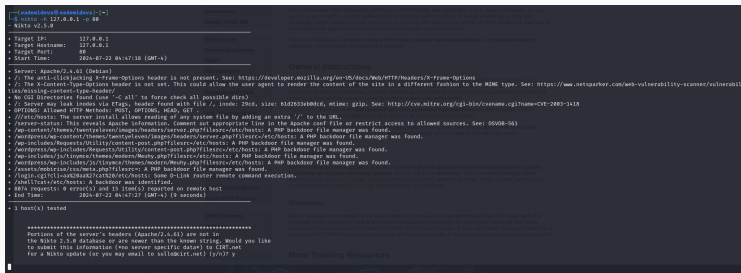


Рис. 4: Проверка уязвимостей с указанием порта

Заключение

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

1. DVWA [Электронный ресурс]. GitHub, Inc, 2024. URL: <https://github.com/digininja/DVWA>.
2. Обзор сканера Nikto для поиска уязвимостей в веб-серверах [Электронный ресурс]. 2006–2024, Habr, 2023. URL: <https://habr.com/ru/companies/first/articles/731696/>.