

Основы информационной безопасности

Индивидуальный проект. Этап № 4. Использование nikto

Нзита Диатезилуа Катенди

Содержание

| | |
|--------------------------------|----|
| Постановка задачи | 4 |
| Теоретические сведения | 5 |
| Выполнение лабораторной работы | 7 |
| Выводы | 11 |
| Список литературы | 12 |

Список иллюстраций

| | | |
|---|---|----|
| 1 | Проверка установки ПО | 7 |
| 2 | Проверка уязвимостей по доменному имени | 8 |
| 3 | Отчет об уязвимостях в формате html | 9 |
| 4 | Проверка уязвимостей с указанием порта | 10 |

Постановка задачи

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

Теоретические сведения

Damn Vulnerable Web Application (DVWA) — это веб-приложение PHP/MySQL, которое чертовски уязвимо[~@dvwa]. Его главная цель — помочь специалистам по безопасности проверить свои навыки и инструменты в правовой среде, помочь веб-разработчикам лучше понять процессы безопасности веб-приложений и помочь студентам и преподавателям узнать о безопасности веб-приложений в контролируемом классе. мебель для спальни.

Цель DVWA — устранить некоторые из наиболее распространенных веб-уязвимостей разного уровня сложности с помощью простого и интуитивно понятного интерфейса. В этом программном обеспечении есть как задокументированные, так и недокументированные уязвимости.

DVWA имеет три уровня безопасности, они изменяют уровень безопасности каждого веб-приложения в DVWA:

- Невозможно — этот уровень должен быть защищен от всех уязвимостей. Он используется для сравнения уязвимого исходного кода с безопасным исходным кодом.
- Высокий — это расширение среднего уровня сложности с комбинацией более сложных плохих практик или обходных путей в попытке защитить код. Уязвимости не допускают такого широкого спектра эксплуатации, как на других уровнях.
- Средний - Этот уровень безопасности в первую очередь предназначен для того, чтобы предоставить пользователю пример плохой практики безопасности, когда разработчик пытался защитить приложение, но потерпел

неудачу.

- Низкий - Этот уровень безопасности полностью уязвим и не имеет никакой защиты. Его цель - быть примером уязвимых веб-приложений, примером плохой практики программирования и служить платформой для обучения основным методам эксплуатации.

Nikto - это бесплатный (с открытым исходным кодом) сканер для поиска уязвимостей в веб-серверах [~@nikto].

В начале сканирования всегда отображается следующий блок информации:

- Целевой IP: IP-адрес сканируемого домена.
- Целевое имя хоста: имя хоста (доменное имя) сканируемого веб-сайта;
- Целевой порт: порт, на котором расположен веб-сайт;
- Время начала: дата и время начала сканирования в формате год-месяц-день час:минута:секунда.

Вывод результатов сканирования имеет несколько форматов:

1. Формат: Тип компонента веб-сайта: Имя компонента. Пример: Сервер: nginx.
2. Описание: Nikto может определить, какие компоненты использует веб-сайт. Сюда входит имя веб-сервера, используемая СУБД, фреймворки, языки программирования, а также их версии. Формат: путь к файлу/каталогу, где была обнаружена уязвимость: описание уязвимости. Пример: /phpinfo.php: Найден вывод функции phpinfo().

Выполнение лабораторной работы

Проверим, что nikto установлен(рис. @fig:001)

```
(dknzita@dknzita)-[~]
$ perl -v

This is perl 5, version 38, subversion 2 (v5.38.2) built for x
86_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 s
ource kit.

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

(dknzita@dknzita)-[~]
$ 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)
  -cgidirs+       Scan these CGI dirs: "none", "all", or values like
"/cgi/ /cgi-a/"
  -config+        Use this config file
```

Рис. 1: Проверка установки ПО

Затем проверим сайт DVWA, указав опции для сохранения отчета в формате html(рис. @fig:002,).

```

(dknzita@dknzita)-[~]
$ nikto -h http://localhost/DVWA/ -o report.html -Format html
- Nikto v2.5.0

+ Target IP: 127.0.0.1
+ Target Hostname: localhost
+ Target Port: 80
+ Start Time: 2024-10-02 07:42:22 (GMT-4)

+ Server: Apache/2.4.62 (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. See: 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: OPTIONS, HEAD, GET, POST .
+ /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: 2024-10-02 07:42:35 (GMT-4) (13 seconds)

+ 1 host(s) tested

*****

```

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/2.4.62 (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 the MIME type. |
| 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: OPTIONS, HEAD, GET, POST . |
| 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

Можем увидеть, что найдены такие уязвимости как отсутствие защиты от кликджекинга, не установлен заголовок X-Content-Type-Options(в связи с чем пользователь может выполнить вредоносный контент не того типа, который предполагает администратор), возможность удаленного доступа к файлам конфигураций, также найдена скрытая папка git, в которой хранятся данные о структуре сайта. Уязвимость типа `This might be interesting...` означает, что необходимо дополнительная ручная проверка(скорей всего это незначительная уязвимость раскрытия информации – доступен просмотр файлов каталога). В конце отчета указано, что найдено 16 уязвимостей.

Также можно посмотреть информацию об уязвимостях по конкретному порту(в нашем случае порт 80 для локального хоста)(рис. @fig:004).

```
(dknzita@dknzita)-[~]
$ 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: 2024-10-02 07:46:24 (GMT-4)

+ Server: Apache/2.4.62 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://develop
r.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 r
ender 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: 622
9b4608334d, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-14
18
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ ///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: OSV08-561
+ /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/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /login.cgi?cli=ask20ask27cat%20/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: 2024-10-02 07:46:37 (GMT-4) (13 seconds)

+ 1 host(s) tested

*****
Portions of the server's headers (Apache/2.4.62) are not in
```

| Vulnerability Scan Results | | | |
|----------------------------|---|-----------------|------------------------|
| Target IP | 127.0.0.1 | Target Hostname | localhost |
| Target Port | 80 | HTTP Server | Apache/2.4.62 (Debian) |
| Site Link (Name) | http://127.0.0.1:80/ | Site Link (URL) | http://127.0.0.1:80/ |
| URI | http://127.0.0.1:80/ | HTTP Method | GET |
| Description | The anti-clickjacking X-Frame-Options header is not present. See: https://develop | | |
| Test Links | https://www.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options | | |
| References | https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ | | |
| URI | http://127.0.0.1:80/ | HTTP Method | GET |
| Description | 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/ | | |
| Test Links | https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ | | |
| References | https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ | | |
| URI | http://127.0.0.1:80/ | HTTP Method | GET |
| Description | 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/ | | |
| Test Links | https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ | | |
| References | https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ | | |
| URI | http://127.0.0.1:80/ | HTTP Method | GET |
| Description | 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/ | | |
| Test Links | https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ | | |
| References | https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/ | | |

Рис. 4: Проверка уязвимостей с указанием порта

Выводы

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

Список литературы

.....