

Домашняя работа № 1

Выполнила Вишняк Евгения

1. Скопировать на машину тестовое приложение test_app_home (с использованием флешки или функционала общих папок), запустить сервер на порту 8000 (python3 manage.py runserver 0.0.0.0:8000).

Тестовое приложение я скопировала в папку Desktop, запустила его в терминале:



```
kali@kali: ~/Desktop/test_app_home
File Actions Edit View Help
^C

(kali@kali)-[~/Desktop/test_app_home]
$ python manage.py migrate
System check identified some issues:

WARNINGS:
core.Guestbook: (models.W042) Auto-created primary key used when not defining a primary key type, by default 'django.db.models.AutoField'.
      HINT: Configure the DEFAULT_AUTO_FIELD setting or the CoreConfig.default_auto_field attribute to point to a subclass of AutoField, e.g. 'django.db.models.BigAutoField'.
Operations to perform:
  Apply all migrations: admin, auth, contenttypes, core, sessions
Running migrations:
  Applying auth.0012_alter_user_first_name_max_length ... OK

(kali@kali)-[~/Desktop/test_app_home]
$ python3 manage.py runserver 0.0.0.0:8000
Watching for file changes with StatReloader
Performing system checks ...

System check identified some issues:

WARNINGS:
core.Guestbook: (models.W042) Auto-created primary key used when not defining a primary key type, by default 'django.db.models.AutoField'.
      HINT: Configure the DEFAULT_AUTO_FIELD setting or the CoreConfig.default_auto_field attribute to point to a subclass of AutoField, e.g. 'django.db.models.BigAutoField'.

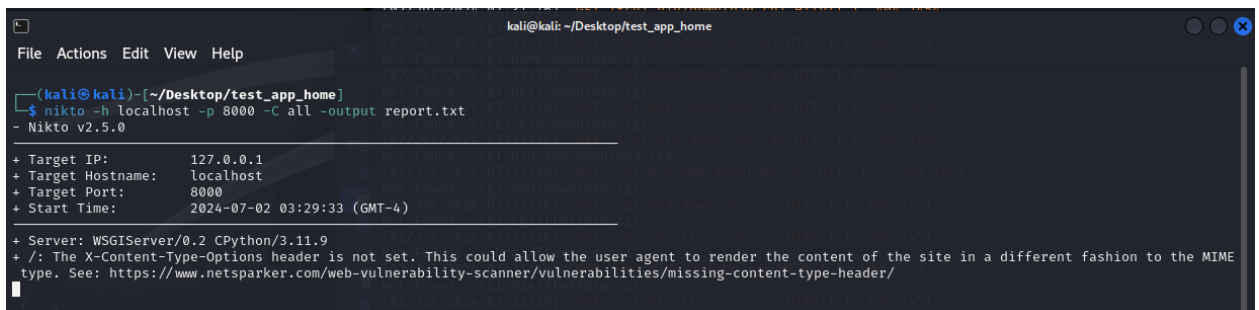
System check identified 1 issue (0 silenced).
July 02, 2024 - 07:18:35
Django version 4.2.13, using settings 'app.settings'
Starting development server at http://0.0.0.0:8000/
Quit the server with CONTROL-C.
```

2. Выполнить сканирование при помощи nikto с параметрами -C all и -output report.txt (это сохранит отчет в файл report.txt).

Командой

nikto -h localhost -p 8000 -C all -output report.txt

запустила сканирование в новом терминале:



```
kali@kali: ~/Desktop/test_app_home
File Actions Edit View Help

(kali@kali)-[~/Desktop/test_app_home]
$ nikto -h localhost -p 8000 -C all -output report.txt
- Nikto v2.5.0

+ Target IP:      127.0.0.1
+ Target Hostname: localhost
+ Target Port:    8000
+ Start Time:     2024-07-02 03:29:33 (GMT-4)

+ Server: WSGIServer/0.2 CPython/3.11.9
+ /: 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/
```

Дождалась завершения сканирования. Результат:

```
kali@kali: ~/Desktop/test_app_home
File Actions Edit View Help

+ Server: WSGIServer/0.2 CPython/3.11.9
+ /: 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/
+ /SilverStream: SilverStream allows directory listing. See: https://web.archive.org/web/20011226154728/http://archives.neohapsis.com/archives/sf/pentest/2000-11/0147.html
+ /cgi.cgi/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /webcgi/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-914/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-915/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /bin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /mcgi/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-bin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /ows-bin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-sys/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-local/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /htbin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgibin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgis/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /scripts/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-win/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /fcgi-bin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-exe/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-home/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-perl/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /scgi-bin/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-bin-sdb/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /cgi-mod/: CGI Directory found. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1607
+ /administrator/: This might be interesting.
+ 26388 requests: 0 error(s) and 26 item(s) reported on remote host
+ End Time: 2024-07-02 03:52:22 (GMT-4) (1369 seconds)

+ 1 host(s) tested
```

Как можно увидеть в отчете, сервер имеет несколько потенциально уязвимых мест, связанных с наличием открытых CGI-директорий. Наличие директории с именем /administrator/ может указывать на наличие административной панели, к которой злоумышленники могут получить доступ, что также можно отнести к уязвимостям.

Файл с результатами сканирования report.txt прилагаю к отчету.

3. На сайте <https://cve.mitre.org/data/refs/refmap/source-OSVDB.html> найти информацию об уязвимости OSVDB-10944, сохранить страницу.

Информация об указанной уязвимости:

Уязвимость OSVDB-10944 относится к проблеме безопасности веб-приложений, связанной с недостаточной фильтрацией входных данных. Она возникает из-за отсутствия или неправильной фильтрации входных данных, поступающих от пользователей. Злоумышленники могут использовать эту уязвимость для внедрения и выполнения вредоносного кода на сервере или для осуществления других атак.

Потенциальные последствия:

- Удаленное выполнение кода
- Перехват данных
- Нарушение конфиденциальности информации
- Отказ в обслуживании (DoS)

Сохраненную страницу прилагаю к отчету.