

**Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

Факультет прикладной информатики

Дисциплина:

«Основы кибербезопасности»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

«Исследование web-уязвимостей»

Выполнил:

Швалов Даниил Андреевич, студент группы К4112с

(подпись)

Проверил:

Кравчук Алексей Владимирович, доцент практики

(отметка о выполнении)

(подпись)

Санкт-Петербург
2025 г.

СОДЕРЖАНИЕ

1 Введение.....	3
2 Ход работы.....	3
2.1 Ручной поиск уязвимостей (скрытых возможностей) web-приложения. .	3
2.2 Работа со сканером уязвимостей nuclei.....	6
2.3 Работа со сканером уязвимостей Acunetix.....	9
3 Вывод.....	12

1 Введение

Цель работы:

- 1) ознакомиться с часто встречающимися уязвимостями в web-приложениях и «худшими» практиками веб-разработки (OWASP Top 10 и уязвимое приложение Juicy Shop);
- 2) получить навыки работы со сканерами web-уязвимостей.

2 Ход работы

2.1 Ручной поиск уязвимостей (скрытых возможностей) web-приложения

В начале выполнения лабораторной работы были загружены образы Ubuntu 24.04 с Juice Shop, Kali Linux с nuclei и Windows 10 с Acunetix. После загрузки данные образы были разархивированы и импортированы в Virtual Box.

После запуска виртуальной машины с Ubuntu с помощью команды `npm start` было запущено уязвимое приложение Juice Shop. Как видно на рисунке 1, приложение было успешно запущено на 3000 порту.

```
user@juice:~$ cd ~/juice-shop/
user@juice:~/juice-shop$ npm start

> juice-shop@19.0.0 start
> node build/app

info: Detected Node.js version v22.12.0 (OK)
info: Detected OS linux (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 20 of 20 are initialized (OK)
(node:2513) [DEP0040] DeprecationWarning: The 'punycode' module is deprecated. Please use a userland alternative instead.
(Use 'node --trace-deprecation ...' to show where the warning was created)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Required file main.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file tutorial.js is present (OK)
info: Port 3000 is available (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
warn: Domain https://www.alchemy.com/ is not reachable (NOT OK in a future major release)
warn: "Mint the Honeypot" challenge will not work as intended without access to https://www.alchemy.com/
warn: "Wallet Depletion" challenge will not work as intended without access to https://www.alchemy.com/
info: Server listening on port 3000
```

Рисунок 1 — Запуск Juice Shop с помощью `npm start`

После этого был открыт браузер Firefox. В нем была открыта веб-страница по адресу `http://127.0.0.1:3000`, которая является главной страницей

Juice Shop, что видно на рисунке 2.

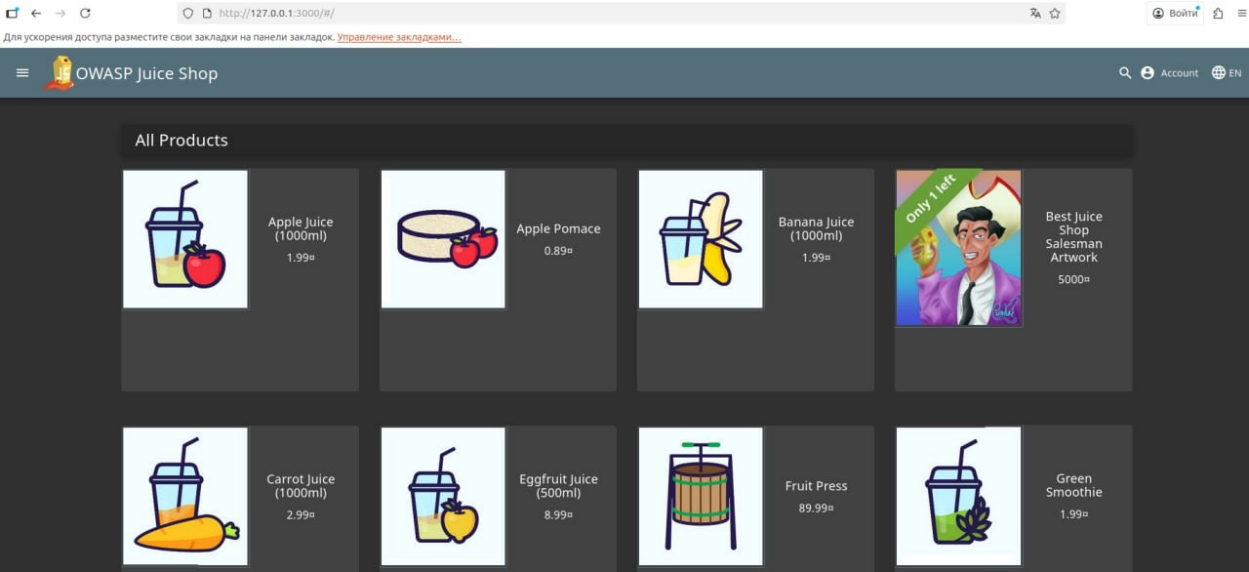


Рисунок 2 — Juice Shop в браузере

После этого с помощью клавиши F12 была открыта вкладка с инструментами разработчика. В ней была открыта вкладка «Сеть», в которой после перезагрузки страницы появились все HTTP-запросы, которые выполнил браузер при загрузке страницы. Содержимое вкладки «Сеть» представлено на рисунке 3.

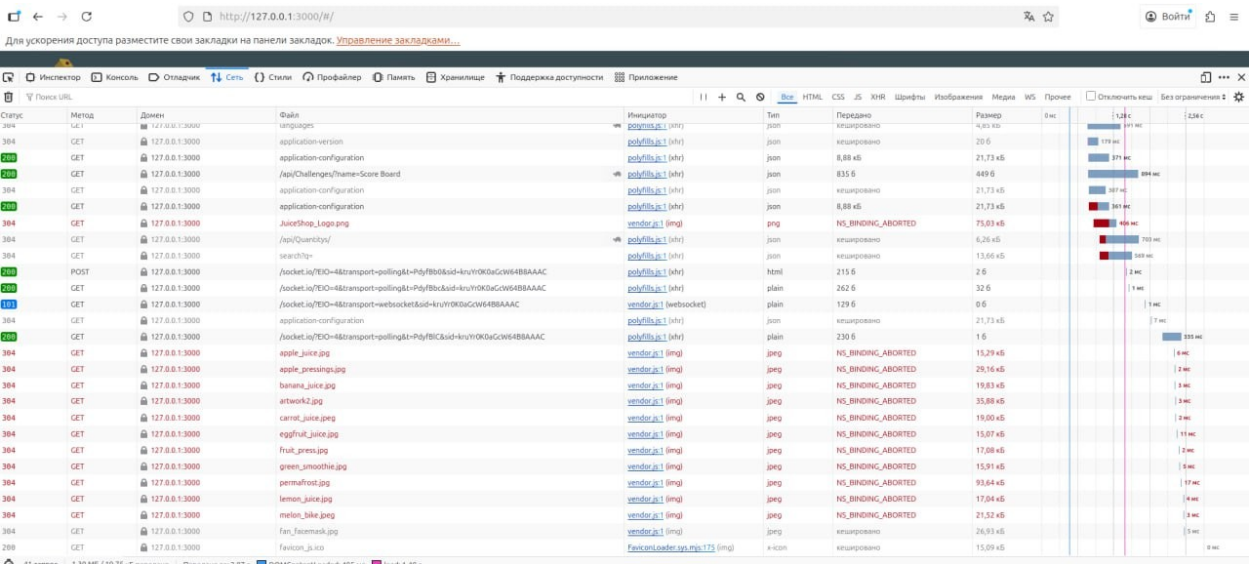
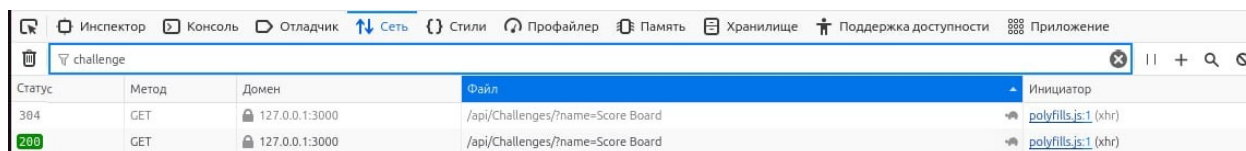


Рисунок 3 — Содержимое вкладки «Сеть» для Juice Shop

Среди запросов были найдены запросы с подстрокой «Challenge» в столбце «Файл». Список подходящих под этот критерий поиска запросов

представлен на рисунке 4.



Статус	Метод	Домен	Файл	Инициатор
384	GET	127.0.0.1:3000	/api/Challenges/?name=Score Board	polyfills.js:1 (xhr)
200	GET	127.0.0.1:3000	/api/Challenges/?name=Score Board	polyfills.js:1 (xhr)

Рисунок 4 — Запросы с «Challenge» в столбце «Файл»

Как видно на рисунке 4, удалось найти два запроса на обработчик `/api/Challenges/` с параметром «name» и значением «Score Board».

После этого в инструментах разработчика была открыта вкладка «Отладчик». С его помощью были проанализированы JavaScript файлы веб-приложения. Как видно на рисунке 5, с помощью ключевого слова «routerLink» в файле `main.js` удалось найти все доступные страницы веб-приложения, в том числе страницу `/score-board`.

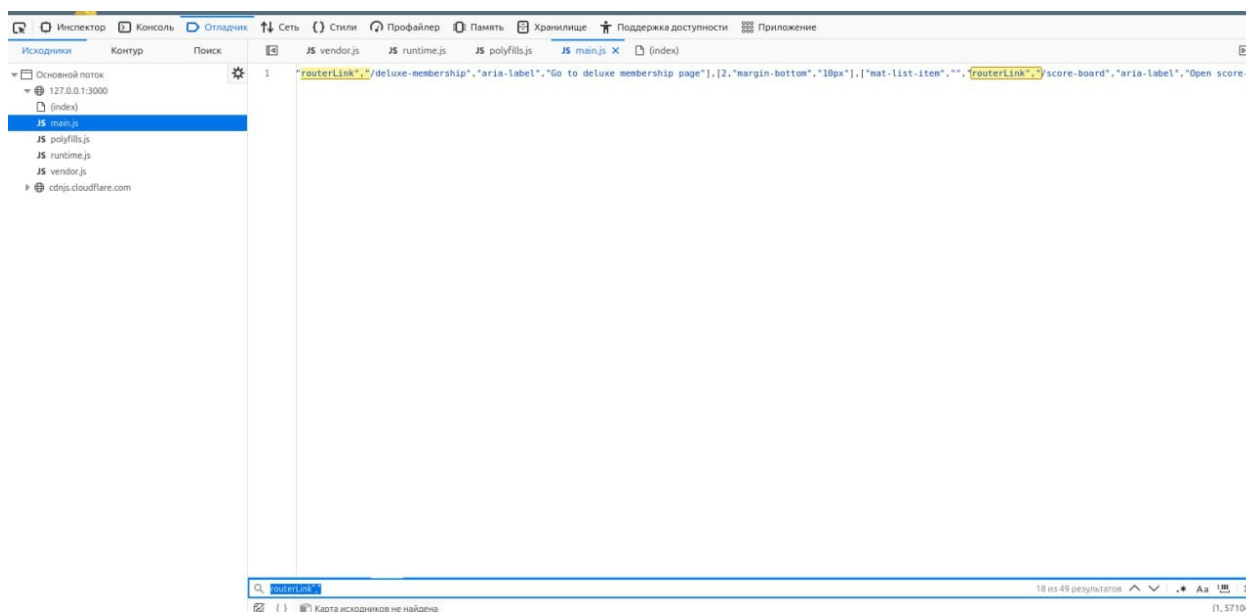


Рисунок 5 — Поиск всех ссылок в веб-приложении

После этого была открыта найденная ранее страница `/score-board`. Как видно на рисунке 6, на данной странице представлена информация о найденных в приложении уязвимостях.

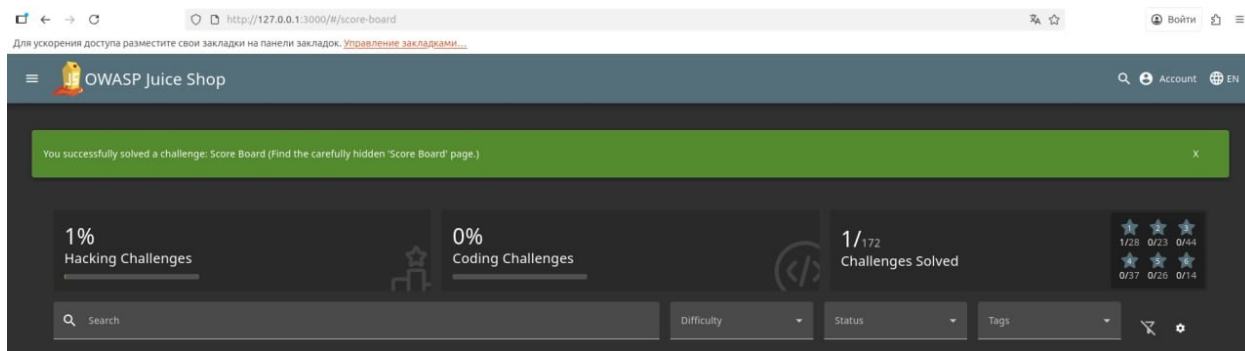


Рисунок 6 — Содержимое страницы /score-board

После завершения работы с Juice Shop был выполнен откат на предыдущее состояние виртуальной машины с помощью снимков. Данный процесс изображен на рисунке 7.

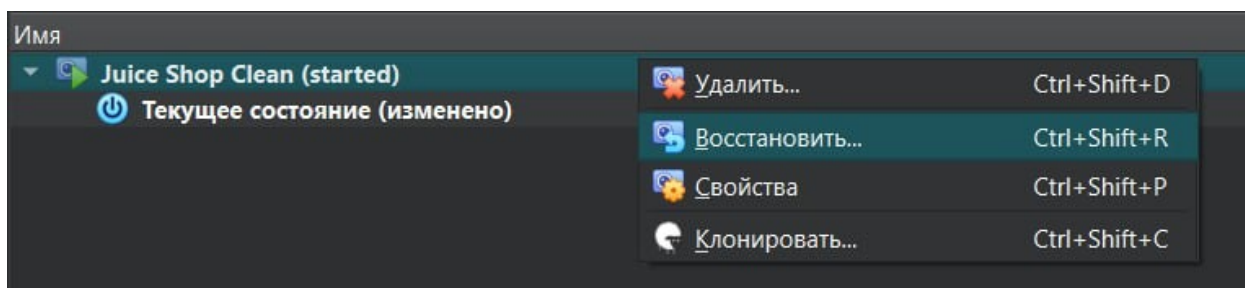


Рисунок 7 — Восстановление изначального состояния виртуальной машины с Ubuntu

2.2 Работа со сканером уязвимостей nuclei

После этого на виртуальной машине с Kali Linux из файла `launch_nuclei.txt` была взята команда запуска `nuclei`. Данная команда была запущена в терминале. Как видно на рисунке 8, удалось найти всего одну уязвимость — это открытый порт для сбора метрик приложения в формате Prometheus.

```
(user@kali)-[~]
└─$ nuclei \
  -u http://192.168.56.10:3000 \
  -headless \
  -code \
  -severity low,medium,high,critical \
  -no-interactsh \
  -no-mhe \
  -retries 3 \
  -markdown-export $PROJECT/nuclei_results \
  -exclude-tags dos

nuclei v3.4.10
projectdiscovery.io

[WRN] Found 1 templates with syntax error (use -validate flag for further examination)
[WRN] Found 96 templates with runtime error (use -validate flag for further examination)
[WRN] Skipping 13 unsigned template[s]
[INF] Current nuclei version: v3.4.10 (outdated)
[INF] Current nuclei-templates version: v10.3.0 (latest)
[INF] New templates added in latest release: 124
[INF] Templates loaded for current scan: 6257
[WRN] Loading 1204 unsigned templates for scan. Use with caution.
[INF] Executing 5053 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 384 (Reduced 334 Requests)
[prometheus-metrics] [http] [medium] http://192.168.56.10:3000/metrics
[INF] Scan completed in 9m. 1 matches found.

(user@kali)-[~]
└─$ cat /home/user/nuclei_lab/nuclei_results/index.md
  |-----|
  | Hostname/IP | Finding | Severity | |
|---|---|---|---|
  | 192.168.56.10:3000 | (prometheus-metrics-192.168.56.10_3000-a3dce772-c17e-4569-b102-6f650ff3489b.md) | prometheus-metrics | medium |
```

Рисунок 8 — Результат запуска nuclei с подготовленными аргументами

Для нахождения большего количества уязвимостей была изучена документация nuclei, существующие аргументы, а также используемые в подготовленной команде аргументы.

Наибольшее количество реальных и потенциальных уязвимостей удалось найти с наименьшим количеством аргументов, указав только URL для сканирования. Используемая команда и результаты сканирования представлены на рисунке 9.

```
(user@kali)-[~]
└─$ nuclei \
  -u http://192.168.56.10:3000

nuclei v3.4.10
projectdiscovery.io

[WRN] Found 1 templates with syntax error (use -validate flag for further examination)
[INF] Current nuclei version: v3.4.10 (outdated)
[INF] Current nuclei-templates version: v10.3.0 (latest)
[INF] New templates added in latest release: 124
[INF] Templates loaded for current scan: 8614
[WRN] Loading 1395 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1804 (Reduced 1691 Requests)
[swagger-api] [http] [info] http://192.168.56.10:3000/api-docs/swagger.json [paths="/api-docs/swagger.json"]
[missing-sri] [http] [info] http://192.168.56.10:3000 ["/cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.js","/cdnjs.cloudflare.com/ajax/libs/jquery/2.2.4/jquery.min.js","/cdnjs.cloudflare.com/ajax/libs/cookieconsent2/3.1.0/cookieconsent.min.css"]
[addeventlistener-detect] [http] [info] http://192.168.56.10:3000
[owasp-juice-shop-detect] [http] [info] http://192.168.56.10:3000
[prometheus-metrics] [http] [medium] http://192.168.56.10:3000/metrics
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.56.10:3000
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.56.10:3000
[security-txt] [http] [info] http://192.168.56.10:3000/.well-known/security.txt ["mailto:donotreply@owasp-juice.shop"]
[x-recruiting-header] [http] [info] http://192.168.56.10:3000 ["/#jobs"]
[robots-txt-endpoint] [http] [info] http://192.168.56.10:3000/robots.txt ["/#jobs"]
[robots-txt] [http] [info] http://192.168.56.10:3000/robots.txt
[fingerprinthub-web-fingerprints:qan-system] [http] [info] http://192.168.56.10:3000
[INF] Scan completed in 17m. 19 matches found.
```

Рисунок 9 — Сканирование с использованием стандартных параметров

Как видно на рисунке 9, с помощью nuclei удалось найти следующие уязвимости помимо тех, что были найдены ранее:

1) у приложения открыт доступ к Swagger — веб-интерфейсу, в котором описаны API-обработчики. Как видно на рисунке 10, в Swagger доступны ручки для создания B2B-заказов;

2) приложение не использует некоторые HTTP-заголовки, которые позволяют предотвратить различные уязвимости, связанные с передачей данных и вызовом обработчиков (например, Cross-Origin-Opener-Policy может предотвратить XSS атаки);

3) в robots.txt указан путь до /ftp, к которому можно получить доступ напрямую из браузера, что видно на рисунке 11.

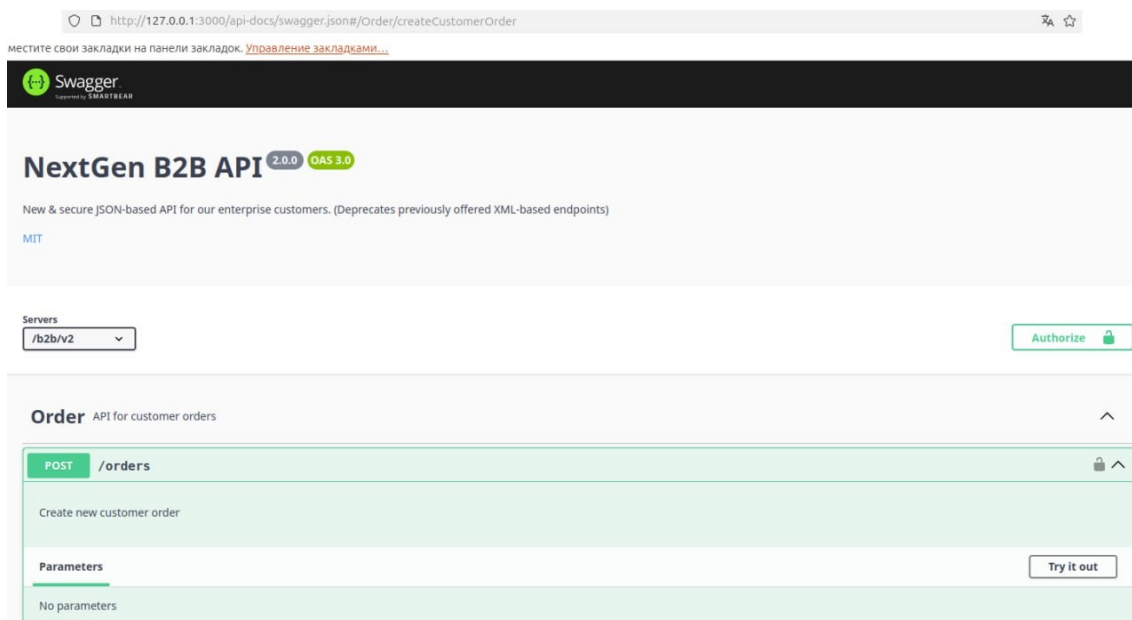


Рисунок 10 — Swagger приложения Juice Shop

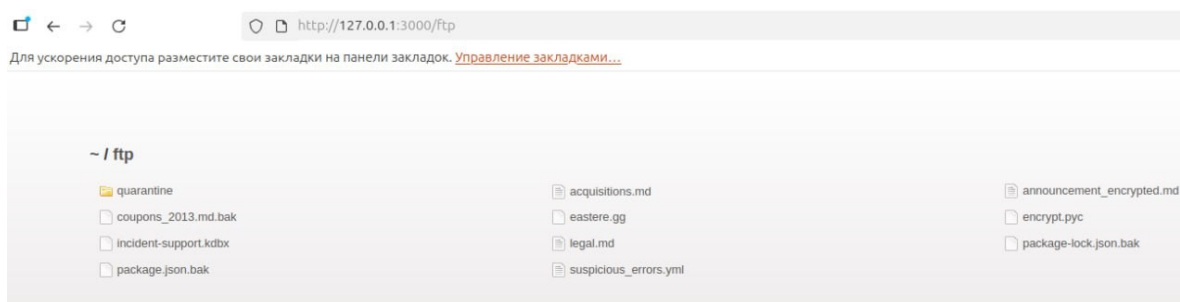


Рисунок 11 — Доступ к FTP через приложение Juice Shop

Также с помощью nuclei удалось найти страницу security.txt — это не является уязвимостью, наоборот с помощью данной страницы у пользователей есть возможность сообщить об уязвимостях соответствующей службе. В данном случае, как видно на рисунке 12, это еще один способ попасть на страницу /score-board.

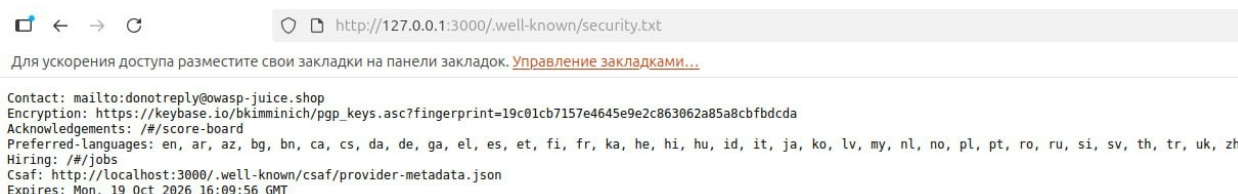


Рисунок 12 — Содержимое security.txt

Других уязвимостей с помощью nuclei найти не удалось.

2.3 Работа со сканером уязвимостей Acunetix

После этого на виртуальной машине с Windows был запущен Acunetix. С помощью браузера Firefox был выполнен вход в Acunetix, после чего был получен доступ к главной странице Acunetix, которая представлена на рисунке 13.

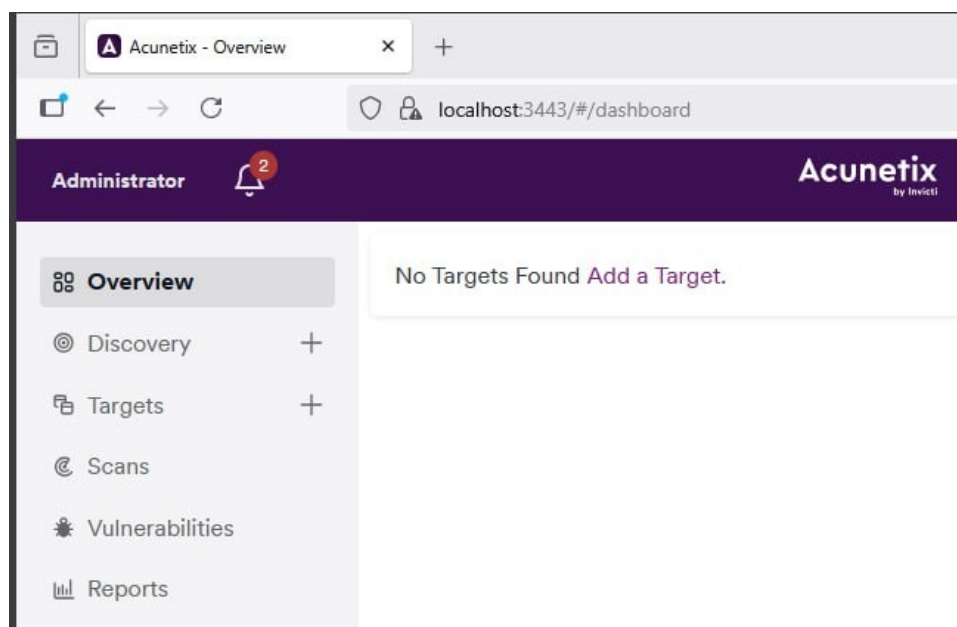


Рисунок 13 — Главная страница Acunetix

После этого была открыта страница «Add Targets», на которой в поле

«Address» был введен IP-адрес виртуальной машины с Ubuntu, а также порт, на котором запущено приложение Juice Shop. Это видно на рисунке 14.

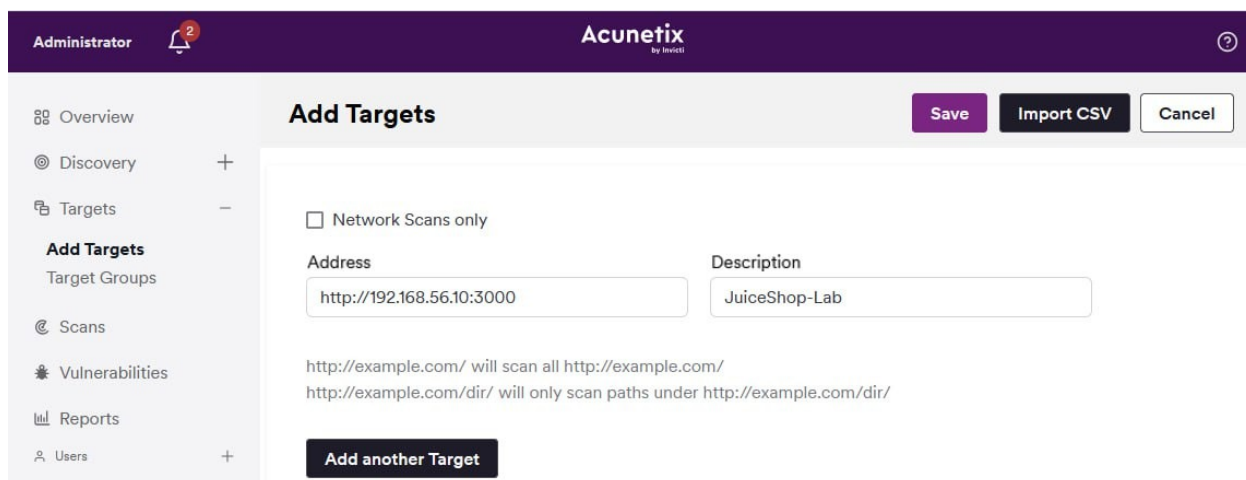


Рисунок 14 — Создание цели в Acunetix

После этого для ранее созданной цели было запущено сканирование, что видно на рисунке 15. Через 18 минут сканирование было завершено, что видно на рисунке 16.

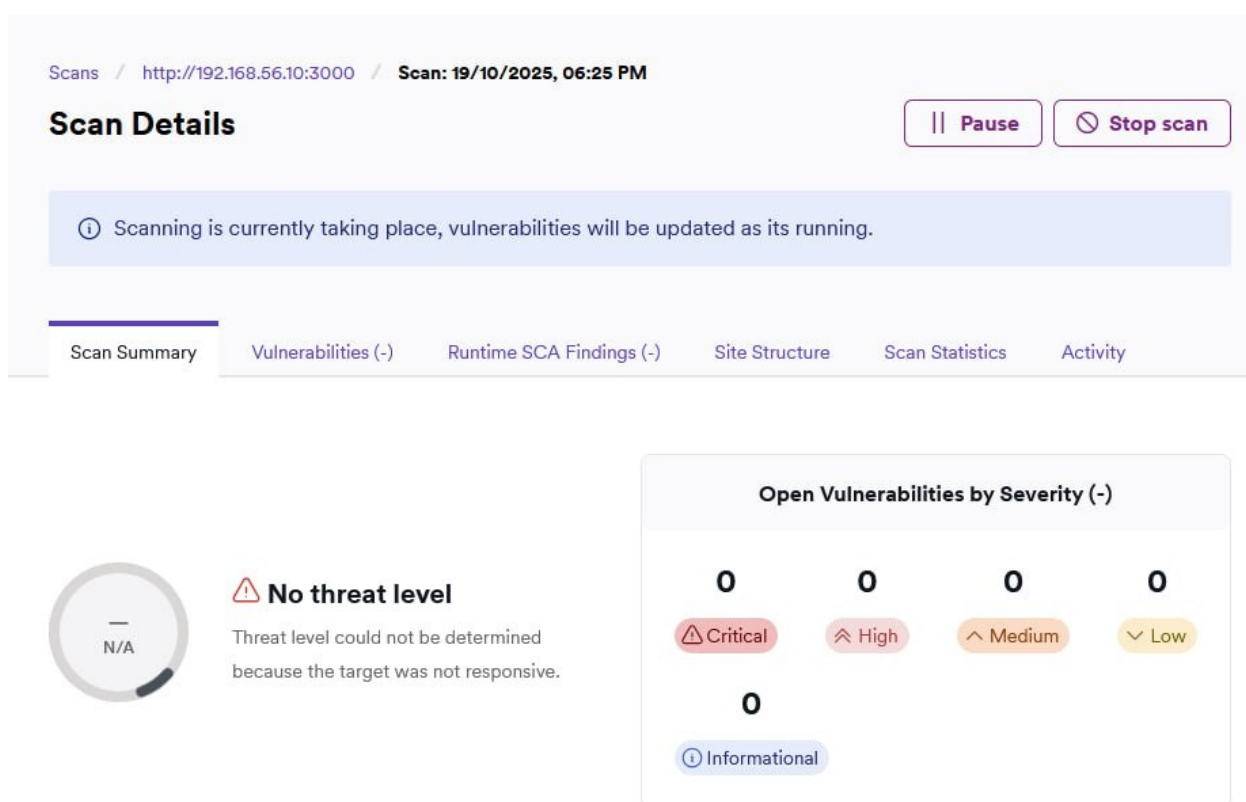


Рисунок 15 — Запущенное сканирование в Acunetix

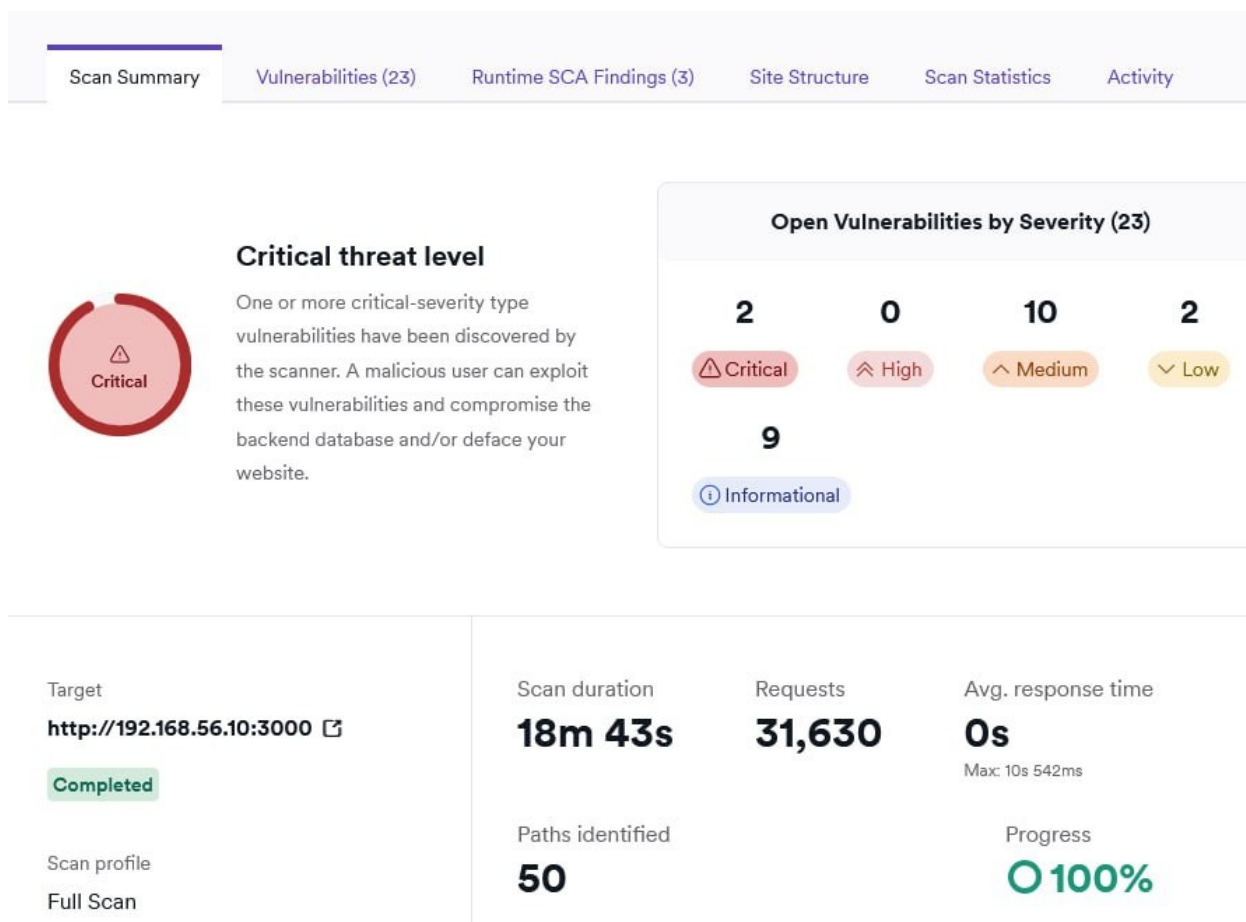


Рисунок 16 — Краткие результаты сканирования

Как видно на рисунке 16, Acunetix обнаружил 23 уязвимости, из них наиболее интересные:

- 1) возможность SQL инъекции на обработках `/rest/products/search` и `/rest/user/login`;
- 2) возможность работы с приложением по HTTP без шифрования (т. е. без HTTPS);
- 3) возможность реализации XSS атаки с помощью множественных уязвимостей в jQuery;
- 4) возможность перенаправить других пользователей на вредоносный сайт с помощью инъекции (т. е. уязвимость Open Redirect);
- 5) возможность получить доступ к конфиденциальным и чувствительным данным (например, API ключи и токены к GitLab и LinkedIn);

6) возможность раскрытия внутреннего устройства инфраструктуры (например, внутренние IP-адреса);

7) возможность несанкционированного доступа к сбору Prometheus метрик;

8) возможность раскрытия внутренних API-обработчиков (например, /rest/admin);

9) приложение не использует некоторые HTTP-заголовки, которые позволяют предотвратить различные уязвимости, связанные с передачей данных и вызовом обработчиков.

В итоге с помощью Acunetix в пару кликов удалось найти большое число уязвимостей приложения Juice Shop.

3 Вывод

В ходе выполнения данной лабораторной работы было проведено знакомство с часто встречающимися уязвимостями в web-приложениях и «худшими» практиками веб-разработки, а также получены навыки работы со сканерами web-уязвимостей.

Сравнивая nuclei и Acunetix между собой, можно прийти к выводу, что Acunetix обладает гораздо более богатыми возможностями по обнаружению уязвимостей в приложениях. Несмотря на большое количество готовых шаблонов, nuclei смог обнаружить очень малое количество уязвимостей. Для того, чтобы приблизить nuclei к результатам Acunetix, необходимо самостоятельно проанализировать приложение и реализовать шаблоны, которые будут проверять приложение на наличие соответствующих уязвимостей. В Acunetix же все это работает «из коробки».

Исходя из вышеописанного, можно сделать вывод, что nuclei является неплохим базовым инструментом для выявления основных уязвимостей, а Acunetix предпочтителен, если нужно проанализировать приложение от и до.