

# **Отчёт по аудиту информационной безопасности информационной системы «E-Commerce»**

## **Ответственный специалист:**

Резепин Николай Артемович, специалист по информационной безопасности.

## **I. План аудита:**

### **1. Объекты проверки:**

#### **Исходный код:**

- Frontend
- Backend

#### **Инфраструктура и конфигурация:**

- Docker-образы
- Репозиторий GitHub
- CI/CD-пайплайн (GitHub Actions)
- Развернутая система через Docker Compose

### **2. Используемые инструменты:**

#### **Автоматическое тестирование:**

- Dependabot
- GitHub Secret Scanning
- SonarQube
- Trivy

## Ручное тестирование:

- hping3
- nmap
- burpsuite
- zaproxy
- hydra
- metasploit-framework
- sqlmap
- nikto

## 3. Методы проверки:

### Автоматическое тестирование:

- Статический анализ – SonarQube
- Проверка зависимостей – Dependabot
- Проверка наличия чувствительных данных - GitHub Secret Scanning

### Инфраструктурная проверка:

- Анализ Docker-файлов и docker-compose.yml - Trivy

### Тестирование на уязвимости с использованием Kali Linux:

- **hping3** - проверка устойчивости системы к DoS атакам
- **burpsuite/zaproxy** - анализ запросов/ответов и поиск логических уязвимостей
- **nmap/metasploit-framework** - сканирование портов, выявление и эксплуатация возможных эксплойтов
- **hydra** - тестирование на устойчивость к brute-force атакам
- **sqlmap** – реализация SQL Injection
- **nikto** - сканирование веб-сервисов на наличие уязвимостей

#### **4. Нормативные документы и стандарты:**

- OWASP Top 10
- ASVS (Application Security Verification Standard)
- WSTG (Web Security Testing Guide)

#### **5. Оценка времени выполнения аудита:**

| Этап:                   | Время (час):    |
|-------------------------|-----------------|
| Подготовка окружения    | 4               |
| Анализ фронтенда        | 7               |
| Анализ бэкенда          | 9               |
| Проверка инфраструктуры | 5               |
| Тестирование приложения | 10              |
| Подготовка отчёта       | 5               |
| <b>Итого:</b>           | <b>40 часов</b> |

#### **6. План сдачи работ:**

Плановая дата начала проведения тестирования: **05.01.2025**

- Подготовка окружения: **05.01**
- Проведение проверки: **06.01-10.01**
- Подготовка отчета и составление рекомендации: **11.01-12.01**
- Передача отчета и рекомендаций заказчику - **13.01**








Плановая дата завершения проведения тестирования: **13.01.2025**

## II. Этап проведения аудита

### Автоматическое тестирование


#### 1. Dependabot - проверка зависимостей:


##### Backend:

|                          |   |          |         |            |
|--------------------------|---|----------|---------|------------|
| <input type="checkbox"/> |  6 Open ✓ 0 Closed   | Author ▾ | Label ▾ | Projects ▾ |
| <input type="checkbox"/> |  Bump jvm from 1.4.10 to 2.1.0 <span>dependencies</span> <span>java</span><br>#6 opened 4 minutes ago by dependabot <span>bot</span>   |          |         |            |
| <input type="checkbox"/> |  Bump com.google.firebase:firebase-admin from 7.0.1 to 9.4.2 <span>dependencies</span> <span>java</span><br>#5 opened 4 minutes ago by dependabot <span>bot</span>           |          |         |            |
| <input type="checkbox"/> |  Bump org.springframework.boot from 2.3.5.RELEASE to 3.4.1 <span>dependencies</span> <span>java</span><br>#4 opened 4 minutes ago by dependabot <span>bot</span>             |          |         |            |
| <input type="checkbox"/> |  Bump org.jetbrains.kotlin.plugin.jpa from 1.4.20-RC to 2.1.20-Beta1 <span>dependencies</span> <span>java</span><br>#3 opened 4 minutes ago by dependabot <span>bot</span> |          |         |            |
| <input type="checkbox"/> |  Bump openjdk from 11 to 18 <span>dependencies</span> <span>docker</span><br>#2 opened 4 minutes ago by dependabot <span>bot</span>  |          |         |            |
| <input type="checkbox"/> |  Bump io.spring.dependency-management from 1.0.10.RELEASE to 1.1.7 <span>dependencies</span> <span>java</span><br>#1 opened 5 minutes ago by dependabot <span>bot</span>   |          |         |            |


Видно, что часть зависимостей уже устарели, необходимо провести обновление компонентов, а также ввести автоматический поиск и установку актуальных версий зависимостей.

## Frontend:


☐  5 Open    ✓ 0 Closed

☐  **Bump react and react-dom** dependencies


#5 opened 1 minute ago by dependabot bot

☐  **Bump web-vitals from 1.1.1 to 4.2.4** dependencies


#4 opened 1 minute ago by dependabot bot

☐  **Bump @testing-library/user-event from 12.8.3 to 14.5.2** dependencies

#3 opened 1 minute ago by dependabot bot

☐  **Bump @testing-library/jest-dom from 5.11.9 to 6.6.3** dependencies

#2 opened 1 minute ago by dependabot bot

☐  **Bump axios from 0.21.1 to 1.7.9** dependencies

#1 opened 1 minute ago by dependabot bot

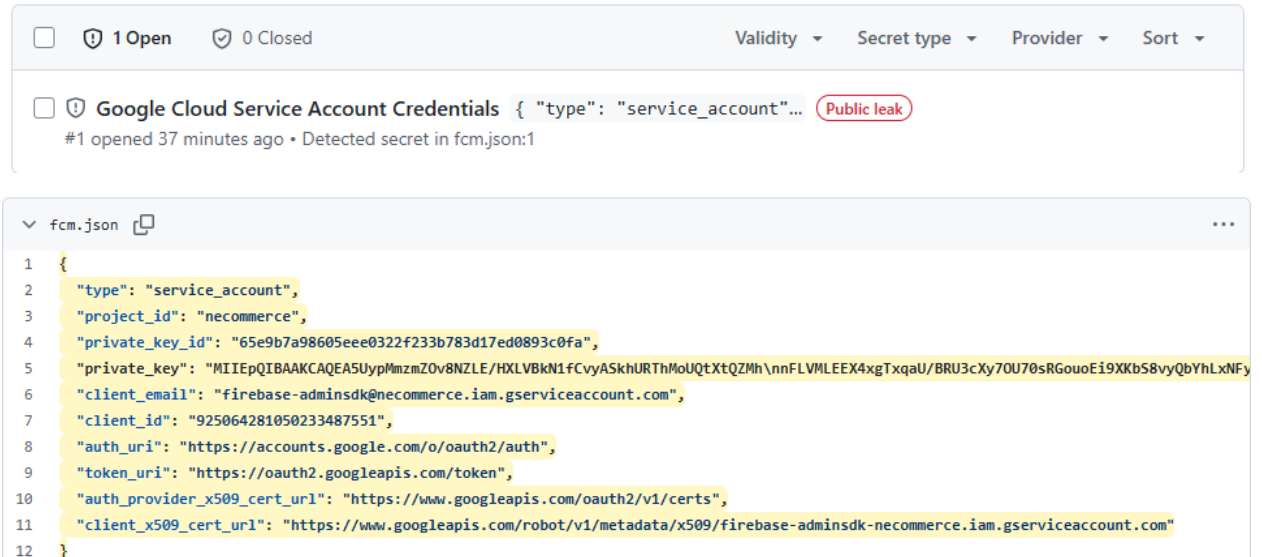
Такая же ситуация, как и с Backend, часть зависимостей устарели, необходимо провести обновление, а также ввести автоматический поиск и установку актуальных версий зависимостей.

| <input type="checkbox"/> ⓘ 102 Open  | ✓ 0 Closed   | Package ▾ | Ecosystem ▾ | Manifest ▾ | Severity ▾ | Sort ▾ |
|--|--|-----------|-------------|------------|------------|--------|
| <input type="checkbox"/> ⓘ   | <b>Prototype Pollution in immer</b> <span>Critical</span>  |           |             |            |            |        |
| #78 opened 4 minutes ago • Detected in immer (npm) • package-lock.json           |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>Babel vulnerable to arbitrary code execution when compiling specifically crafted malicious code</b> <span>Critical</span> |           |             |            |            |        |
| #66 opened 4 minutes ago • Detected in @babel/traverse (npm) • package-lock.json |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>Prototype Pollution in minimist</b> <span>Critical</span>   |           |             |            |            |        |
| #58 opened 4 minutes ago • Detected in minimist (npm) • package-lock.json        |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>Prototype pollution in webpack loader-utils</b> <span>Critical</span>   |           |             |            |            |        |
| #48 opened 4 minutes ago • Detected in loader-utils (npm) • package-lock.json    |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>Prototype pollution in webpack loader-utils</b> <span>Critical</span>   |           |             |            |            |        |
| #47 opened 4 minutes ago • Detected in loader-utils (npm) • package-lock.json    |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>Improper Neutralization of Special Elements used in a Command in Shell-quote</b> <span>Critical</span>                    |           |             |            |            |        |
| #43 opened 4 minutes ago • Detected in shell-quote (npm) • package-lock.json     |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>Exposure of Sensitive Information in eventsource</b> <span>Critical</span>  |           |             |            |            |        |
| #41 opened 4 minutes ago • Detected in eventsource (npm) • package-lock.json     |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>ejs template injection vulnerability</b> <span>Critical</span>  |           |             |            |            |        |
| #40 opened 4 minutes ago • Detected in ejss (npm) • package-lock.json            |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>Authorization Bypass Through User-Controlled Key in url-parse</b> <span>Critical</span>                                   |           |             |            |            |        |
| #30 opened 4 minutes ago • Detected in url-parse (npm) • package-lock.json       |  |           |             |            |            |        |
| <input type="checkbox"/> ⓘ   | <b>json-schema is vulnerable to Prototype Pollution</b> <span>Critical</span>  |           |             |            |            |        |
| #19 opened 4 minutes ago • Detected in json-schema (npm) • package-lock.json     |  |           |             |            |            |        |

На скриншоте отображен список обнаруженных уязвимостей в проекте, связанные с использованием зависимостей. Все уязвимости помечены как «**Critical**» и их огромное количество, а значит требуют срочного устранения.

## 2. GitHub Secret Scanning - проверка наличия чувствительных данных:

### Backend:

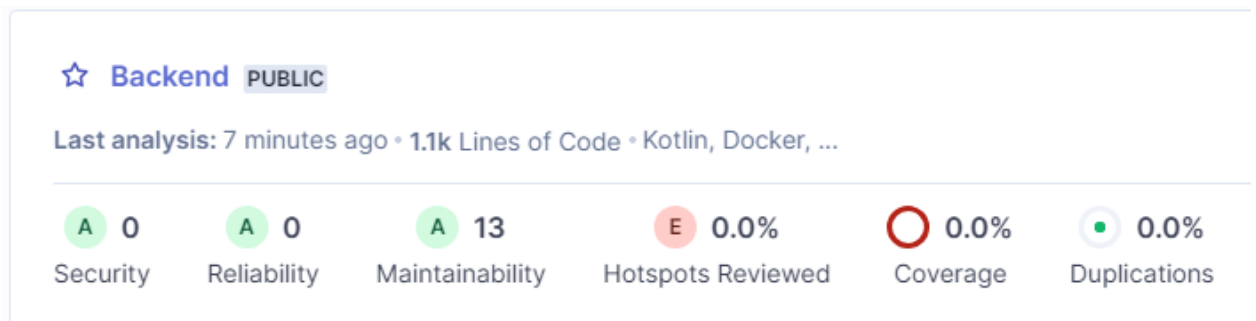


Обнаружены утечки конфиденциальных данных, а именно учетные данные сервисного аккаунта Google Cloud.

Секрет классифицирован как **публичная утечка**, что указывает на то, что файл, содержащий учетные данные, находится в общедоступном репозитории.

### 3. SonarCube:

#### Backend:



Исходя из результатов видно, что код Backend сервиса абсолютно не покрыт автоматическими тестами, хотя заявлено было обратное, исходя из этого автоматизированные проверки кода просто отсутствуют.

Также по самому коду есть нюансы, которые были выявлены SonarCube, они не являются критическими, но подлежат исправлению:

Review priority: Medium

Denial of Service (DoS) 2

The content length limit of 52428800 bytes is greater than the defined limit of 8388608; make sure it is safe here.

The content length limit of 52428800 bytes is greater than the defined limit of 8388608; make sure it is safe here.

Permission 2

The openjdk image runs with root as the default user. Make sure it is safe here.

Copying recursively might inadvertently add sensitive data to the container. Make sure it is safe here.

Weak Cryptography 1

Make sure that using this pseudorandom number generator is safe here.



## Frontend:



Ситуация аналогичная что и с Backend, код абсолютно не покрыт автоматическими тестами, хотя заявлено было обратное, исходя из этого автоматизированные проверки кода просто отсутствуют.

Также по самому коду есть нюансы, которые были выявлены SonarCube, они не являются критическими, но подлежат исправлению:

Review priority: ⬆ Medium

⬆ Permission 2 ▾

The nginx image runs with root as the default user. Make sure it is safe here.

Copying recursively might inadvertently add sensitive data to the container. Make sure it is safe here.

Review priority: ⬇ Low

⬇ Others 1 ▾

Omitting --ignore-scripts can lead to the execution of shell scripts. Make sure it is safe here.

# Инфраструктурная проверка:

## 4. Trivy:

### Backend:

```
a68f8d87c946 (debian 10.8)
Total: 794 (UNKNOWN: 14, LOW: 251, MEDIUM: 226, HIGH: 240, CRITICAL: 63)
```

| Library  | Vulnerability       | Severity | Status   | Installed Version | Fixed Version      | Title   |
|----------|---------------------|----------|----------|-------------------|--------------------|---|
| apt      | CVE-2011-3374       | LOW      | affected | 1.8.2.2           |                    | It was found that apt-key in apt, all versions, do not correctly ...<br><a href="https://avd.aquasec.com/nvd/cve-2011-3374">https://avd.aquasec.com/nvd/cve-2011-3374</a>   |
| bash     | CVE-2019-18276      |          |          | 5.0-4             |                    | bash: when effective UID is not equal to its real UID the ...<br><a href="https://avd.aquasec.com/nvd/cve-2019-18276">https://avd.aquasec.com/nvd/cve-2019-18276</a>  |
|          | TEMP-0841856-B18BAF |          |          |                   |                    | [Privilege escalation possible to other user than root]<br><a href="https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF">https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF</a>        |
| bsdutils | CVE-2024-28085      | HIGH     | fixed    | 1:2.33.1-0.1      | 2.33.1-0.1+deb10u1 | util-linux: CVE-2024-28085: wall: escape sequence injection<br><a href="https://avd.aquasec.com/nvd/cve-2024-28085">https://avd.aquasec.com/nvd/cve-2024-28085</a>  |
|          | CVE-2021-37600      | MEDIUM   |          |                   |                    | util-linux: integer overflow can lead to buffer overflow in get_sem_elements() in sys-utils/ipcutils.c ...<br><a href="https://avd.aquasec.com/nvd/cve-2021-37600">https://avd.aquasec.com/nvd/cve-2021-37600</a> |
|          | CVE-2022-0563       | LOW      | affected |                   |                    | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled ...<br><a href="https://avd.aquasec.com/nvd/cve-2022-0563">https://avd.aquasec.com/nvd/cve-2022-0563</a>                         |
| bzip2    | DLA-3112-1          | UNKNOWN  | fixed    | 1.0.6-9.2-deb10u1 | 1.0.6-9.2-deb10u2  | bzip2 - bugfix update   |

Контейнер Backend сервиса имеет огромное количество уязвимостей, в том числе и критических, они должны быть исправлены в срочном порядке, поскольку это несет огромные риски для компании.

### Frontend:

```
142c29187ec5 (debian 10.8)
Total: 620 (UNKNOWN: 9, LOW: 171, MEDIUM: 209, HIGH: 178, CRITICAL: 53)
```

| Library  | Vulnerability       | Severity | Status   | Installed Version | Fixed Version      | Title   |
|----------|---------------------|----------|----------|-------------------|--------------------|---|
| apt      | CVE-2011-3374       | LOW      | affected | 1.8.2.2           |                    | It was found that apt-key in apt, all versions, do not correctly ...<br><a href="https://avd.aquasec.com/nvd/cve-2011-3374">https://avd.aquasec.com/nvd/cve-2011-3374</a>   |
| bash     | CVE-2019-18276      |          |          | 5.0-4             |                    | bash: when effective UID is not equal to its real UID the ...<br><a href="https://avd.aquasec.com/nvd/cve-2019-18276">https://avd.aquasec.com/nvd/cve-2019-18276</a>  |
|          | TEMP-0841856-B18BAF |          |          |                   |                    | [Privilege escalation possible to other user than root]<br><a href="https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF">https://security-tracker.debian.org/tracker/TEMP-0841856-B1-8BAF</a>        |
| bsdutils | CVE-2024-28085      | HIGH     | fixed    | 1:2.33.1-0.1      | 2.33.1-0.1+deb10u1 | util-linux: CVE-2024-28085: wall: escape sequence injection<br><a href="https://avd.aquasec.com/nvd/cve-2024-28085">https://avd.aquasec.com/nvd/cve-2024-28085</a>  |
|          | CVE-2021-37600      | MEDIUM   |          |                   |                    | util-linux: integer overflow can lead to buffer overflow in get_sem_elements() in sys-utils/ipcutils.c ...<br><a href="https://avd.aquasec.com/nvd/cve-2021-37600">https://avd.aquasec.com/nvd/cve-2021-37600</a> |
|          | CVE-2022-0563       | LOW      | affected |                   |                    | util-linux: partial disclosure of arbitrary files in chfn and chsh when compiled ...<br><a href="https://avd.aquasec.com/nvd/cve-2022-0563">https://avd.aquasec.com/nvd/cve-2022-0563</a>                         |

Ситуация аналогичная с Backend, огромное количество критических и не только уязвимостей, которые должны быть исправлены в срочном порядке, пока они не привели к компрометации системы.

## Ручное тестирование (пентест):

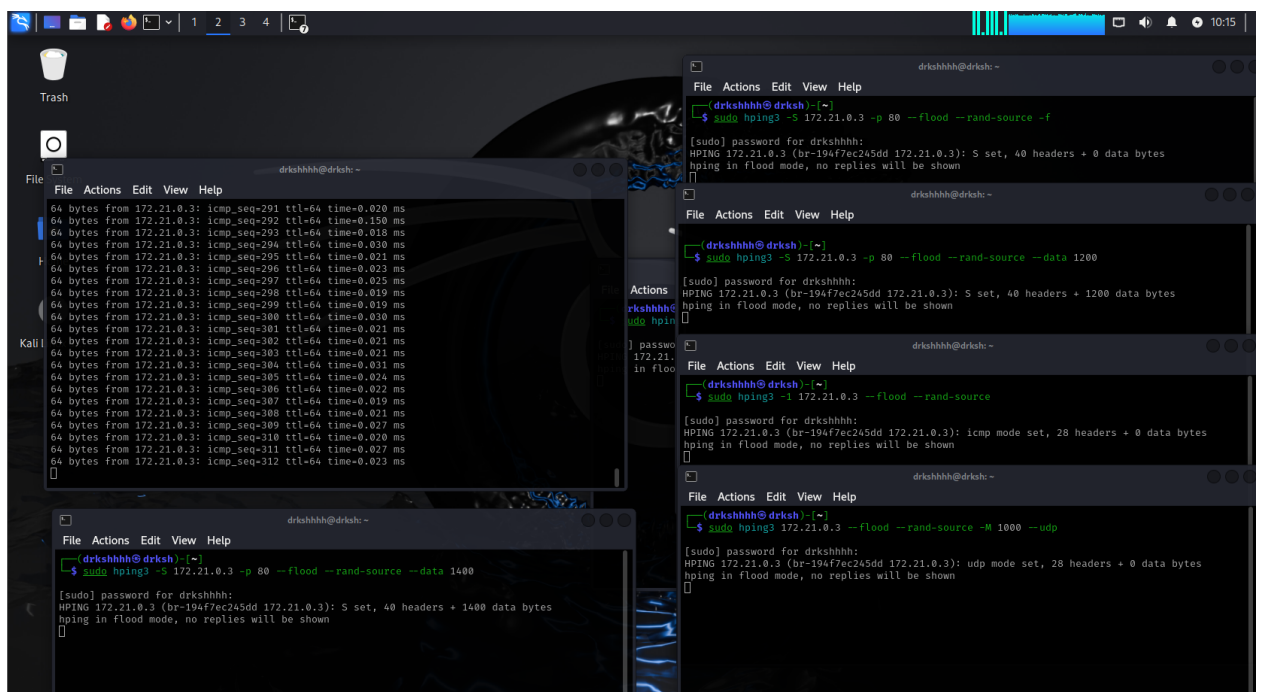
Тестирование буду проводить, опираясь на актуальный список уязвимостей **OWASP Top 10** и другие широко распространённые уязвимости:

### 1. Отказ в обслуживании (nmap/hping3):

**Nmap** – сканирование открытых портов

```
└─$ nmap -A 172.21.0.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-09 10:04 CST
Nmap scan report for 172.21.0.3
Host is up (0.000039s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.19.8
```

**Hping3** – DoS атака



**Результат:** была проведена комплексная DoS атака на целевой сервис, тестирование не выявило проблем, связанных с отказом в обслуживании, сервис работает стабильно.

## 2. Brute-force атака (HYDRA/ZAP):

## Hydra:

```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-09 11:40:07
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100011 login tries (l1/p:100011), ~6251 tries per task
[DATA] attacking http-post-form://172.21.0.3:80/auth:login=^USER^&pass=^PASS^:F=Произошла ошибка. Попробуйте повторить свой запрос позже
[80][http-post-form] host: 172.21.0.3 login: admin password: qwerty
[80][http-post-form] host: 172.21.0.3 login: admin password: 111111
[80][http-post-form] host: 172.21.0.3 login: admin password: 123456
[80][http-post-form] host: 172.21.0.3 login: admin password: 123456789
[80][http-post-form] host: 172.21.0.3 login: admin password: password
[80][http-post-form] host: 172.21.0.3 login: admin password: 12345678
[80][http-post-form] host: 172.21.0.3 login: admin password: abc123
[80][http-post-form] host: 172.21.0.3 login: admin password: 1234567
[80][http-post-form] host: 172.21.0.3 login: admin password: password1
[80][http-post-form] host: 172.21.0.3 login: admin password: 12345
[80][http-post-form] host: 172.21.0.3 login: admin password: 1234567890
[80][http-post-form] host: 172.21.0.3 login: admin password: 123123
[80][http-post-form] host: 172.21.0.3 login: admin password: 000000
[80][http-post-form] host: 172.21.0.3 login: admin password: iloveyou
[80][http-post-form] host: 172.21.0.3 login: admin password: 1234
[80][http-post-form] host: 172.21.0.3 login: admin password: 1q2w3e4r5t
1 of 1 target successfully completed, 16 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-01-09 11:40:08
```

**Zap:**

The screenshot shows the 'New Fuzzer' application window. At the top, the progress bar is at 100%. Below the progress bar, the 'Messages Sent' count is 99979, and the 'Errors' count is 0. The 'Current fuzzers: 0' is also displayed. The main table lists the results of the fuzzing process, including Task ID, Message Type, Code, Reason, RTT, Size Resp. Header, Size Resp. Body, Highest Alert, State, and Payloads. The table shows 10 rows of data, with the first row having a Task ID of 226 and a State of 'Reflected'. The bottom status bar shows 'Alerts: 0' and 'Current Scans: 0'.

| Task ID | Message Type | Code | Reason | RTT    | Size Resp. Header | Size Resp. Body | Highest Alert | State     | Payloads |
|---------|--------------|------|--------|--------|-------------------|-----------------|---------------|-----------|----------|
| 226     | Fuzzed       | 400  |        | 96 ms  | 515 bytes         | 128 bytes       |               | Reflected | user     |
| 16,403  | Fuzzed       | 400  |        | 136 ms | 515 bytes         | 128 bytes       |               | Reflected | u        |
| 8,536   | Fuzzed       | 400  |        | 198 ms | 515 bytes         | 128 bytes       |               | Reflected | time     |
| 11,404  | Fuzzed       | 400  |        | 147 ms | 515 bytes         | 128 bytes       |               | Reflected | tim      |
| 2,307   | Fuzzed       | 400  |        | 133 ms | 515 bytes         | 128 bytes       |               | Reflected | the      |
| 95,895  | Fuzzed       | 400  |        | 112 ms | 515 bytes         | 128 bytes       |               | Reflected | th       |
| 46,087  | Fuzzed       | 400  |        | 272 ms | 515 bytes         | 128 bytes       |               | Reflected | tat      |
| 52,835  | Fuzzed       | 400  |        | 72 ms  | 515 bytes         | 128 bytes       |               | Reflected | tam      |
| 20,271  | Fuzzed       | 400  |        | 117 ms | 515 bytes         | 128 bytes       |               | Reflected | T        |
| 3,716   | Fuzzed       | 400  |        | 186 ms | 515 bytes         | 128 bytes       |               | Reflected | t        |

**Результат:** ни одна из программ не смогла реализовать Brute атаку, сервис защищен от ручного перебора.

### 3. SQL Injection (sqlmap):

Auth (авторизация) – POST запрос:

```
[07:43:08] [INFO] testing MySQL UNION query (random number) - 41 to 50 columns
[07:43:08] [WARNING] parameter 'Host' does not seem to be injectable
[07:43:08] [CRITICAL] all tested parameters do not appear to be injectable
[07:43:08] [WARNING] HTTP error codes detected during run:
405 (Method Not Allowed) - 78478 times
[*] ending @ 07:43:08 /2025-01-09/
```

Reg (регистрация) – POST запрос:

```
[07:58:38] [WARNING] parameter 'Host' does not seem to be injectable
[07:58:38] [CRITICAL] all tested parameters do not appear to be injectable. If you suspect th
at there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use
option '--tamper' (e.g. '--tamper=space2comment')
[07:58:38] [WARNING] HTTP error codes detected during run:
405 (Method Not Allowed) - 94112 times
```

**Результат:** ни один из методов SQLI не сработал, сервис защищен от атаки методом инъекций.

## 4. Exploit проникновение (Metasploit/nmap):

### Nmap:

```
└─$ nmap -A 172.21.0.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-09 10:04 CST
Nmap scan report for 172.21.0.3
Host is up (0.000039s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    nginx 1.19.8
```

### Metasploit:

Show 15 ▾ Search: nginx 1.19.8

| Date                      | D | A | V | Title | Type | Platform | Author |
|---------------------------|---|---|---|-------|------|----------|--------|
| No matching records found |   |   |   |       |      |          |        |

Showing 0 to 0 of 0 entries (filtered from 46,102 total entries) FIRST PREVIOUS NEXT LAST


```
msf6 > search nginx 1.19.8
[-] No results from search
msf6 > █
```

**Результат:** на единственном открытом порту работает сервис nginx версии 1.19.8, который не имеет известных уязвимостей и эксплойтов, является безопасным для реализации.

## 5. Security Misconfiguration (ZAP):

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 80217
Access-Control-Allow-Origin: *
Access-Control-Expose-Headers: *
Timing-Allow-Origin: *
Cache-Control: public, max-age=31536000, s-maxage=31536000, immutable
Cross-Origin-Resource-Policy: cross-origin
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
```

### Cross-Domain Misconfiguration

URL: <https://cdn.jsdelivr.net/npm/bootstrap@5.0.0-beta2/dist/js/bootstrap.bundle.min.js>  
Risk:  Medium  
Confidence: Medium  
Parameter:  
Attack:  
Evidence: Access-Control-Allow-Origin: \*  
CWE ID: 264  
WASC ID: 14  
Source: Passive (10098 - Cross-Domain Misconfiguration)  
Input Vector:

**Результат:** Неправильная конфигурация заголовка Access-Control-Allow-Origin может привести к различным проблемам в веб-приложениях, особенно при попытках выполнения запросов между разными доменами.



## 6. XSS (ZAP):

### ZAP:

| Alert type   | Risk          | Count        |
|--|---------------|--------------|
| <a href="#">Cloud Metadata Potentially Exposed</a>                                       | High          | 1<br>(12.5%) |
| <a href="#">Content Security Policy (CSP) Header Not Set</a>                             | Medium        | 1<br>(12.5%) |
| <a href="#">Missing Anti-clickjacking Header</a>   | Medium        | 1<br>(12.5%) |
| <a href="#">Server Leaks Version Information via "Server" HTTP Response Header Field</a> | Low           | 5<br>(62.5%) |
| <a href="#">Timestamp Disclosure - Unix</a>  | Low           | 1<br>(12.5%) |
| <a href="#">X-Content-Type-Options Header Missing</a>                                    | Low           | 4<br>(50.0%) |
| <a href="#">Information Disclosure - Suspicious Comments</a>                             | Informational | 1<br>(12.5%) |
| <a href="#">Modern Web Application</a>   | Informational | 1<br>(12.5%) |
| Total  |               | 8            |

**Результат:** ZAP не выявил возможные XSS уязвимости, но в процессе проверки были найдены другие, их также необходимо исправить.

## **7. Сканирование веб-сервисов (Nikto):**

### **Основные выводы:**

#### **I. Отсутствие ключевых заголовков безопасности:**

- X-Frame-Options: Отсутствие этого заголовка позволяет уязвимость к атаке типа clickjacking.
- X-Content-Type-Options: Отсутствие заголовка может привести к неправильной интерпретации контента.

#### **II. Обнаружение чувствительных файлов:**

- Множество потенциально конфиденциальных файлов, включая архивы, сертификаты, резервные копии и файлы базы данных
- Такие файлы могут содержать чувствительную информацию, что представляет серьезный риск для безопасности.

#### **III. Уязвимости:**

- Nortel Contivity VxWorks
- HTTPd

#### **IV. Необычные заголовки и пути:**

- Заголовок Content-Disposition в /api/jsonws/index.jsp может указывать на доступ к редким или потенциально полезным файлам

**Результат:** Nikto нашел уязвимости в веб-сервисах, они не являются критическими, но должны быть исправлены.

## 8. CSRF-токен (Burp Suite):

### Request

Pretty   Raw   Hex

```
2 Host: localhost:8888
3 Content-Length: 27
4 sec-ch-ua-platform: "Linux"
5 Accept-Language: en-US,en;q=0.9
6 Accept: application/json, text/plain, */*
7 sec-ch-ua: "Chromium";v="131", "Not_A Brand";v="24"
8 Content-Type: application/x-www-form-urlencoded;charset=UTF-8
9 sec-ch-ua-mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.86 Safari/537.36
11 Origin: http://localhost:8888
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:8888/auth
16 Accept-Encoding: gzip, deflate, br
17 Connection: keep-alive
18
19 login=student&pass=study123
```

**Результат:** отсутствуют CSRF-токены, что потенциально может привести к атаке.

### **III. Рекомендации для улучшения процессов, кода и общей безопасности приложения**

#### **1. Контроль зависимостей:**

- Устаревшие зависимости требуют обновления. Настройте Dependabot для автоматического создания pull-запросов с обновлениями.
- Внедрить политику регулярного аудита зависимостей и тестирования после обновлений.

#### **2. Чувствительные данные и секреты:**

- Убедиться, что все секреты хранятся в защищённых хранилищах (например, GitHub Secrets).
- Регулярно использовать инструменты типа GitHub Secret Scanning для мониторинга репозитория на утечки.

#### **3. Покрытие тестами:**

- Увеличьте покрытие автоматическими тестами.
- Настройте регулярные проверки тестов в пайплайне CI/CD.

#### **4. Уязвимости инфраструктуры (Docker):**

- Проверьте и исправьте найденные Trivy критические уязвимости в контейнерах.
- Настройте автоматическую проверку Docker-образов перед их публикацией с использованием Trivy.

## **5. Безопасность конфигурации:**

- Улучшить конфигурации заголовков безопасности (Frame-Options, X-Content-Type-Options).
- Внедрить CSRF-токены для защиты от атак.

## **6. CI/CD процессы:**

- Расширить проверки в GitHub Actions.
- Ограничить привилегии токенов до минимально необходимых.

## **7. Мониторинг:**

Внедрить систему мониторинга, способную отслеживать изменения в коде, инфраструктуре и приложении в реальном времени.

## **8. Документация и обучение:**

- Организуйте обучение для разработчиков, акцентируя внимание на безопасной разработке.
- Обновите документацию по процессам безопасности для сотрудников компании.