

Отчет содержит результаты проведенных работ по проверке наличия уязвимостей тестируемых приложений. В отчете содержится описание выявленных недостатков и связанных с ними уровней критичности, а также детальные описания и рекомендации по устранению уязвимостей.

ЦЕЛИ И ЗАДАЧИ

Целью работы является получение независимой оценки текущего уровня защищенности периметра исследуемой сети. В ходе выполнения тестирования на проникновение были поставлены следующие задачи:

- сбор информации о сервисе
- поиск недостатков и уязвимостей в сервисе;
- определение степени критичности полученных результатов и последствий в случае успешной эксплуатации;
- разработка рекомендаций с целью повышения уровня защищенности сервиса.

ШАГИ, ПРЕДПРИНЯТЫЕ ПРИ ПРОВЕДЕНИИ ТЕСТИРОВАНИЯ

- идентификация запущенных сетевых служб, включающая определение открытых сетевых портов
- сканирование на наличие недостатков и уязвимостей при помощи ручного анализа и автоматизированных средств;
- поиск информации об уязвимостях по идентифицированным версиям в открытых источниках;
- анализ веб-приложений на наличие уязвимостей

ПЕРЕЧЕНЬ ИССЛЕДУЕМЫХ РЕСУРСОВ

АРЕНДОВАННЫЕ IP-АДРЕСА

- 92.51.39.106/8060
- 92.51.39.106/7799

ОПИСАНИЕ ИСПОЛЬЗУЕМОЙ МЕТОДИКИ

Для выполнения поставленных задач Исполнителем было проведено тестирование на проникновение методом «черного ящика» (black-box). Данный метод предполагает моделирование действий потенциального внешнего нарушителя, который не обладает привилегиями в системе и имеет минимальный уровень знаний об исследуемой системе.

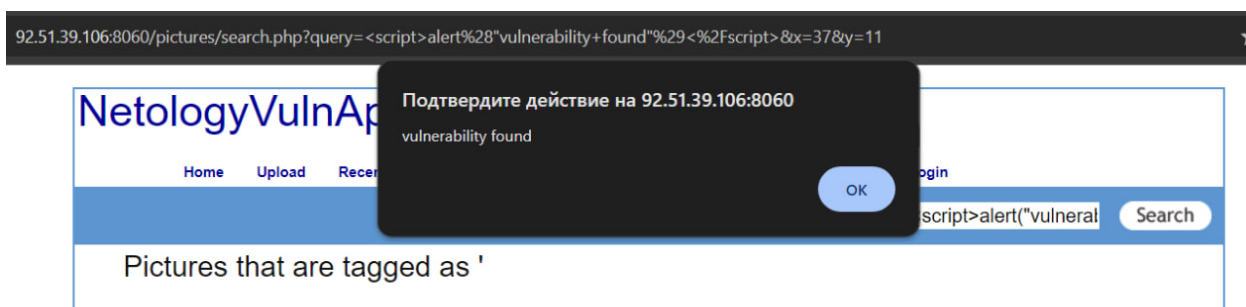
ПОДРОБНОЕ ОПИСАНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

АНАЛИЗ ЗАЩИЩЕННОСТИ УЗЛА 92.51.39.106/8060

В ходе анализа защищенности была выявлена критическая уязвимость XSS (CVE-2023-24322), при эксплуатации которой злоумышленник может получить доступ к чувствительным данным, например, платежным картам, паспортным данным, гаджетам пользователей.

Критичность: высокая

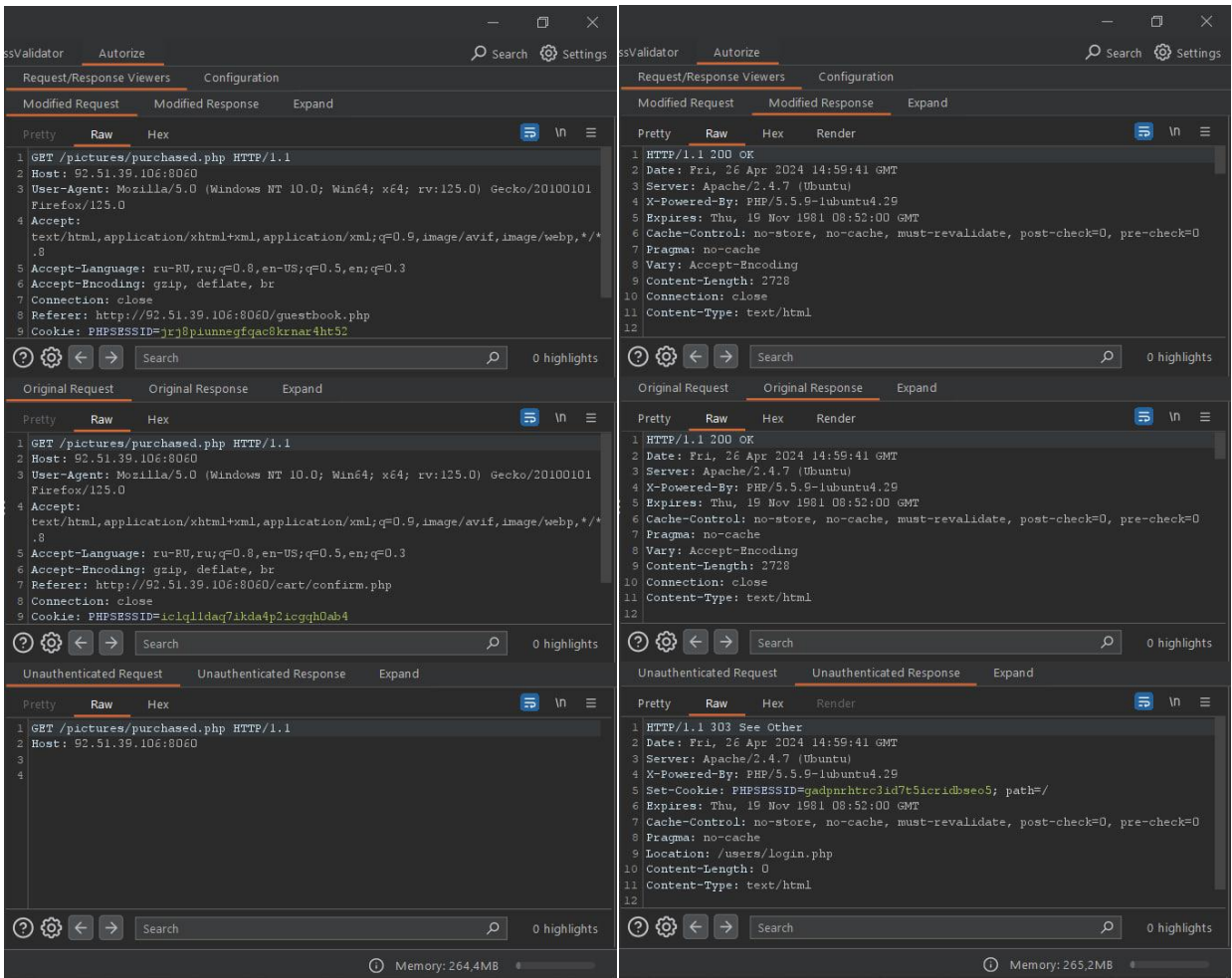
Рекомендации по устранению: Валидация входных данных, экранирование выходных данных и реструктуризация приложения таким образом, чтобы код загружался из строго определенных конечных точек.



В ходе анализа защищенности была выявлена критическая уязвимость IDOR (CVE-2024-32166), эксплуатация которой позволяет получить несанкционированный доступ к веб-страницам, файлам, или конфиденциальным данным.

Критичность: высокая

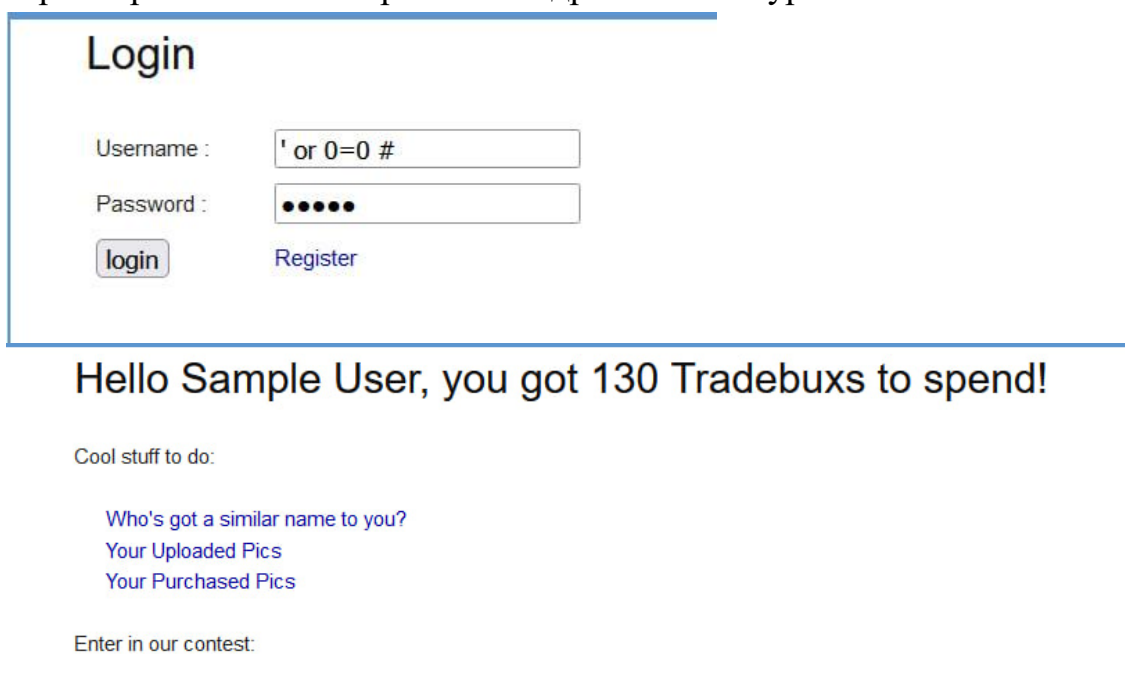
Рекомендации по устранению: реализовать корректную проверку контроля доступа к ресурсам веб-приложения. Реализовать механизм контроля доступа к ресурсам и разграничивать доступ к ним в соответствии с правами пользователя. Использовать косвенные ссылки на объекты;



В ходе анализа защищенности была выявлена критическая уязвимость SQLi (CVE-2023-50071) Успешная реализация данной атаки позволяет обойти систему безопасности приложения и получить доступ к конфиденциальной информации, которая содержится в БД, а также к функциональным возможностям СУБД и в некоторых случаях – доступ к операционной системе сервера, на котором функционирует СУБД.

Критичность: высокая

Рекомендации по устранению: Подход с нулевым доверием. Ограничить привилегии. Использование хранимых процедур. Использование параметризованных запросов. Внедрение многоуровневой безопасности



Login

Username :

Password :

[Register](#)

Hello Sample User, you got 130 Tradebuxs to spend!

Cool stuff to do:

- [Who's got a similar name to you?](#)
- [Your Uploaded Pics](#)
- [Your Purchased Pics](#)

Enter in our contest:

В ходе анализа защищенности была выявлена критическая уязвимость Broken Access Control (CVE-2024-22234), при эксплуатации которой злоумышленник может получить несанкционированный доступ к ресурсам или выполнить действия, к которым он не должен иметь возможности

Критичность: высокая

Рекомендации по устранению: Внедрить надлежащие средства контроля доступа, обеспечить разделение обязанностей, использовать принцип наименьших привилегий, реализовать шифрование, использовать безопасные методы кодирования

| ← → ↻ 92.51.39.106:8060/upload/ | | | |
|---|-------------------------------|----------------------|-----------------------------|
| <div> </div> | | | |
| Index of /upload | | | |
| Name | Last modified | Size | Description |
| <hr/> | | | |
| Parent Directory | | - | |
| 3/ | 2021-07-25 18:07 | - | |
| <script>alert('test');</script> | 2024-05-10 06:49 | - | |
| againlxwsed | 2021-07-25 17:57 | 47K | |
| againJ42nH | 2021-07-25 17:57 | 47K | |
| doggie/ | 2021-07-25 18:07 | - | |
| flowers/ | 2021-07-25 18:07 | - | |
| foos/ | 2021-07-25 18:07 | - | |
| house/ | 2021-07-25 18:07 | - | |
| quarters/ | 2021-07-25 18:07 | - | |
| testing/ | 2021-07-25 18:07 | - | |
| toga/ | 2021-07-25 18:07 | - | |
| twister/ | 2021-07-25 18:07 | - | |
| twister_funeXz3uM | 2021-07-25 17:57 | 47K | |
| twister_funxJObBz | 2021-07-25 17:57 | 47K | |
| waterfall/ | 2021-07-25 18:07 | - | |
| <hr/> | | | |
| Apache/2.4.7 (Ubuntu) Server at 92.51.39.106 Port 8060 | | | |

В ходе анализа защищенности была выявлена критическая уязвимость Information disclosure (CVE-2023-27317), при эксплуатации которой злоумышленник может определить используемые дистрибутивы ПО, номера версий клиента и сервера и установленные обновления. В других случаях, в утекающей информации может содержаться расположение временных файлов или резервных копий.

Критичность: высокая

Рекомендации по устранению: Проводить аудит любого кода на предмет возможного раскрытия информации в рамках процессов контроля качества или сборки. Как можно чаще используйте общие сообщения об ошибках. Проверить, отключены ли какие-либо функции отладки или диагностики в рабочей среде.

```
Warning: mysql_connect(): Can't connect to local MySQL server through socket '/var/run/mysqld/mysqld.sock' (2) in /app/include/database.php on line 8

Warning: mysql_select_db() expects parameter 2 to be resource, boolean given in /app/include/database.php on line 9

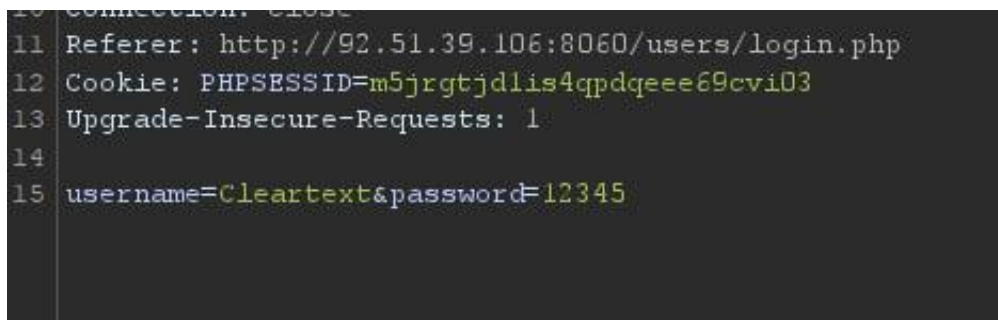
Warning: mysql_set_charset(): Can't connect to local MySQL server through socket '/var/run/mysqld/mysqld.sock' (2) in /app/include/database.php on line 10

Warning: mysql_set_charset(): A link to the server could not be established in /app/include/database.php on line 10
```

В ходе анализа защищенности была выявлена критическая уязвимость Cleartext submission of password (CVE-2013-2672), при эксплуатации которой злоумышленник может перехватить пароль по незашифрованному соединению

Критичность: высокая

Рекомендации по устранению: Использовать шифрование на транспортном уровне (SSL или TLS) для защиты всех конфиденциальных сообщений, проходящих между клиентом и сервером. Использовать собственный механизм обработки сеансов, а используемые токены сеансов никогда не должны передаваться по незашифрованным каналам связи.



```
11 Referer: http://92.51.39.106:8060/users/login.php
12 Cookie: PHPSESSID=m5jrgtjdlis4qpdqeee69cvi03
13 Upgrade-Insecure-Requests: 1
14
15 username=Cleartext&password=12345
```

В ходе анализа защищенности была выявлена уязвимость Cross-site request forgery (CVE-2024-23319), при эксплуатации которой злоумышленник может обманом заставить невинного конечного пользователя отправить веб-запрос, который он не собирался делать. Это может привести к выполнению на веб-сайте действий, которые могут включать непреднамеренную утечку данных клиента или сервера, изменение состояния сеанса или манипулирование учетной записью конечного пользователя.

Критичность: средняя

Рекомендации по устранению: Проверка подлинности на основе токенов. Ограничение чувствительные действия, которые может выполнять пользователь без подтверждения паролем или другими способами аутентификации.

92.51.39.106

Яндекс

Яндекс Маркет

VirusTotal

NetologyVulnApp

HomeUploadRecent

Register for an account

Protect yourself from hackers and check your account regularly

All fields are required

Username :
First Name :
Last Name :
Password :
Password again :

qwerty
rom
tom
•••••
•••••

Create Account!

CSRF PoC generator

Request to: http://92.51.39.106:8060

Options?

Inspector

Request attributes: 2
Request query parameters: 0
Request body parameters: 5
Request cookies: 1

CSRF HTML:

```
1 <html>
2 <!-- CSRF PoC - generated by Burp Suite Professional -->
3 <body>
4 <form action="http://92.51.39.106:8060/users/register.php" method="POST">
5 <input type="hidden" name="username" value="qwerty" />
6 <input type="hidden" name="firstname" value="rom" />
7 <input type="hidden" name="lastname" value="tom" />
8 <input type="hidden" name="password" value="12345" />
9 <input type="hidden" name="againpass" value="12345" />
10 <input type="submit" value="Submit request" />
11 </form>
12 <script>
13 history.pushState('', '', '/');
14 document.forms[0].submit();
15 </script>
16 </body>
17 </html>
18
```

Regenerate Test in browser Copy HTML Close

92.51.39.106:8060/users/register.php

Яндекс

Яндекс Маркет

VirusTotal - HTML

NetologyVulnApp

HomeUploadRecentGallery

Hello qwertwwwy, you

Cool stuff to do:

Who's got a similar name to you?

Your Uploaded Pics

Your Purchased Pics

Enter in our contest:

CSRF PoC generator

Request to: http://92.51.39.106:8060

Options?

Inspector

Request attributes: 2
Request query parameters: 0
Request body parameters: 5
Request cookies: 1

CSRF HTML:

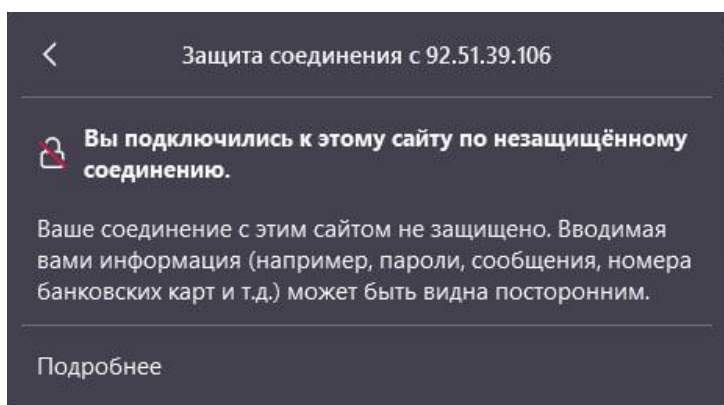
```
1 <html>
2 <!-- CSRF PoC - generated by Burp Suite Professional -->
3 <body>
4 <form action="http://92.51.39.106:8060/users/register.php" method="POST">
5 <input type="hidden" name="username" value="qwertwwwy" />
6 <input type="hidden" name="firstname" value="rom" />
7 <input type="hidden" name="lastname" value="tom" />
8 <input type="hidden" name="password" value="12345" />
9 <input type="hidden" name="againpass" value="12345" />
10 <input type="submit" value="Submit request" />
11 </form>
12 <script>
13 history.pushState('', '', '/');
14 document.forms[0].submit();
15 </script>
16 </body>
17 </html>
18
```

Regenerate Test in browser Copy HTML Close

В ходе анализа защищенности была выявлена уязвимость Unencrypted communications (CVE-2023-40729), при эксплуатации которой злоумышленник, имеющий возможность просматривать сетевой трафик законного пользователя, может записывать и отслеживать его взаимодействие с приложением, а также получать любую информацию, которую предоставляет пользователь.

Критичность: низкая

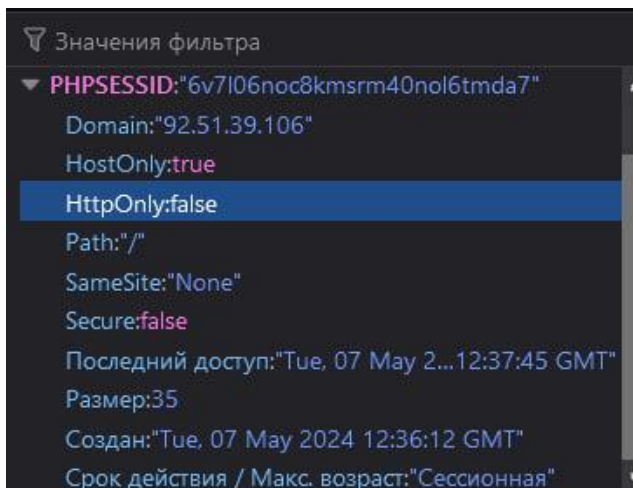
Рекомендации по устранению: Приложения должны использовать шифрование транспортного уровня (SSL/TLS) для защиты всех сообщений, проходящих между клиентом и сервером. HTTP-заголовок Strict-Transport-Security следует использовать, чтобы гарантировать, что клиенты откажутся от доступа к серверу через небезопасное соединение.



В ходе анализа защищенности была выявлена уязвимость Cookie without HttpOnly flag set (CVE-2021-27764), что означает, что доступ к файлу cookie возможен с помощью JavaScript. Если на этой странице можно запустить вредоносный скрипт, файл cookie будет доступен и может быть передан на другой сайт. Если это файл cookie сеанса, то возможен перехват сеанса.

Критичность: низкая

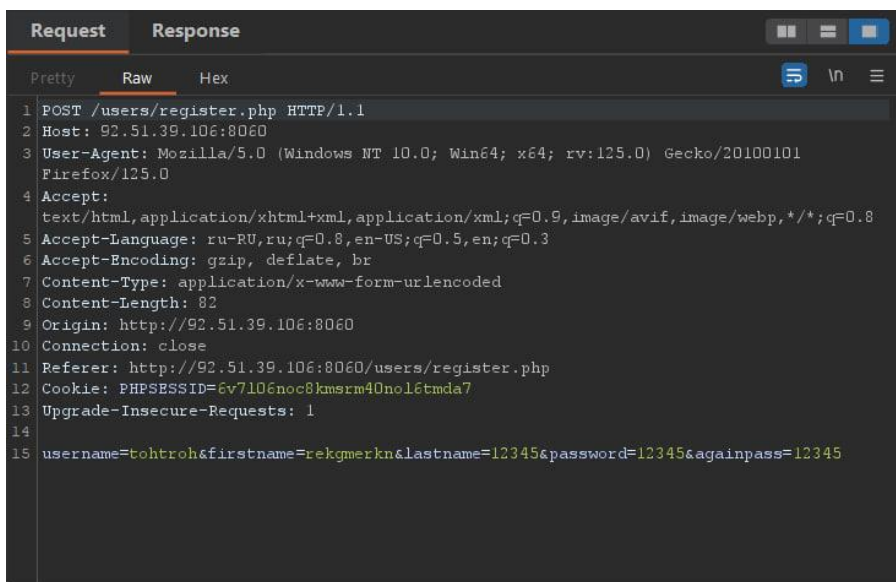
Рекомендации по устранению: Убедиться, что для всех файлов cookie установлен флаг HttpOnly, включив этот атрибут в соответствующую директиву Set-cookie.



В ходе анализа защищенности была выявлена уязвимость From action hijacking (reflected) (CWE-73, CWE-20), злоумышленник может использовать эту уязвимость для создания URL-адреса, который, если его посетит другой пользователь приложения, изменит URL-адрес действия формы, указав на сервер злоумышленника.

Критичность: низкая

Рекомендации по устранению: Рассмотреть возможность жесткого кодирования URL-адреса действия формы или внедрения белого списка разрешенных значений.

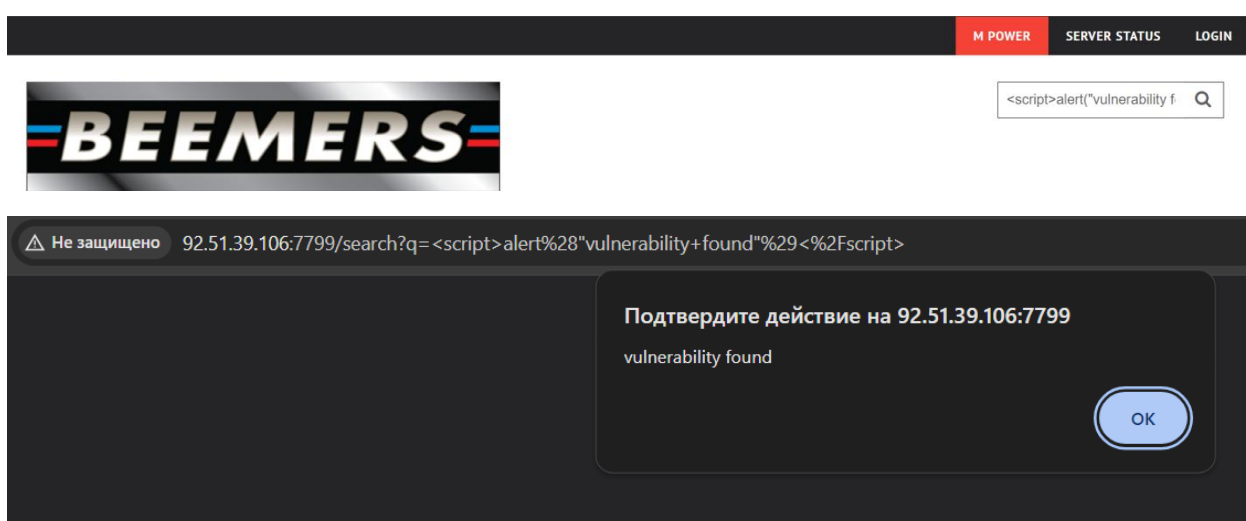


АНАЛИЗ ЗАЩИЩЕННОСТИ УЗЛА 92.51.39.106/7799

В ходе анализа защищенности была выявлена критическая уязвимость XSS (CVE-2023-24322), при эксплуатации которой злоумышленник может получить доступ к чувствительным данным, например, платежным картам, паспортным данным, гаджетам пользователей.

Критичность: высокая

Рекомендации по устранению: Валидация входных данных, экранирование выходных данных и реструктуризация приложения таким образом, чтобы код загружался из строго определенных конечных точек.



В ходе анализа защищенности была выявлена критическая уязвимость SQLi (CVE-2023-50071) Успешная реализация данной атаки позволяет обойти систему безопасности приложения и получить доступ к конфиденциальной информации, которая содержится в БД, а также к функциональным возможностям СУБД и в некоторых случаях – доступ к операционной системе сервера, на котором функционирует СУБД.

Критичность: высокая

Рекомендации по устранению: Подход с нулевым доверием. Ограничить привилегии. Использование хранимых процедур. Использование параметризованных запросов. Внедрение многоуровневой безопасности

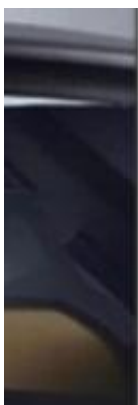
Login

Login Success, Hello admin

В ходе анализа защищенности была выявлена критическая уязвимость Information disclosure (CVE-2023-27317), при эксплуатации которой злоумышленник может определить используемые дистрибутивы ПО, номера версий клиента и сервера и установленные обновления. В других случаях, в утекающей информации может содержаться расположение временных файлов или резервных копий.

Критичность: высокая

Рекомендации по устранению: Проводить аудит любого кода на предмет возможного раскрытия информации в рамках процессов контроля качества или сборки. Как можно чаще используйте общие сообщения об ошибках. Проверить, отключены ли какие-либо функции отладки или диагностики в рабочей среде.



Веб-сервер



TornadoServer 5.1.1



Apache HTTP
Server

2.4.7

В ходе анализа защищенности была выявлена критическая уязвимость Cleartext submission of password (CVE-2013-2672), при эксплуатации которой злоумышленник может перехватить пароль по незашифрованному соединению

Критичность: высокая

Рекомендации по устранению: Использовать шифрование на транспортном уровне (SSL или TLS) для защиты всех конфиденциальных сообщений, проходящих между клиентом и сервером. Использовать собственный механизм обработки сеансов, а используемые токены сеансов никогда не должны передаваться по незашифрованным каналам связи.

```
10 Connection: close
11 Referer: http://92.51.39.106:7799/login.html
12 Cookie: PHPSESSID=m5jrgtjdlis4qpdqeee69cvi03
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=admin&Login=Login
```

В ходе анализа защищенности была выявлена критическая уязвимость File path traversal (CVE-2023-23760), при эксплуатации которой злоумышленник может прочитать конфиденциальные файлы конфигурации, содержащие секретные ключи и пароли, получить доступ к исходному коду приложения, который он может просмотреть на наличие уязвимостей, или получить другие файлы привилегированных данных.

Критичность: высокая

Рекомендации по устранению: Проверить введенные пользователем данные перед их обработкой. В идеале сравнить вводимые пользователем данные с белым списком разрешенных значений. После проверки предоставленных входных данных добавить их в базовый каталог и использовать API файловой системы платформы для канонизации пути.

```
1 HTTP/1.1 200 OK
2 Content-Length: 926
3 Server: TornadoServer/5.1.1
4 Connection: close
5 Etag: "5160dcbcc73a9d0876e3ada9ca4c95f2d7c63bb5"
6 Date: Thu, 16 May 2024 10:27:05 GMT
7 Content-Type: text/html; charset=UTF-8
8
9 root:x:0:0:root:/root:/bin/bash
10 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
11 bin:x:2:2:bin:/bin:/usr/sbin/nologin
12 sys:x:3:3:sys:/dev:/usr/sbin/nologin
13 sync:x:4:65534:sync:/bin:/bin/sync
14 games:x:5:60:games:/usr/games:/usr/sbin/nologin
15 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
16 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
17 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
18 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
19 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
20 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
21 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
22 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
23 list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
24 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
25 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
26 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
27 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
28
```

В ходе анализа защищенности была выявлена критическая уязвимость OS command injection (CVE-2022-26085), при эксплуатации которой злоумышленник может выполнять команды операционной системы (ОС) на сервере, на котором запущено приложение, и обычно полностью подвергать риску приложение и его данные. Часто злоумышленник может использовать уязвимость внедрения команд ОС для компрометации других частей хостинговой инфраструктуры и использовать доверительные отношения для перенаправления атаки на другие системы внутри организации.

Критичность: высокая

Рекомендации по устранению: Использовать эквивалентные команды. Фильтровать входные значения

M Power Server is running

```
92.51.39.106 > /dev/null; ls
```

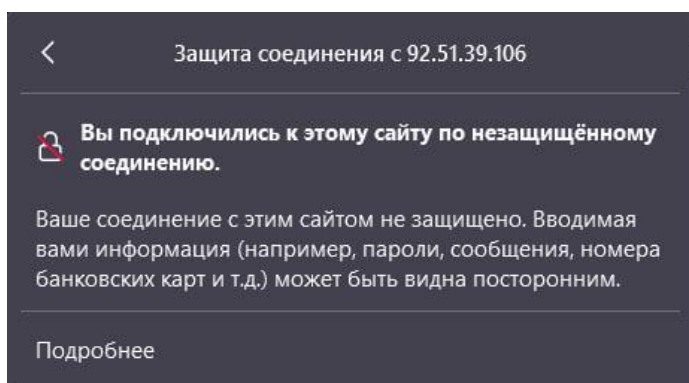
Check

```
Dockerfile
LICENSE
README.md
read
requirements.txt
server.py
static
templates
test.db
```

В ходе анализа защищенности была выявлена уязвимость Unencrypted communications (CVE-2023-40729), при эксплуатации которой злоумышленник, имеющий возможность просматривать сетевой трафик законного пользователя, может записывать и отслеживать его взаимодействие с приложением, а также получать любую информацию, которую предоставляет пользователь.

Критичность: низкая

Рекомендации по устранению: Приложения должны использовать шифрование транспортного уровня (SSL/TLS) для защиты всех сообщений, проходящих между клиентом и сервером. HTTP-заголовок Strict-Transport-Security следует использовать, чтобы гарантировать, что клиенты откажутся от доступа к серверу через небезопасное соединение.



В ходе анализа защищенности была выявлена уязвимость Vulnerable JavaScript dependency (CVE-2015-9251). Использование сторонних библиотек JavaScript может привести к появлению ряда уязвимостей на основе DOM, в том числе некоторых, которые можно использовать для взлома учетных записей пользователей, таких как DOM-XSS.

Критичность: низкая

Рекомендации по устранению: Разработайте стратегию управления исправлениями, чтобы гарантировать своевременное применение обновлений безопасности ко всем сторонним библиотекам в вашем приложении. Кроме того, рассмотрите возможность уменьшения поверхности атаки, удалив все библиотеки, которые больше не используются.

AdvisoryRequestResponsePath to issue

?

Vulnerable JavaScript dependency

Issue:

Vulnerable JavaScript dependency

Severity:

Low

Confidence:

Tentative

Host:

http://92.51.39.106:7799

Path:

/static/js/jquery1111.min.js

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery** version **1.11.1**, which has the following vulnerabilities:

- [CVE-2015-9251](#): 3rd party CORS request may execute
- [CVE-2015-9251](#): 3rd party CORS request may execute
- jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates
<https://github.com/jquery/jquery.com/issues/162>
- [CVE-2019-11358](#): jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution
- [CVE-2020-11023](#): passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code.
- [CVE-2020-11022](#): `Regex` in its `jQuery.htmlPrefilter` sometimes may introduce XSS

AdvisoryRequestResponsePath to issue

?

Vulnerable JavaScript dependency

Issue:

Vulnerable JavaScript dependency

Severity:

Low

Confidence:

Tentative

Host:

http://92.51.39.106:7799

Path:

/static/js/lightbox-plus-jquery.min.js

Issue detail

We observed a vulnerable JavaScript library.

We detected **jquery** version **2.1.4**, which has the following vulnerabilities:

- [CVE-2015-9251](#): 3rd party CORS request may execute
- jQuery 1.x and 2.x are End-of-Life and no longer receiving security updates
<https://github.com/jquery/jquery.com/issues/162>
- [CVE-2015-9251](#): 3rd party CORS request may execute
- [CVE-2019-11358](#): jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {}, ...)` because of Object.prototype pollution
- [CVE-2020-11023](#): passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `.html()`, `.append()`, and others) may execute untrusted code.
- [CVE-2020-11022](#): `Regex` in its `jQuery.htmlPrefilter` sometimes may introduce XSS