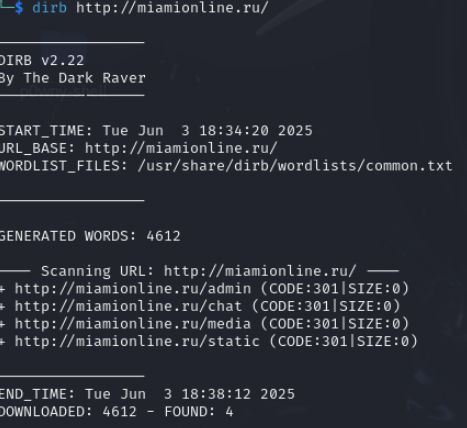
Надо:

Баги: как работает, критичность, скрин, как починить, предположительное место в коде с багом.

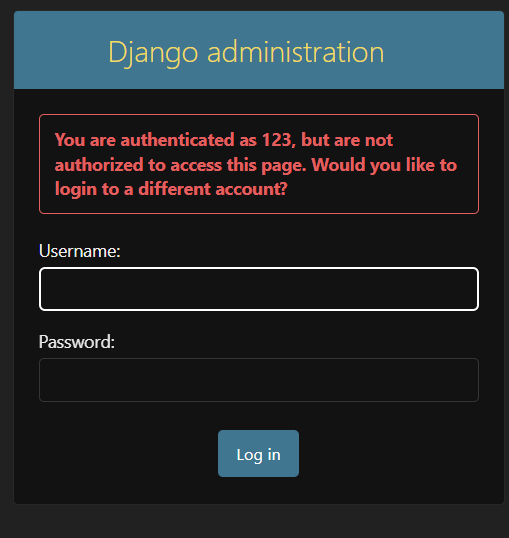
вывод.

для начала dirb директорий сайта:



картинка 1: отчет Dirb

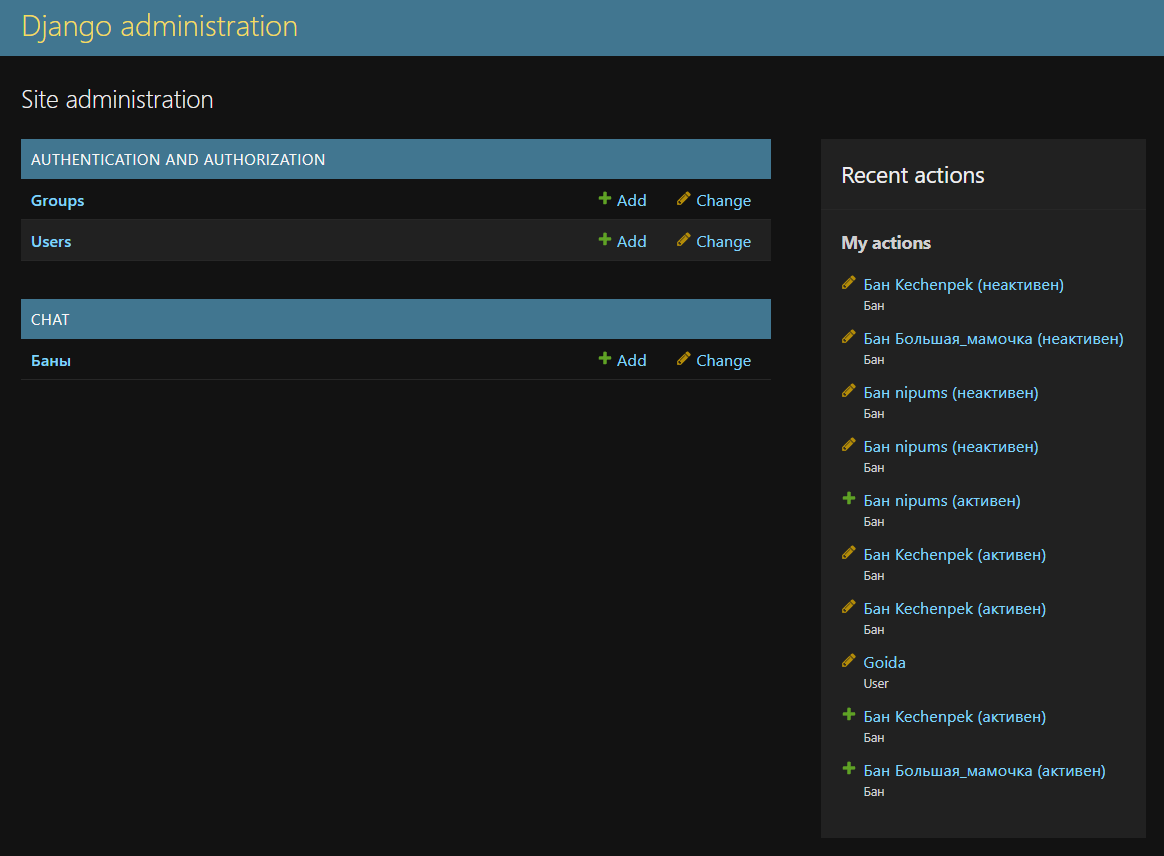
Из интересно можно выделить: директорию admin, продемонстрирована на картинке 2.



Картинка 2 - админка сайта

критичность максимальная. Возможен bruteforce.

Угроза: частичный доступ к БД

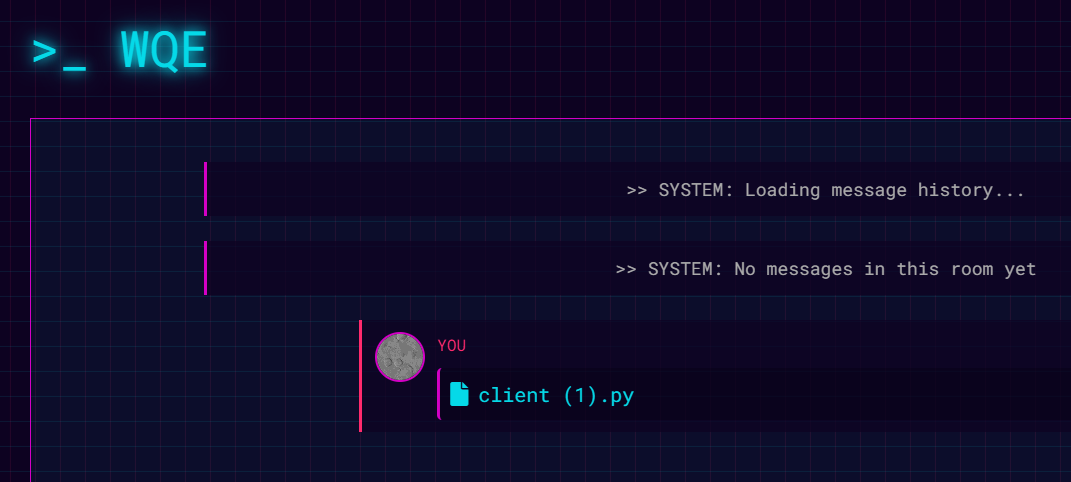


Доступ получен не при помощи bruteforce.

Варианты исправления: назвать директорию администратора не /admin.

Bug 1: Доступ к файлам из директории /media

пример атаки: в чате есть файл, как например на картинке 3



картинка 3: файл в чате

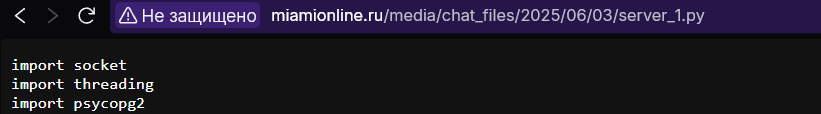
при открытии файла нас кидает по следующей ссылке: <http://miamionline.ru/media/chat_files/2025/06/03/client_1.py>

попытаемс получить доступ к файлу из другой комнаты в которой нас нет, зная название и примерное время файла. Файл, который мы хотим получить на картинке 4.



картинка 4: необходимый нам файл.

было: 

стало:

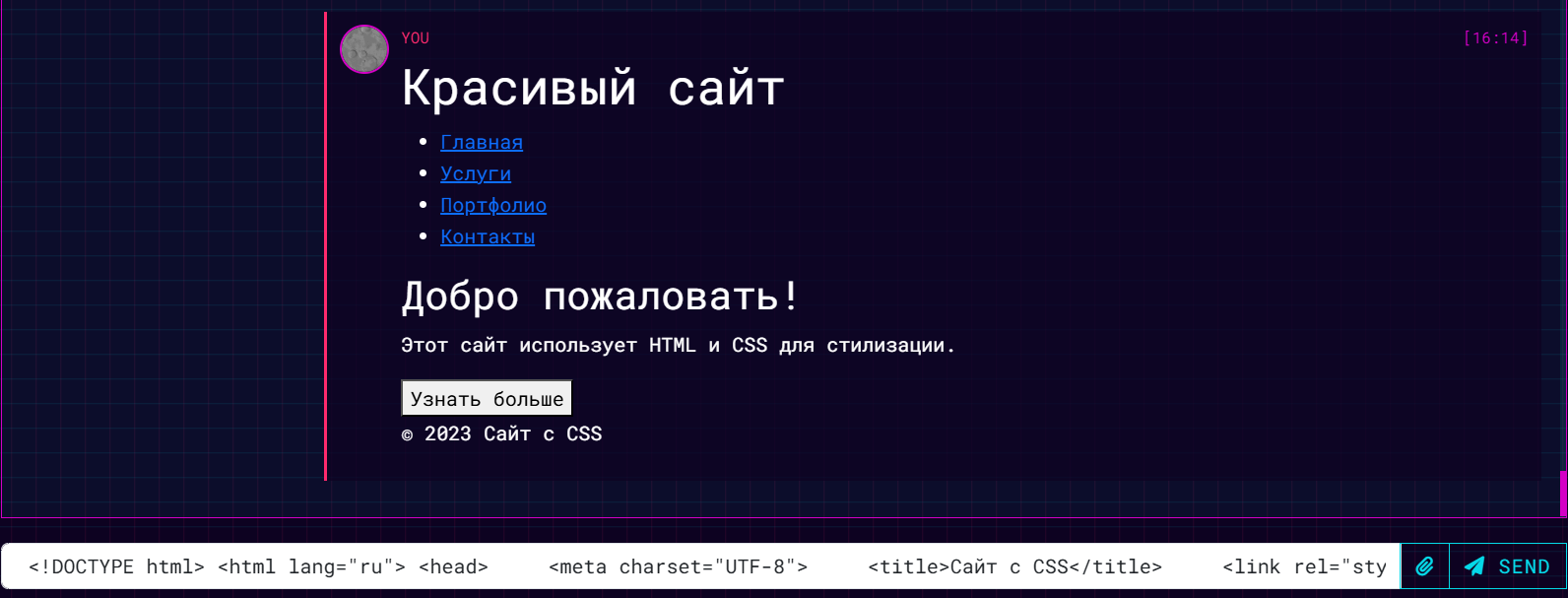
данная атака позволяет читать файлы из других чатов в которой нет нашего пользователя. Возможна кража конфиденциальной информации

Bug 2: Исполнение HTML Кода внутри чата

Сообщение с HTML кодом которое будет послано

1. <!DOCTYPE html>
2. <html lang="ru">
3. <head>
4. <meta charset="UTF-8">
5. <title>Сайт с CSS</title>
6. <link rel="stylesheet" href="style.css">
7. </head>
8. <body>
9. <header class="site-header">
10. <h1>Красивый сайт</h1>
11. <nav>
12. <ul class="nav-links">
13. <li><a href="#">Главная</a></li>
14. <li><a href="#">Услуги</a></li>
15. <li><a href="#">Портфолио</a></li>
16. <li><a href="#">Контакты</a></li>
17. </ul>
18. </nav>
19. </header>
20. <main>
21. <section class="hero">
22. <h2>Добро пожаловать!</h2>
23. <p>Этот сайт использует HTML и CSS для стилизации.</p>
24. <button class="cta-button">Узнать больше</button>
25. </section>
26. </main>
27. <footer class="site-footer">
28. <p>© 2023 Сайт с CSS</p>
29. </footer>
30. </body>
31. </html>

отображение в чате на рисунке 1



рисонок 1 - выполнение HTML развертки в окне чата.

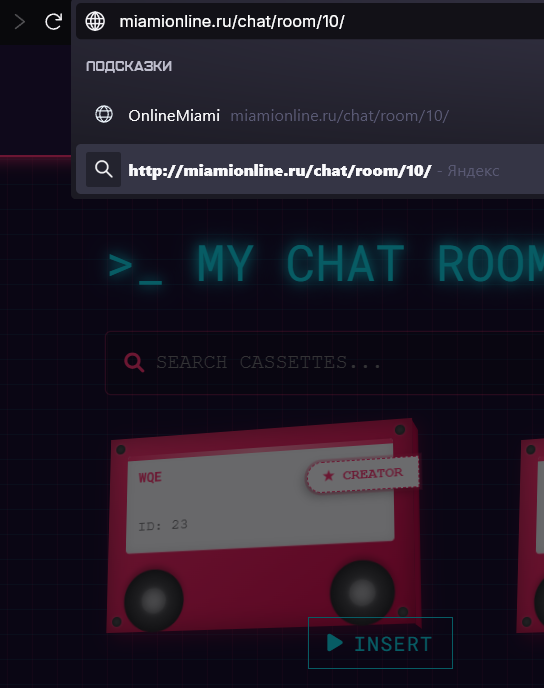
Критичность: высокая

Опасность: возможность выполнения JS кода, если ввести сложный HTML код с CSS, JS это может поломать всю логику работы чата.

Bug 2: error-based SQLi:

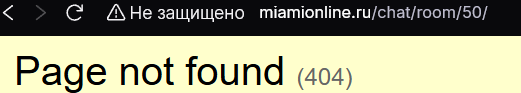
при переходе в чат наш URL меняется на <http://miamionline.ru/chat/room/1/>, если изменить номер чата например на 10. то нас перенаправляет в стандартное окно.

пример на 8.



картинка 8 - если такой чат существует но нас в нем нет.

если же чата с ID не существует то нас кидает на страницу 404. пример показан на картинке 9.



картинка 9: page not found.

данная атака позволяет узнать все ID чатов

Bug 3: сервер принимает все виды файлов, что может повлечь за собой атаку по типу:

reverse shell;

исполнения троянов на сервере.

Через утилиту Postman был проведен запрос на изменение пароля на сайте. Так выяснилось, что пароль можно сменить по этой ссылке: http://miamionline.ru/accounts/password\_change/