

Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»

«Информационная безопасность»

Работа 2:

Анализ и устранение уязвимости на примере реального CVE с использованием Vulhub

Выполнил:

Румский Александр Максимович

Группа:

P3407

Преподаватель:

Маркина Татьяна Анатольевна

Санкт-Петербург, 2025 год

Содержание

Название выбранной уязвимости (CVE ID) и краткое ее описание	3
Последовательность действий по воспроизведению уязвимости	4
Анализ root cause	6
Описание примененного исправления.....	7
Доказательство устранения уязвимости	7

Название выбранной уязвимости (CVE ID) и краткое ее описание

CVE-2017-12794

Уязвимость межсайтового скриптинга (XSS) на отладочных страницах с ошибками. При включении режима отладки в проекте, страницы с ошибкой могут потенциально раскрыть конфиденциальную информацию через незэкранированный HTML-код в сообщении об ошибке.

Последовательность действий по воспроизведению уязвимости

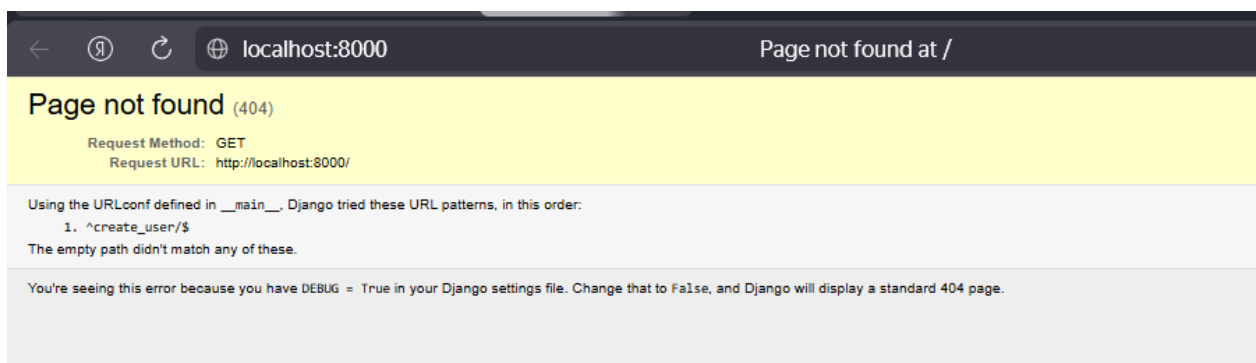
1. Создание docker-контейнера для запуска уязвимости

```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

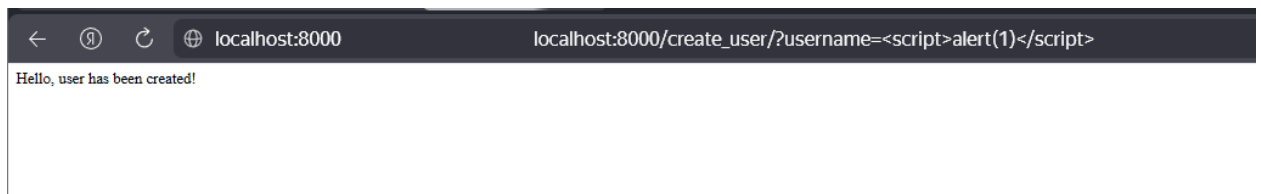
Установите последнюю версию PowerShell для новых функций и улучшения! https://aka.ms/PSWindows

PS D:\ITMO\3-re\University\stage 4\autmn\Information security\lab2\CVE-2017-12794> docker-compose up -d
time="2025-10-20T12:49:37+03:00" level=warning msg="D:\\ITMO\\3-re\\University\\stage 4\\autmn\\Information security\\la
b2\\CVE-2017-12794\\docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avo
id potential confusion"
[+] Running 23/23
  ✓ db Pulled
    ✓ 59bfc3509f3 Pull complete
    ✓ 587cf5e11ca1 Pull complete
    ✓ 696b75eaa88e Pull complete
    ✓ 0d83746bb80b Pull complete
    ✓ c50e01d57241 Pull complete
    ✓ 3a431a2253cd Pull complete
    ✓ a0646b0f1ead Pull complete
    ✓ 24ff05c04760 Pull complete
    ✓ 912227b294ee Pull complete
  ✓ web Pulled
    ✓ e9afc4f90ab0 Pull complete
    ✓ 989e6b19a265 Pull complete
    ✓ 7117a74960bb Pull complete
    ✓ 04806fde3470 Pull complete
    ✓ 103e995be0a8 Pull complete
    ✓ 33180336d878 Pull complete
    ✓ 11a88e764313 Pull complete
    ✓ 5fbfb8c90ca7 Pull complete
    ✓ 7c1fc11e28b7 Pull complete
    ✓ 5573c4b30949 Pull complete
    ✓ af14b6c2f878 Pull complete
    ✓ b037f750ed71 Pull complete
[+] Running 3/3
  ✓ Network cve-2017-12794_default Created
  ✓ Container cve-2017-12794-db-1 Started
  ✓ Container cve-2017-12794-web-1 Started
PS D:\ITMO\3-re\University\stage 4\autmn\Information security\lab2\CVE-2017-12794> |
```

2. Проверить доступность страницы http://localhost:8000

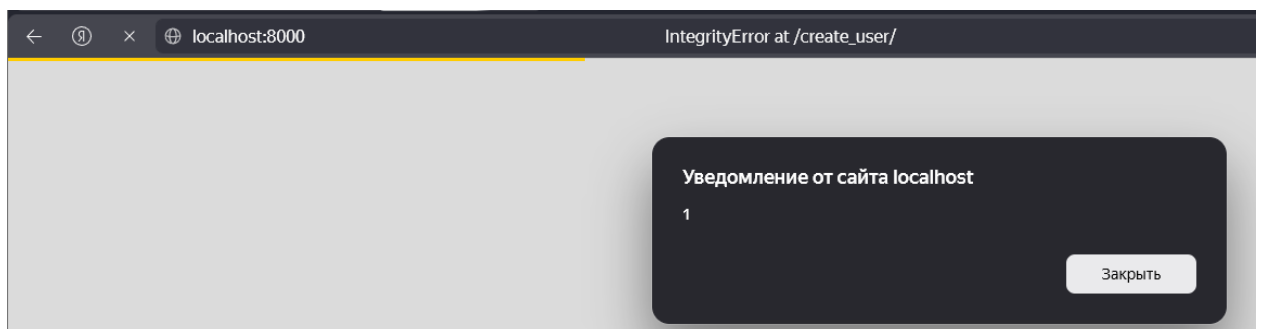


3. Выполнить запрос к бэкенду, демонстрирующий уязвимость http://localhost:8000/create_user/?username=<script>alert(1)</script> Данный запрос, выполненный в первый раз, создаст пользователя



4. Повторный запрос вызовет срабатывание кода, переданного как имя пользователя

Причина: Повторный вызов повлечет ошибку в БД, связанную с ограничением на уникальность имен пользователей, что, в свою очередь, вызовет страницу с отладочной информацией, на которой и сработает код, переданный в username.



Анализ root cause

Ключевым условием для эксплуатации этой уязвимости является запуск Django-приложения в режиме отладки: `DEBUG = True` в `app.py`.

Уязвимость заключалась в обработке и выводе информации о связанных исключениях. В шаблоне `technical_500.html` был блок кода, который отвечал за отображение причины исходного исключения.

В уязвимых версиях она выглядела так:

```
{% autoescape off %}
...
{% ifchanged frame.exc_cause %}{% if frame.exc_cause %}
...
    The above exception ({{ frame.exc_cause }}) was the direct cause of
the following exception:
...
{% endif %}{% endifchange %}
...
{% endautoescape %}
```

`{% autoescape off %}` отключает автоматическое экранирование HTML-тегов для всего заключенного в нее блока. Это означает, что любые переменные, выводимые внутри этого блока, будут отображаться "как есть", без преобразования символов `<`, `>` и других в безопасные HTML-элементы (прим. `>` станет `>`;

`{{ frame.exc_cause }}` содержит текстовое описание исключения, которое стало причиной возникшей ошибки 500.

Django имеет механизм для "связывания" исключений, чтобы предоставить разработчику более полную картину ошибки. Например, если код приложения вызывает ошибку целостности данных в базе (например, нарушение уникальности поля), драйвер базы данных генерирует свое исключение. Django перехватывает его и создает свое, более высокоуровневое исключение, при этом сохраняя исходное исключение от драйвера в атрибуте `__cause__`, что и позволяет встроить код.

Описание примененного исправления

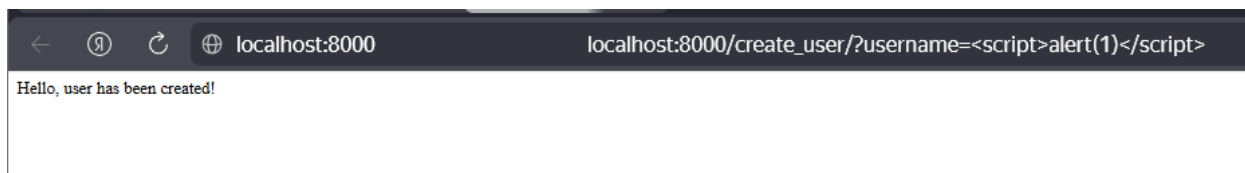
Данная уязвимость исправляется достаточно просто – установкой флага DEBUG в настройках приложения в значение False. После этого страницы с ошибками перестают формироваться с использованием шаблона technical_500.html, как при DEBUG = True, что позволяет избежать данной уязвимости. Сервер просто возвращает Server Error (500).

Доказательство устранения уязвимости

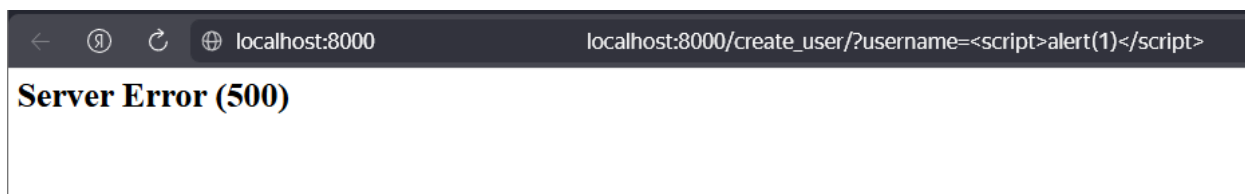
Остановка и перезапуск контейнера с внесенными изменениями

```
PS D:\ITMO\3-re\University\stage 4\autmn\Information security\lab2\CVE-2017-12794> docker-compose down
time="2025-10-20T13:33:24+03:00" level=warning msg="D:\\ITMO\\3-re\\University\\stage 4\\autmn\\Information security\\lab2\\CVE-2017-12794\\docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 3/3
  ✓ Container cve-2017-12794-web-1   Removed      10.4s
  ✓ Container cve-2017-12794-db-1    Removed      0.2s
  ✓ Network cve-2017-12794_default   Removed      0.3s
PS D:\ITMO\3-re\University\stage 4\autmn\Information security\lab2\CVE-2017-12794> docker-compose up -d
time="2025-10-20T13:34:07+03:00" level=warning msg="D:\\ITMO\\3-re\\University\\stage 4\\autmn\\Information security\\lab2\\CVE-2017-12794\\docker-compose.yml: the attribute 'version' is obsolete, it will be ignored, please remove it to avoid potential confusion"
[+] Running 3/3
  ✓ Network cve-2017-12794_default   Created      0.0s
  ✓ Container cve-2017-12794-db-1    Started      0.4s
  ✓ Container cve-2017-12794-web-1   Started      0.5s
```

Запрос на создание пользователя:



Повторный запрос:



Как можно видеть, сервер вернул только код ошибки, без выполнения каких-либо скриптов.