

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



Работа №4:

Анализ уязвимостей веб-приложения с помощью OWASP ZAP

по дисциплине

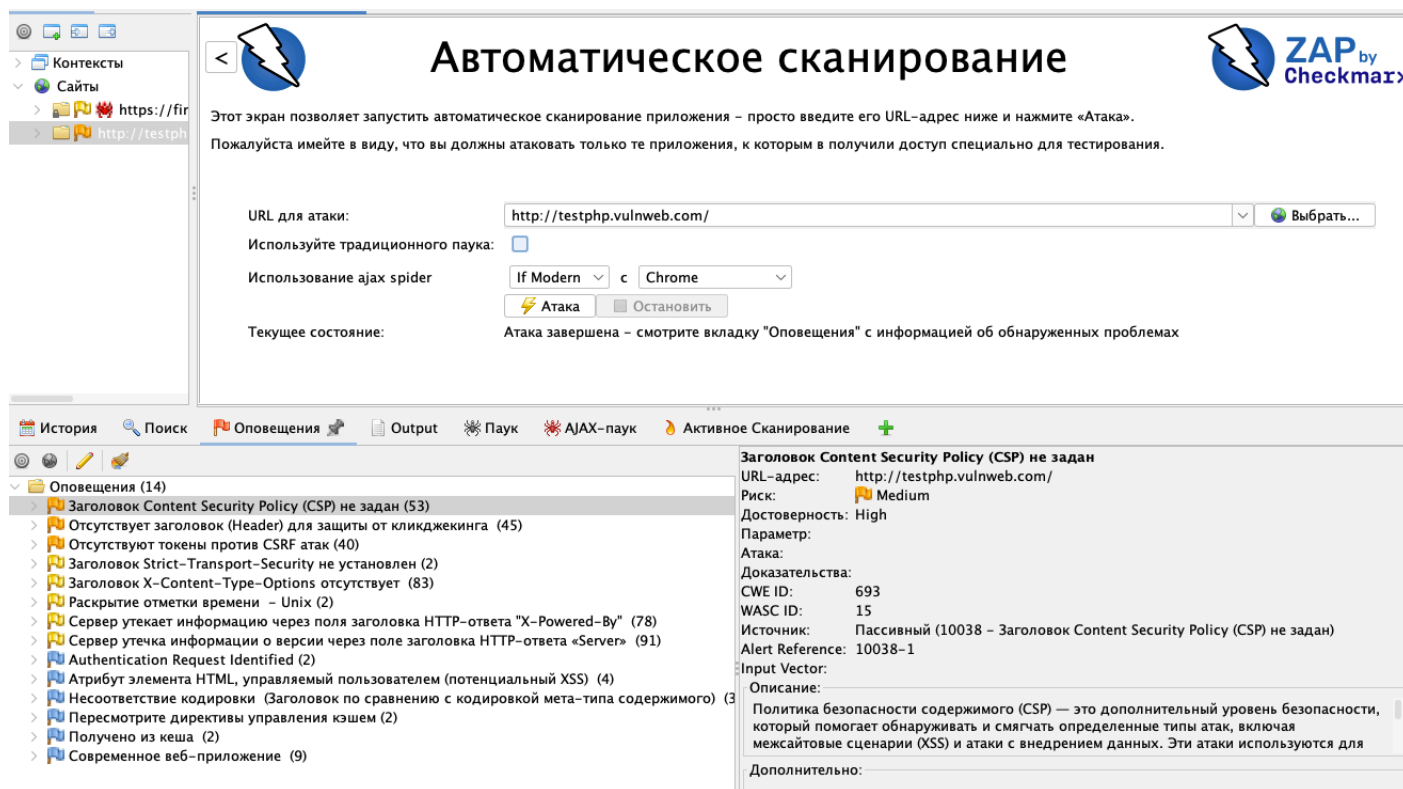
Информационная безопасность

Выполнил Студент группы Р3412
Кобелев Роман Павлович

2025г.

1 Анализ сайта

В этой работе я, с помощью приложения ZAP, провел анализ сайта <http://testphp.vulnweb.com/>. Вот какие уязвимости программа нашла:



Автоматическое сканирование

Этот экран позволяет запустить автоматическое сканирование приложения – просто введите его URL-адрес ниже и нажмите «Атака».

Пожалуйста имейте в виду, что вы должны атаковать только те приложения, к которым в получили доступ специально для тестирования.

URL для атаки:

Используйте традиционного паука: ☐

Использование ajax spider: If Modern Chrome

Текущее состояние: Атака завершена – смотрите вкладку "Оповещения" с информацией об обнаруженных проблемах

Оповещения (14)

- Заголовок Content Security Policy (CSP) не задан (53)
- Отсутствует заголовок (Header) для защиты от кликджекинга (45)
- Отсутствуют токены против CSRF атак (40)
- Заголовок Strict-Transport-Security не установлен (2)
- Заголовок X-Content-Type-Options отсутствует (83)
- Раскрытие отметки времени – Unix (2)
- Сервер утекает информацию через поля заголовка HTTP-ответа "X-Powered-By" (78)
- Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server» (91)
- Authentication Request Identified (2)
- Атрибут элемента HTML, управляемый пользователем (потенциальный XSS) (4)
- Несоответствие кодировки (Заголовок по сравнению с кодировкой мета-типа содержимого) (3)
- Пересмотрите директивы управления кэшем (2)
- Получено из кеша (2)
- Современное веб-приложение (9)

Заголовок Content Security Policy (CSP) не задан

URL-адрес: <http://testphp.vulnweb.com/>

Риск: Medium

Достоверность: High

Параметр:

Атака:

Доказательства:

CWE ID: 693

WASC ID: 15

Источник: Пассивный (10038 – Заголовок Content Security Policy (CSP) не задан)

Alert Reference: 10038-1

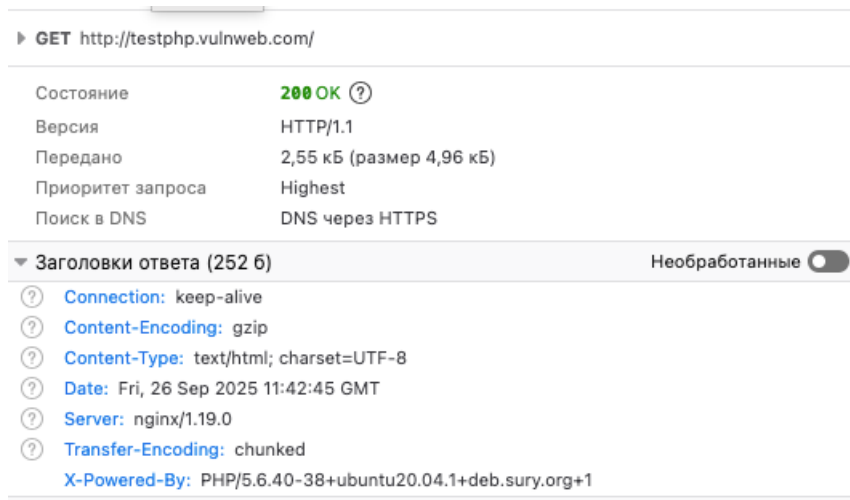
Input Vector:

Описание: Политика безопасности содержимого (CSP) — это дополнительный уровень безопасности, который помогает обнаруживать и смягчать определенные типы атак, включая межсайтовые сценарии (XSS) и атаки с внедрением данных. Эти атаки используются для

Дополнительно:

Разберу уязвимости с наибольшим риском (XSS, кликджекинг, CSRF):

- Отсутствие заданного Content Security Policy



GET http://testphp.vulnweb.com/

Состояние: 200 OK

Версия: HTTP/1.1

Передано: 2,55 кБ (размер 4,96 кБ)

Приоритет запроса: Highest

Поиск в DNS: DNS через HTTPS

Заголовки ответа (252 6) Необработанные

- Connection: keep-alive
- Content-Encoding: gzip
- Content-Type: text/html; charset=UTF-8
- Date: Fri, 26 Sep 2025 11:42:45 GMT
- Server: nginx/1.19.0
- Transfer-Encoding: chunked
- X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

CSP - дополнительный уровень безопасности, который помогает обнаруживать и смягчать определенные типы атак, включая межсайтовые сценарии (XSS) и атаки с внедрением данных. Отсутствие данного заголовка позволяет злоумышленнику проворачивать манипуляции разного спектра - от кражи данных до порчи сайта.

- Отсутствует заголовок для защиты от кликджекинга

Отсутствие заголовка **X-Frame-Options** дает злоумышленнику возможность провести кликджекинг. Заголовок **X-Frame-Options** защищает от кликджекинга, сообщая браузеру, что страница не может быть встроена в фрейм (iframe) другого сайта без разрешения сервера. Кликджекинг — это вредоносная техника, при которой злоумышленники обманом заставляют пользователя кликнуть на невидимую ссылку или кнопку на веб-странице, тем самым выполняя нежелательные действия.

- Отсутствуют токены против **CSRF** атак

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Fri, 26 Sep 2025 11:19:44 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
content-length: 4958

<div id="navBar">
  <div id="search">
    <form action="search.php?test=query" method="post">
      <label>search art</label>
      <input name="searchFor" type="text" size="10">
      <input name="goButton" type="submit" value="go">
    </form>
  </div>
  <div id="sectionLinks">
    <ul>
      <li><a href="categories.php">Browse categories</a></li>
```

Запрос не привязан к намерению пользователя, а браузер автоматически прикрепляет его куки/сессию, поэтому сервер не отличит легитимный запрос от поддельного. Злоумышленник может заставить авторизованного пользователя незаметно выполнить действие в приложении (смена пароля/почты, перевод денег и т.д.) просто наведя его на специально подготовленную страницу/ссылку. Итог — действия от имени жертвы, потеря данных и денег.