

МОЛДАВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАТИКИ  
ДЕПАРТАМЕНТ ИНФОРМАТИКИ

Отчет по дисциплине:

“Безопасность информационных систем”

**Лабораторная работа №5**

Инструменты сканирования уязвимостей OWASP-ZAP

**Автор:** Калинкова С.

группа I2302

**Проверила:** Новак Л.

doctor conferentiar universitar

Кишинев, 2024

## Цель работы:

1. Использовать инструменты OWASP для сканирования уязвимостей в веб-приложениях (2-3 веб-приложения).
2. Определить, какие уязвимости встречаются, и описать их.
3. Каковы методы решения тех проблем, которые вызваны определенными уязвимостями?
4. Определить другие приложения для сканирования уязвимостей для веб-приложений.

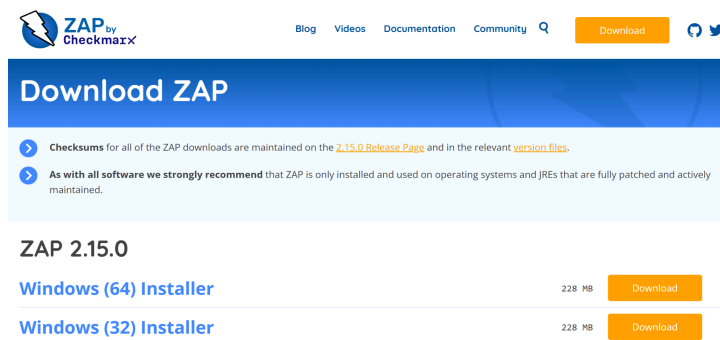
## Ход работы:

OWASP ZAP (Zed Attack Proxy) — это инструмент с открытым исходным кодом для тестирования безопасности веб-приложений. Он используется для выявления уязвимостей в веб-приложениях, таких как XSS (межсайтовый скриптинг), SQL-инъекции и другие. ZAP поддерживает ручное и автоматическое сканирование, позволяет перехватывать и изменять HTTP-запросы, анализировать ответы, а также предоставляет отчеты об обнаруженных уязвимостях.

В качестве преимуществ OWASP ZAP можно выделить:

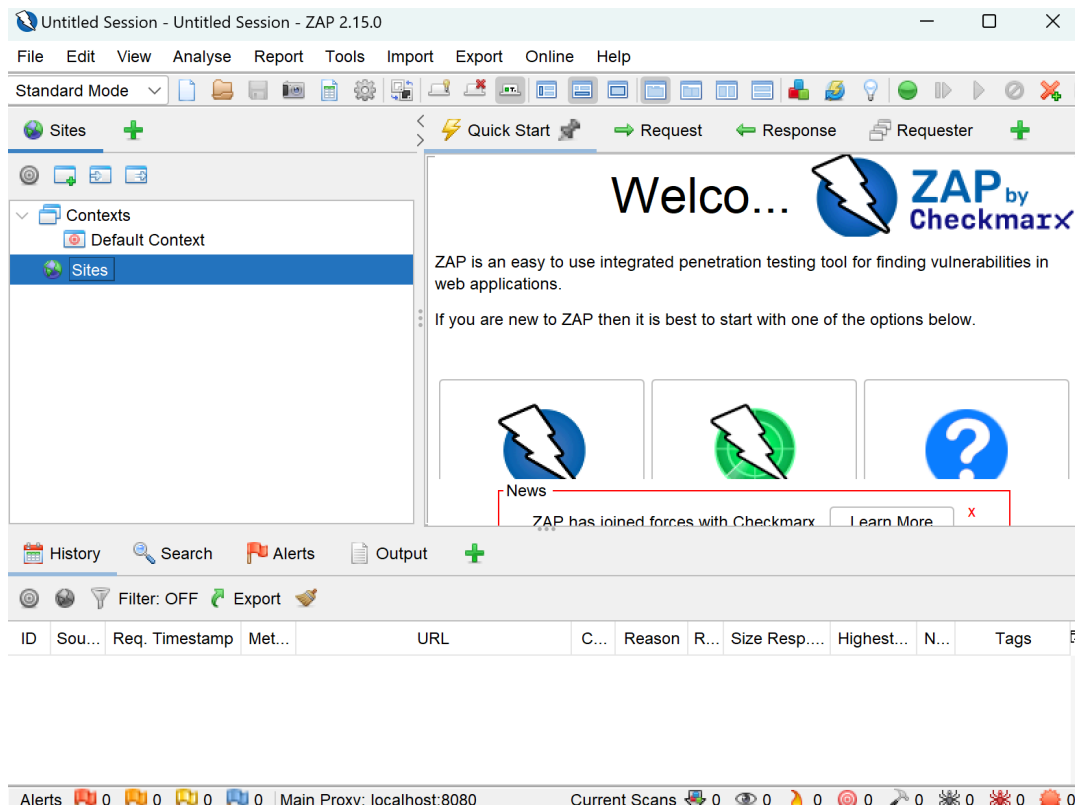
- поддержка всех основных ОС (Windows, Linux, MacOS);
- Бесплатный проект [с открытым исходным кодом](#);
- Поддержка плагинов для расширения функциональности;
- Возможность работы как через графический интерфейс (GUI), так и через командную строку;
- Обширный набор функций
- Простота использования

Для начала скачиваю OWASP ZAP с официального сайта



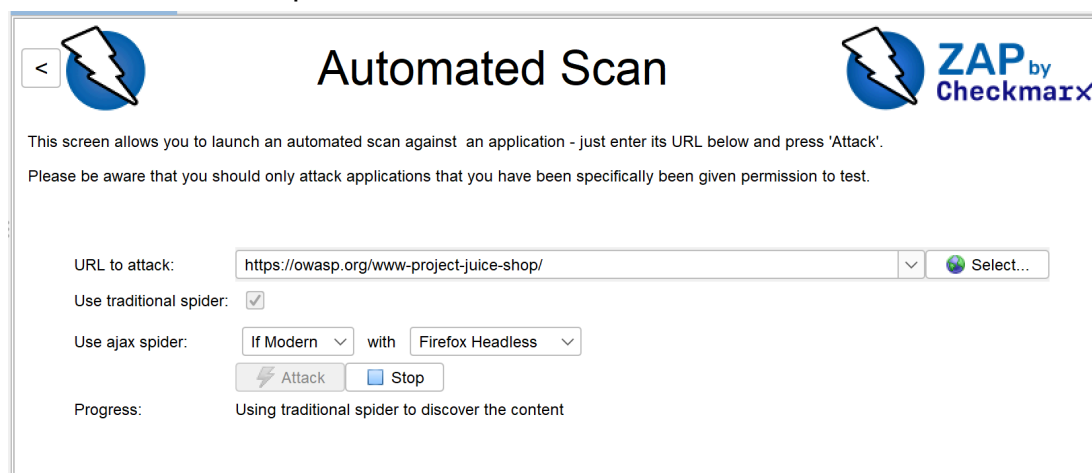
The screenshot shows the official OWASP ZAP download page. At the top, there is a navigation bar with links for Blog, Videos, Documentation, Community, and a search icon. A prominent orange 'Download' button is also present. Below the navigation bar, the main heading is 'Download ZAP'. A blue banner contains two important notices: one about checksums being maintained on the 2.15.0 Release Page and version files, and another strongly recommending that ZAP be installed and used on fully patched and actively maintained operating systems and JREs. Below this, the version 'ZAP 2.15.0' is displayed. Two download options are listed: 'Windows (64) Installer' and 'Windows (32) Installer'. Each option shows a file size of 228 MB and a corresponding orange 'Download' button.

OS/Architecture	File Size	Action
Windows (64) Installer	228 MB	<a href="#">Download</a>
Windows (32) Installer	228 MB	<a href="#">Download</a>



после установки открылся экран приветствия, где указаны основные функции программы для тестирования безопасности веб-приложений. Слева дерево контекстов, где отображен и раздел "Sites", который будет заполняться информацией о сканируемых сайтах. В нижней части интерфейса находятся вкладки для просмотра истории запросов, поиска, предупреждений и вывода данных. Прокси-сервер настроен на `localhost:8080`

Я выбираю автоматическое сканирование ввожу URL сайта и нажимаю атака, чтобы начать тестирование



Processed	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	Tags
	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-pdf-archive/image/O...	301	Moved Perm...	261 ms	2,836 bytes	162 bytes		
Not Text	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-chapter-uruguay/asset...	200	OK	299 ms	2,905 bytes	253,733 bytes		Comment
Not Text	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-chapter-uruguay/asset...	200	OK	307 ms	2,909 bytes	425,671 bytes		Comment
Not Text	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-chapter-uruguay/asset...	200	OK	259 ms	2,907 bytes	210,504 bytes		Comment
Not Text	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-chapter-uruguay/asset...	200	OK	294 ms	2,909 bytes	627,534 bytes		Comment
	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-community/attacks/C...	404	Not Found	278 ms	2,757 bytes	29,283 bytes		Form, Script, Com...
Not Text	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-community/assets/ima...	200	OK	239 ms	2,907 bytes	54,057 bytes		Comment
Not Text	11/12/24, 11:17:41 PM	GET	https://owasp.org/www-chapter-uruguay/asset...	200	OK	256 ms	2,907 bytes	363,146 bytes		Comment

Первое, что я буду тестировать, это <https://owasp.org/www-project-juice-shop/>

**OWASP Juice Shop** — это уязвимое веб-приложение, разработанное для обучения и тренировки в области безопасности. Оно предоставляет платформу для практического тестирования различных типов уязвимостей, таких как SQL-инъекции, XSS, CSRF, а также других распространенных угроз.

**User Agent Fuzzer**

URL: <https://owasp.org/www-project-juice-shop/>

Risk: Informational

Confidence: Medium

Parameter: Header User-Agent

Attack: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)

Evidence:

CWE ID: 0

WASC ID: 0

Source: Active (10104 - User Agent Fuzzer)

Input Vector:

Description:

Check for differences in response based on fuzzed User Agent (eg. mobile sites, acces


После того как тестирование выполнено на 100% захожу во вкладку "Alerts" В левой части отображается древовидная структура, представляющая список предупреждений, здесь это "User Agent Fuzzer". инструмент нашел 96 предупреждений, связанных с манипуляцией заголовком "User-Agent".

справа отображается более подробная информация про предупреждения, например:


- **URL:** адрес страницы, на которую был направлен запрос.
- **Risk (Риск):** Уровень риска для этого предупреждения помечен как "Informational" (Информационный), что означает, что это низкий уровень риска, требующий внимания, но не представляющий прямой угрозы.
- **Confidence (Уверенность):** "Medium" (Средний) — степень уверенности в том, что это предупреждение актуально.

Для решения проблем, связанных с уязвимостями, выявленными "User Agent Fuzzer", можно предпринять следующие меры:

1. **Проверка и фильтрация заголовков** — убедиться, что User-Agent фильтруется и проверяется на корректность, чтобы избежать внедрения вредоносных данных.
2. **Скрытие информации о сервере** — исключить заголовки, раскрывающие серверное ПО и его версию (Server, X-Powered-By).
3. **Единый ответ на нестандартные User-Agent** — настройте сервер так, чтобы он одинаково отвечал на необычные User-Agent, чтобы избежать утечки информации.
4. **Логирование подозрительных User-Agent** — логировать необычные заголовки для отслеживания активности возможных ботов.
5. **Content Security Policy (CSP)** — добавьте заголовок CSP, чтобы защититься от XSS-атак.




## Automated Scan



This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically given permission to test.

URL to attack:

 Select...

Use traditional spider:


☒


Use ajax spider:

If Modern

with

Chrome

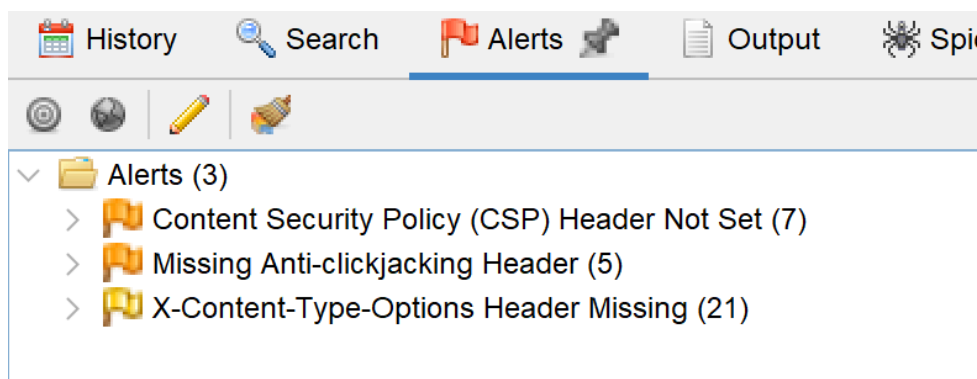
 Attack

 Stop

Progress:

Using traditional spider to discover the content

Следующим мы будем тестировать <http://www.itsecgames.com/> **bWAPP** (buggy Web Application) — это уязвимое веб-приложение, созданное для практики в области кибербезопасности и тестирования. Оно содержит более 100 уязвимостей, включая SQL-инъекции, XSS, CSRF и другие, позволяя пользователям тренироваться в их выявлении и эксплуатации в безопасной среде.



после завершения тестирования в ZAP в разделе "Alerts" (предупреждения) отображаются найденные предупреждения, связанные с отсутствием некоторых заголовков безопасности.

Цвета флажков помогают визуально разделить уровни риска: оранжевые указывают на средний риск, а желтые — на низкий.

1. **Content Security Policy (CSP) Header Not Set (7)** — Отсутствует заголовок Content Security Policy, который помогает предотвратить атаки, такие как XSS (межсайтовый скриптинг). Зафиксировано 7 таких предупреждений.

решение: Настройка заголовка *Content-Security-Policy* позволяет ограничить источники контента, которые браузер может загружать (скрипты, изображения, стили).

например, написать заголовок, чтобы загружать контент только с самого сайта и доверенного домена для скриптов, запрещая загрузку объектов .

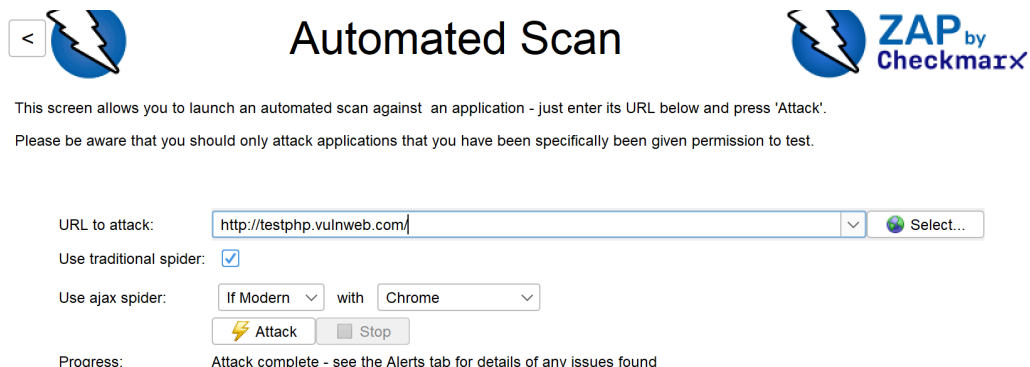
2. **Missing Anti-clickjacking Header (5)** — Отсутствует заголовок защиты от кликджекинга (например, X-Frame-Options), который предотвращает отображение содержимого сайта в iframe на других доменах, защищая от атак типа "clickjacking". Зафиксировано 5 предупреждений.

решение: Настройка заголовка *X-Frame-Options* помогает предотвратить использование вашего сайта в iframe на других доменах.

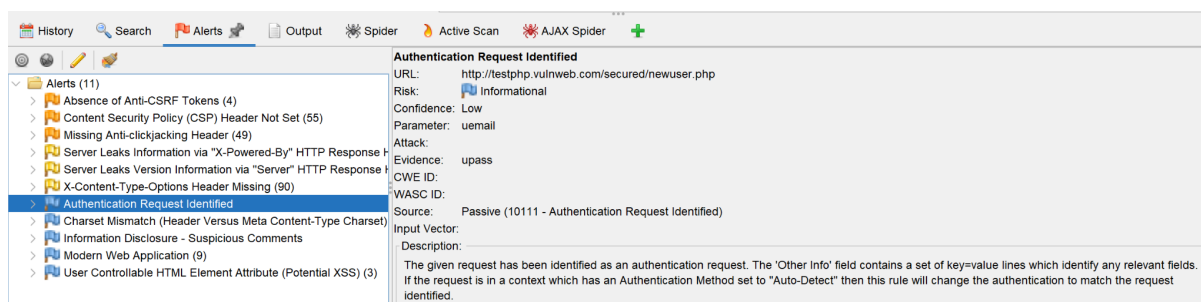
например написать заголовок, который запрещает загрузку сайта в iframe вообще. Либо указать конкретный домен, который может использовать ваш сайт в iframe.

3. **X-Content-Type-Options Header Missing (21)** — Отсутствует заголовок X-Content-Type-Options, который предотвращает MIME-сниффинг, помогая защититься от загрузки файлов с неправильным типом контента. Зафиксировано 21 предупреждение.

решение: Настройка заголовка **X-Content-Type-Options** с значением **nosniff** помогает предотвратить MIME-сниффинг, заставляя браузер обрабатывать контент строго по указанному типу.



Последнее, что я проверяю <http://testphp.vulnweb.com/> — это учебный веб-сайт, предоставленный компанией Asynetix для практики навыков тестирования безопасности. Сайт специально создан с уязвимостями для тестирования, чтобы пользователи могли изучать и отрабатывать методы обнаружения и эксплуатации уязвимостей, таких как SQL-инъекции, XSS (межсайтовый скриптинг), CSRF, управление сессиями и другие распространенные веб-уязвимости, в безопасной среде.



После завершения тестирования в левой части вкладки alerts отображается список предупреждений: Вот некоторые:

- **Absence of Anti-CSRF Tokens (4)** — отсутствие токенов CSRF (средний риск, оранжевый флаг).
- **Content Security Policy (CSP) Header Not Set (55)** — отсутствие заголовка CSP (средний риск, оранжевый флаг).

- **Missing Anti-clickjacking Header (49)** — отсутствие заголовка защиты от clickjacking (низкий риск, желтый флаг).
- **X-Content-Type-Options Header Missing (90)** — отсутствие заголовка X-Content-Type-Options (средний риск, оранжевый флаг).
- **Authentication Request Identified** — идентифицирован запрос аутентификации. и в правой части показаны детали этого предупреждения:
  - **Risk (Риск):** Уровень риска указан как "Informational" (Информационный), что означает, что это предупреждение носит информативный характер и не представляет угрозы.
  - **Confidence (Уверенность):** "Low" (Низкая) — низкая степень уверенности в том, что это предупреждение связано с уязвимостью.

#### 4. Определить другие приложения для сканирования уязвимостей для веб-приложений.

**Burp Suite:** инструмент для тестирования безопасности, с функциями сканирования уязвимостей, захвата и анализа трафика. Поддерживает ручное и автоматическое тестирование, а также предоставляет различные плагины.

**Acunetix:** Коммерческий сканер уязвимостей, который ищет SQL-инъекции, XSS и другие веб-уязвимости. Инструмент предоставляет подробные отчеты и функции управления рисками.

**TestingWhiz:** Автоматизированный инструмент для тестирования веб-приложений и API. Поддерживает тестирование функциональности, безопасности и производительности, с интеграцией в CI/CD и графическим интерфейсом для создания тестов.

**Astra Pentest:** Облачное решение для автоматического сканирования и ручного тестирования уязвимостей. Покрывает широкие спектры веб-уязвимостей и предлагает отчеты с рекомендациями по исправлению.

### **Вывод**

В ходе лабораторной работы проведено сканирование уязвимостей в веб-приложениях с использованием инструментов OWASP, выявлены такие уязвимости (отсутствие CSP, Отсутствие защиты от clickjacking, риск загрузки опасного контента) и предложены методы их устранения. Также рассмотрены дополнительные инструменты для выявления и предотвращения угроз в веб-приложениях.



## **Библиография**

<https://www.zaproxy.org/download/>

<https://habr.com/ru/companies/first/articles/709586/>

<https://owasp.org/www-project-juice-shop/>

<http://testphp.vulnweb.com/>

<https://www.it-courses.by/12-great-web-service-testing-tools/>