ZAP by Checkmarx Scanning Report

Сайт: http://10.10.10.17:8080

Создано вс, 22 февр. 2026 07:54:35

ZAP Version: 2.17.0

ZAP by Checkmarx

Сводка предупреждений

Уровень риска	Количество предупреждений
Высокий	0
Средний	4
Низкий	6
Информационный	5

Insights

Level	Reason	Site	Description	Statistic
Информация	Информационный	http://10.10.10.17:8080	Percentage of responses with status code 2xx	78 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of responses with status code 3xx	20 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of responses with status code 5xx	1 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of endpoints with content type application/javascript	9 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of endpoints with content type application/octet-stream	9 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of endpoints with content type text/css	3 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of endpoints with content type text/html	67 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of endpoints with content type text/plain	9 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of endpoints with method GET	87 %
Информация	Информационный	http://10.10.10.17:8080	Percentage of endpoints with method POST	12 %

Информация	Информационный	http://10.10.10.17:8080	Count of total endpoints	31

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Оповещения

Название	Уровень риска	Количество экземпляров
Sub Resource Integrity Attribute Missing	Средний	Systemic
Заголовок Content Security Policy (CSP) не задан	Средний	Systemic
Отсутствует заголовок (Header) для защиты от кликджекинга	Средний	Systemic
Уязвимость JS Библиотеки (Library)	Средний	1
Cookie No HttpOnly Flag	Низкий	3
Cookie без атрибута SameSite	Низкий	3
Заголовок X-Content-Type-Options отсутствует	Низкий	Systemic
Раскрытие информации - сообщения об ошибках отладки	Низкий	3
Раскрытие ошибок приложения	Низкий	3
Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server»	Низкий	Systemic
Authentication Request Identified	Информационный	1
Session Management Response Identified	Информационный	3
Атрибут элемента HTML, управляемый пользователем (потенциальный XSS)	Информационный	1
Раскрытие информации - подозрительные комментарии	Информационный	2
Современное веб-приложение	Информационный	3

Сведения об оповещении

Средний	Sub Resource Integrity Attribute Missing
Описание	The integrity attribute is missing on a script or link tag served by an external server. The integrity tag prevents an attacker who have gained access to this server from injecting a malicious content.
URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	

Атака	
Свидетельство	<link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet">
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/
Node Name	http://10.10.10.17:8080/courses/
Метод	GET
Параметр	
Атака	
Свидетельство	<link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet">
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/robots.txt
Node Name	http://10.10.10.17:8080/robots.txt
Метод	GET
Параметр	
Атака	
Свидетельство	<link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet">
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/sitemap.xml
Node Name	http://10.10.10.17:8080/sitemap.xml
Метод	GET
Параметр	
Атака	
Свидетельство	<link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet">
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/students/
Node Name	http://10.10.10.17:8080/students/
Метод	GET
Параметр	
Атака	

Свидетельство	<link href="https://fonts.googleapis.com/icon?family=Material+Icons" rel="stylesheet">
Дополнительная информация	
Экземпляры	Systemic
Решение	Provide a valid integrity attribute to the tag.
Ссылка	https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity
CWE Идентификатор	345
WASC ID	15
Идентификатор плагина	90003

Средний **Заголовок Content Security Policy (CSP) не задан**

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 всего: от кражи данных до порчи сайта или распространения вредоносных программ. CSP предоставляет набор стандартных HTTP-заголовков, которые позволяют владельцам веб-сайтов объявлять утвержденные источники контента, которые браузеры должны разрешить загружать на эту страницу. Охватываемые типы включают JavaScript, CSS, HTML-фреймы, шрифты, изображения и встраиваемые объекты, такие как апплеты Java. ActiveX, аудио и видео файлы.
URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	
Атака	
Свидетельство	
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/
Node Name	http://10.10.10.17:8080/courses/
Метод	GET
Параметр	
Атака	
Свидетельство	
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/robots.txt
Node Name	http://10.10.10.17:8080/robots.txt

Метод	GET
Параметр	
Атака	
Свидетельство	
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/sitemap.xml
Node Name	http://10.10.10.17:8080/sitemap.xml
Метод	GET
Параметр	
Атака	
Свидетельство	
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/students/
Node Name	http://10.10.10.17:8080/students/
Метод	GET
Параметр	
Атака	
Свидетельство	
Дополнительная информация	
Экземпляры	Systemic
Решение	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Ссылка	https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Идентификатор	693
WASC ID	15
Идентификатор плагина	10038

Средний **Отсутствует заголовок (Header) для защиты от кликджекинга**

Описание	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	x-frame-options
Атака	
Свидетельство	
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/
Node Name	http://10.10.10.17:8080/courses/
Метод	GET
Параметр	x-frame-options
Атака	
Свидетельство	
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/robots.txt
Node Name	http://10.10.10.17:8080/robots.txt
Метод	GET
Параметр	x-frame-options
Атака	
Свидетельство	
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/sitemap.xml
Node Name	http://10.10.10.17:8080/sitemap.xml
Метод	GET
Параметр	x-frame-options
Атака	
Свидетельство	

Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/students/
Node Name	http://10.10.10.17:8080/students/
Метод	GET
Параметр	x-frame-options
Атака	
Свидетельство	
Дополнительная информация	
Экземпляры	Systemic
Решение	Современные веб-браузеры поддерживают Content-Security-Policy и заголовки HTTP X-Frame-Options.Убедитесь, что один из них установлен на всех веб-страницах, возвращаемых вашим сайтом/приложением.Если вы ожидаете, что страница будет обрамлена только страницами на вашем сервере (например, это часть FRAMESET), вам следует использовать SAMEORIGIN, в противном случае, если вы никогда не ожидаете, что страница будет обрамлена, вам следует использовать DENY.В качестве альтернативы рассмотрите возможность реализации директивы Content Security Policy «frame-ancestors».
Ссылка	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options
CWE Идентификатор	1021
WASC ID	15
Идентификатор плагина	10020

Средний **Уязвимость JS Библиотеки (Library)**

Описание	The identified library appears to be vulnerable.
URL-адрес	http://10.10.10.17:8080/static/js/jquery-3.2.1.min.js
Node Name	http://10.10.10.17:8080/static/js/jquery-3.2.1.min.js
Метод	GET
Параметр	
Атака	
Свидетельство	jquery-3.2.1.min.js
Дополнительная информация	The identified library jquery, version 3.2.1 is vulnerable. CVE-2020-11023 CVE-2020-11022 CVE-2019-11358 https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
Экземпляры	1
Решение	Upgrade to the latest version of the affected library.
Ссылка	https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/
CWE Идентификатор	1395

WASC ID	
Идентификатор плагина	10003
Низкий	**Cookie No HttpOnly Flag**
Описание	Файл cookie был установлен без флага HttpOnly, что означает, что к нему можно получить доступ с помощью JavaScript. Если на этой странице может быть запущен вредоносный сценарий, cookie будет доступен и может быть передан на другой сайт. Если это файл cookie сеанса, то возможен захват сеанса.
URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	Set-Cookie: AIOHTTP_SESSION
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/
Node Name	http://10.10.10.17:8080/
Метод	GET
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	Set-Cookie: AIOHTTP_SESSION
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/
Node Name	http://10.10.10.17:8080/ ()(_csrf_token,password,username)
Метод	POST
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	Set-Cookie: AIOHTTP_SESSION
Дополнительная информация	
Экземпляры	3
Решение	Убедитесь, что для всех файлов cookie установлен флаг HttpOnly.
Ссылка	https://owasp.org/www-community/HttpOnly

CWE Идентификатор	1004
WASC ID	13
Идентификатор плагина	10010

Низкий **Cookie без атрибута SameSite**

Описание	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	Set-Cookie: AIOHTTP_SESSION
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/
Node Name	http://10.10.10.17:8080/
Метод	GET
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	Set-Cookie: AIOHTTP_SESSION
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/
Node Name	http://10.10.10.17:8080/ ()(_csrf_token,password,username)
Метод	POST
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	Set-Cookie: AIOHTTP_SESSION
Дополнительная информация	
Экземпляры	3
Решение	Убедитесь, что для атрибута SameSite установлено значение «слабый» ('lax')или в идеальном случае «строгий» (strict') для всех файлов cookie.

Ссылка	https://datatracker.ietf.org/doc/html/draft-ietf-httpbis-cookie-same-site
CWE Идентификатор	1275
WASC ID	13
Идентификатор плагина	10054

Низкий **Заголовок X-Content-Type-Options отсутствует**

Описание

Для заголовка Anti-MIME-Sniffing X-Content-Type-Options не задано значение «nosniff».

Это позволяет более старым версиям Internet Explorer и Chrome выполнять MIME-сниффинг тела ответа, что может привести к интерпретации и отображению тела ответа как тип контента,

отличный от объявленного типа контента.

Текущая (начало 2014 г.) и устаревшая версии Firefox будут использовать объявленный тип содержимого (если он установлен), а не выполнять сниффинг MIME.

URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	x-content-type-options
Атака	
Свидетельство	
Дополнительная информация	Эта проблема по-прежнему относится к страницам с типами ошибок (401, 403, 500 и т. д.), Поскольку на эти страницы часто по-прежнему влияют проблемы с внедрением, и в этом случае по-прежнему существует проблема, связанная с тем, что браузеры отслеживают страницы с их фактическим типом содержимого. При пороговом значении «Высокий» ("High") это правило сканирования не будет предупреждать об ошибках клиента или сервера.
URL-адрес	http://10.10.10.17:8080/courses/
Node Name	http://10.10.10.17:8080/courses/
Метод	GET
Параметр	x-content-type-options
Атака	
Свидетельство	
Дополнительная информация	Эта проблема по-прежнему относится к страницам с типами ошибок (401, 403, 500 и т. д.), Поскольку на эти страницы часто по-прежнему влияют проблемы с внедрением, и в этом случае по-прежнему существует проблема, связанная с тем, что браузеры отслеживают страницы с их фактическим типом содержимого. При пороговом значении «Высокий» ("High") это правило сканирования не будет предупреждать об ошибках клиента или сервера.
URL-адрес	http://10.10.10.17:8080/robots.txt
Node Name	http://10.10.10.17:8080/robots.txt
Метод	GET

Параметр	x-content-type-options
Атака	
Свидетельство	
Дополнительная информация	Эта проблема по-прежнему относится к страницам с типами ошибок (401, 403, 500 и т. д.), Поскольку на эти страницы часто по-прежнему влияют проблемы с внедрением, и в этом случае по-прежнему существует проблема, связанная с тем, что браузеры отслеживают страницы с их фактическим типом содержимого. При пороговом значении «Высокий» ("High") это правило сканирования не будет предупреждать об ошибках клиента или сервера.
URL-адрес	http://10.10.10.17:8080/sitemap.xml
Node Name	http://10.10.10.17:8080/sitemap.xml
Метод	GET
Параметр	x-content-type-options
Атака	
Свидетельство	
Дополнительная информация	Эта проблема по-прежнему относится к страницам с типами ошибок (401, 403, 500 и т. д.), Поскольку на эти страницы часто по-прежнему влияют проблемы с внедрением, и в этом случае по-прежнему существует проблема, связанная с тем, что браузеры отслеживают страницы с их фактическим типом содержимого. При пороговом значении «Высокий» ("High") это правило сканирования не будет предупреждать об ошибках клиента или сервера.
URL-адрес	http://10.10.10.17:8080/students/
Node Name	http://10.10.10.17:8080/students/
Метод	GET
Параметр	x-content-type-options
Атака	
Свидетельство	
Дополнительная информация	Эта проблема по-прежнему относится к страницам с типами ошибок (401, 403, 500 и т. д.), Поскольку на эти страницы часто по-прежнему влияют проблемы с внедрением, и в этом случае по-прежнему существует проблема, связанная с тем, что браузеры отслеживают страницы с их фактическим типом содержимого. При пороговом значении «Высокий» ("High") это правило сканирования не будет предупреждать об ошибках клиента или сервера.
Экземпляры	Systemic
Решение	Убедитесь, что приложение / веб-сервер правильно задает заголовок Content-Type и что он устанавливает заголовок X-Content-Type-Options равным «nosniff» для всех веб-страниц. Если возможно, убедитесь, что конечный пользователь использует современный веб-браузер, соответствующий стандартам, который вообще не выполняет сниффинг MIME или который может быть направлен веб-приложением / веб-сервером, чтобы не выполнять сниффинг MIME.
Ссылка	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Идентификатор	693
WASC ID	15

Идентификатор плагина	10021
Низкий	**Раскрытие информации - сообщения об ошибках отладки**
Описание	Ответ, по-видимому, содержал типичные сообщения об ошибках, возвращаемые такими платформами, как ASP.NET, и веб-серверами, такими как IIS и Apache. Вы можете настроить список общих отладочных сообщений.
URL-адрес	http://10.10.10.17:8080/courses/1/review
Node Name	http://10.10.10.17:8080/courses/1/review ()(_csrf_token,review_text)
Метод	POST
Параметр	
Атака	
Свидетельство	Internal Server Error
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/2/review
Node Name	http://10.10.10.17:8080/courses/2/review ()(_csrf_token,review_text)
Метод	POST
Параметр	
Атака	
Свидетельство	Internal Server Error
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/3/review
Node Name	http://10.10.10.17:8080/courses/3/review ()(_csrf_token,review_text)
Метод	POST
Параметр	
Атака	
Свидетельство	Internal Server Error
Дополнительная информация	
Экземпляры	3
Решение	Отключите отладочные сообщения перед отправкой в производство.
Ссылка	

CWE Идентификатор	1295
WASC ID	13
Идентификатор плагина	10023

Низкий **Раскрытие ошибок приложения**

Описание

Эта страница содержит сообщение об ошибке / предупреждении, которое может раскрывать конфиденциальную информацию, такую как расположение файла, вызвавшего необработанное исключение. Эта информация может быть использована для дальнейших атак на веб-приложение. Предупреждение может быть ложным, если сообщение об ошибке находится на странице документации.

URL-адрес	http://10.10.10.17:8080/courses/1/review
Node Name	http://10.10.10.17:8080/courses/1/review ()(_csrf_token,review_text)
Метод	POST
Параметр	
Атака	
Свидетельство	HTTP/1.1 500 Internal Server Error
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/2/review
Node Name	http://10.10.10.17:8080/courses/2/review ()(_csrf_token,review_text)
Метод	POST
Параметр	
Атака	
Свидетельство	HTTP/1.1 500 Internal Server Error
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/3/review
Node Name	http://10.10.10.17:8080/courses/3/review ()(_csrf_token,review_text)
Метод	POST
Параметр	
Атака	
Свидетельство	HTTP/1.1 500 Internal Server Error
Дополнительная информация	
Экземпляры	3
Решение	Просмотрите исходный код этой страницы.

	Реализуйте настраиваемые страницы ошибок. Подумайте о реализации механизма для предоставления уникальной ссылки / идентификатора ошибки клиенту (браузеру), регистрируя при этом детали на стороне сервера и не раскрывая их пользователю.
Ссылка	
CWE Идентификатор	550
WASC ID	13
Идентификатор плагина	90022
Низкий	**Сервер утечка информации о версии через поле заголовка HTTP-ответа «Server»**
	Веб-сервер / сервер приложений передает информацию о версии через HTTP-заголовок ответа «Server».
Описание	Доступ к такой информации может облегчить злоумышленникам определение других уязвимостей, которым подвержен ваш веб-сервер / сервер приложений.
URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	
Атака	
Свидетельство	Python/3.7 aiohttp/3.5.3
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/courses/
Node Name	http://10.10.10.17:8080/courses/
Метод	GET
Параметр	
Атака	
Свидетельство	Python/3.7 aiohttp/3.5.3
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/robots.txt
Node Name	http://10.10.10.17:8080/robots.txt
Метод	GET
Параметр	
Атака	

Свидетельство	Python/3.7 aiohttp/3.5.3
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/sitemap.xml
Node Name	http://10.10.10.17:8080/sitemap.xml
Метод	GET
Параметр	
Атака	
Свидетельство	Python/3.7 aiohttp/3.5.3
Дополнительная информация	
URL-адрес	http://10.10.10.17:8080/students/
Node Name	http://10.10.10.17:8080/students/
Метод	GET
Параметр	
Атака	
Свидетельство	Python/3.7 aiohttp/3.5.3
Дополнительная информация	
Экземпляры	Systemic
Решение	Убедитесь, что ваш веб-сервер, сервер приложений, балансировщик нагрузки и т. д. настроен на подавление заголовка «Server» или предоставление общих сведений.
Ссылка	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Идентификатор	497
WASC ID	13
Идентификатор плагина	10036
Информационный	**Authentication Request Identified**
Описание	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL-адрес	http://10.10.10.17:8080/
Node Name	http://10.10.10.17:8080/ ()(_csrf_token,password,username)

Метод	POST
Параметр	username
Атака	
Свидетельство	password
Дополнительная информация	userParam=username userValue=ZAP passwordParam=password referer=http://10.10.10.17:8080 csrfToken=_csrf_token
Экземпляры	1
Решение	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Ссылка	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Идентификатор	
WASC ID	
Идентификатор плагина	10111

Информационный **Session Management Response Identified**

Описание	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL-адрес	http://10.10.10.17:8080
Node Name	http://10.10.10.17:8080
Метод	GET
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	AIOHTTP_SESSION
Дополнительная информация	cookie:AIOHTTP_SESSION
URL-адрес	http://10.10.10.17:8080/
Node Name	http://10.10.10.17:8080/
Метод	GET
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	AIOHTTP_SESSION
Дополнительная информация	cookie:AIOHTTP_SESSION
URL-адрес	http://10.10.10.17:8080/

Node Name	http://10.10.10.17:8080/ ()(_csrf_token,password,username)
Метод	POST
Параметр	AIOHTTP_SESSION
Атака	
Свидетельство	AIOHTTP_SESSION
Дополнительная информация	cookie:AIOHTTP_SESSION
Экземпляры	3
Решение	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Ссылка	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id/
CWE Идентификатор	
WASC ID	
Идентификатор плагина	10112

Информационный **Атрибут элемента HTML, управляемый пользователем (потенциальный XSS)**

Описание	Эта проверка проверяет вводимые пользователем данные в параметрах строки запроса и данных POST, чтобы определить, где можно управлять определенными значениями атрибутов HTML. Это обеспечивает обнаружение горячих точек для XSS (межсайтового сценария), который потребует дальнейшего изучения аналитиком безопасности для определения возможности использования.
URL-адрес	http://10.10.10.17:8080/
Node Name	http://10.10.10.17:8080/ ()(_csrf_token,password,username)
Метод	POST
Параметр	_csrf_token
Атака	
Свидетельство	
Дополнительная информация	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: http://10.10.10.17:8080/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: _csrf_token=a576dbd3228741468c1a876732d8b92a The user-controlled value was: a576dbd3228741468c1a876732d8b92a
Экземпляры	1
Решение	Проверяйте весь ввод и очищайте вывод перед записью в какие-либо атрибуты HTML.
Ссылка	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Идентификатор	20
WASC ID	20
Идентификатор плагина	10031

Информационный **Раскрытие информации - подозрительные комментарии**

Описание	The response appears to contain suspicious comments which may help an attacker.
URL-адрес	http://10.10.10.17:8080/static/js/jquery-3.2.1.min.js
Node Name	http://10.10.10.17:8080/static/js/jquery-3.2.1.min.js
Метод	GET
Параметр	
Атака	
Свидетельство	Db
Дополнительная информация	The following pattern was used: \bDB\b and was detected in likely comment: "//,Ib={},Jb={},Kb="*/".concat("*"),Lb=d.createElement("a");Lb.href=tb.href;function Mb(a){return function(b,c){"string"!=typeof ", see evidence field for the suspicious comment/snippet.
URL-адрес	http://10.10.10.17:8080/static/js/materialize.min.js
Node Name	http://10.10.10.17:8080/static/js/materialize.min.js
Метод	GET
Параметр	
Атака	
Свидетельство	select
Дополнительная информация	The following pattern was used: \bSELECT\b and was detected in likely comment: "//www.w3.org/2000/svg","rect"):i.createElement("div");b.init(c),t.myParent.appendChild(c),p.each(["overflow","overflowX","overfl", see evidence field for the suspicious comment/snippet.
Экземпляры	2
Решение	Удалите все комментарии, которые возвращают информацию, которая может помочь злоумышленнику, и устраните все основные проблемы, на которые они ссылаются.
Ссылка	
CWE Идентификатор	615
WASC ID	13
Идентификатор плагина	10027

Информационный	**Современное веб-приложение**
	Приложение выглядит как современное веб-приложение.
Описание	Если вам нужно изучить его автоматически, то Ajax Spider может оказаться более эффективным, чем стандартный.
URL-адрес	http://10.10.10.17:8080/favicon.ico

Node Name	http://10.10.10.17:8080/favicon.ico
Метод	GET
Параметр	
Атака	
Свидетельство	<script type="text/javascript" defer src="/static/js/jquery-3.2.1.min.js"></script>
Дополнительная информация	Ссылки не найдены пока есть скрипты, что свидетельствует о том, что это современное веб-приложение.
URL-адрес	http://10.10.10.17:8080/robots.txt
Node Name	http://10.10.10.17:8080/robots.txt
Метод	GET
Параметр	
Атака	
Свидетельство	<script type="text/javascript" defer src="/static/js/jquery-3.2.1.min.js"></script>
Дополнительная информация	Ссылки не найдены пока есть скрипты, что свидетельствует о том, что это современное веб-приложение.
URL-адрес	http://10.10.10.17:8080/sitemap.xml
Node Name	http://10.10.10.17:8080/sitemap.xml
Метод	GET
Параметр	
Атака	
Свидетельство	<script type="text/javascript" defer src="/static/js/jquery-3.2.1.min.js"></script>
Дополнительная информация	Ссылки не найдены пока есть скрипты, что свидетельствует о том, что это современное веб-приложение.
Экземпляры	3
Решение	Это информационное предупреждение, поэтому никаких изменений не требуется.
Ссылка	
CWE Идентификатор	
WASC ID	
Идентификатор плагина	10109

Sequence Details

With the associated active scan results.