Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет прикладной информатики

Дисциплина:

«Основы кибербезопасности»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №6

«Формирование CVSS-векторов и плана устранения уязвимостей, включая компенсирующие меры»

Выполнил:

Швалов Даниил Андреевич, студент группы K4112c

_____

(подпись)

Проверил:

Кравчук Алексей Владимирович, доцент практики

_____

(отметка о выполнении)

_____

(подпись)

Санкт-Петербург
2025 г.

СОДЕРЖАНИЕ

1 Введение

Цель работы:

1) закрепить навыки анализа отчётов сканеров безопасности (на примере Acunetix);

2) Получить навыки формирования векторов оценки уязвимостей по стандарту CVSS v4.0;

3) разработать план устранения выявленных проблем, включая компенсирующие меры (mitigation).

2 Ход работы

2.1 Анализ обнаруженных уязвимостей

В лабораторной работе №5 был получен список уязвимостей в веб-приложении OWASP Juice Shop. В отчете содержится как краткая сводка о найденных уязвимостях, так и полноценное описание того, где эти уязвимости были найдены, какие риски они несут и как их устранить. Это видно на рисунках 1-3.

Scan of 192.168.56.10:3000

Scan details

Scan information	
Start time	2025-10-12T13:16:10.803005+03:00
Start url	http://192.168.56.10:3000/
Host	192.168.56.10:3000
Scan time	46 minutes, 4 seconds
Profile	Full Scan
Responsive	True
Server OS	Unknown
Application build	25.5.250613157

Threat level

Acunetix Threat Level 4

One or more critical-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	22
Critical	2
High	0
Medium	10
Low	2
Informational	8

Рисунок 1 — Краткая сводка об уязвимостях

SQL Injection

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N Base Score: 9.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: High Integrity Impact to the Vulnerable System: High Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None

Рисунок 2 — Детальная информация о типе уязвимости

SQL Injection

Severity	**Critical**
Reported by module	/Scripts/PerScheme/Sql_Injection.script

Description

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

Recommendation

Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

References

SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection/)
Types of SQL Injection (SQLi) - Acunetix (https://www.acunetix.com/websitesecurity/sql-injection2/)
Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix (https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/)
SQL Injection - OWASP (https://www.owasp.org/index.php/SQL_Injection)
Bobby Tables: A guide to preventing SQL injection (https://bobby-tables.com/)
SQL Injection Cheet Sheets - Pentestmonkey (http://pentestmonkey.net/category/cheat-sheet/sql-injection)

Affected items

/rest/products/search
Details
URL encoded GET input **q** was set to **""** Error message found: `near \"\"%' OR description LIKE '%'\"\": syntax error`

Рисунок 3 — Информация о месте, в котором есть уязвимость, а также предложения по устранению

Среди полученных уязвимостей были выделены следующие уязвимости, имеющие уровни критичности High, Medium и Low соответственно:

1) SQL Injection;

2) Open Redirection;

3) Unrestricted access to Prometheus Metrics.

Описание данных уязвимостей, т. е. тип, место возникновения и потенциальное воздействие, представлено в таблице 1.

Таблица 1 — Описание уязвимостей

Название уязвимости	**Тип уязвимости**	**Место возникновения**	**Потенциальное воздействие**
SQL Injection	CWE-89	В веб-приложении в обработчиках /rest/products/search, /rest/user/login пользовательский ввод не проверяется и не экранируется, из-за чего появляется возможность инъекции стороннего SQL-кода при запросах в БД	Злоумышленник получает несанкционированный доступ к чтению, изменению или удалению данных. Это может повлечь утечку, кражу или полное удаление данных
Open Redirection	CWE-601	Веб-приложение не обрабатывает пользовательский ввод в ссылках, из-за чего возникает возможность перенаправления пользователей на сторонние ресурсы	Реализация фишинговых атак, распространение ВПО, кража чувствительных данных

Unrestricted access to Prometheus Metrics	CWE-200	В веб-приложении на том же порту, на котором обрабатываются основные пользовательские запросы, открыт обработчик /metrics, позволяющий получить метрики в формате Prometheus. Обработчик доступен без аутентификации и авторизации	В метриках Prometheus может содержаться чувствительная информация, с помощью которой злоумышленник может нанести вред. Например, в метрики может записываться информация о созданных заказах, об используемых ресурсах и т. п.

Для данных уязвимостей были сформированы следующие базовые CVSS v4.0-векторы:

1) SQL Injection — CVSS:4.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H, где

— Attack Vector — Network, поскольку атака реализуется по сети через протокол HTTP;

— Attack Complexity — Low, поскольку для атаки не требуется подготовки, глубоких знаний инфраструктуры или инсайдеров, достаточно сделать HTTP-запрос;

— Privileges Required — None, поскольку атака может быть совершена с помощью поиска или формы логина в аккаунт, где не требуется иметь каких-либо привилегий;

— User Interaction — None, поскольку не требуется какого-либо специального взаимодействия с другими пользователями;

— Scope — Changed, поскольку уязвимость предоставляет злоумышленнику возможность изменять данные, хранимые в БД;

— Confidentiality — High, поскольку злоумышленник получает практически неограниченный доступ ко всем данным;

— Integrity — High, поскольку данные могут быть простым способом искажены;

— Availability — High, поскольку данная атака может привести к нарушению доступности.

2) Open Redirection — CVSS:4.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N, где

— Attack Vector — Network, поскольку атака реализуется по сети через протокол HTTP;

— Attack Complexity — Low, поскольку для атаки не требуется подготовки, глубоких знаний инфраструктуры или инсайдеров, достаточно сделать HTTP-запрос;

— Privileges Required — None, поскольку атака может быть совершена с помощью главной страницы, где не требуется иметь каких-либо привилегий;

— User Interaction — None, поскольку не требуется какого-либо специального взаимодействия с другими пользователями;

— Scope — Unchanged, поскольку уязвимость не позволяет воздействовать на недоступные ресурсы;

— Confidentiality — Low, поскольку данная атака не открывает прямой несанкционированный доступ к данным, только через фишинг;

— Integrity — Low, поскольку данная атака не нарушает целостность данных напрямую, только через фишинг;

— Availability — None, поскольку данная атака не влияет напрямую на доступность данных.

3) Unrestricted access to Prometheus Metrics — CVSS:4.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N, где

— Attack Vector — Network, поскольку атака реализуется по сети через протокол HTTP;

— Attack Complexity — Low, поскольку для атаки не требуется

подготовки, глубоких знаний инфраструктуры или инсайдеров, достаточно сделать HTTP-запрос;

— Privileges Required — None, поскольку обработчик доступен без аутентификации или авторизации;

— User Interaction — None, поскольку не требуется какого-либо специального взаимодействия с другими пользователями;

— Scope — Unchanged, поскольку уязвимость не позволяет воздействовать на недоступные ресурсы;

— Confidentiality — Low, поскольку атака позволяет получить доступ к очень ограниченному количеству данных, чаще всего эти данные не очень чувствительные;

— Integrity — None, поскольку данная атака не нарушает целостность данных;

— Availability — None, поскольку данная атака не нарушает доступность данных.

Для данных уязвимостей рассчитана оценка с помощью калькулятора FIRST. Результаты представлены на рисунках 4-6.

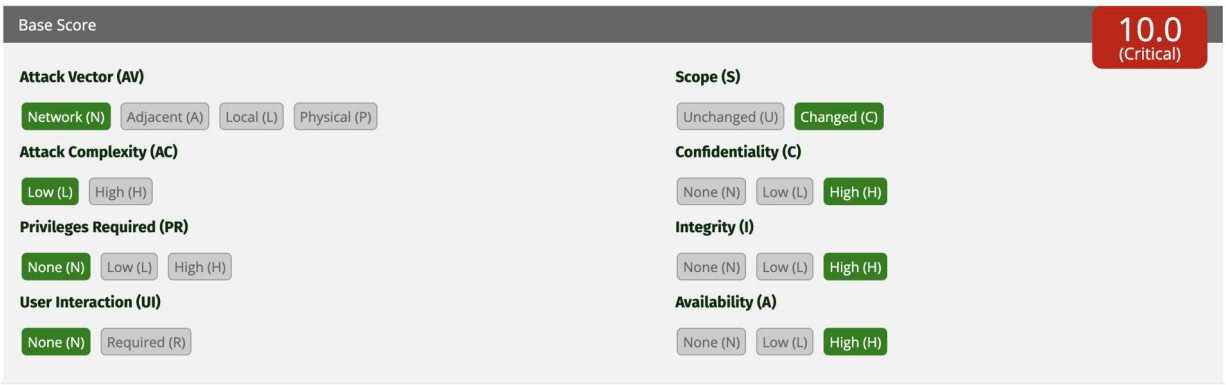

Рисунок 4 — Оценка уязвимости SQL Injection

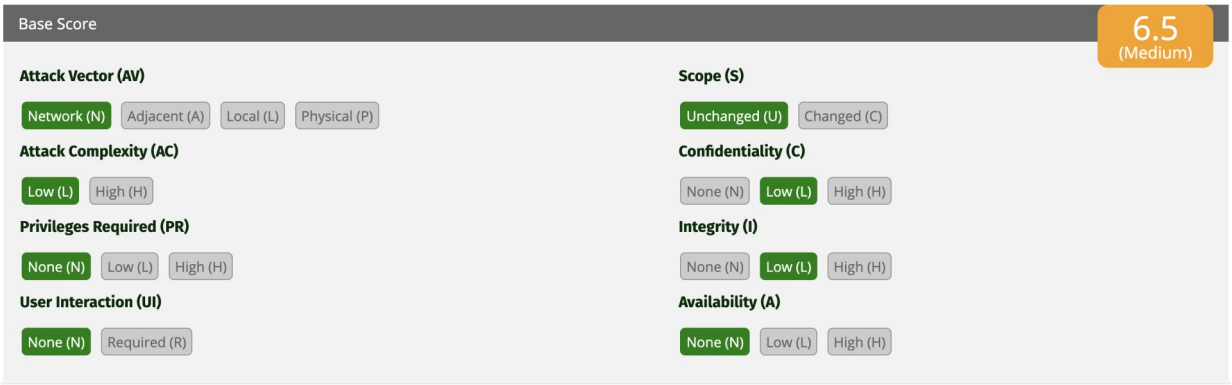

Рисунок 5 — Оценка уязвимости Open Redirection

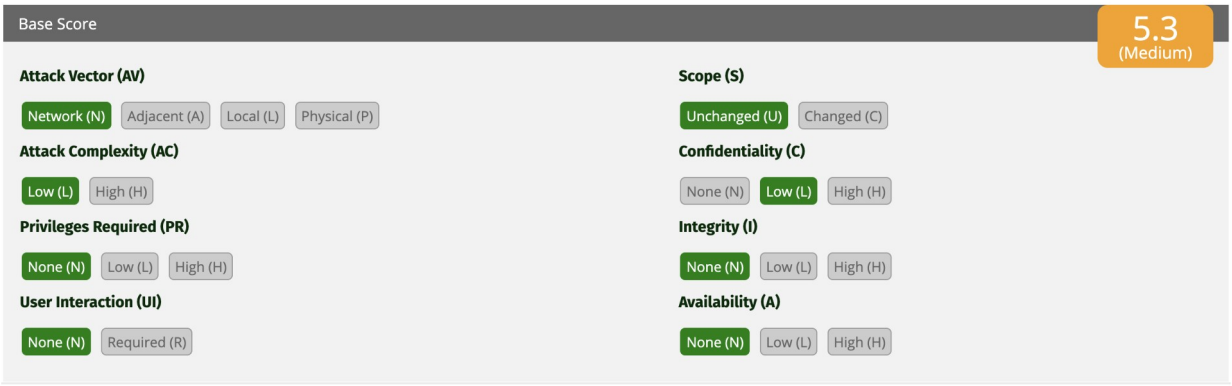

Рисунок 6 — Оценка уязвимости Unrestricted access to Prometheus Metrics

2.2 Анализ типов уязвимостей

Анализ трех выбранных типов уязвимостей, т. е. описание и их реализация в Juice Shop, представлен в таблице 2.

Таблица 2 — Типы уязвимостей

Тип уязвимости	Описание	Реализация в Juice Shop
CWE-89	Внедрение вредоносный SQL-код в запросы к базе данных через форму запроса или URL-адрес	Обработчики /rest/products/search и /rest/user/login в Juice Shop позволяют реализовать SQL-инъекцию
CWE-319	Приложение позволяет передачу данных в открытом (незашифрованном) виде	Juice Shop позволяет получать и отправлять данные по протоколу HTTP без шифрования (т. е. без

		HTTPS)
CWE-1395	Приложение имеет зависимость (например, использует определенную версию библиотеки), в которой есть известные уязвимости	Juice Shop использует устаревшую версию jQuery, которая содержит различные уязвимости, позволяющие реализовать, например, XSS-атаки

2.3 Составление плана устранения уязвимостей

В таблице 3 представлен план по устранению выявленных с помощью Acunetix уязвимостей.

Таблица 3 — План устранения уязвимостей в Juice Shop

№ п/п	**Приоритет**	**Уязвимость**	**Действия для устранения**	**Компенсирующие меры**	**Ответственный**
1	Высокий	SQL Injection	Добавление проверки пользовательского ввода на наличие инъекций	Использование API и оберток, предотвращающих возможность инъекций	Разработчик Backend
2	Высокий	Sensitive Data Exposure	Убрать доступ к API ключам	Не хранить и не передавать API ключи в открытом виде	Разработчик Backend
3	Высокий	Insecure HTTP Usage, SSL/ TLS Not Implemented	Настроить перенаправление с HTTP на HTTPS	Запрет использования HTTP без шифрования	Системный администратор
4	Средний	Vulnerable JavaScript	Обновить версию jQuery и	Регулярно обновлять версию	Разработчик Frontend

		libraries, jQuery Improper Neutralization of Input During Web Page Generation	других зависимостей	jQuery и других зависимостей, следить за актуальными уязвимостями в библиотеках	
5	Средний	Open Redirection	Использовать белый список доменов для перенаправления	Использовать безопасные API, использовать белые списки доменов, использовать токены для защиты перенаправлений	Разработчик Backend
6	Средний	Cross site scripting	Добавить проверку пользовательского ввода на XSS	Использовать безопасные API и обертки, предотвращающие XSS	Разработчик Frontend
7	Средний	Access-Control-Allow-Origin header with wildcard (*) value	Ограничить список Access-Control-Allow-Origin белым списком доменов	Запретить использовать * в Access-Control-Allow-Origin	Системный администратор
8	Средний	Content Security Policy (CSP) Not Implemented	Реализовать CSP политику	Проверять, что CSP политика реализована	Разработчик Backend
9	Средний	Generic Email Address Disclosure	Не показывать email пользователей	Проверять, что персональные данные пользователей не доступны кому	Разработчик Backend

				попало	
10	Низкий	Internal Path Disclosure	Блокировать доступ к страницам, к которому доступа быть не должно	Использовать непоследовательные идентификаторы (например, UUID вместо INT), блокировать доступ к страницам, к которому доступа быть не должно	Разработчик Backend
11	Низкий	Unrestricted access to Prometheus Metrics	Вынести обработчик получения метрик Prometheus на отдельный порт, ввести белый список IP-адресов	Не использовать один и тот же порт для внутренних и внешних потребителей, внутренние обработчики ограничивать белым списком IP-адресов	DevOps

3 Вывод

В ходе выполнения данной лабораторной работы были закреплены навыки анализа отчётов сканеров безопасности, получены навыки формирования векторов оценки уязвимостей по стандарту CVSS v4.0, разработан план устранения выявленных проблем, включая компенсирующие меры.