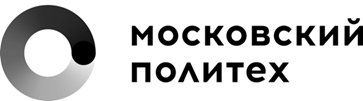
Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)



ЛАБОРАТОРНАЯ РАБОТА 9

**БЕЗОПАСНОСТЬ ВЕБ-ПРИЛОЖЕНИЙ**

По курсу

**Проектирование Веб-сервисов**

ВыполнилКилеев С.И**.**

**студент группы 211-321**

Проверил

Пардаев А.А.

Москва, 2024

**Лабораторная работа 9**

**Цель работы:** Изучить основные уязвимости веб-приложений.

**Задачи:**

Индивидуальная работа

1. Исследовать уязвимость из OWASP Топ 10 (номер уязвимости рассчитать по формуле\*):

a. Сколько и какие (привести два, три примера) CWE и CVE связаны с уязвимостью;

b. Перечислить способы предотвращения возможного использования уязвимости и выделить одно наиболее важное;

c. Исследовать одно связанное с уязвимостью CWE:

* Номер, название;
* Пример зафиксированного случая использования дефекта, отраженный в CVE (номер, описание).

2. Решить задачи по выявлению ошибок в коде, имеющих уязвимости:

**Отчёт по выполнению:**

1. Иссле довать уязвимость OWASP A06:2021-Vulnerable and Outdated Components (Уязвимые или устаревшие компоненты);
2. Сколько и какие (привести два, три примера) CWE и CVE связаны с уязвимостью.

С уязвимостью связаны 2 примера:

CWE-1104 Использование неподдерживаемых или устаревших компонентов сторонних производителей,

CVE-2021-44228 (Log4Shell)Критическая уязвимость в библиотеке Apache Log4j, позволяющая удалённое выполнение кода (RCE) через уязвимость в обработке строковых параметров.

1. Перечислить способы предотвращения возможного использования уязвимости и выделить одно наиболее важное;

**Инвентаризация компонентов**: Регулярное отслеживание и обновление используемых сторонних компонентов.

Мониторинг уязвимостей: Использовать инструменты для сканирования зависимостей на наличие известных уязвимостей (например, OWASP Dependency-Check или CVE).

Политика обновлений: Внедрить процесс обновления компонентов до безопасных версий.

1. Исследовать одно связанное с уязвимостью CWE:

CWE-89: SQL injection

CVE-2022–36635 — A SQL Injection in ZKSecurityBio to RCE

ZKSecurityBio содержит уязвимость SQL Injection, которая возникает при обработке небезопасного пользовательского ввода в SQL-запросах. Злоумышленник может внедрить вредоносный SQL-код в систему и выполнить команды в базе данных. При анализе работы приложения в среде было замечено, что приложение устанавливает свой собственный экземпляр postgres, то есть той версии ZKSecurity все используют одну и ту же версию базы данных, используя одного и того же пользователя, в данном случае: root. Было подтверждено, что версия PostgreSQL была уязвима для RCE «COPY FROM PROGRAM»

## **2. Решить задачи по выявлению ошибок в коде, имеющих уязвимости.**

Какой уязвимости подвержен следующий код (название и код из OWASP Top 10):

Уязвимость в данном коде связана с недостаточной аутентификацией и авторизацией. Это соответствует категории "Broken Access Control" из OWASP Top 10.

Конкретно, проблема заключается в том, что роль пользователя изменяется без должной аутентификации и авторизации. Функция changeUserRole(newRole) позволяет изменить роль пользователя на любую другую роль без каких-либо проверок, кто может вызвать эту функцию и какие права у него должны быть для выполнения такого действия.

Для исправления этой уязвимости необходимо внедрить должные проверки аутентификации и авторизации перед изменением роли пользователя. Это может включать в себя проверку подлинности пользователя (например, аутентификацию с использованием пароля или токена сеанса) и проверку его прав для выполнения операции изменения роли (авторизацию).

Какой уязвимости подвержен следующий код (название и код из OWASP Top 10):

Данный код подвержен уязвимости "Weak Encryption"(A02:2021-Cryptographic Failures ) из OWASP Top 10. Проблема заключается в использовании слабого ключа шифрования (в данном случае - "123456").

Использование слабого ключа шифрования делает систему уязвимой к атакам перебора ключа и атакам словарным методом

Для защиты от данной уязвимости необходимо использовать достаточно длинные и случайные ключи шифрования, а также регулярно обновлять их.

Какой уязвимости подвержен следующий код (название и код из OWASP Top 10):

Данный код подвержен уязвимости "Cross-Site Scripting (XSS)" (A03:2021-Injection) из OWASP Top 10. Проблема заключается в том, что пользовательский ввод (переменная userInput) прямо встраивается в HTML-код страницы без достаточной фильтрации или экранирования.

Это позволяет злоумышленнику внедрить вредоносный JavaScript код (в данном случае вызов алерта), который будет выполнен в контексте пользовательского браузера при открытии страницы. Это может привести к различным атакам, включая кражу сессий, перенаправление пользователя на фальшивые сайты, или даже выполнение действий от имени пользователя.

Чтобы защититься от этой уязвимости, необходимо правильно обрабатывать пользовательский ввод, например, путем экранирования специальных символов или использования Content Security Policy (CSP), который ограничивает источники выполнения JavaScript на странице.