К. С. Кручковский, А. Ш. Хакимов, И. П. Петров
Тюменский государственный университет, г. Тюмень
УДК 004.056

АКТУАЛЬНЫЕ ВЕБ-УЯЗВИМОСТИ И СПОСОБЫ ЗАЩИТЫ ОТ НИХ

Аннотация. В данной статье обсуждается важность обнаружения и устранения уязвимостей в веб-ресурсах, поскольку злоумышленники используют эти уязвимости для реализации тактики первоначального доступа.

Ключевые слова: информационная безопасность, веб-уязвимость, веб-атака, эксплуатация веб-уязвимостей, сканирование веб-уязвимостей.

Введение. Показатель использования различных эксплуатаций уязвимостей растет с каждым днем. В России этот показатель усугубляется еще и тем, что иностранные IT-компании ушли из страны и прекратили поставлять новые версии и обновления своего программного обеспечения (далее ПО), наибольшую опасность представляют эксплуатации веб-уязвимостей, что может оказаться начальной точкой для развития масштабной атаки [1].

Обеспечение безопасности веб-приложений включает комплекс мер, направленных на предотвращение несанкционированного доступа к конфиденциальной информации как извне, так и изнутри компании [2]. Это сложная задача, которая включает множество аспектов, связанных как с сетевыми службами, так и с особенностями веб-продуктов. Важными аспектами безопасности веб-приложений являются безопасность веб-сервера и его настройки в качестве службы, а также безопасность скриптов, реализующих основные функции приложения [3].

В настоящий момент из-за стремления достичь доступности своих сервисов в компаниях появляются «обязательные» части инфраструктуры, ими могут выступать веб-сервер, облачные хранилища, почтовый сервер и т. д. Доступность данных активов компании сопутствует появлению различных уязвимостей в их веб-ресурсах. Ознакомление с актуальными уязвимостями и способами их решений может помочь справиться с угрозами и предотвратить возможные атаки злоумышленников [4].

Также увеличение количества взломанных веб-ресурсов можно объяснить наличием уязвимостей, возникающих из-за неправильной проверки входных данных, недостаточной проверки результатов, применения неправильных методов программирования и ошибок кодирования [5]. Динамические сканеры уязвимостей, хотя и способны обнаружить некоторые уязвимости с помощью интерактивного подхода, часто не улавливают критические уязвимости, которые могут быть выявлены статическим подходом. Статические сканеры уязвимостей, хотя требуют значительных затрат времени, эффективно выявляют сложные уязвимости и способствуют улучшению навыков разработчиков в области программирования и передовых практик [6]. Современные сканеры обычно объединяют и динамический, и статический подходы, позволяя разработчикам выбирать подход в зависимости от их конкретных требований и условий.

Проблема исследования. Увеличение числа атак, направленных на веб-ресурсы, связано с активностью со стороны хактивистов — непрофессиональных хакеров, преследующих продвижение политических идей, а не коммерческие мотивы. Вызван такой рост целью хактивистов — создать массовую панику пользователей/граждан.

Цель данного исследования — рассмотреть актуальные уязвимости, которые часто используют злоумышленники для атак на веб-ресурсы компаний. Для достижения данной цели были поставлены следующие задачи:

1. Проанализировать и выявить наиболее актуальные эксплуатации уязвимостей на российские компании.

2. Изучить характеристики и принципы работы каждой из актуальных уязвимостей.

3. Рассмотреть способы защиты от каждой из уязвимостей и представить практические рекомендации по обеспечению безопасности веб-ресурсов.

Материалы и методы. Для проведения исследования были исследованы атаки, направленные на инфраструктуры крупных российских компаний, а также получены данные из открытых источников [1, 7, 8], таких как научные статьи и отчеты об информационной безопасности.

По итогам анализа эксплуатируемых уязвимостей было выявлено 14 типов актуальных уязвимостей веб-приложений (рис. 1) и рекомендации для них (табл. 1).

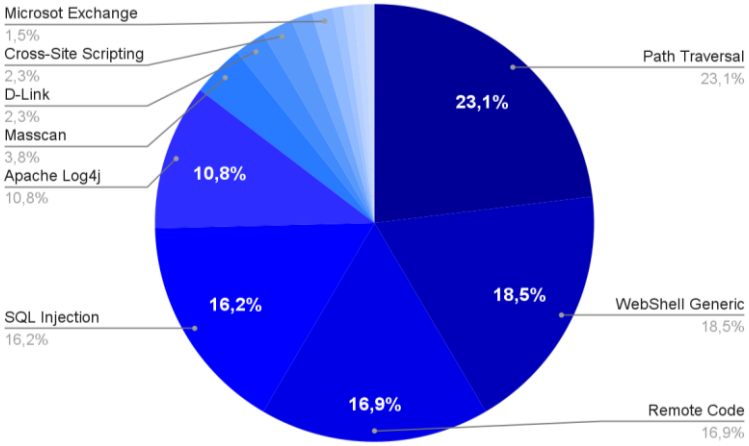

Рис. 1. Актуальные веб-уязвимости

Таблица 1

Уязвимости веб-ресурсов и способы защиты от них

Определение	*Способы защиты*
1	*2*
Path Traversal — позволяет злоумышленникам обходить защиту и получать доступ к файлам и директориям, находящимся за пределами корневой директории веб-сервера. Злоумышленники могут использовать Path Traversal для чтения, записи или удаления файлов, а также для выполнения команд на сервере	1) Проверка входных данных (фильтрация специальных символов); 2) Использование квотирования при работе с файлами и директориями; 3) Проверка наличия и доступности запрашиваемых файлов и директорий; 4) При возможности — отключение непосредственного доступа к файловой системе.

Продолжение табл. 1

1	*2*
WebShell Generic (wget) — позволяет злоумышленникам загружать и выполнять свой код на сервере	1) Мониторинг файловой системы на наличие web-shell скриптов; 2) Ограничение доступа к файловой системе для web-сервера; 3) Установка правильных прав доступа к файлам и директориям; 4) Фильтрация системных команд; 5) При возможности — запретить осуществление исходящих подключений сервером.
Remote Code Execution — позволяет злоумышленникам выполнить код на сервере удаленно, без необходимости иметь прямой доступ к серверу. Часто RCE уязвимости связаны с неправильным входным фильтром или обработкой входных данных на стороне сервера, что позволяет злоумышленникам внедрять и выполнять свой собственный код на сервере	1) Установка ПО только из надежных источников; 2) Регулярные обновления и патчи установленного ПО; 3) Фильтрация блоков кода.
SQL Injection — позволяет злоумышленнику производить различные несанкционированные действия с базой данных, похищая информацию, а также изменяя или удаляя данные, хранящиеся в приложении	1) Использование параметризованных запросов; 2) Фильтрация и валидация входных данных; 3) Ограничение доступа к базе данных для web-сервера.
Apache Log4j (CVE-2021-44228) — связана с логированием и обработкой логов на стороне сервера. Уязвимость может быть использована злоумышленниками для выполнения удаленного кода на сервере, используя специально сформированные логи, которые содержат зловредный код	1) Установка последней версии Apache Log4j и регулярные обновления; 2) Ограничение доступа к серверу и к файлам логов; 3) Мониторинг логов на наличие аномалий.

Продолжение табл. 1

1	*2*
Masscan — массовое сканирование используется для обнаружения уязвимых систем и приложений, которые могут быть атакованы	1) Регулярные сканирования на наличие уязвимостей, открытых портов и мониторинг общего состояния системы; 2) Установка файрволла и других инструментов защиты, таких как IDS/IPS; 3) Установка ограничений на количество входящих подключений от одного адреса; 4) Регулярное обновление баз систем защиты.
D-Link (CVE-2022-26258) — была обнаружена в маршрутизаторах D-Link. Уязвимость позволяет злоумышленникам выполнить произвольный код на устройстве без необходимости аутентификации. Это может привести к удаленному доступу к устройству и получению контроля над сетью, на которой оно находится	1) При возможности — обновление прошивки до последней версии, в ином случае замена на поддерживающиеся оборудование; 2) Ограничение доступа к управлению маршрутизатором через интернет; 3) Изменение учетных данных для входа в управление маршрутизатором; 4) Фильтрация сетевого трафика, ограничение доступа к уязвимым файлам/директориям.
Cross-Site Scripting (XSS) — связанная с обработкой пользовательского ввода на стороне клиента. Уязвимость позволяет злоумышленникам выполнять произвольный код на клиентской стороне, что может привести к краже конфиденциальной информации, перенаправлению на зловредные сайты и другим опасным действиям	1) Фильтрация и валидация входных данных; 2) Использование Content Security Policy (CSP); 3) Использование XSS фильтров.

Продолжение табл. 1

1	*2*
Zimbra (CVE-2022-27925, CVE-2022-41352) — связана с электронной почтой и календарем, используемыми многими компаниями. Уязвимость позволяет злоумышленникам получать доступ к электронной почте и календарю пользователей без необходимости аутентификации. Это может привести к утечке конфиденциальной информации, а также к выполнению произвольного кода на сервере	1) Установка последней версии Zimbra и регулярные обновления; 2) Мониторинг логов на наличие аномалий; 3) Регулярное резервное копирование данных
Microsoft Exchange (CVE-2022-41082) — связана с неправильной обработкой входных данных при работе с почтовыми ящиками на сервере Exchange, что позволяет злоумышленникам получать удаленный доступ к серверу и выполнять произвольный код на сервере	1) Многофакторная аутентификация; 2) Применить патчи безопасности; 3) Отключить неиспользуемые функции; 4) Использовать сетевой экран для ограничения доступа к Exchange серверу; 5) Ограничить доступ к административным интерфейсам
Buffer Overflow — возникает при обработке входных данных на стороне сервера. Злоумышленник может отправить слишком большой объем данных, что приведет к переполнению буфера и выполнению зловредного кода на сервере	1) Использовать защитные механизмы, такие как DEP и ASLR; 2) Проверять входные данные на наличие вредоносного кода; 3) Использовать компиляторы с поддержкой безопасности, такие как GCC с флагом -fstack-protector; 4) Ограничить размер передаваемых данных
Php Shell Upload 3 — связана с возможностью загрузки вредоносных файлов на сервер через уязвимые страницы загрузки файлов. Злоумышленник может загрузить на	1) Проверять загружаемые файлы на содержимое; 2) Ограничить доступ к директории, в которой размещаются загружаемые файлы;

Продолжение табл. 1

1	*2*
сервер зловредный PHP-скрипт, который будет выполняться на сервере при обращении к нему	3) Использовать средства аутентификации для повышения безопасности; 4) Фильтрация передаваемых php-скриптов
Cisco RV320/RV325 Config Disclosure Attempt (CVE-2019-1653) — позволяет злоумышленникам получить удаленный доступ к устройству Cisco RV	1) Обновлять устройство до последней версии ПО; 2) Ограничить доступ к административным интерфейсам устройства; 3) Использовать средства аутентификации для повышения безопасности

Исходя из этого можно выделить общие рекомендации, направленные на защиту веб-ресурсов:

1) Внедрение и настройка:

a) межсетевого экрана баз данных (DBF), приложений (WAF) и/или нового поколения (NGFW);

b) средств активного мониторинга баз данных (DAM);

c) средств автоматического детектирования (IDS) и реагирования (IPS) на уязвимости;

d) средств антивирусной защиты.

2) Систематические обнаружения и анализ уязвимостей в информационных системах и приложениях с целью выявления и предотвращения потенциальных уязвимостей;

3) Регулярное обновление устройств и программного обеспечения до актуальных версий;

4) Разграничение прав пользователей (распределение пользователей по группам и создание учетной записи для каждой группы и пользователя в соответствии с их правами, авторизация пользователей, запрет доступа к определенным объектам);

5) Обеспечение многофакторной аутентификации, сложных паролей, а также их периодическое обновление;

6) Сегментация сети с ограничением DMZ и основной зон инфраструктуры;

7) Закрытие и ограничение неиспользуемых портов и протоколов;

8) Для мониторинга и обнаружение кибератак, а также реагирование на них — стоит развернуть внутренний и/или внешний центр реагирования на инциденты (SOC).

Также рекомендации для быстрого реагирования на инциденты:

1) Полная (частичная) блокировка внешнего IP-адреса (диапазона IP-адресов) средствами МЭ;

2) Ограничение доступа атакующего источника к критичным портам, опубликованным в сети Интернет;

3) Проведение внепланового сканирования атакуемого ресурса на предмет наличия нерегламентированных открытых портов и наличия активных (непропатченных) уязвимостей;

4) Устранение выявленных уязвимостей.

Результаты. В результате исследования были выявлены основные характеристики и принципы работы каждой из актуальных веб-уязвимостей. Были рассмотрены способы защиты от каждой из уязвимостей, включая обновление программного обеспечения и установку дополнительных мер безопасности, на основе которых разработаны соответствующие рекомендации.

Заключение. В заключение, необходимо отметить, что актуальные уязвимости веб-ресурсов могут привести к серьезным последствиям, поэтому обеспечение безопасности в веб-системах является одной из наиболее важных задач для любой компании или организации. В данной статье были рассмотрены основные угрозы безопасности, способы защиты от них и рекомендации по обеспечению безопасности. Важно помнить, что безопасность веб-ресурсов — это постоянный процесс, и необходимо постоянно следить за новыми уязвимостями и принимать меры для их предотвращения.

СПИСОК ЛИТЕРАТУРЫ

1. Какие уязвимости будут главными угрозами в 2023 году. — Текст : электронный // Positive Technologies: [сайт]. — URL: https://www.

ptsecurity.com/ru-ru/about/news/positive-technologies-kakie-uyazvimosti-budut-glavnymi-ugrozami-v-2023-godu/ (дата обращения: 28.04.2023).
2. Кондауров С. Н. Актуальные угрозы цифровых сервисов / С. Н. Кондауров, А. В. Митрофанов. — Текст : непосредственный // Современные информационные технологии и информационная безопасность. — Курск : Юго-Западный государственный университет, 2023. — С. 46-49.
3. Кодацкий, Н. М. Решения в кибербезопасности / Н. М. Кодацкий, И. А. Муратов. — Текст : непосредственный // Научно-образовательный журнал для студентов и преподавателей «StudNet». — 2022. — № 1. — С. 615-622.
4. Анализ типовых уязвимостей при построении веб-приложений / М. М. Путято, А. М. Самвелович, В. В. Лещенко, В. О. Немчинова. — Текст : непосредственный // Ежеквартальный рецензируемый, реферируемый научный журнал «Вестник АГУ». — 2022. — № 3. — С. 77-85.
5. Прошина, Т. Д. Анализ сетевых атак и их проявлений / Т. Д. Прошина, Н. А. Сальникова. — Текст : непосредственный // Тенденции развития науки и образования. — 2022. — № 2. — С. 29-33.
6. Челухин В. А. Сетевые уязвимости / В. А. Челухин, Е. П. Душкин. — Текст : непосредственный // Наука, инновации и технологии: от идей к внедрению. — Комсомольск-на-Амуре : Комсомольский-на-Амуре государственный университет, 2022. — С. 300-302.
7. Кибератаки на российские компании в 2022 году. — Текст : электронный // Ростелеком солар : [сайт]. — URL: https://rt-solar.ru/analytics/reports/3332/ (дата обращения: 31.05.2023).
8. Exploit Public-Facing Application. — Текст : электронный // Mittre Att&ck: [сайт]. — URL: https://attack.mitre.org/techniques/T1190/ (дата обращения: 31.05.2023).