Инженерный вестник Дона, №2 (2024)
ivdon.ru/ru/magazine/archive/n2y2024/9017

Обнаружение уязвимостей и применение методов обеспечения безопасности веб-сайта

Нгуен Фук Хау[1], Ле Дюк Хуи[1], Нгуен Тхуй Чанг[1], Р.С. Зарипова[2]

[1]Университет Тхань До, Ханой, Вьетнам
[2]Казанский государственный энергетический университет, Казань

Аннотация: Уязвимости в безопасности всегда являются актуальной проблемой, на исследование которой администраторы веб-сайтов тратят много времени в целях обеспечения безопасности их работы. Эти уязвимости позволяют хакерам использовать, атаковать, проникать и влиять на данные веб-сайтов любых компаний. Для стабильной, бесперебойной и безопасной работы веб-сайта необходимо знать основную информацию об уязвимостях в безопасности онлайн-платформ. Данная статья посвящена анализу методов обнаружения уязвимостей веб-сайтов и применению эффективных мер по обеспечению их безопасности. В статье приводятся актуальные задачи в области информационной безопасности, описываются методы обнаружения уязвимостей и даны рекомендации по применению конкретных мер по безопасности веб-сайтов.
Ключевые слова: безопасность веб-сайтов, уязвимость, защита информации, код, программное обеспечение, сканирование уязвимостей безопасности.

С ростом числа интернет-пользователей и развитием цифровой экономики вопрос обеспечения безопасности онлайн-платформ становится все более актуальным. Уязвимости веб-сайтов могут привести к краже конфиденциальной информации, взлому сайта или другим серьезным проблемам, поэтому обнаружение и устранение уязвимостей есть важная задача для владельцев веб-сайтов и специалистов по информационной безопасности [1]. Обеспечение безопасности веб-сайтов является сложной задачей, требующей постоянного мониторинга и реагирования на уязвимости [2]. В данной статье будет рассмотрено обнаружение уязвимостей и применение методов обеспечения безопасности веб-сайта на основе современных технологий и методик.

Целью данной статьи является представление комплексного подхода к обеспечению безопасности веб-сайтов на основе обнаружения уязвимостей и применения соответствующих методов защиты. Новизна данной работы заключается в анализе и объединении современных методов обнаружения

уязвимостей с передовыми подходами к обеспечению безопасности веб-сайтов, что позволяет получить комплексное представление о проблеме и ее решениях. Для достижения поставленной цели необходимо выполнение следующих задач: изучение методов обнаружения уязвимостей веб-сайтов; анализ основных угроз и уязвимостей, с которыми сталкиваются веб-сайты; предложение эффективных методов обеспечения безопасности веб-сайтов на основе обнаруженных уязвимостей; демонстрация практических примеров успешной реализации методов обеспечения безопасности.

Любой веб-сайт может стать целью хакерских атак [3, 4]. Тестирование безопасности – это чрезвычайно важная деятельность по обеспечению безопасности веб-сайта во время его эксплуатации. Это одна из необходимых процедур, помогающая построить надежную систему сетевой безопасности, которая позволит избежать рисков и ущерба в случае хакерских атак. Поэтому тестирование безопасности веб-сайтов является предметом серьезной озабоченности для всех компаний [5]. Эта проверка помогает заранее обнаружить уязвимости в системе, а также угрозы безопасности, с которыми сталкивается веб-сайт.

Уязвимость веб-сайта – это дефект или ошибка программного кода, неправильная конфигурация системы или какая-либо другая слабость веб-сайта, веб-приложения или его компонентов и процессов. Уязвимости веб-приложений позволяют злоумышленникам получить несанкционированный доступ к системам, процессам или важнейшим активам компаний [6]. Имея такой доступ, злоумышленники могут организовывать атаки, захватывать приложения, участвовать в повышении привилегий для кражи данных, вызывать масштабные сбои в работе служб и т. д.

Рассмотрим причины возникновения уязвимостей. Любой элемент технологии будет содержать уязвимости [7]. Конечно, не существует никаких указаний на то, сколько уязвимостей может иметь каждый из них. Однако

очень грубый метод определения количества возможных уязвимостей основан на количестве строк кода. Другими словами, чем больше строк кода, тем больше количество возможных уязвимостей. Так называемая средняя плотность дефектов. Согласно исследованию, проведенному компанией Coverity, специализирующейся в области информационной безопасности, количество дефектов на 1000 строк кода оценивается в 0,62.

Основной причиной постоянных и повторяющихся уязвимостей веб-сайтов и веб-приложений по словам директора Masergy Communications и бывшего сборщика разведданных NSA является сильно модифицированный или полностью разработанный по индивидуальному заказу характер этих технологий. Результатом являются в основном непроверенные сайты и приложения, которые не проходят такое же строгое и тщательное тестирование, как большинство коммерческих пакетов программного обеспечения, таких как операционные системы и серверные пакеты [8, 9].

Чтобы иметь эффективные меры защиты веб-сайтов, сначала необходимо знать уязвимости, которые часто встречаются на веб-сайтах [10]. Поэтому необходимо действовать как настоящий хакер и для сканирования уязвимостей безопасности веб-сайта можно выполнить следующие шаги:

1. Сбор информации о веб-сайте. Необходимо собрать информацию о веб-сайте, а именно: платформа разработки веб-сайта, язык программирования веб-сайта, операционная система [11]. Также можно использовать веб-сайт онлайн-проверки, например, check-host.net для сбора информации об IP-адресе веб-приложения. Используются инструменты сканирования и сбора информации, такие, как Nmap, Nessus, OWASP ZAP.

2. Выполнение сканирования и получение предварительных результатов. Чтобы выполнить сканирование и сообщить о предварительных результатах, можно использовать инструменты, которые специализируются на сканировании уязвимостей веб-сайтов, например, приложение Nessus –

это собственный инструмент сканирования уязвимостей, разработанный компанией Tenable Cyber Security и выпущенный бесплатно для некоммерческого использования (рис. 1).

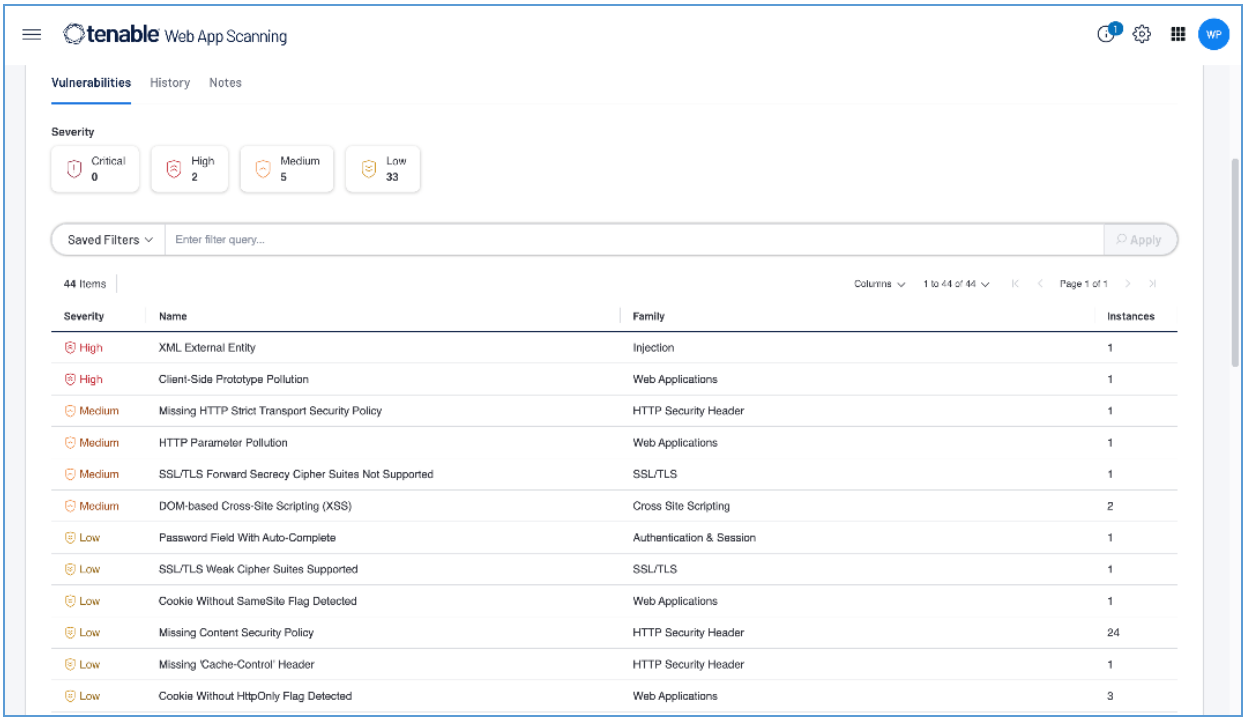

Рис. 1. – Результаты сканирования уязвимостей приложения Nessus

3. Оценка результатов предварительного сканирования. Когда предварительные результаты возвращаются из приложения Nessus, далее анализируются признаки уязвимостей, сравниваются уязвимости с информацией веб-сайта, чтобы устранить их. Ложные предупреждения, такие как уязвимости в результатах предварительного сканирования, которые появляются только в операционной системе Windows, но так как в качестве операционной системы веб-приложения используется Linux, то их можно удалить. Или, например, операционные системы, использующие PHP версии 8.0, вряд ли будут иметь исправленную ошибку, поскольку версия PHP 7.4 была анонсирована на домашней странице PHP.

4. Эксперименты с атаками и тестированием эксплойтов. Можно выполнять атаки и тестировать эксплойты с помощью инструментов

поддержки, таких, как Burp Suite, чтобы доказать существование и использование уязвимостей. Инструмент Burp Suite может блокировать цели веб-сайтов, сканировать веб-сайты и особенно моделировать атаки через разделы «Нарушитель» и «Повторитель» (рис. 2). При необходимости можно взять информацию о сканировании из отчета об испытаниях, прошедшего оценку на этапе 3, чтобы смоделировать атаку на веб-сайт, который требуется протестировать, чтобы обнаружить и подтвердить наличие уязвимости. Таким образом, можно определить сложность развертывания атак на уязвимости и серьезность уязвимостей безопасности.

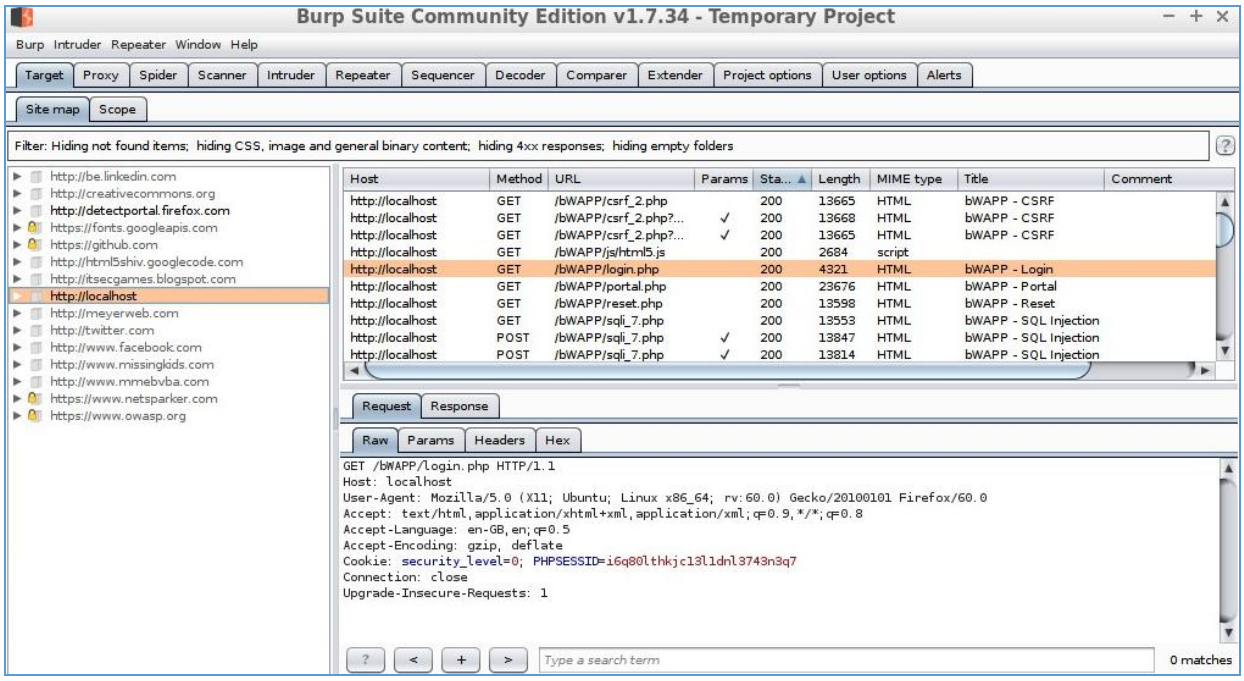

Рис. 2. – Интерфейс Burp Suite для тестирования веб-сайтов на уязвимость

5. Сообщение о результатах и рекомендациях по устранению. На этом этапе требуется обобщить информацию из всех пройденных этапов, чтобы суммировать количество уязвимостей, уровень серьезности и дать рекомендации по устранению уязвимостей на основе опыта пользователей или оценку информационной безопасности от разработчиков операционных систем, платформ веб-сайтов. Известно, что языки программирования также позволяют быстро устранять уязвимости безопасности веб-приложений.

Рассмотрим другие способы проверки уязвимостей сайта.

Метод локальной проверки. Это метод обнаружения уязвимостей путем непосредственной проверки исходного кода устройства и приложения, проверки и чтения библиотек (двоичных), таких как файлы .exe и т.д. Этот метод поможет точно обнаружить уязвимости безопасности и найти множество уязвимостей, которые не может обнаружить Remote Check. Однако он требует много времени и не может непрерывно проверять несколько целей одновременно.

Метод удаленной проверки. Метод удаленного обнаружения уязвимостей через сетевые протоколы, суть которого заключается в удаленном обнаружении уязвимостей. Поэтому он обнаруживает быстро, просто и сканирует множество целей одновременно, особенно не затрагивая работающие службы. Однако существует множество уязвимостей, которые Remote Check не может обнаружить.

Использование других инструментов сканирования уязвимостей безопасности. Обычно компании используют инструменты для сканирования уязвимостей [10]. Это облегчает процесс подключения к веб-приложениям через интерфейс. В то же время гораздо проще найти потенциальные уязвимости и слабые места в веб-структуре. Можно упомянуть бесплатные инструменты, такие, как Nmap, Openvas, Nikto, а также платные высокоточные инструменты, такие как Nessus, Acunetix, Nexpose, Netsparker, Securitybox 4Network, Securitybox 4Website и др.

Следовательно, на основе проведенных исследований можно сделать вывод о том, что для оптимизации безопасности веб-сайта возможно использование некоторых методов, а именно:

– установка сертификата SSL для веб-сайта. Сертификат SSL очень важен для веб-сайта. Это самый безопасный способ защитить информацию

на веб-сайте. Безопасность веб-сайта SSL основана на механизме шифрования информации между сервером и веб-браузером;

– обновление прикладного программного обеспечения на веб-сайте. Регулярное обновление прикладного программного обеспечения поможет хорошо защитить веб-сайт. Процесс поможет обновить уязвимости и ошибки старых версий. Тем самым не позволяя хакерам воспользоваться уязвимостями для проведения DDoS-атак;

– инвестиции в большую пропускную способность. Чем больше пропускная способность, тем быстрее можно будет обрабатывать запросы клиентов без необходимости тратить много времени на ожидание. Помогает большому количеству клиентов получить доступ к веб-сайту одновременно без перегрузок. В то же время покупка большей пропускной способности также помогает ограничить возможность DDoS-атак из-за внезапного увеличения трафика веб-сайта;

– сокрытие исходного IP-адрес сервера. Ограничение IP-адреса при доступе к веб-сайту или установка плагинов для защиты веб-сайта – эти вышеуказанные меры предназначены только для поддержания процесса обеспечения безопасности веб-сайта и по-прежнему имеют множество ограничений по цене и времени.

Таким образом, в результате проведенного исследования были выявлены основные уязвимости веб-сайтов и предложены методы их обнаружения и обеспечения безопасности. Приведены примеры реализации предложенных методов. Обеспечение безопасности веб-сайтов требует постоянного мониторинга и реагирования на уязвимости. Продолжительность мониторинга и реагирования на уязвимости являются ключевыми факторами в обеспечении безопасности веб-сайтов. Эффективные методы обнаружения уязвимостей и соответствующие меры безопасности должны постоянно совершенствоваться и адаптироваться к

новым угрозам для обеспечения эффективной защиты веб-ресурсов. Важно уделять внимание обучению персонала и его осведомленности о современных методах атак, чтобы поддерживать ресурс в защищенном состоянии.

Литература

1. Шакиров А.А. Зарипова Р.С. Современные тенденции web-разработки // Russian Journal of Education and Psychology. 2019. Т. 10. № 3. С. 85-88.

2. Гибадуллин Р.Ф., Вершинин И.С., Глебов Е.Е. Разработка приложения для ассоциативной защиты файлов // Инженерный вестник Дона. 2023. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8462.

3. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети интернет и контрмеры (обзор) / Инженерный вестник Дона. 2019. № 3. URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

4. Шакиров А.А., Зарипова Р.С. Актуальность обеспечения информационной безопасности в условиях цифровой экономики // Инновационное развитие экономики. Будущее России: Сборник материалов и докладов V Всероссийской (национальной) научно-практической конференции. 2018. С. 257-260.

5. Пырнова О.А. Информационная безопасность в эпоху квантовых технологий // Энергетика, инфокоммуникационные технологии и высшее образование: материалы Международной конференции. Казань, 2023. С. 439-443.

6. Юртаев В.В., Николаева С.Г. Базы данных как уязвимость организации // Технологический суверенитет и цифровая трансформация. Международная научно-техническая конференция. Казань, 2023. С. 256-260.

7. Gizatullin Z., Nuriev M. Modeling the electromagnetic compatibility of electronic means under the influence of interference through the power supply

network // Proceedings – 2022 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2022. 2022. pp. 321-326.

8. Злыгостев Д.Д., Зарипова Р.С. Информационная безопасность как инструмент обеспечения экономической безопасности предприятий // Инновации в информационных технологиях, машиностроении и автотранспорте: сборник материалов Международной научно-практической конференции. 2017. С. 23-25.

9. Gibadullin R.F., Nikonorov V.V. Development of the system for automated incident management based on open-source software // Proceedings – 2021 International Russian Automation Conference, RusAutoCon. 2021. pp. 521-525.

10. Чудинов Н.В., Халидов А.А. Разработка программного комплекса для защиты программ от нелегального использования / Современные цифровые технологии: проблемы, решения, перспективы. национальная (с международным участием) научно-практическая конференция. Казань, 2022. С. 140-142.

11. Аникин И.В., Катасёв А.С., Черняков А.С. Модель и программный комплекс анализа атак на web-приложения // Научно-технический вестник Поволжья. 2023. № 7. С. 17-20.

References

1. SHakirov A.A. Russian Journal of Education and Psychology. 2019. T. 10. № 3. pp. 85-88.

2. Gibadullin R.F., Vershinin I.S., Glebov E.E. Inzhenernyj vestnik Dona. 2023. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2023/8462.

3. Menciev A.U., CHebieva H.S. Inzhenernyj vestnik Dona. 2019. № 3. URL: ivdon.ru/ru/magazine/archive/n4y2019/5859.

4. SHakirov A.A., Zaripova R.S. Aktual'nost' obespecheniya informacionnoj bezopasnosti v usloviyah cifrovoj ekonomiki [The relevance of information security in the digital economy]. Innovacionnoe razvitie ekonomiki. Budushchee

Rossii: Sbornik materialov i dokladov V Vserossijskoj (nacional'noj) nauchno-prakticheskoj konferencii. 2018. pp. 257-260.

5. Pyrnova O.A. Informacionnaya bezopasnost' v epohu kvantovyh tekhnologij [Information security in the age of quantum technologies]. Energetika, infokommunikacionnye tekhnologii i vysshee obrazovanie: materialy Mezhdunarodnoj konferencii. Kazan, 2023. pp. 439-443.

6. YUrtaev V.V., Nikolaeva S.G. Bazy dannyh kak uyazvimost' organizacii [Databases as a vulnerability of the organisation]. Tekhnologicheskij suverenitet i cifrovaya transformaciya. Mezhdunarodnaya nauchno-tekhnicheskaya konferenciya. Kazan, 2023. pp. 256-260.

7. Gizatullin Z., Nuriev M. Proceedings – 2022 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2022. 2022. pp. 321-326.

8. Zlygostev D.D., Zaripova R.S. Informacionnaya bezopasnost' kak instrument obespecheniya ekonomicheskoj bezopasnosti predpriyatij [Information security as a tool for ensuring economic security of enterprises]. Innovacii v informacionnyh tekhnologiyah, mashinostroenii i avtotransporte: sbornik materialov Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2017. pp. 23-25.

9. Gibadullin R.F., Nikonorov V.V. Proceedings – 2021 International Russian Automation Conference, RusAutoCon 2021. 2021. pp. 521-525.

10. CHudinov N.V., Halidov A.A. Razrabotka programmnogo kompleksa dlya zashchity programm ot nelegal'nogo ispol'zovaniya [Development of a software complex to protect programmes from illegal use]. Sovremennye cifrovye tekhnologii: problemy, resheniya, perspektivy. nacional'naya (s mezhdunarodnym uchastiem) nauchno-prakticheskaya konferenciya. Kazan', 2022. pp. 140-142.

11. Anikin I.V., Katasyov A.S., CHernyakov A.S. Nauchno-tekhnicheskij vestnik Povolzh'ya. 2023. № 7. pp. 17-20.

Дата поступления: 3.01.2024 Дата публикации: 9.02.2024