ДОСЛІДЖЕННЯ ЗАСОБІВ ЗАХИСТУ ВЕБСИСТЕМИ ВІД КІБЕРАТАК НА ПРИКЛАДІ САЙТУ

Шестаков В.О.

Харківський національний університет радіоелектроніки,
кафедра інфокомунікаційної інженерії ім. В.В. Поповського,
Україна.

E-mail: shestakov.vladyslav@nure.ua

Abstract

The study focuses on researching methods to protect web systems from cyberattacks. The main threats in web systems based on OWASP TOP 10 are analyzed. Special attention is given to implementing security measures for various types of attacks, such as SQL injections and cross-site scripting (XSS). The research highlights the use of testing tools like Nmap, Sqlmap, and XSStrike on the web system of the Infocommunication Engineering Department, aiming to eliminate vulnerabilities and ensure robust protection.

Об'єкт дослідження – процес забезпечення захисту веб-систем від кібератак.
Предмет дослідження – механізми захисту веб-систем від кібератак.
Мета роботи – дослідження механізмів захисту веб-систем.
Методи досліджень – емпіричний аналіз, формалізація та порівняння.

Актуальність проблеми

У сучасних умовах майже кожне підприємство, незалежно від його масштабу, має власний веб-сайт для представлення своїх послуг або продукції. Це робить веб-системи привабливою ціллю для кібератак. Основні загрози включають SQL-ін'єкції, міжсайтовий скриптинг, грубі атаки на облікові записи, атаки на FTP/SSH протоколи та експлуатацію відомих вразливостей веб-серверів і систем управління змістом. Такі загрози можуть призвести до витоку конфіденційної інформації, пошкодження даних та порушення роботи сайту, що може мати серйозні наслідки для компаній, особливо у фінансовій та репутаційній сферах.

Згідно висновків дослідження, проведеного українським агентством інформаційної безпеки Shalb, в рамках глобального дослідження безпеки інтернет ресурсів, було виявлено, що 80% інтернет ресурсів не оновлюють своєчасно програмне забезпечення. Разом з тим було відмічено, що якщо сайт містить принаймні одну загрозу, то з вірогідністю, близькою до ста відсотків, даний сайт містить принаймні ще декілька загроз, та всі вони належать до різних категорій. Було виявлено, що найбільш захищеними є веб ресурси платіжних систем, бо вони регулярно проводять аудити веб безпеки та підводять її під міжнародні стандарти.

Інше дослідження, проведене компанією Sitesecure, в якому взяли участь 270 представників компаній, що займаються комерційною розробкою сайтів, виявило декілька важливих результатів. Зокрема, 75% компаній не мають у своєму штаті фахівця з інформаційної безпеки, який би відповідав за захист сайтів клієнтів. Лише 7% опитаних повідомили про наявність регламентованих правил безпеки та плану реагування на випадок кібератак. Більше половини (59%) організацій не підписують із співробітниками договори про дотримання конфіденційності та правил безпеки, а 26% не мають політики щодо паролів. Також було встановлено, що 40% компаній принаймні раз на рік стикаються з кібератаками.

Ще одне дослідження, проведене компанією Sitesecure, виявило взаємозв'язок між загрозами безпеці на сайті, його індексацією в пошукових системах і ймовірністю потрапляння в чорні списки. Зокрема, дослідження показало, що сайти на безкоштовних системах управління контентом є в середньому у 4 рази більш вразливими, ніж ті, що використовують платні рішення. Крім того, своєчасне оновлення систем управління змістом зменшує ризик виникнення загроз у два рази, а понад 50% сайтів залишаються без захисту SSL-сертифікатом, що значно підвищує їхню вразливість.

Одним з основних інструментів для аналізу веб-загроз є рейтинг OWASP TOP 10, який оновлюється на основі нових даних про загрози. У рамках цього дослідження було проведено детальний аналіз кожної з категорій загроз, зазначених у цьому рейтингу, і розроблено рекомендації для захисту веб-систем.

Рішення з захисту

Регулярний аудит та моніторинг безпеки веб-системи. За даними досліджень, майже 80% інтернет-ресурсів не проводять оновлення програмного забезпечення своєчасно, що значно підвищує ризик успішних атак. Регулярний аудит допомагає виявити такі вразливості на ранніх етапах та мінімізувати ризик.

Firewall Summary: Attacks Blocked for ice.nure.ua

Block Type	Complex	Brute Force
Today	79	0
Week	83	0
Month	85	0

Рис. 1. Зведена статистика атак на веб-систему

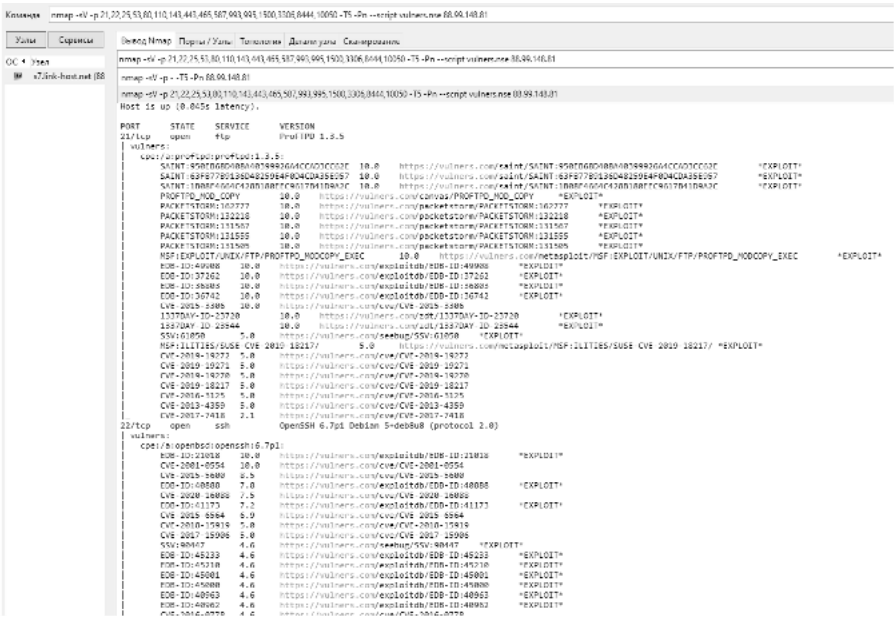

Рис. 2. Перевірка програмного забезпечення, що використовує веб-сервер на рахунок наявності відомих загроз

В результаті перевірки, що показана на рисунку 2, було виявлено 26 відомих загроз з програмним забезпеченням, що використовує FTP порт, 27 загроз з SSH порту, 13 проблем з DNS серверу, 3 вразливості http порту та 3 вразливості SSL/https порту. Усі дані виконаної перевірки були відправлені до технічної служби підтримки хостинг провайдера з проханням оновити версії ПЗ веб-сервера, що

використовується, для закриття відомих загроз. У відповідь було запропоновано безкоштовно перенести сайт кафедри на новіший веб-сервер, де вже оновлено програмне забезпечення.

Впровадження багатофакторної аутентифікації. Багатофакторна аутентифікація захищає систему від атак на облікові записи, що включають підбір паролів та методи типу «грубої сили». Згідно з даними досліджень, використання багатофакторної аутентифікації знижує ймовірність успішної атаки на обліковий запис на 70% та робить процес автентифікації надійнішим для захисту конфіденційних даних.

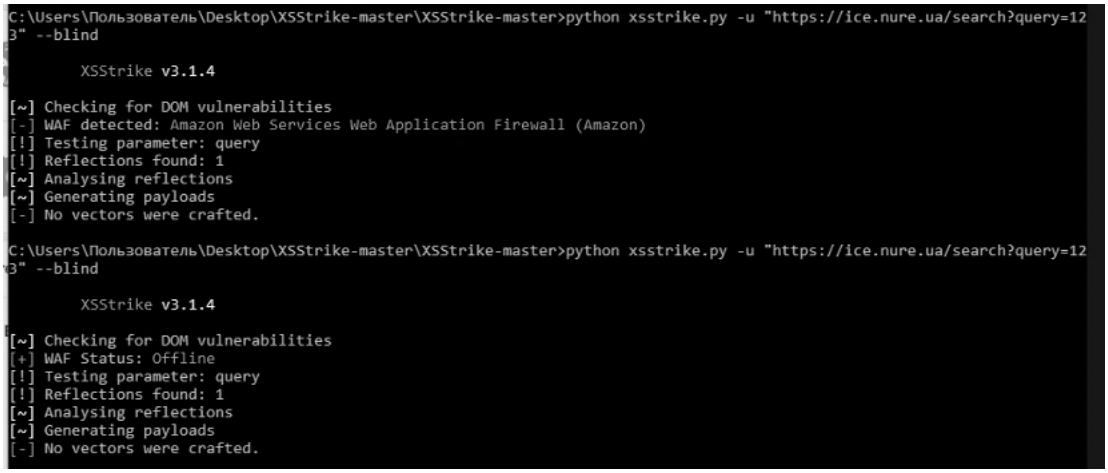

Рис. 3. Перевірка сторінки на наявність XSS ін'єкцій програмою XSStrike

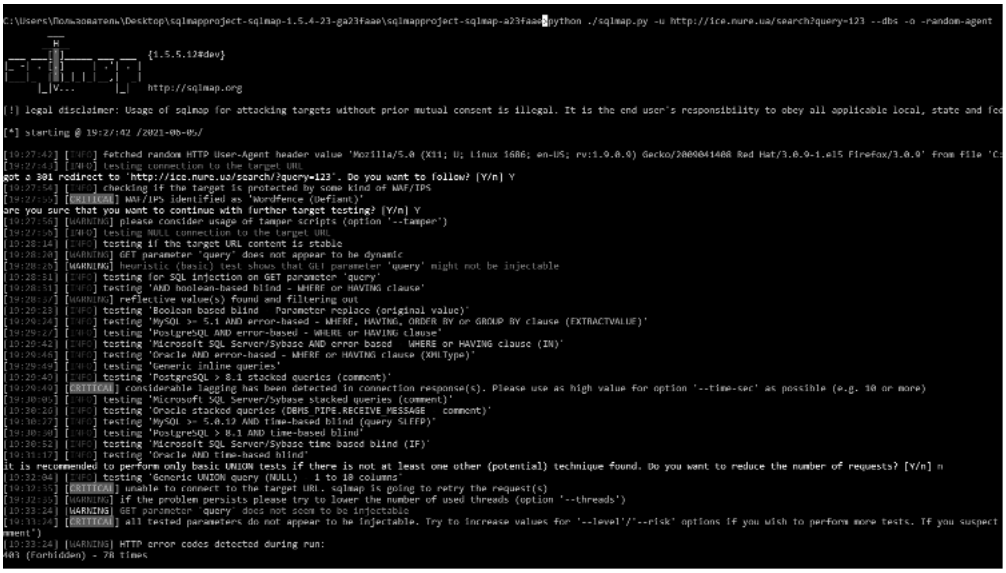

Рис. 4. Перевірка сторінки на наявність SQL ін'єкцій програмою Sqlmap

Захист від SQL-ін'єкцій та XSS-атак. Для запобігання таким атакам була застосована фільтрація та перевірка введених даних на стороні сервера. На тестованому сайті за допомогою інструментів Nmap, Sqlmap, і XSStrike було виявлено та виправлено декілька потенційних вразливостей. Виявлені та усунуті уразливості запобігли можливому витоку даних та значно знизили ризик успішних атак на систему.

Налаштування SSL-шифрування. Згідно з дослідженням, наявність SSL-сертифікату знижує ризик перехоплення даних під час передачі. Встановлення SSL забезпечує захист чутливих даних на всіх етапах передачі, що особливо важливо для запобігання витоку конфіденційної інформації.

Подальші напрямки розвитку

Адаптивні моделі кіберзахисту, які реагують на змінні загрози, є перспективним напрямом розвитку систем безпеки. На основі аналізу існуючих загроз та вразливостей веб-систем такі моделі можуть автоматично підлаштовувати свої параметри під конкретні ризики, реагуючи на нові загрози. Вони можуть застосовувати алгоритми машинного навчання для визначення аномальної активності, що дозволяє виявляти нетипову поведінку і нейтралізувати загрози в реальному часі.

Для підвищення ефективності захисту важливим є дослідження вразливостей, характерних для кожного з веб-фреймворків, як-от Angular, React, Vue тощо. Це дозволить розробити специфічні рекомендації для захисту веб-систем, враховуючи різноманіття архітектур та особливості кожного фреймворка.

Крім того, математичне моделювання ризиків з урахуванням змінних параметрів загроз є необхідним для створення надійних моделей безпеки. Диференційовані рівняння або методи стохастичного моделювання дозволять оцінювати рівень ризику та обирати оптимальні стратегії захисту, адаптуючи їх залежно від типу та інтенсивності загрози.

Переваги впроваджених рішень

Завдяки регулярному моніторингу та проведенню аудиту безпеки було виявлено та усунено низку вразливостей у веб-системі, що значно знизило ризик успішної атаки. Ці заходи підвищили загальну захищеність системи та дозволили своєчасно усувати потенційні загрози, запобігаючи витоку даних та підвищуючи ефективність захисних механізмів. Сталість до автентифікаційних атак значно покращилася завдяки багатофакторній аутентифікації, що унеможливило успішний підбір пароля. Захист від SQL-ін'єкцій та XSS забезпечив цілісність бази даних, запобігши можливим витокам даних і втратам. Крім того, безпечна передача даних через SSL-шифрування підвищила довіру до системи та забезпечила збереження інформації користувачів.

Застосовані заходи підвищили загальну безпеку системи, суттєво зменшивши ризик успішної кібератаки. Цей комплексний підхід може слугувати прикладом для інших підприємств, які прагнуть захистити свої веб-системи.

Висновки

Дослідження підкреслює важливість комплексного підходу до кібербезпеки веб-систем, що включає не лише технічні рішення, але й постійний моніторинг, адаптацію до нових загроз та навчання персоналу. Отримані результати можуть слугувати основою для детальних рекомендацій для підприємств, які прагнуть посилити захист своїх веб-ресурсів. Тестування веб-сайту кафедри інфокомунікаційної інженерії показало ефективність застосованих заходів і необхідність їх постійного вдосконалення.

Запропоновану систему можна порівняти з методологією IT-Grundschutz, яка пропонує модульний підхід і готові рішення щодо кіберзагроз. Робота містить конкретні приклади захисних заходів для веб-сайту та інструменти захисту від атак, тоді як IT-Grundschutz надає універсальні інструкції для будь-яких організацій.

Результати дослідження можуть бути корисними як відправна точка для впровадження ефективного захисту веб-систем на підприємствах і підвищення обізнаності щодо кібербезпеки.

Література

1. OWASP Top-10 2021. Statistics-based proposal [Електронний ресурс]. – 2021. Режим доступу до ресурсу: https://lab.wallarm.com/owasp-top-10-2021-proposal-based-on-a-statistical-data/.

2. Логін С. A1:Injection OWASP TOP 10 [Електронний ресурс] / Святослав Логін. – 2018. Режим доступу до ресурсу: https://svyat.tech/A1Injection-OWASP-TOP-10/.