DOI: https://doi.org/10.33216/2222-3428-2023-25-1
УДК: 004.056

Деркач М.В., Хомишин В.Г., Гудзенко В.О.

ТЕСТУВАННЯ БЕЗПЕКИ ВЕБРЕСУРСУ НА БАЗІ ІНСТРУМЕНТІВ ДЛЯ СКАНУВАННЯ ТА ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ

У статті розглянуте актуальне питання тестування безпеки вебресурсу структурного підрозділу, створеного на базі системи керування вмістом WordPress, різними інструментами сканування та виявлення вразливостей, а саме Mozilla Observatory, Qualys, ImmuniWeb. Оскільки важливою умовою для безперервного процесу забезпечення безпеки бізнес-процесів сайту компанії, збереження ділової репутації, економічного зростання та розвитку бізнесу є саме регулярні діагностичні та відновлювальні процедури різного характеру та рівня у складі аудиту безпеки сайту, спрямованого на підвищення безпеки та надійності інтернет-ресурсу. Частина таких робіт присвячена пошуку вразливостей безпосередньо у структурі, виявлення помилок у коді та програмному забезпеченні сервера, якими зловмисники можуть атакувати та зламати сайт. В результаті проведено тестування безпеки вебресурсу структурного підрозділу зазначеними автоматизованими інструментами, кожний з яких виявив певні недоліки. Результат сканування двома останніми інструментами відповідає вищій категорії оцінки поточного рівня захищеності сайту. Завдяки інструменту Mozilla Observatory отримана посередня оцінка, що обумовлено більш широкими можливостями цього сервісу. Оскільки він застосовує інтегровані інструменти та рекомендації від OWASP, Probely, а також ті самі Qualys й ImmuniWeb, тим самим комплексна оцінка враховує не лише захист зашифрованого мережевого з'єднання з іншою системою за допомогою протоколу SSL/TLS. В цілому вебресурс забезпечує надійний обмін інформацією між браузером користувача та сервером. А з розвитком мережевих технологій та інтернету взаємодія різних систем, сервісів і додатків одна з одною набула значної актуальності, тому до тестування взаємодії варто підходити з усією серйозністю.

Ключові слова: *безпека, вебресурс, вразливість, криптографічні алгоритми, сканування, сертифікат, тестування.*

Вступ. Головне для власника вебсайту – це розуміння важливості безпеки власного сайту, розуміння необхідності забезпечувати його безпеку та перевіряти її (періодично), для чого і проводиться тестування безпеки. Тестування безпеки - це стратегія тестування, яка використовується для перевірки безпеки вебресурсу, а також для аналізу ризиків, пов'язаних із забезпеченням цілісного підходу до захисту додатків, хакерів, вірусів, несанкціонованого доступу до конфіденційних даних. Проведення тестування дозволяє виявити ці слабкі місця та усунути їх, забезпечуючи більш високий рівень безпеки для вебресурсу та його користувачів. На сьогодні це стає мірою необхідності, так як вебресурси постійно піддаються різноманітним загрозам, а вразливості можуть бути використані зловмисниками для атак або порушення принципів безпеки вебресурсу, таких як конфіденційність, цілісність та довіра, пошкодження та відновлення, доступність. Запобіжним заходом, який дозволяє отримати об'єктивну оцінку рівня захисту вебресурсу компанії, детальну інформацію про знайдені вразливості, можливі сценарії атак та рекомендації щодо їх усунення, стає аудит безпеки сайту, що являє собою низку процедур, спрямованих на забезпечення стабільної роботи вебресурсу, безпеки даних та зниження ризиків.

Аудит безпеки вебресурсу є важливою складовою для забезпечення його стійкості до потенційних загроз і вразливостей. Зазвичай, визначають такі критерії оцінки виявлених вразливостей, як:

1. Severity (Серйозність).
2. Responsibility (Відповідальність).
3. Assignment (Призначення).
4. Status (Статус).

Ці критерії грають важливу роль у пріоритизації та управлінні вразливостями. Вони дозволяють оцінити серйозність проблеми, призначити відповідальних осіб чи команди для її вирішення та відслідковувати стан виправлення. Такий підхід допомагає ефективно управляти безпекою та ризиками в вебресурсах.

Аналіз останніх досліджень і публікацій. Поряд з такими етапами проведення аудиту безпеки вебресурсу [1], як планування, що включає визначення мети аудиту та складання плану дій; збір інформації, що передбачає збір загальної інформації про вебресурс, його архітектуру, функціональність, потенційні слабкі місця та оцінка загроз і ризиків, пов'язаних з вебресурсом [2,3]; необхідно провести сканування та виявлення вразливостей, що, в свою чергу, включає:

– Вибір інструментів і методів для аналізу безпеки.

– Використання автоматизованих інструментів для сканування вебресурсу на предмет виявлення потенційних вразливостей.

– Оцінка виявлених вразливостей на серйозність і потенційний вплив на безпеку вебресурсу.

– Підготовка звіту про проведення аудиту безпеки з описом виявлених вразливостей та рекомендацій щодо виправлення.

Для проведення періодичного аудиту безпеки існує безліч інструментів для сканування та виявлення вразливостей, що варіюються за функціоналом, типом вразливостей, які вони можуть знайти, та рівнем

деталізації наданих звітів. Всі ці інструменти сканують вебресурси на предмет різних вразливостей, таких як відкриті порти, використання застарілих версій ПЗ, SQL-ін'єкції, XSS, недоліки аутентифікації, слабкі паролі та інші [4,5].

Мета статті. Провести тестування безпеки для аналізу автоматизованих інструментів сканування вебресурсу на предмет виявлення потенційних вразливостей.

Основний зміст роботи. Аналіз інструментів сканування та виявлення вразливостей для тестування безпеки вебресурсу структурного підрозділу, створеного на базі системи керування вмістом WordPress, проведено наступними сервісами:

– Mozilla Observatory.
– Qualys.
– ImmuniWeb.

Mozilla Observatory сканує сайти на найпопулярніші вразливості, серед них: потенційно небезпечні cookies, XSS-уразливості та редиректи, також оцінює мережеву безпеку сайтів та роботу механізмів CORS, HPKP, HSTS та інших. Допомагає швидко перевірити технічні параметри і оцінити поточний рівень захищеності сайту.

Проведемо сканування вебресурсу структурного підрозділу (рис.1-2).

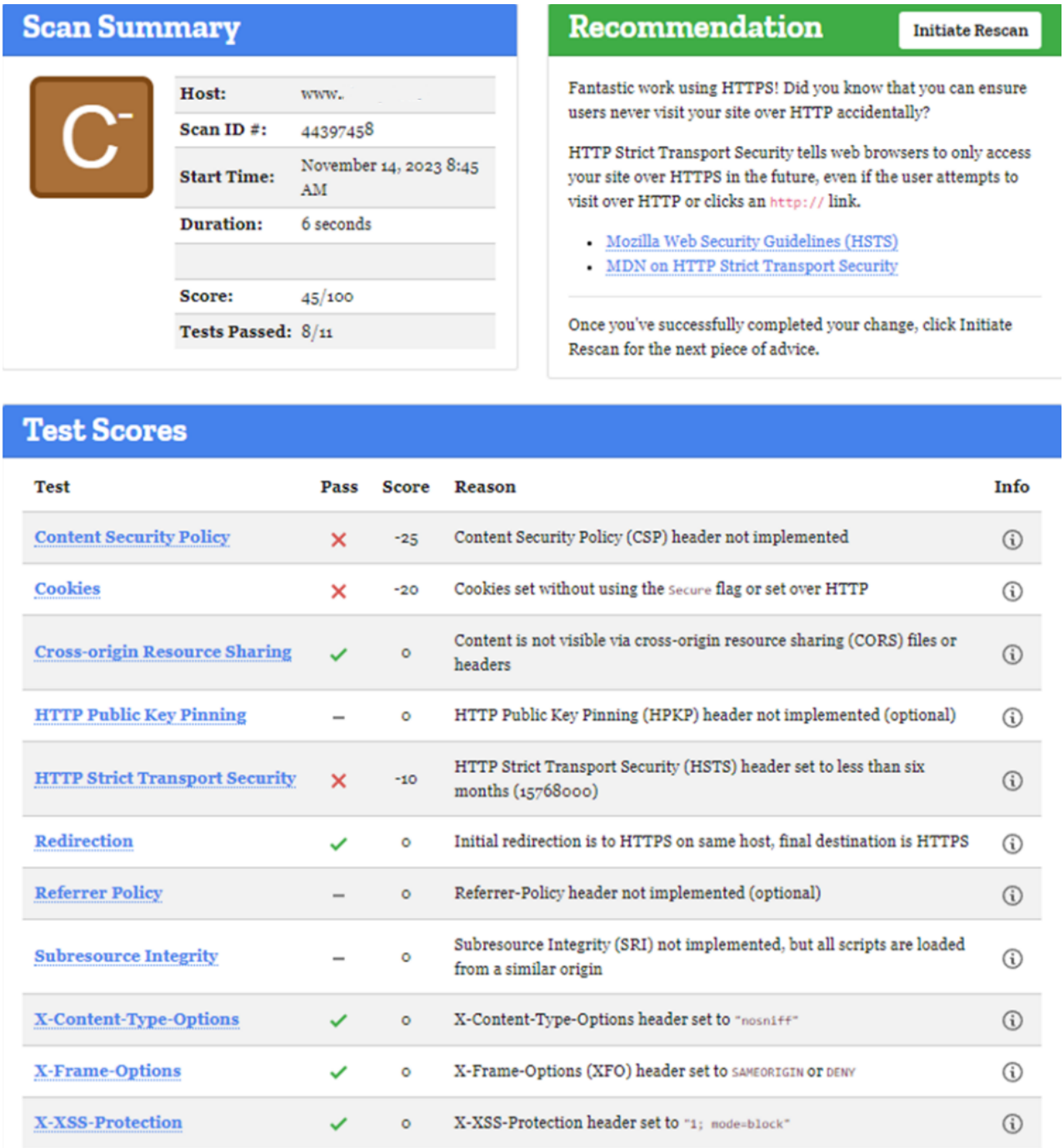

Рисунок 1 - Результат сканування сайту завдяки Mozilla Observatory

Mozilla Observatory перевіряє сайт завдяки тестам, представленим в табл. 1.

Таблиця 1 – Набір тестів інструменту Mozilla Observatory

Назва	Значення
Content Security Policy	Стандарт комп'ютерної безпеки, введений для запобігання міжсайтових сценаріїв, клікджекінгу та інших атак шляхом впровадження коду
Cookies	Застосовується для збереження даних на стороні користувача, може захистити користувача від викрадення даних
Cross-origin Resource Sharing	Технологія сучасних браузерів, яка дозволяє надати вебсторінкам доступ до ресурсів іншого домену
HTTP Public Key Pinning	Дозволяє вебсайтам HTTPS протистояти уособленню зловмисників, які використовують неправильно випущені або іншим чином шахрайські цифрові сертифікати
HTTP Strict Transport Security	Політика безпеки дозволяє відразу ж встановлювати безпечне з'єднання замість використання протоколу HTTP
Redirection	Технологія, що використовується у Всесвітньому павутинні для того, щоб вебсторінка була доступна під кількома URL
Referrer Policy	Використовується для аналітики, логування, оптимізації кешу та ін. Однак також може використовуватися для стеження або крадіжки інформації, виконання побічних ефектів, що призводять до витоку чутливих даних користувача і т.п.
Subresource Integrity	Рекомендація W3C для надання способу захисту доставки вебсайту. Зокрема, перевіряє активи, що обслуговуються третьою стороною, наприклад, мережею доставки контенту. Це гарантує, що ці активи не були скомпрометовані у ворожих цілях
X-Content-Type-Options	Заголовок, який підтримується Internet Explorer, Chrome і Firefox 50+, який повідомляє не завантажувати сценарії та таблиці стилів, якщо сервер не вказує правильний тип MIME. Без цього заголовка ці браузери можуть неправильно виявляти файли як сценарії та таблиці стилів, що призводить до атак XSS
X-Frame-Options	X-Frame-Options - це HTTP-заголовок, який дозволяє сайтам контролювати, як сайт може бути розміщений у фреймі iframe. Clickjacking — це практична атака, яка дозволяє зловмисним сайтам обманом змусити користувачів натиснути посилання на сайті
X-XSS-Protection	Використання може створити уразливості XSS на безпечних вебсайтах. Це не слід використовувати, якщо не потрібна підтримка старих вебпереглядачів, які ще не підтримують CSP

Після сканування вебресурсу інструмент видає звіт з рекомендаціями щодо покращення безпеки та посиланнями на корисні матеріали. Оцінка формується за шкалою від 0 до 100, тобто сайт набирає певну кількість балів — йому присвоюється категорія якості “A”, “B”, “C”, “D”, “F”.

За результатами проведеного сканування сайту присвоєна категорія “C-”, оскільки набрано 45 балів зі 100 можливих. Проведено 8 тестів з 11, завдяки яких виявлено слабкі місця вебсайту:

1. Не реалізовано механізм безпеки вебзастосунків, який використовується для скорочення ризиків, пов'язаних з атаками, такими як впровадження скриптів (XSS) та виконання небажаного коду (ін'єкція).
2. Файли cookie встановлюються без використання прапора Secure або через HTTP.
3. Заголовок HTTP Strict Transport Security (HSTS), що використовується для перемикання користувача, який зайшов по HTTP на HTTPS-сервер, встановлено на менше ніж шість місяців.

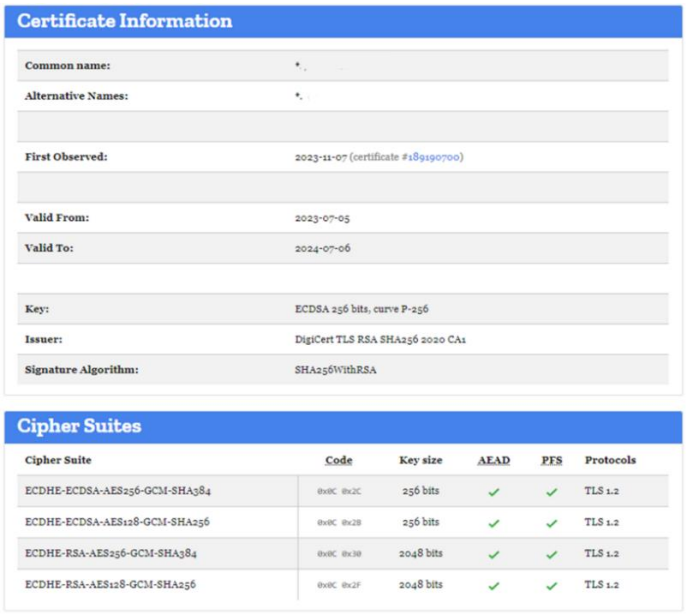

Рисунок 2 - Результат сканування сайту завдяки Mozilla Observatory

При роботі з HTTPS шифрування застосовується у чотирьох випадках: під час обміну ключами, у SSL-сертифікатах, при пересиланні повідомлень та складанні хеш-суми (дайджесту). У кожному з цих випадків використовуються різні набори алгоритмів, про які домовляються клієнт і сервер. Вони вибирають асиметричний шифр для встановлення з'єднання, симетричний шифр для кодування повідомлень та алгоритм хешування для дайджесту.

Для налаштування криптографічних методів, які використовуються сервером, у мережі є спеціальні інструменти. Mozilla пропонує три рекомендовані конфігурації для серверів, які використовують TLS:

1. Сучасна – для роботи з клієнтами, які використовують TLS 1.3 без зворотної сумісності.
2. Проміжна — рекомендована конфігурація більшості серверів.
3. Застаріла - доступ до сервісу здійснюється за допомогою старих клієнтів або бібліотек, таких як IE8, Java 6 або OpenSSL 0.9.8.

За результатами сканування сервіс виявив чотири алгоритми хешування, які належать до протоколу TLS 1.2 таких груп, як:

– SHA384.
– SHA256.

Алгоритми хешування SHA384 і SHA256 належать до стандарту TLS 1.2.

TLS, як і його попередник SSL, — криптографічні протоколи, що забезпечують захищену передачу даних між вузлами у мережі Інтернет. TLS і SSL використовують асиметричне шифрування для автентифікації, симетричне шифрування для конфіденційності та коди автентичності повідомлень для збереження цілісності повідомлень.

Основні функції сертифікату SSL/TLS:

1. Захищати особисті дані.
2. Зміцнювати довіру клієнтів.
3. Відповідати нормативним вимогам.
4. Поліпшити пошукову оптимізацію (SEO).

Наступний інструмент ***Qualys.*** Він проводить сканування вебдодатків та оцінку всіх 10 найбільш критичних ризиків для безпеки вебдодатків OWASP, включаючи міжсайтовий сценарій (XSS), впровадження SQL і розкриття конфіденційних даних.

Інструмент працює наступним чином - спочатку переглядається сертифікат, щоб переконатися, що він дійсний і надійний, а вже потім перевіряється конфігурація SSL у трьох категоріях:

1. Підтримка протоколу.
2. Обмін ключами.
3. Надійність шифру.

Кожна категорія отримує оцінку, ці бали об’єднуються для отримання загальної оцінки 0-100. Нуль у будь-якій категорії призводить до нульової загальної оцінки. Загальна числова оцінка перетворюється на буквену оцінку (A-F). Оцінку A буде підвищено до A+ для виняткових конфігурацій і знижено до A-, якщо буде одне або більше попереджень. Інші оцінки, які можна побачити: T (сертифікат не є надійним), M (невідповідність назви сертифіката) і NA (незастосовно, інформацію про сервер SSL не отримано).

Проведемо сканування вебресурсу структурного підрозділу і цим інструментом (рис.3-4).

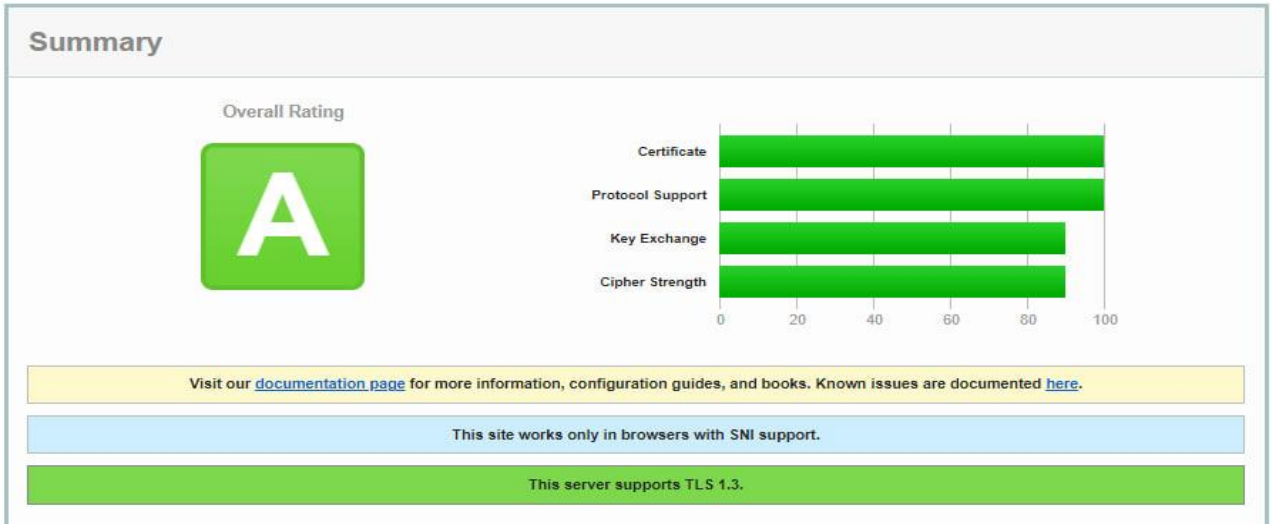

Рисунок 3 - Результат сканування сайту завдяки Qualys

За результатами сканування сайт отримав оцінку “A”. Оскільки інструмент виявив TLS протокол декількох версій: TLS 1.2 і TLS 1.3, а також те, що сайт працює тільки в браузерах з підтримкою SNI (Server Name Indication є розширенням протоколу TLS).

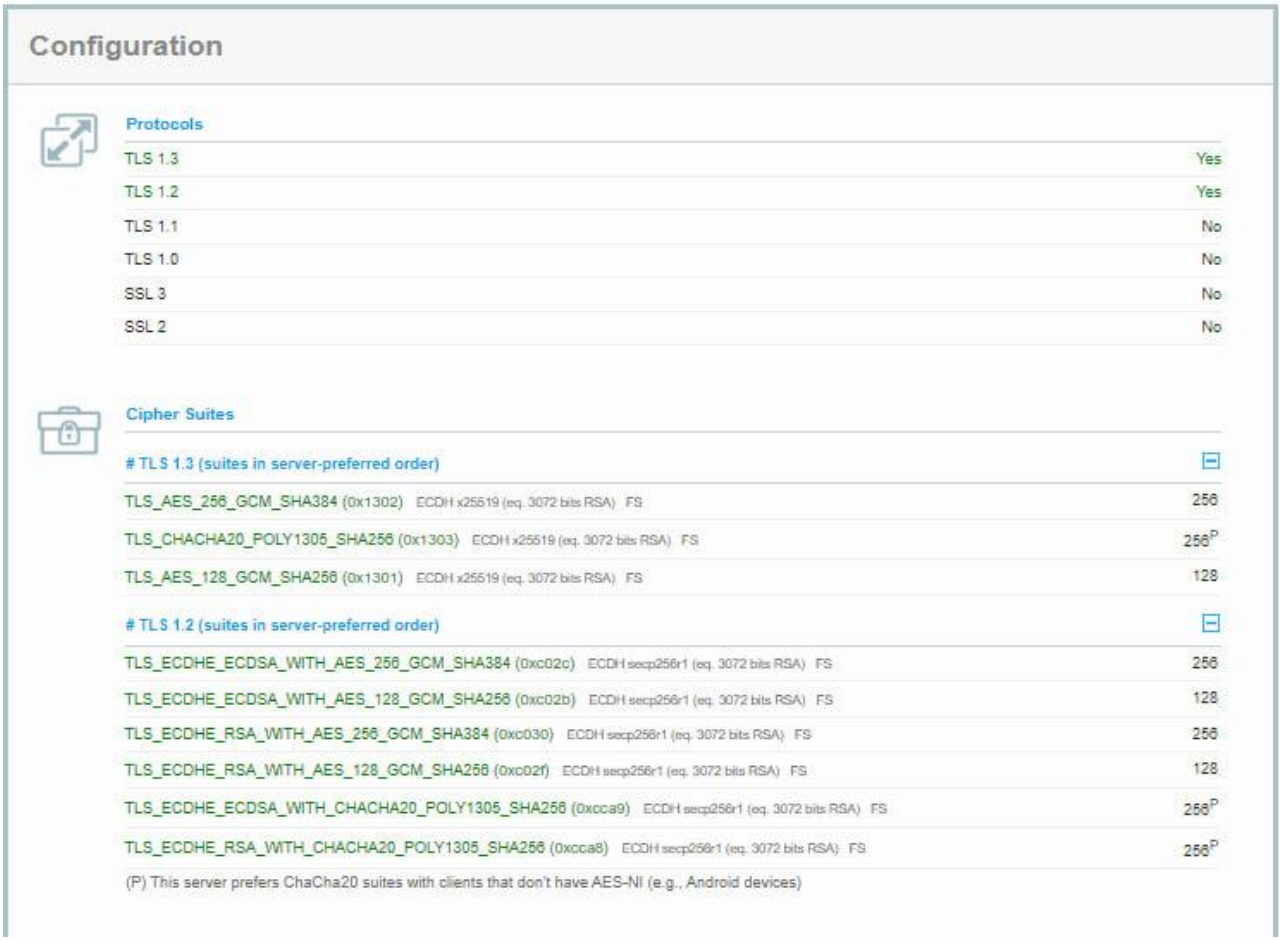

Рисунок 4 - Результат сканування сайту завдяки Qualys

За результатами сканування сервіс виявив три алгоритми хешування, які належать до новішої версії протоколу TLS 1.3:

– SHA384.
– SHA256.
– SHA256 with CHACHA20 POLY1305.

Отже, оцінка “A” виправдана.

І ще один інструмент ***ImmuniWeb***. Є комплексом інструментів для безкоштовної перевірки вебресурсів. Включає такі модулі як: Website Security Test, Cloud Security Test, Email Security Test, Mobile App Security Test, SSL Security Test, Dark Web Exposure Test. Доступний безкоштовний моніторинг безпеки, а також API і CLI-інтерфейс.

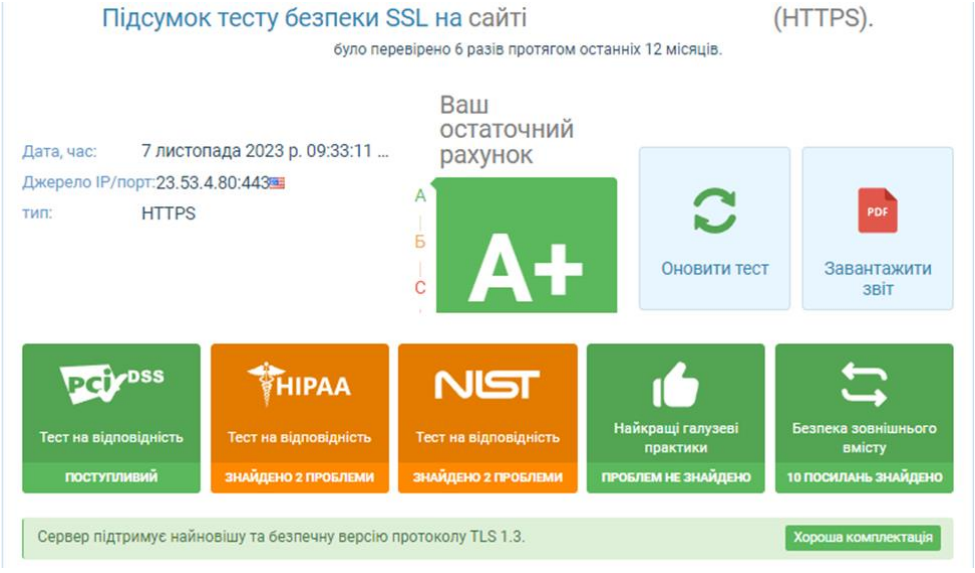

Рисунок 5 - Результат сканування сайту завдяки ImmuniWeb

За результатами проведеного сканування сайту формується оцінка за шкалою від 0 до 100 і присвоюється категорія якості “A”, “B”, “C”, “F”.

За допомогою даного інструменту вебресурс структурного підрозділу отримав категорію “A+” (рис. 5-6), виявлено, що сервер сайту має хорошу конфігурацію захисту завдяки підтримки сучасних протоколів захисту TLS 1.2 і TLS 1.3.

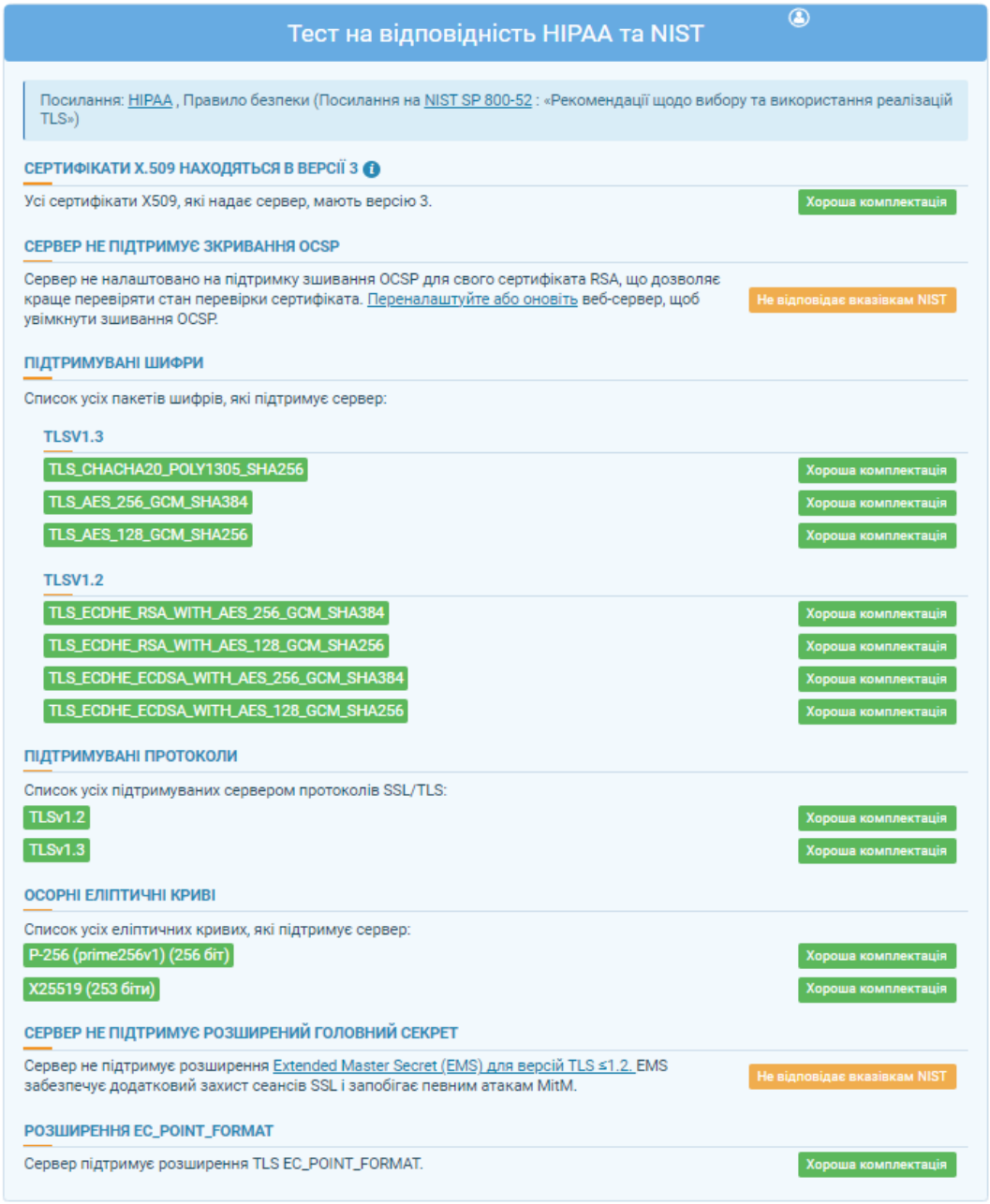

Рисунок 6 - Результат сканування сайту завдяки ImmuniWeb

Також виявлено, що сайт не дотримує усіх вимог щодо протоколів HIPPA та NIST, а саме:

1. Сервер не налаштовано на підтримку зшивання OCSP для свого сертифіката RSA, що дозволяє краще перевіряти стан перевірки сертифіката.
2. Сервер не підтримує розширення Extended Master Secret (EMS) для версій TLS ≤1.2. EMS забезпечує додатковий захист сеансів SSL і запобігає певним атакам MitM.

HIPPA - акт (закон), щоб модернізувати потік медичної інформації, передбачити, як особиста інформація, що зберігається в медичних установах та медичних страхових галузях, має бути захищена від шахрайства та крадіжок.

NIST Cybersecurity Framework – це платформа або керівництво, яка містить набір рекомендацій щодо зниження організаційних ризиків кібербезпеки.

Проведено тестування безпеки вебресурсу структурного підрозділу автоматизованими інструментами сканування на предмет виявлення потенційних вразливостей. В результаті сканування інструментами Qualys та ImmuniWeb, хоча і виявлено недоліки, але все одно присвоєна вища категорія оцінки поточного рівня

захищеності сайту. В той час, як за результатами сканування завдяки інструменту Mozilla Observatory отримана посередня оцінка. Це свідчить про надійніший результат, обумовлений більш широкими можливостями цього сервісу, оскільки він застосовує інтегровані інструменти та рекомендації від OWASP, Probely, а також ті самі Qualys й ImmuniWeb. В цілому вебресурс забезпечує надійний обмін інформацією між браузером користувача та сервером, але завжди є над чим працювати, щоб мати кращий захист.

Так, наприклад, нещодавно були опубліковані нові уразливості, такі як Zombie POODLE, GOLDENDOODLE, 0-Length OpenSSL і Sleeping POODLE, для вебсайтів, які використовують режими блокового шифрування CBC (Cipher Block Chaining). Ці вразливості застосовні, лише якщо сервер використовує TLS 1.2 і версії нижче із режимами шифрування CBC.

У разі оригінального POODLE потрібно вимкнути підтримку SSL 3.0. Однак у цьому випадку є ризик отримати проблеми із сумісністю. Альтернативним рішенням може стати механізм TLS_FALLBACK_SCSV - він гарантує, що обмін даними SSL 3.0 буде проводитися тільки зі старими системами, тим самим зловмисники більше не зможуть ініціювати зниження версії протоколу. Спосіб захисту від Zombie POODLE та GOLDENDOODLE – відключення підтримки CBC у додатках на базі TLS 1.2, але кардинальним рішенням стане перехід на TLS 1.3, так як у новій версії протоколу не використовується CBC-шифрування.

Висновок. Прикладів вразливостей та атак існує величезна кількість. Навіть провівши повний цикл тестування безпеки, не можна бути на 100% впевненим, що вебресурс по-справжньому убезпечено. Але можна бути впевненим у тому, що відсоток несанкціонованих проникнень, крадіжок інформації та втрат даних буде в рази меншим, ніж у тих, хто не проводив тестування безпеки.

Література

1. Vikas V. Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security / V. Vikas, G. Saisri, T. Sai Meghana, A. Sree Harshini, G. Kaveri // International Journal for Research in Applied Science & Engineering Technology (IJRASET). – 2023. – Volume 11. Issue VII. – p. 794–805.
2. Sudirman D. Network Penetration dan Security Audit Menggunakan Nmap / D. Sudirman, A. N. Yaqin // SATIN Sains dan Teknologi Informasi. – 2021. – Vol. 7 № 1. – p. 32-44.
3. Zagorodna N. Network Attack Detection Using Machine Learning Methods / N. Zagorodna, M. Stadnyk, B. Lypa, M. Gavrylov, R. Kozak // Challenges to national defence in contemporary geopolitical situation. – 2022. – no. 1. – p. 55-61.
4. Bhanwarlal. XSS and SQL Injection Detection and Prevention Techniques (A Review) / Bhanwarlal, I. Khan // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. – 2022. – Volume 8. Issue I. – p. 53–60.
5. Yesin V. Technique for Searching Data in a Cryptographically Protected SQL Database / V. Yesin, M. Karpinski, M. Yesina, V. Vilihura, R. Kozak, R. Shevchuk // Applied Sciences. – 2023. – Vol.13(20):11525.
6. Галузін І.С. Управління уразливостями корпоративних інформаційних систем на базі рішень QUALYS / І.С. Галузін, Г.Г. Найман // Сучасний захист інформації. – 2021. – № 2(46). – p. 26–31.
7. Dowling B. A cryptographic analysis of the TLS 1.3 handshake protocol. / B. Dowling, M. Fischlin, F. Günther, D. Stebila // J. Cryptol. – 2021. – № 34(4), 37.
8. Chan K.Y. DIDO: data provenance from restricted TLS 1.3 websites / K.Y. Chan, H. Cui, T.H. Yuen // Cryptology ePrint Archive. – 2023. – Paper 2023/1056.

References

1. Vikas V. Web Security Audit and Penetration Testing: Identifying Vulnerabilities and Strengthening Website Security / V. Vikas, G. Saisri, T. Sai Meghana, A. Sree Harshini, G. Kaveri // International Journal for Research in Applied Science & Engineering Technology (IJRASET). – 2023. – Volume 11. Issue VII. – p. 794–805.
2. Sudirman D. Network Penetration dan Security Audit Menggunakan Nmap / D. Sudirman, A. N. Yaqin // SATIN Sains dan Teknologi Informasi. – 2021. – Vol. 7 № 1. – p. 32-44.
3. Zagorodna N. Network Attack Detection Using Machine Learning Methods / N. Zagorodna, M. Stadnyk, B. Lypa, M. Gavrylov, R. Kozak // Challenges to national defence in contemporary geopolitical situation. – 2022. – no. 1. – p. 55-61.
4. Bhanwarlal. XSS and SQL Injection Detection and Prevention Techniques (A Review) / Bhanwarlal, I. Khan // International Journal of Scientific Research in Computer Science, Engineering and Information Technology. – 2022. – Volume 8. Issue I. – p. 53–60.
5. Yesin V. Technique for Searching Data in a Cryptographically Protected SQL Database / V. Yesin, M. Karpinski, M. Yesina, V. Vilihura, R. Kozak, R. Shevchuk // Applied Sciences. – 2023. – Vol.13(20):11525.
6. Galuzin I.S. Vulnerability management of corporate information systems based on QUALYS solutions / I. S. Galuzin, G. G. Naiman // Modern Information Security. – 2021. – № 2(46). – p. 26–31.
7. Dowling B. A cryptographic analysis of the TLS 1.3 handshake protocol. / B. Dowling, M. Fischlin, F. Günther, D. Stebila // J. Cryptol. – 2021. – № 34(4), 37.
8. Chan K.Y. DIDO: data provenance from restricted TLS 1.3 websites / K.Y. Chan, H. Cui, T.H. Yuen // Cryptology ePrint Archive. – 2023. – Paper 2023/1056.

The article discusses the topical issue of testing the security of a web resource of a structural unit created based on the WordPress content management system, using various scanning and vulnerability detection tools, namely Mozilla Observatory, Qualys, ImmuniWeb. Since an important condition for the continuous process of ensuring the security of business processes of a company's website, maintaining business reputation, economic growth and business development are regular diagnostic and recovery procedures of various nature and levels as part of a website security audit aimed at increasing the security and reliability of the Internet resource. Several such works are devoted to searching for vulnerabilities directly in the structure, detecting errors in the code and server software that attackers can use to attack and hack the site. As a result, the security of the structural unit's web resource was tested using the specified automated tools, each of which revealed shortcomings. The result of scanning with the last two tools corresponds to a higher category for assessing the current level of site security. The Mozilla Observatory tool received a mediocre rating, which is due to the broader capabilities of this service. Because it leverages integrated tools and guidance from OWASP, Probely, as well as Qualys and ImmuniWeb, the comprehensive assessment considers more than just securing an encrypted network connection to another system using SSL/TLS. In general, the web resource ensures reliable exchange of information between the user's browser and the server. And with the development of network technologies and the Internet, the interaction of various systems, services, and applications with each other has acquired significant relevance, therefore interaction testing should be approached with the utmost seriousness.
Keywords: *security, web resource, vulnerability, cryptographic algorithms, scanning, certificate, testing.*

Деркач М.В. – к.т.н., доц, доцент кафедри комп'ютерних наук та інженерії Східноукраїнського національного університету імені Володимира Даля, доцент кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя, e-mail: gln459@gmail.com

Хомишин В.Г. – асистент кафедри кібербезпеки Тернопільського національного технічного університету імені Івана Пулюя, e-mail: homyshyn@gmail.com

Гудзенко В.О. – здобувач вищої освіти Тернопільського національного технічного університету імені Івана Пулюя, e-mail: gfd.lah@gmail.com