УДК 004.056
DOI: 10.31673/2409-7292.2022.015055

Бородань В.В., Васильченко Д.І.

АНАЛІЗ АТАК НА УРАЗЛИВОСТІ WEB-РЕСУРСІВ

У даній статті наведено основні відомості про можливі веб-атаки на веб-ресурси звичайного користувача чи організації. Проаналізовано статистику атак за останні декілька років, а також можливі уразливості, які дозволяють проведення цих атак. Проаналізована кореляція рівні збитків в різних типах галузей. Приведено список найчастіших вразливостей.

Ключові слова: атака, веб-ресурси, веб-сайт, уразливості веб-ресурсу, збитки, тенденції.

Вступ

У зв'язку зі стрімким розвитком IT- технологій дедалі більше людей та організацій починають використовувати веб-ресурси у своїх цілях. Веб-ресурси для когось стають просто «іграшкою», проте багато організацій ведуть свій бізнес використовуючи ті самі веб-ресурси та веб-сайти. Під час налаштування безпеки веб-ресурсів випадково можна допустити помилки, яка буде уразливістю та потенційним місцем для майбутньої атаки. Веб-ресурси щодня потерпають від спроб провести вдалу атаку. Зловмисники намагаються використати знайдену уразливість для розповсюдження потенційно шкідливого ПЗ, викрадення конфіденційних даних, або інших своїх цілей. Проте правильне налаштування параметрів безпеки допоможе знизити ризик її успішності.

Мета статті – аналіз основних веб-атак, що спрямовані на уразливості веб-ресурсів.

Викладення основного матеріалу

Щодня користувачі та компанії використовують веб-ресурси у своїх цілях. Проте ці ресурси можуть містити різноманітні уразливості, які можуть бути фатальними для жертви. Зловмисники можуть використовувати різноманітні веб-атаки, до яких веб-ресурс чи звичайний веб-сайт може бути не захищений. Тому ми розглянемо найбільш застосовувані веб-атаки, які використовують зловмисники, серед яких є: DoS та DDoS, різноманітне шкідливе ПЗ, брутфорс паролів, мережева розвідка, ін'єкцій, міжсайтовий скриптинг, IP spoofing, Broken Authentication, прогнозування сеансу, Insecure deserialization, Cross-Site Request Forgery, Man-In-the-Middle.

1) DDoS та DoS

Розподілена атака типу «відмова в обслуговуванні» (DDoS) – це зловмисна спроба порушити нормальний трафік цільового сервера, служби або мережі шляхом переповнення цілі або її інфраструктури потоком інтернет-трафіку.

DDoS-атаки досягають ефективності за рахунок використання кількох скомпрометованих комп'ютерних систем як джерела атакуючого трафіку. До машин, що експлуатуються, можуть належати комп'ютери та інші мережеві ресурси, такі як пристрої IoT. На високому рівні DDoS-атака подібна до несподіваної пробки на шосе, що не дозволяє звичайному трафіку дістатися місця призначення [1].

2) Брутфорс паролів

Атака методом грубої сили є популярним методом злому: за деякими даними, атаки методом грубої сили становлять п'ять відсотків підтверджених порушень безпеки. Атака грубої сили включає «вгадування» імені користувача і пароля для отримання несанкціонованого доступу до системи. Груба сила – це простий метод атаки з високою ймовірністю успіху.

Деякі зловмисники використовують програми та скрипти як інструменти для перебору. Ці інструменти пробують численні комбінації паролів, щоб уникнути процесів аутентифікації. В інших випадках зловмисники намагаються отримати доступ до веб-програм, шукаючи правильний ідентифікатор сеансу. Мотивація зловмисника може включати крадіжку інформації, зараження сайтів шкідливим ПЗ або порушення роботи служби [2].

3) Ін'єкції

SQL-ін'єкція — це вразливість веб-безпеки, яка дозволяє зловмиснику втручатися в запити, які робить програма до своєї бази даних. Зазвичай це дозволяє зловмиснику переглядати дані, які він не може отримати. Це можуть бути дані, що належать іншим користувачам, або будь-які інші дані, до яких може отримати доступ сама програма. У багатьох випадках зловмисник може змінити або видалити ці дані, що призведе до постійних змін вмісту або поведінки програми. У деяких ситуаціях зловмисник може ескалувати атаку шляхом впровадження SQL-коду, щоб скомпрометувати базовий сервер або іншу внутрішню інфраструктуру, або виконати атаку типу "відмова в обслуговуванні" [3].

PHP ін'єкція — це вразливість на рівні програми, яка може дозволити зловмиснику виконувати різні види шкідливих атак, таких як впровадження коду, впровадження SQL, обхід шляху та відмова в обслуговуванні програми, залежно від контексту. Вразливість виникає, коли дані, що введені користувачем, не очищаються належним чином перед передачею в PHP-функцію unserialize(). Оскільки PHP припускає серіалізацію об'єктів, зловмисники можуть передавати спеціальні серіалізовані рядки вразливому виклику unserialize(), що призводить до впровадження довільних об'єктів PHP до програми [4].

LDAP ін'єкція — це вразливість, коли запити створюються на основі ненадійних вхідних даних без попередньої перевірки або очищення. LDAP використовує запити, складені з предикатів, у яких використовуються спеціальні символи (наприклад, дужки, зірочки, амперсанди чи лапки). Подібні метасимволи керують значенням запиту; таким чином, впливаючи на тип та кількість об'єктів, вилучених з базового каталогу. Якщо зловмисник може надіслати введення, що містить ці керуючі символи, він може змінити запит і змінити можливу поведінку [5].

XPath – це тип атаки, при якому шкідливе введення може призвести до несанкціонованого доступу або розкриття конфіденційної інформації, такої як структура та вміст XML-документа. Це відбувається, коли введення користувача використовується при побудові рядка запиту. Багато методів, які можна використовувати в атаці з використанням SQL, залежать від параметрів діалекту SQL, використовуваного цільовою базою даних, тоді як атаки з використанням XPath можуть бути більш адаптованими і повсюдними [6].

SSI – це експлойт на стороні сервера, який дозволяє зловмиснику відправити код до програми для подальшого виконання локально на веб-сервері. Атаки з використанням SSI можуть бути успішними лише в тому випадку, якщо веб-сервер дозволяє виконання SSI без належної перевірки [7].

4) Міжсайтовий скриптинг

Атаки з використанням міжсайтових сценаріїв (XSS) — це тип застосування, при якому шкідливі сценарії впроваджуються на безпечні та надійні веб-сайти. Атаки XSS відбуваються, коли зловмисник використовує веб-програму для відправки шкідливого коду, як правило, у вигляді сценарію на стороні браузера, іншому кінцевому користувачеві. Недоліки, які дозволяють цим атакам увінчатися успіхом, досить широко поширені і виникають скрізь, де веб-додаток використовує вхідні дані від користувача в вихідних даних, що генеруються ним, без їх перевірки або кодування. Зловмисник може використовувати XSS для відправки шкідливого скрипта нічого не підозрюваному користувачеві. Браузер кінцевого користувача не може дізнатися, що скрипту не можна довіряти і виконає його. Оскільки він вважає, що сценарій отримано з надійного джерела, шкідливий сценарій може отримати доступ до будь-яких файлів cookie, маркерів сеансу або іншої конфіденційної інформації, збереженої браузером та використовуваної на цьому сайті. Ці сценарії можуть навіть переписувати вміст сторінки HTML [8].

5) IP spoofing

Це тип зловмисної атаки, при якій зловмисник приховує справжнє джерело IP-пакетів, щоб було важко дізнатися, звідки вони прийшли. Зловмисник створює пакети, змінюючи вихідну IP-адресу, щоб видати себе за іншу комп'ютерну систему, приховати особистість

відправника або те й інше. Поле заголовка підробленого пакета для вихідної IP-адреси містить адресу, яка відрізняється від фактичної вихідної IP-адреси [9].

6) Man-in-the-middle

Це тип кібератаки, при якій зловмисники перехоплюють існуючу розмову або передачу даних, або підслуховуючи або видаючи себе за законного учасника. Жертві здаватиметься, що відбувається стандартний обмін інформацією, але, впровадившись у «середину» розмови чи передачі, зловмисник може непомітно перехопити інформацію [10].

7) Підробка міжсайтових запитів

Є вектором атаки, який обманом змушує веб-браузер виконувати небажану дію в додатку, до якого увійшов користувач. Успішна CSRF-атака може мати руйнівні наслідки як бізнесу, так користувача. Це може призвести до пошкодження відносин з клієнтами, несанкціонованих переказів коштів, зміни паролів та крадіжки даних, включаючи вкрадені файли cookie сеансу [11].

8) Broken authentication

Це загальний термін для кількох вразливостей, які зловмисники використовують для видачі законних користувачів в Інтернеті. У широкому сенсі порушення автентифікації відноситься до слабкостей у двох областях: управління сеансом та управління обліковими даними. І те, й інше класифікується як порушена автентифікація, оскільки зловмисники можуть використовувати будь-який спосіб маскування під користувача: вкрадені ідентифікатори сеансу або вкрадені облікові дані для входу [12].

9) Шкідливе програмне забезпечення

Це будь-яка програма, створена для виконання будь-якого несанкціонованого - і, як правило, шкідливого - дії на пристрої користувача. Приклади шкідливих програм: вірус, руткіт, шпигунська програма, троянський кінь, рекламні програми [13].

10) Прогнозування сеансу

Атака передбачення сеансу зосереджена на передбаченні значень ідентифікатора сеансу, які дозволяють зловмиснику обійти схему аутентифікації програми. Аналізуючи та розуміючи процес генерації ідентифікатора сеансу, зловмисник може передбачити справжнє значення ідентифікатора сеансу та отримати доступ до програми [14].

11) **Insecure deserialization**

Небезпечна десеріалізація — це відома вразливість, що рідко зустрічається, при якій зловмисник вставляє шкідливі об'єкти в веб-додаток. Це дозволяє їм викликати атаки типу

«відмова в обслуговуванні» (DoS), атаки з віддаленим виконанням коду, SQL-ін'єкції, обхід шляху та обхід автентифікації. Атаки десеріалізації є серйозною загрозою і можуть мати серйозні наслідки для компаній та їх клієнтів. Потенційні вразливості були виявлені у найпопулярніших мовах програмування, включаючи Java, Python, .NET, PHP, Node.js та Ruby [15].

12) **Buffer overflow**

Атака переповнення буфера відбувається, коли зловмисник маніпулює помилкою кодування для виконання зловмисних дій та компрометації вразливої системи. Зловмисник змінює шлях виконання програми та перезаписує елементи пам'яті, що змінює шлях виконання програми, щоб пошкодити існуючі файли або розкрити дані. Атака переповнення буфера зазвичай включає порушення мов програмування та перезапис кордонів буферів, у яких вони існують. Більшість переповнень буфера викликано поєднанням маніпулювання пам'яттю та помилкових припущень про склад або розмір даних [16].

13) **Insufficient Logging & Monitoring**

Журнали дають уявлення про діяльність організації. Створені журнали та контрольні журнали дозволяють організації усувати неполадки, відстежувати події, виявляти інциденти та дотримуватися нормативних вимог. Недостатнє ведення журналу та моніторинг – це відсутність журналів важливої для безпеки інформації або відсутність належного формату журналу, контексту, сховища, безпеки та своєчасного реагування для виявлення інциденту

чи порушення. Відповідно до звіту IBM про витоку даних за 2020 рік, середній час виявлення та припинення витоку даних становить 280 днів. Журнали є важливою частиною реагування на інциденти. Організація може бути приголомшена порушенням, яке може залишитися непоміченим із непоправними нормативними, фінансовими та юридичними проблемами. Належне управління журналами забезпечить швидше виявлення та усунення порушень, що заощадить час, гроші та репутацію бізнесу.

Збитки від атак

Виток даних коштували компаніям у 3,92 мільйона доларів у 2019 році та 3,86 мільйона доларів у 2020, і багато з цих інцидентів можна було б запобігти при правильному підході та проведенні комплексного аудиту для усунення уразливостей у безпеці веб- додатків.

У 2021 році охорона здоров'я, енергетика, фінансові послуги та фармацевтичні компанії зазнали середню загальну вартість злому даних значно вище, ніж менш регульовані галузі, такі як туризм, медіа та дослідження. Організації державного сектору традиційно мають найнижчі витрати на злом даних у цьому дослідженні, тому що вони навряд чи відчути значну втрату клієнтів у результаті порушення даних [19]. Це показано на рис.1.

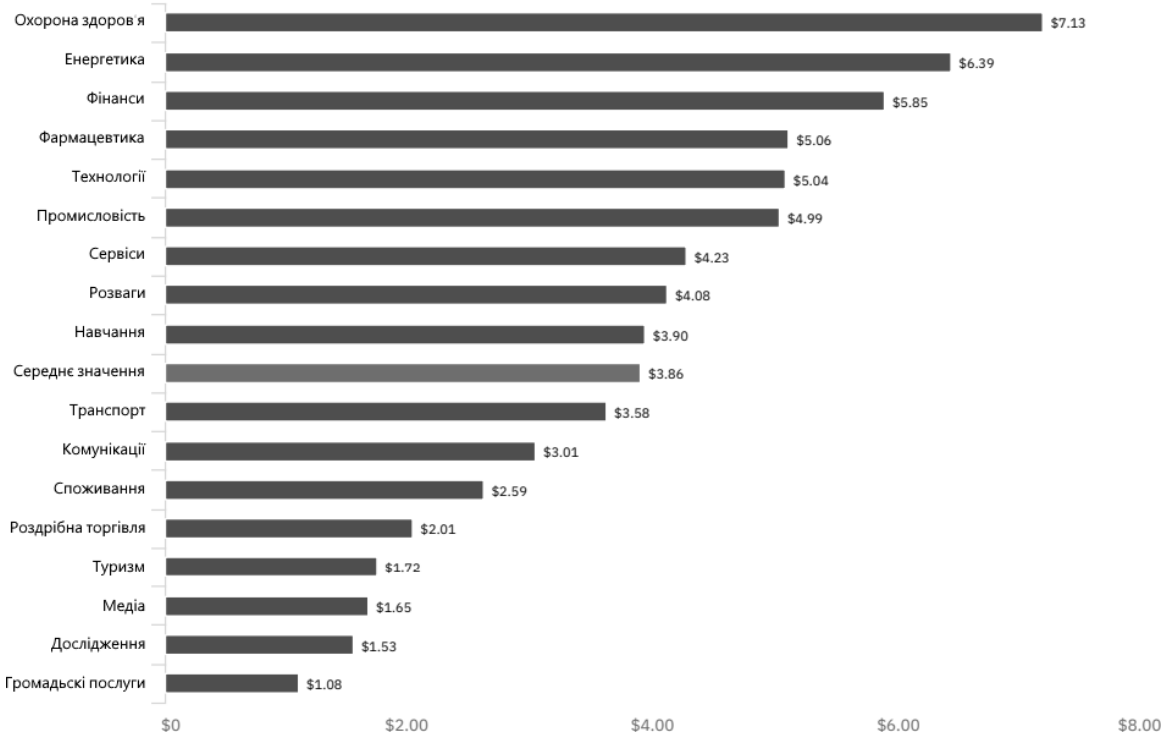

Рис. 1. Втрати через атаки у різних галузях

OWASP Топ-10 та тенденції

Відкритий проект безпеки веб-додатків (OWASP) – це відкрита спільнота інженерів та IT-фахівців з безпеки, мета якої – зробити Інтернет безпечнішим для користувачів та інших організацій.

OWASP «Топ 10» — це набір стандартів для поширених вразливостей та способів запобігти їх перетворенню на проломи для вашої компанії та користувачів. Зрештою, OWASP Топ 10 є галузевим стандартом і повинен враховуватися при розгортанні будь-якої веб-програми або мобільної програми [17, 18]. Складники цього топу наведено на рис. 2.

У період з 2016 по 2019 рік кількість вразливостей високого та середнього ступеня серйозності неухильно знижувалась з кожним роком. У 2020 році їх кількість трохи збільшилася, швидше за все, внаслідок бізнес-рішень, пов'язаних із впливом COVID-19 на організацію роботи у всьому світі. Більшість організацій потребують дистанційної роботи.

Віддалені працівники, як і раніше, будуть мішенню для кіберзлочинців. Підприємствам довелося перенаправити свої IT-ресурси. Пандемія змусила їх змінити організацію роботи. В результаті підприємства відклали багато проектів веб-додатків. Процент організацій, що використовують віддалену працю є 54 відсотки. З початку пандемії ФБР повідомило про зростання кількості зареєстрованих кіберзлочинів на 300%, що є непрямим натяком його вплив [20].

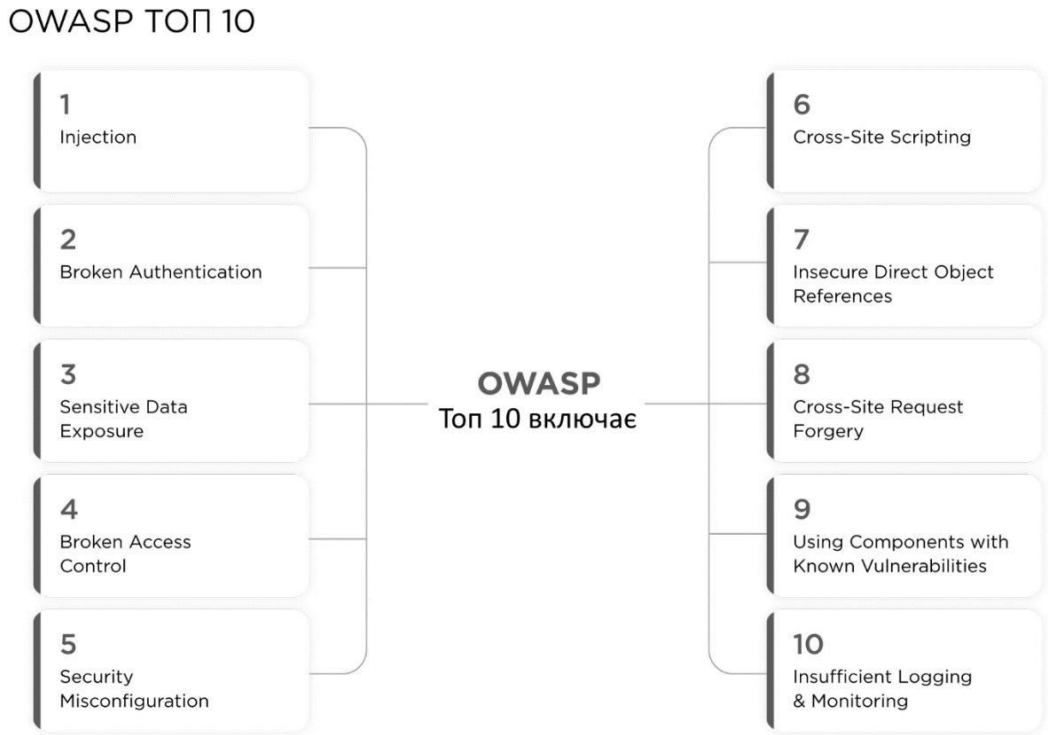

Рис. 2 Найпоширеніші уразливості веб-сайтів

Кількість кібератак у 2021 році збільшилась на 6,5% порівняно з 2020 роком. Серед кіберзагроз помічено домінування шифрувальників серед шкідливого ПЗ, підвищення інтенсивності атак на криптовалютні біржі, поява критично небезпечних вразливостей, які відразу ж експлуатувалися зловмисниками у багатьох організаціях у всьому світі. Серед таких уразливостей, наприклад, ProxyLogon у MS Exchange, PrintNightmare у службі друку Windows, CVE-2021-40444 у модулі MSHTML в Internet Explorer. У грудні 2021 року навіть з'явився термін «кіберпандемія» через велику кількість атак з використанням вразливості CVE-2021-44228 у бібліотеці Log4j. У 2021 році частка хакінгу та експлуатації веб-уразливостей сумарно склала 43% серед усіх використаних методів в атаках на організації, що на 8 п. п. більше, ніж у попередньому році.

Висновок

Розглянуто найбільш поширені веб-атаки на різноманітні веб-ресурси, а також «дірки в безпеці», які можуть бути причиною можливої майбутньої атаки та, у разі її успішності, отримання збитків жертвою. Проаналізовано можливі збитки у різних галузях за статистикою минулих років.

Перелік посилань

1. DoS та DDoS атаки [Електронний ресурс] – Режим доступу до ресурсу: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

2. Атака грубої сили [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/brute-force-attack/

3. SQL [Електронний ресурс] – Режим доступу до ресурсу: https://portswigger.net/web-security/sql-injection
4. PHP [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-community/vulnerabilities/PHP_Object_Injection
5. LDAP [Електронний ресурс] – Режим доступу до ресурсу: https://www.synopsys.com/glossary/what-is-ldap-injection.html
6. XPath [Електронний ресурс] – Режим доступу до ресурсу: https://medium.com/@shatabda/security-xpath-injection-what-how-3162a0d4033b
7. SSI [Електронний ресурс] – Режим доступу до ресурсу: https://www.whitehatsec.com/glossary/content/ssi-injection
8. XSS [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-community/attacks/xss/
9. IP spoofing [Електронний ресурс] – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/IP-spoofing
10. Man-in-the-middle [Електронний ресурс] – Режим доступу до ресурсу: https://www.pandasecurity.com/en/mediacenter/security/man-in-the-middle-attack/
11. CSRF [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/application-security/csrf-cross-site-request-forgery/
12. Broken authentication [Електронний ресурс] – Режим доступу до ресурсу: https://auth0.com/blog/what-is-broken-authentication/
13. Malware [Електронний ресурс] – Режим доступу до ресурсу: https://www.kaspersky.ru/resource-center/preemptive-safety/faq
14. Session_Prediction [Електронний ресурс] – Режим доступу до ресурсу: https://owasp.org/www-community/attacks/Session_Prediction
15. Insecure deserialization [Електронний ресурс] – Режим доступу до ресурсу: https://crashtest-security.com/insecure-deserialization/
16. Buffer overflow [Електронний ресурс] – Режим доступу до ресурсу: https://www.fortinet.com/resources/cyberglossary/buffer-overflow
17. OWASP Top 10 : Insufficient Logging & Monitoring [Електронний ресурс] – Режим доступу до ресурсу: https://www.siemba.io/post/owasp-top-10-insufficient-logging- monitoring
18. Common Web Application Security Vulnerabilities and How to Prevent Them [Електронний ресурс] – Режим доступу до ресурсу: https://relevant.software/blog/web- application-security-vulnerabilities/
19. Cost of a Data Breach Report [Електронний ресурс] – Режим доступу до ресурсу: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data- Breach-Study-2020.pdf
20. COVID-19 News [Електронний ресурс] – Режим доступу до ресурсу: https://www.imcgrupo.com/covid-19-news-fbi-reports-300-increase-in-reported-cybercrimes/

Надійшла: 19.01.2022 Рецензент: д.т.н., доцент Ахрамович В.М.