УДК 629.735.018.7.015.3.025.1

Д.А. Хижняк, О. Туровський, д.т.н., професор
(Національний авіаційний університет, Україна)

Кібератаки на веб-ресурси та способи захисту від атак

Кібератаки на веб-ресурси стають все поширенішими, що може призвести до серйозних наслідків для бізнесу та індивідуальних користувачів. У цій анотації розглядаються різні види кібератак на веб-ресурси, а також наводяться методи захисту від атак .

Із початком військової агресії зі сторони росії на території України, розпочалася також “комп’ютерна війна” між державами. Під найбільший удар попали офіційні державні ресурси, більш менше страждали приватні підприємницькі веб-ресурси (новинні блоги, інтернет магазини, повчальні та розважальні сервіси).

До найпоширеніших типів атак на веб-ресурсів належать: SQL-ін'єкції, Кросс-сайтові скрипти, Кросс-сайтові запити між сайтами, Напад на переповнення буферу, Деніал-сервіс атаки, Атака на розкриття конфіденційної інформації. Усі перераховані методи мають велику відміну один від одного але їх об’єднує тільки одне – виведення зі строю вер-ресурсу. Для розуміння як власник може забезпечити безпеку своєму сайту, потрібно розібрати кожен тип атаки окремо.

SQL ін'єкція — спосіб атаки на веб-додатки, що базуються на SQL-запитах до баз даних. Ін'єкція полягає в тому, що зловмисник вводить у веб-форму або параметри URL підрядок коду SQL, який потім виконується в базі даних без перевірки на правильність введених даних. За допомогою SQL-ін'єкції, зловмисник може отримати доступ до бази даних та змінювати її вміст, виконувати злочинні дії, такі як видалення, зміна або витік конфіденційної інформації. Цей вид атаки є дуже небезпечним, тому важливо забезпечити захист веб-додатків від SQL-ін'єкції шляхом використання практик безпеки програмного забезпечення, таких як параметризовані запити, фільтрація введення користувача та обмеження доступу до бази даних.

Кросс-сайтовий скриптинг (XSS) - атаки на веб-додатки, що дозволяє зловмисникам внедрювати шкідливий код у веб-сторінки, що відображаються на браузері користувача. За допомогою XSS-атак, зловмисники можуть отримати доступ до конфіденційних даних користувачів, таких як паролі, номери кредитних карток та інші особисті дані. Крім того, XSS може використовуватися для розповсюдження шкідливих програмних засобів, які можуть спричинити витік даних або завдати шкоди системі. Одним із способів захисту від XSS є валідація введеного користувачем контенту та використання методів екранизації, що дозволяють забезпечити безпеку відображення даних користувачів на сторінках веб-додатків. Також важливо оновлювати програмне забезпечення та плагіни браузера, щоб зменшити ризик XSS-атак.

Кросс-сайтові запити між сайтами (CSRF): це атака, при якій зловмисник надсилає запити від імені авторизованого користувача, щоб змінити його дані або виконати дії в його імені.

Напад на переповнення буферу - це атака, при якій зловмисник вводить більше даних, ніж дозволено в певному полі введення, що може призвести до виконання шкідливого коду на сервері.

Атака на відмову в обслуговуванні, розподілена атака на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (distributed) denial-of-service attack) — перевантаження ресурсів веб-серверів, що призводять до тимчасової недоступності веб-сайтів та інших онлайн сервісів. У DoS-атаках, зловмисники відправляють велику кількість запитів на веб-сервер, що призводить до перевантаження ресурсів та зниження доступності веб-сайту. У DDoS-атаках, зловмисники використовують ботнети (мережі комп'ютерів, що були заражені шкідливим ПЗ), щоб здійснювати атаки з різних точок одночасно. Ці атаки можуть завдати серйозної шкоди бізнесу та іншим веб-сайтам, зокрема, призводять до втрати грошей, даних та клієнтів. Захист від DoS та DDoS атак може включати використання захисних технологій, таких як вогнезахисні стіни, програмне забезпечення для виявлення та блокування атак, та планів відновлення після атаки. . Взагалі відмова сервісу здійснюється:

- примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу;
- заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам.

Якщо атака відбувається одночасно з великої кількості IP-адрес, то її називають розподіленою (англ. distributed denial-of-service — DDoS). Виділемо найголовшніше DDoS атак, а саме те, що вони поділяються за рівнями моделі OSI. Найпоширеніші з них L3/L4 та L7. Розглянемо більш детальніше:

Атаки на рівні L3 / L4 (по моделі OSI):

- UDP flood з ботнету (прямо із інфікованих пристроїв на атакуючий сервіс відправляється багато запитів, серверам завалюють канал);
- Посилення DNS/NTP/etc (із інфікованих пристроїв відправляється багато запитів на небезпечні DNS/NTP/etc, адрес відправника підсилюється, туча пакетів з відповіддю на запит завалює канал тому, кого атакують; так само виконуються найбільш масові атаки в сучасному Інтернеті);
- SYN / ACK flood (на атакувані сервери відправляється багато запитів на встановлення з'єднань, відбувається переповнення чергових з'єднань);
- атаки з фрагментацією пакетів, ping of death, ping flood.

Ці атаки ставлять за мету «завалити» канал-сервер або «збити» його здатність приймати новий трафік.

Хоча SYN/ACK флуд і ампліфікація сильно відрізняються, багато компаній борються з ними одинаково добре. Проблеми виникають з атаками наступної групи.

Атаки на L7 (рівень додатку):

- http flood (якщо атакується веб-сайт або який-небудь http api);

- атаки на слабкі ділянки сайта (не мають кеша, дуже сильно навантажують сайт, атаку тощо).

Ціль — задати сервер «тяжко працювати», обробляти багато «як будто реальних запитів» і залишитися без ресурсів для поточних запитів.

Хоча є й інші форми атаки, ці — самі.

Серйозні атаки на рівні L7 створюються унікальним способом під кожен атакуючий проект.

Основні методи захисту веб-ресурсу від кібератак:

Використовуйте надійне програмне забезпечення для веб-серверів і баз даних, а також регулярно оновлюйте їх до останніх версій.

Застосуйте SSL-шифрування для захисту передачі даних між веб-сайтом і користувачем.

Використовуйте парольний захист та багаторівневу автентифікацію для доступу до веб-інтерфейсу адміністратора.

Використовуйте захист від Cross-Site Scripting (XSS) та SQL Injection.

Обмежуйте доступ до файлів на сервері, що містять конфіденційну інформацію.

Встановіть захист від атак відмови в обслуговуванні (DoS) та розподіленої відмови в обслуговуванні (DDoS).

Регулярно стежте за системами журналів, щоб виявити якісь загрози та надзвичайні ситуації.

Проведіть тестування на проникнення для слабких місць у системі та їх виправлення.

Список літератури

1. Братвейт Ш., “5 найпоширеніших атак на веб-сайти та як від них захиститися” 2023 рік - https://www.websiterating.com/uk/online-security/most-common-website-attacks-how-to-defend-against-them/
2. Fortinet Company, “What is DDoS Protection?” 2020 рік – https://www.fortinet.com/resources/cyberglossary/ddos-protection
3. Web Security Academy, “What is SQL Injection? Tutorial & Examples” 2023рік - https://portswigger.net/web-security/sql-injection
4. Owasp Company, “Cross Site Request Forgery (CSRF)”, 2023 рік - https://owasp.org/www-community/attacks/csrf