УДК 004.056.5

Дмитро КАРПЕЦ

Західноукраїнський національний університет

НАСЛІДКИ CROSS SITE SCRIPTING АТАК У ВЕБ ДОДАТКАХ

Вступ. Згідно зі статистикою у звіті Incident Response Report 2024 від Palo Alto Network Unit 42, веб додатки є постійною ціллю атак та набувають зростання. Частка розслідувань інцидентів, саме атак на веб додатки займала приблизно 12.7% у 2021, а в останній час досягла 21.2%. Це вказує на те, що компрометація веб додатків залишається значною загрозою для компаній, а використання вразливостей зазвичай пов'язане з отриманням несанкціонованого доступу [1].

Однією з поширених вразливостей безпеки веб додатків є можливість реалізації Cross-Site Scripting атак, в результаті яких зловмисник може отримати несанкціонований доступ через викрадання кукі та сесійних токенів користувачів. Не допущення можливості реалізації таких атак є надзвичайно важливою задачею та досягається під час процесів розробки веб додатків.

Мета: дослідження наслідків Cross-Site Scripting атак у веб додатках**.**

1. Нехтування процесом перевірки безпеки під час життєвого циклу програмного забезпечення

Сьогодні під час розробки програмного забезпечення часто не приділяється увага перевірці на наявність вразливостей та інших помилок, а згадують про це тільки на стадії розгортання. Такий підхід є помилковим та часто призводить до майбутніх надлишкових фінансових витрат [2].

Для запобігання подібного, одним із найефективніших підходів є покращення процесу життєвого циклу програмного забезпечення (ЖЦПЗ), а саме впровадження перевірок безпеки на кожному з його етапів. ЖЦПЗ починається з визначення ПЗ та закінчується його підтримкою після розгортання [3].

На рисунку 1 зображено в загальному вигляді процес ЖЦПЗ та кореляція зростання економічних втрат для виправлення вразливостей відносно проходження етапів розробки ПЗ

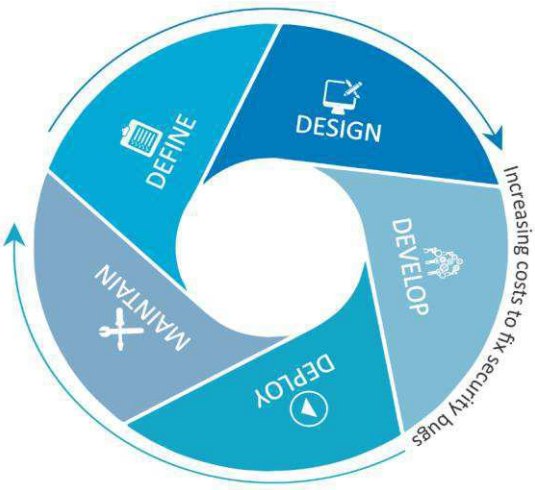

Рисунок 1 - Зростання ціни виправлення вразливостей безпеки відносно етапів життєвого циклу програмного забезпечення

2. Наслідки успішних реалізацій Cross Site Scripting атак у веб додатках

У разі успішного виконання Cross Site Scripting атаки, зловмисник може спричинити різного рівня наслідки. Розгляньмо їх в таблиці 1.

Таблиця 1 - Наслідки Cross Site Scripting атак у веб додатках

Дії	Наслідки
Викрадення кукі файлів	Доступ до особистої інформації користувача. Від інформації про взаємодію із сайтом, такої як мова, історія про відвідувані сторінки, адреси, імена - до електронних адрес, логінів, паролів.
Викрадення сесійного токена	У разі якщо сесійний токен зберігається у кукі файлах, його захоплення призводить до повної компрометації облікового запису користувача.
Перенаправлення користувача на іншу сторінку чи сайт	Залежно від плану зловмисника, наслідки можуть бути дуже різними, від фішингу до зараження шкідливим ПЗ
Модифікація відображеного контенту	Ціль такої модифікації залежить від призначення сайту на якому сидить користувач. Одна із популярних це зниження позитивного відношення до компанії, сервісу, тощо.
Встановлення шкідливого ПЗ	Залежно від типу шкідливого ПЗ, наслідки можуть бути менш чи більш значними, проте сам факт можливості його встановлення не піддається оцінці серйозності проблеми

Залежно від дій зазначених в таблиці 1, кінцеві наслідки деяких з них можуть бути від не серйозних до надзвичайно серйозних, це залежить від типу, навичок та мети зловмисника. В той час коли скрипт виконає шкідливі дії на стороні жертви, фаховий спеціаліст може здійснити компрометацію облікового запису жертви.

Висновок. Досліджено на порівняно наслідки Cross Site Scripting атак у веб додатках. Даний тип атак може спричинити серйозні наслідки як зі сторони користувача веб додатка, так і зі сторони його власника. Головним фактором для їх запобігання є процеси перевірки безпеки на кожному етапі розробки веб додатків.

Популярність веб додатків та взаємодія між ними є невід'ємною частиною сучасної людини. Це значить що особисті дані користувачів мають бути конфіденційними та захищеними від компрометації.

Перелік використаних джерел.

1. Unit 42 Palo Alto Networks - Incident Response Report 2024. [Електронний ресурс]. - Режим доступу: https://unit42.paloaltonetworks.com/unit42-incident-response-report-2024-threat-guide/

2. OWASP - Cross Site Scripting (XSS). [Електронний ресурс]. - Режим доступу: https://owasp.org/www-community/attacks/xss/

4. CGISecurity - The Cross-Site Scripting (XSS) FAQ. [Електронний ресурс]. - Режим доступу: https://www.cgisecurity.com/xss-faq.html