НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

ТОМ 1

14 травня – 23 травня 2024 р.

УДК 004.05

АТАКА ВЕБ-БРАУЗЕРА – BROWSER EXPLOITATION FRAMEWORK

Асистент Калашнікова Ю.В.,
студент групи 101 КБ Топчій Ю. П.
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Фактично, кожен бізнес, кожна електронно-комунікаційна система, апаратно-програмна платформа потенційно вразлива і потребує перевірки. Щодня з'являються десятки і сотні нових кіберзагроз, включаючи вразливості нульового дня (0-Zero Day Vulnerabilities), про які самі розробники не знають. Тому тестування на проникнення є своєрідним "щепленням" від майбутніх загроз. Регулярне тестування на проникнення рекомендується для підготовки до Advanced Persistent Threats, які являють собою широкомасштабні цільові атаки.

Актуальність даної роботи полягає у потребі вирішення проблеми щодо незахищеності веб-застосунків, які розробляються з нуля або на основі CMS. Метою та завданням проведеного дослідження є аналіз та розробка методів автоматизації та інтеграція їх у програми для сканування.

Як і у випадку з багатьма іншими програмами, веб-браузери, які не мають належних виправлень безпеки, вразливі до атак та пост-експлойтів. Більше того, навіть повністю виправлений веб-браузер вразливий до атак, якщо не повністю виправлені надбудови браузера. Слід пам'ятати, що коли користувач вносить патчі у браузер, додатки не виправляються автоматично.

Браузерні атаки зазвичай походять зі шкідливих веб-сайтів. Однак невиконання політик безпеки веб-додатків або вразливості в обслуговуванні програмного забезпечення веб-сайтів можуть дозволити зловмисникам скомпрометувати веб-сайти, впровадити шкідливе програмне забезпечення відвідувачам, які нічого не підозрюють.

Сценарій реалізації браузерної атаки:

- додавання скрипта;
- перенаправлення користувача на інший веб-сайт;
- завантаження шкідливого програмного забезпечення.

Сьогодні Browser Exploitation Framework (далі – BeEF) – це потужний та інтуїтивно зрозумілий інструмент безпеки; BeEF є інноваційним підходом, який надає тестувальникам на проникнення практичну реалізацію атак на стороні клієнта. На відміну від інших фреймворків безпеки, BeEF фокусується на використанні вразливостей браузерів для оцінки стану безпеки цілі.

Даний фреймворк досягає своїх цілей шляхом викрадення інформації або отримання віддаленого доступу до системи за допомогою різних

методів, а саме впровадження коду, маніпуляції з пам'яттю браузера, проведення тестів на проникнення, атаки на веб-додатки.

Основні риси BeEF:

- підтримка різних браузерів (Google Chrome, Mozilla Firefox, Microsoft Edge, Safari та інші);
- модульна структура (проведення атак та збір інформації про цільового користувача);
- атаки через вразливості браузера (Cross-Site Scripting – XSS);
- підтримка скриптів (використання вбудованих JavaScript для створення власних модулів та атак);
- гнучкість та розширюваність (відкритий вихідний код);
- віддалене управління (керування атаками через веб-інтерфейс).

Вперше BEF застосовувався як спроба використати вразливості веб-браузерів для здійснення атак. З тих пір BEF вдосконалився. Цей інструмент став більш потужним і ефективним. Зростаюча популярність веб-додатків і збільшення кількості вразливостей веб-браузерів зробили BEF важливим інструментом для тестування систем захисту інформації та кібербезпеки та захисту веб-додатків.

Переваги використання BEF:

- висока ефективність;
- широкі можливості експлуатації вразливостей у веб-браузерах;
- отримання доступу до системи;
- виконання різних видів атак на веб-додатки.

Недоліки:

- обмежена сумісність з певними браузерами або операційними системами;
- можливість виявлення атаки антивірусними програмами та захисними заходами.

У порівнянні з іншими інструментами, BEF відрізняються широким спектром функціональних можливостей, гнучкістю та ефективністю використання. Вони можуть підтримувати більшу кількість експлойтів і більше веб-браузерів та операційних систем.

Унікальними особливостями BEFs є можливість роботи в режимі реального часу, широкий набір інструментів і можливість їх розширення за допомогою модулів і плагінів.

Перспективою подальшого розвитку BEF є розробка нових експлойтів, підтримка нових версій веб-браузерів та операційних систем, а також вдосконалення застосування за допомогою нових модулів та плагінів.

Підсумовуючи, необхідно зазначити, що атаки веб-браузера є доволі широкою та розгалуженою темою. В умовах сьогодення зловмисники можуть здійснювати всі види атак від XSS до переповнення буфера. BeEF – це простий інструмент тестування на проникнення, який може використовуватися будь-ким для тестування деяких атак або злому системи. Такі програми зазвичай призначені для дистанційного керування

комп’ютером та отримання особистої інформації, наприклад, даних кредитної картки та банківських реквізитів.

Література:

1. PortSwigger. Products, Research and Academy [Електронний ресурс]. – 2021. – https://portswigger.net/.

2. Acunetix. Acunetix Vulnerability Scanner [Електронний ресурс]. – 2021. – https://www.acunetix.com/vulnerability-scanner/.

3. OWASP. OWASP Zed Attack Proxy (ZAP) [Електронний ресурс]. – 2021. – https://owasp.org/www-project-zap/.