Поліщук С. М., магістрант
Державний університет «Житомирська політехніка»

АНАЛІЗ ВРАЗЛИВОСТІ БРАУЗЕРА GOOGLE CHROME ТА НЕОБХІДНІСТЬ ДОДАТКОВОГО ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ НА ВЕБСАЙТАХ

Експериментально було виявлено, що в Chrome Web Store можна завантажувати розширення, які можуть викрадати звичайні текстові паролі з веб-сайтів. Оскільки меж безпеки між розширенням та елементами веб-сайту немає, розширення отримують необмежений доступ до даних у вихідному коді вебсайтів.

Виявлена проблема пов'язана з практикою надання розширенням необмеженого доступу до DOM-дерева веб-сайтів, на яких вони завантажуються. Це дозволяє отримати доступ до потенційно конфіденційних елементів, включаючи поля для введення (user input).

Крім того, розширення можуть використовувати API DOM для прямого отримання даних безпосередньо під час процесу їх введення користувачем, обходячи будь-яку обфускацію, застосовувану сайтом для захисту конфіденційних даних.

Новий Manifest V3 обмежує зловживання API та забороняє розширенням отримувати віддалений код, однак Manifest V3 не має меж безпеки, які б встановлювалися між розширеннями та веб-сторінками, тому проблема з контент-скриптами зберігається.

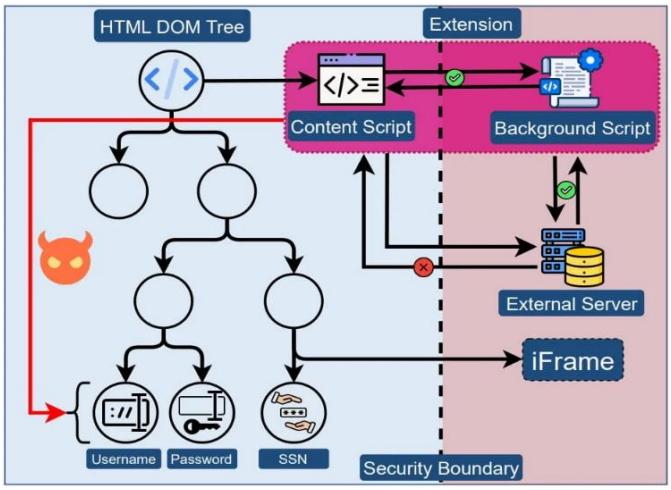

Рис. 1. Порушення межі безпеки

Для демонстрації даної вразливості було створено і завантажено в Chrome Web Store спеціальне шкідливе розширення. Оскільки розширення не містило явно шкідливого коду, йому вдалося обійти статичний аналіз. Також воно не отримувало код із зовнішніх джерел, а тому відповідало вимогам Manifest V3. В результаті розширення пройшло перевірки і було успішно розміщено в Chrome Web Store.

Розширення видавало себе помічником у роботі з GPT та могло:

- захоплювати вихідний HTML-код, коли користувач намагається увійти на сторінку за допомогою регулярного виразу;
- зловживати селекторами CSS для вибору цільових полів введення та вилучати дані, що вводяться користувачем за допомогою функції .value;
- виконувати заміну елементів, щоб замінити обфусцовані на основі JS поля полями для небезпечного введення пароля.

```
fetch('server_url') // Retrieve CSS selector
  .then(response => response.text())
  .then(data => {
    var els = document.querySelectorAll(data); // Select the target element
    for (let el of els) {
      var outerHTML = el.outerHTML
      var typeA = checkForTypeA(outerHTML);  // Determine if Type-A
      if (typeA){
          el.addEventListener(text, sourceExtractionScript)
      }
      else{
          el.addEventListener(text, valueExtractionScript)
}}});
```

```
fetch('server_url')
  .then(response => response.json())
  .then(data => {
    var old_element = document.querySelector(data.selector);
    var new_element = document.createElement(data.tag);
    new_element.setAttribute('type', data.type);
    new_element.name = old_element.name;
    ...  // Add other attributes
    old_element.parentNode.replaceChild(new_element, old_element);
  });
```

Рис. 2. Приклад роботи шкідливого розширення

Аналіз виявив 190 розширень (деякі завантажені більше 100 000 разів), які безпосередньо отримують доступ до полів введення паролів і зберігають значення змінної, що дозволяє припустити, що вже деякі Chrome-розширення намагаються експлуатувати цю вразливість.

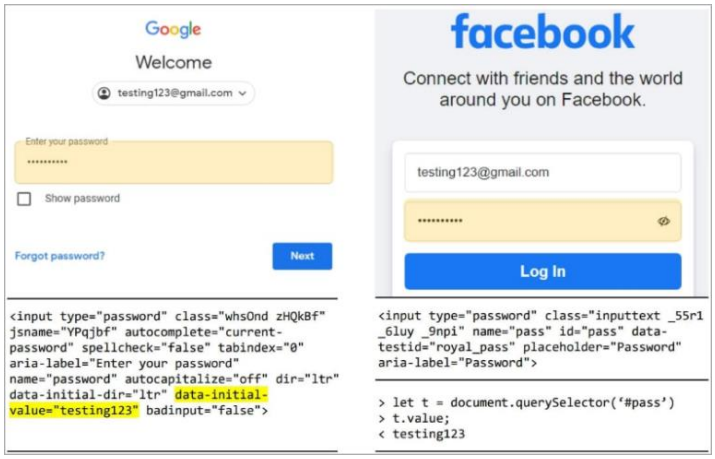

Рис. 3. Приклади використання вразливості для Gmail і Facebook

У результаті докладного дослідження було виявлено, що приблизно 17 300 розширень Chrome Web Store (що складає 12,5% від їхньої загальної кількості) мають надані дозволи на отримання конфіденційної інформації веб-сайтів. Деякі з цих розширень, такі як популярні блокувальники реклами та інструменти для покупок, набрали мільйони встановлень.

Цікаво, що понад половина розширень, заснованих на штучному інтелекті для браузера Chrome, становлять потенційну загрозу для безпеки користувачів. В ході дослідження було ретельно проаналізовано 70 розширень Chrome, які використовують штучний інтелект, належать до 7 різних категорій. Важливим висновком є те, що 69% з цих розширень мають високий рівень ризику і, у випадку зловживання, можуть нанести суттєвий шкідливий вплив на кібербезпеку користувачів. Додатково виявлено, що 59% проаналізованих розширень здатні збирати особисті дані користувачів, а 44% отримують доступ до особистої інформації.

Список використаних джерел

1. Asmit Nayak, Rishabh Khandelwal, Kassem Fawaz. Exposing and Addressing Security Vulnerabilitie in Browser Text Input Fields. 30 August 2023. University of Wisconsin – Madison. URL: https://arxiv.org/pdf/2308.16321.pdf.

2. Incogni. AI Chrome extensions: convenience vs privacy and security. URL: https://blog.incogni.com/ai-chrome-extensions-research.