АНАЛІЗ XSS–АТАК

Хая А.О., В'юхін Д.О.
Харківський національний університет радіоелектроніки Харків, Україна

В епоху інтернет-технологій, коли цифровий світ стає все більш необхідною частиною нашого повсякденного життя, безпека в інтернеті стає питанням критичної важливості. Однією з найпоширеніших та загрозливих атак, з якими стикаються веб-розробники і користувачі, є XSS-атака, або "міжсайтовий скриптінг". Ця атака, відома своєю вразливістю та складністю виявлення, може мати серйозні наслідки, які поширюються від крадіжки конфіденційної інформації до поширення шкідливих програм. Таким чином, зловмисний сценарій може отримати доступ до важливих даних, таких як файли cookie, сесійні маркери та інша конфіденційна інформація. Більше того, ці сценарії можуть навіть змінювати вміст сторінки HTML на вразливому веб-сайті.

Метою доповіді є аналіз XSS-атак, які передбачають вставлення шкідливих сценаріїв на безпечні та надійні веб-сайти. Зловмисники використовують ці атаки для доставки шкідливого коду іншим користувачам через веб-додатки. Враховуючи зростання Інтернет-технологій та їх важливість у повсякденному житті, безпека в Інтернеті є надзвичайно важливою. Виявлення та запобігання атакам XSS вимагає постійного моніторингу та покращення безпеки веб-додатків і веб-сайтів [1, 2].

XSS-атаки стають можливими, коли виконуються дві основні умови:

– ненадійне джерело даних - дані надходять в веб-програму з ненадійного джерела, часто через веб-запит або інші вхідні механізми;

– включення даних без перевірки у вихідні дані - отримані дані включаються в динамічний веб-контент, який потім надсилається користувачеві без належної перевірки на наявність шкідливого вмісту.

Наслідки XSS-атак можуть бути різноманітними, включаючи доступ зловмисника до особистих даних, таких як файли cookie або інформація про сеанс, перенаправлення користувача на контент, контрольований зловмисником, або виконання інших шкідливих дій на комп'ютері користувача під прикриттям вразливого веб-сайту [3].

Отже, зловмисники можуть використовувати XSS для надсилання шкідливих сценаріїв користувачам, які не мають підстав підозрювати небезпеку. Загалом, XSS-атаки є серйозною загрозою і вимагають постійної уваги до безпеки веб-додатків та сайтів для їх вчасного виявлення та запобігання.

Список літератури

1. Cross Site Scripting (XSS). 2023. URL: Cross Site Scripting (XSS) | OWASP Foundation

2. Port Swigger. Cross site scripting. 2022. URL: What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy (portswigger.net)

3. OWASP. Cross Site Scripting (XSS). 2022. URL: Cross Site Scripting (XSS) | OWASP Foundation.