УДК 004.7:004.056.53

ШКІДЛИВІ МІЖДОМЕННІ ЗАПИТИ

Л. П. Ковальчук, Л. В. Загоруйко

Анотація. У статті подано матеріал дослідження шкідливих міждоменних запитів. Також розглянуто природу та механізми міжсайтового скриптингу (XSS) як однієї з найпоширеніших кіберзагроз для вебдодатків. Розглянуто основні типи XSS-атак, їх методи реалізації та наслідки для безпеки користувачів. Проаналізовано сучасні підходи до виявлення та запобігання XSS-вразливостей, включно з динамічним аналізом забруднень, контекстно-залежне кодування та використання алгоритмів машинного навчання. Визначено перспективи подальших досліджень у сфері кібербезпеки, зокрема інтеграцію штучного інтелекту для протидії кіберзлочинності.

Ключові слова: міждоменні запити, міжсайтовий скриптинг, кібератака, кіберзлочин.

Постановка проблеми. З кожним роком кількість користувачів і пристроїв у глобальній мережі Інтернет збільшується. Водночас збільшується і кількість вебсайтів із контентом на різноманітні теми, що охоплює широкий спектр операцій, починаючи від особистого спілкування до складних фінансових операцій. Сучасні бізнеси надають багато послуг за допомогою інтернету. Це призводить до того, що люди надають особисту інформацію, яка передається через глобальну мережу і залишається на серверах. Виникає потреба в захисті цих персональних даних. Безпрецедентне зростання рівня кіберзлочинності та атак на вебсайти спонукало до розгляду нових технологій для захисту даних та інформації в інтернеті.

Через бажання збільшити користування і функціональність вебсайтів технології їх розробки постійно створюються і вдосконалюються. Так виникла мова програмування JavaScript. Наразі це дуже популярний інструмент для створення динамічних вебсайтів. Так виникла кібератака, яка використовує вразливості сучасних вебсайтів та браузерів, які підтримують роботу коду JavaScript, під назвою XSS.

XSS (англ. *Cross Site Scripting* – «міжсайтовий скриптинг») – це особливий тип вразливості, який може з'являтися на вебсейтах через недосконалості вихідного коду. Вона виникає, коли зловмисник може передати вебдодатку шкідливі дані, які без належних перевірок включаються у вихідну вебсторінку. Коли ця сторінка обробляється браузером жертви, шкідливий код може змінити поведінку додатка, що призводить до несанкціонованих дій на стороні жертви.

За даними Symantec і OWASP, XSS-вразливості є одними з найпоширеніших вразливостей безпеки у вебдодатках. Деякі з них дають змогу виконати лише обмежені атаки, як-от підміна параметрів [1]. Інші ж дають змогу зловмиснику виконувати довільний JavaScript-код у браузері жертви. Хоча браузер зазвичай виконує JavaScript у захищеному середовищі, зловмисник все одно може здійснити широкий спектр атак, зокрема викрадення облікових даних, перехоплення сеансів або реєстрацію натискань клавіш на враженій сторінці.

Аналіз останніх досліджень і публікацій. Аналіз наукової літератури показав, що є різні напрями дослідження та вирішення проблеми XSS атаки. Стаття «DjangoChecker: Applying Extended Taint Tracking and Server Side Parsing for Detection of Context-Sensitive XSS Flaws» представляє інструмент динамічного аналізу забруднень, який поєднує розширене відстеження забруднень із синтаксичним аналізом вихідних даних HTML на стороні сервера, щоб виявити контекстно-залежні недоліки XSS у вебдодатках. На відміну від наявних підходів, ця робота не вимагає статичного аналізу або виправлення під час виконання, що відкриває новий напрям розвитку технологій захисту [2].

Дослідження «Fighting Against XSS Attacks: A Usability Evaluation of OWASPESAPI Output Encoding» демонструє нам процес навчання програмістів усуненню вразливостей XSS. Висвітлено недоліки, які призводять до того, що спеціаліст не може коректно вирішити поставлене перед ним завдання [3].

У роботі «AlgoXSSF: Detection and analysis of cross-site request forgery (XSRF) and cross-site scripting (XSS) attacks via Machine learning algorithms» показано, що комбінація новітніх технологій вкрай необхідна для боротьби з різними варіантами кібератак. Виявлення тенденцій кіберзлочинності та шаблонів атак із поступовим удосконаленням можливе за допомогою штучного інтелекту та машинного навчання [4].

Сучасні дослідження XSS-атак охоплюють різні напрями, зокрема розробку інструментів для виявлення вразливостей, аналіз ефективності захисних механізмів та використання штучного інтелекту для кібербезпеки. Один із підходів передбачає вдосконалення методів динамічного аналізу, що дає змогу знаходити загрози без значних змін у коді. Інший напрям фокусується на підвищенні обізнаності розробників щодо захисту вебдодатків, досліджуючи фактори, які впливають на якість їхніх рішень. Також перспективним є застосування алгоритмів машинного навчання для виявлення атак та прогнозування нових загроз, що сприяє ефективнішій протидії кіберзлочинності. Отже, комплексний підхід, що поєднує різні технології та освітні стратегії, є ключовим у протидії XSS-атакам.

Мета статті – дослідити шкідливі міждоменні запити, їх типи та особливості виконання у браузері.

Виклад основного матеріалу. Міжсайтовий скриптинг (XSS) – це техніка ін'єкції, за якої шкідливі скрипти вставляються у довірені вебсайти. Зловмисник може впливати на взаємодію користувачів із вразливою програмою через вразливість безпеки. Це дає змогу обійти політику однакового походження, яка зазвичай розділяє різні вебсайти. Через такі вразливості зловмисник може видавати себе за цільового користувача, виконувати будь-які дії, доступні користувачеві, та отримувати доступ до його даних.

XSS-атака ґрунтується на здатності шкідливих даних змінювати поведінку вебдодатка всередині браузера жертви. Це зазвичай відбувається через використання символів зі спеціальним значенням, як-от роздільники рядків або роздільники команд, що змушує браузер інтерпретувати частину шкідливого коду інакше, ніж це було задумано. XSS-атаки можуть спричиняти різноманітні проблеми для кінцевих користувачів – від незначних незручностей до повної компрометації їхніх облікових записів. Найсерйозніші XSS-атаки роблять дані користувачів вразливими, надаючи зловмиснику несанкціонований доступ до їхніх облікових записів. Додаткові шкідливі дії можуть включати зміну або викрадення файлів, розгортання троянських програм, перенаправлення користувачів на шкідливі вебсайти та зміну способу відображення даних.

За типом реалізації кібератаки, яка використовує XSS-вразливість, можна виділити такі типи:

1. Stored XSS (збережений XSS) виникає, коли шкідливий код зберігається у базі даних. Якщо відсутнє кодування виводу, запитувані дані відображаються іншим користувачам.

2. Reflected XSS (відображений XSS) – це вразливість безпеки, за якої зловмисник може вставити шкідливий код у вебсайт, і він виконується у браузері жертви. Коли вебдодаток передає текст, отриманий від зловмисника, на комп'ютер користувача, браузер розпізнає частину цього вмісту як виконуваний код. Відсутність кодування виводу на сервері дає змогу цьому коду повернутися користувачеві.

3. DOM-based XSS (XSS через Document Object Model) відбувається, коли зловмисник вставляє скрипт глибше у відповідь сервера. Він може змінювати структуру DOM, щоб створити шкідливу URL-адресу, яку надсилає жертві під виглядом нешкідливого посилання. Якщо користувач натисне на нього, зловмисник отримає доступ до активної сесії жертви, натискань клавіш та інших конфіденційних даних. На відміну від відображеного та збереженого XSS, DOM-орієнтовані атаки націлені виключно на браузер і не відправляють дані назад на сервер. Безперечно, XSS-атака відбувається, коли зловмисник впроваджує шкідливий код на сторінку. Коли користувач відвідує цю сторінку, його можуть змусити ввести конфіденційну інформацію або, у гіршому випадку, неусвідомлено передати паролі шахрайському вебсайту. Основним фактором, що сприяє успішності XSS-атак, є відсутність перевірки введених користувачем даних.

4. Non-persistent XSS (непостійна (відображена) атака міжсайтового скриптингу). Цей тип атаки називається відображеною, оскільки вебсервер віддзеркалює свою дію у відповідь на запит користувача про сервіс, наприклад, пошукові результати, відтворене повідомлення від сервера або будь-яку іншу відповідь, що містить частину або всі передані на сервер дані. У таких атаках зловмисники надсилають спеціально створене посилання з впровадженим XSS-кодом, щоб отримати доступ до конфіденційних даних у вебдодатку. У цій атаці браузерна програма негайно надає інформацію без її перевірки, а самі дані не зберігаються на вебсер-

вері. Зловмисник намагається викрасти файли cookie або перенаправити користувача на зовсім інший вебсайт.

5. Persistent XSS (постійна атака міжсайтового скриптингу). На відміну від непостійної атаки, яка проявляється лише як миттєвий результат, ця атака активно взаємодіє з вебсторінками. Вона використовує впроваджений скрипт, який неминуче впливає на базу даних сервера різними способами, зокрема через поля для коментарів, журнали, форуми та схожі компоненти. Жертва прагне отримати доступ до раніше збереженої інформації, яка, ймовірно, містить впроваджений скрипт. Зловмисники додають шкідливий виконуваний скрипт у вебдодаток, який зберігається у вигляді запису в базі даних або файлі журналу на цільовому сервері чи вебсервері. Цей впроваджений скрипт може отримати доступ до даних сесії та файлів cookie користувача, щоб виконувати дії від імені клієнта. Якщо JavaScript зберігається у комп'ютерній системі (зазвичай у базі даних), кожен, хто відкриє сайт, завантажить шкідливий скрипт разом із вебсторінкою.

Ця атака найчастіше використовується для викрадення конфіденційних даних, як-от файли cookie, маркери сесій та інша конфіденційна інформація. Якщо користувач передає свій логін або пароль, ці дані можуть бути викрадені через впроваджений шкідливий контент або XSS-атаку як із браузера, так і з вебсервера [5; 6].

Висновки. Варто пам'ятати, що з розвитком систем захисту будуть вдосконалюватися і схеми кіберзлочинців. Але дослідження уже наявних способів здійснення кібератаки дасть нам змогу врахувати наявні вразливості сучасних вебсайтів та браузерів.

Такі дослідження є необхідними як матеріали для подальших розробок у галузі кібербезпеки в інтернеті. На основі цих даних ми можемо будувати модель безпеки для вебсайтів, яка, окрім навчання з кібербезпеки, знадобиться для навчання з кіберобізнаності щодо кожної кібератаки.

Перспективні напрями. Детальний розбір і огляд типів атаки та використовуваних зловмисниками скриптів є навчальним матеріалом для машинного навчання та вдосконалення штучного інтелекту, що відкриває перспективу подальшого дослідження та створення продуктивніших моделей безпеки, які будуть інтегровані у програмні продукти в майбутньому.

Abstract. The article presents a study of malicious cross-domain requests. It also examines the nature and mechanisms of cross-site scripting (XSS) as one of the most common cybersecurity threats to web applications. The main types of XSS attacks, their implementation methods, and their consequences for user security are analyzed. Modern approaches to detecting and preventing XSS vulnerabilities are considered, including dynamic taint analysis, context-sensitive encoding, and the use of machine learning algorithms. Prospects for further research in the field of cybersecurity are identified, particularly the integration of artificial intelligence to counter cybercrime.

Keywords: cross-domain requests, cross site scripting, cyberattacks, cybercrimes.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Symantec. Internet security threat report 2016. Tech. rep., April 2016. URL:https://www.symantec

2. DjangoChecker: Applying Extended Taint Tracking and Server Side Parsing for Detection of Context-Sensitive XSS Flaws. 2020. URL: https://arxiv.org/abs/2005.06990

3. Fighting Against XSS Attacks: A Usability Evaluation of OWASP ESAPI Output Encoding. 2018. URL: https://arxiv.org/abs/1810.01017

4. algoXSSF: Detection and analysis of cross-site request forgery (XSRF) and cross-site scripting (XSS) attacks via Machine learning algorithms. 2024. URL: https://arxiv.org/abs/2402.01012

5. An Analysis of XSS Vulnerabilities and Prevention of XSS Attacks in Web Applications / H. D. Jayawardana, M. I. Uyanahewa, V. Hapugala, T. Thilakarathne. 2023, June 20.

6. What is cross-site scripting (XSS) and how to prevent it? What is cross-site scripting (XSS) and how to prevent it? *Web security academy.* 2023. URL:https://portswigger.net/web-security/cross-site-scripting