(або) реалізує функції кооперації і керування. Якщо буде потреба, агенти можуть як клонуватися (утворювати нові сутності), так і припиняти своє функціонування. Залежно від ситуації (виду й кількості атак на комп'ютерні мережі, наявності обчислювальних ресурсів для виконання функцій захисту) може знадобитися генерація декількох екземплярів агентів кожного класу.

Такий підхід дозволяє створити систему з розширюваною адаптивною архітектурою для виявлення атак різних видів.

Список бібліографічних посилань

1. Csubak D., Szucs K., Voros P. and Kiss A. Big Data Testbed for Network Attack Detection. *Acta Polytechnica Hungarica*. 2016. № 13. P. 47-57.

2. Chen Z., Xu G., Mahalingam V., Ge L., Nguyen J., Yu W. and Lu C. A Cloud Computing Based Network Monitoring and Threat Detection System for Critical Infrastructures. *Big Data Research*. 2016. № 3. P. 10-23.

3. Singh K., Guntuku S.C., Thakur A. and Hota C. Big Data Analytics Framework for Peer-to-Peer Botnet Detection using Random Forests. *Information Sciences*. 2014. № 278. P. 488-497.

Одержано 30.10.2018

УДК 004.056.53

Захар Георгійович ДЕМИДОВ,
науковий співробітник науково-дослідної лабораторії захисту інформації та кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ;
Олексій Володимирович ХЛЕСТКОВ,
старший науковий співробітник науково-дослідної лабораторії захисту інформації та кібербезпеки факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

АКТУАЛЬНІСТЬ XSS-АТАК ТА СПОСОБИ ЗАХИСТУ ВІД НИХ

Web-додатки є одними з найбільш небезпечних систем на сьогоднішній день. І, звичайно, хакери цим користуються. Одним з видів атак на додаток є міжсайтовий скриптинг або XSS атака. Зараз вони складають близько 15% всіх атак виявлених вразливостей сайтів.

XSS атака – це атака на вразливість, яка існує на сервері, що дозволяє впровадити в генеруєму сервером HTML-сторінку якийсь довільний код, в якому може бути взагалі все що завгодно і передавати цей код в якості значення змінної, фільтрація по якій не працює, тобто сервер не перевіряє дану змінну на наявність в ній заборонених знаків -, <,>, ', ".

Значення цієї змінної передається від генеруємої HTML-сторінки на сервер в скрипт, її викликавший шляхом відправки запиту. А далі починається найцікавіше для зловмисника. PHP-скрипт у відповідь на даний запит генерує HTML-сторінку, в якій відображаються значення

потрібних хакеру змінних, і відправляє цю сторінку на браузер зловмисника. [1] Тобто, кажучи простіше, XSS атака - це атака за допомогою вразливостей на сервері на комп'ютери клієнтів. XSS атака найчастіше використовується для крадіжки Cookies. У них зберігається інформація про сесії перебування користувача на сайтах, що і буває потрібним хакерам для перехоплення управління особистими даними користувача на сайті в межах, поки сесія не буде закрита сервером, на якому розміщений сайт.Крім цього в Cookies зберігається зашифрований пароль, під яким користувач входить на даний сайт, і при наявності необхідних утиліт і бажання зловмисникам не дуже важко розшифрувати даний пароль. Тепер опишемо інші можливості XSS атак (звичайно за умови їх успішного проведення). Можливо при відкритті сторінки викликати відкриття великої кількості непотрібних користувачеві вікон. Можлива взагалі переадресація на інший сайт (наприклад, на сайт конкурента або якого-небудь "Parimatch").

Існує можливість завантаження на комп'ютер користувача скрипта з довільним кодом (навіть шкідливого) шляхом впровадження посилання на виконуваний скрипт зі стороннього сервера. Найчастіше відбувається крадіжка особистої інформації з комп'ютера користувача, крім Cookies в якості об'єкта крадіжки виступає інформація про відвідані сайти, про версії браузера і операційної системи, встановленої на комп'ютері користувача, та до того ж ще й плюсується IP-адреса комп'ютера користувача.

XSS атака може бути проведена не тільки через сайт, але і через уразливості в програмному забезпеченні (зокрема, через браузери). Тому рекомендується оновлювати використовуєме програмне забезпечення. Також можливе проведення XSS атак через використання SQL-коду. Хакер може опанувати вашою особистою інформацією аж до отримання паролів доступу до сайтів, а це дуже неприємно. До того ж XSS атака завдає шкоди виключно клієнтським машинам, залишаючи сервер в повністю робочому стані, і у адміністрації різних серверів часом мало стимулів встановлювати захист від цього виду атак.

Розрізняють XSS атаки двох видів: активні і пасивні. При першому виді атаки шкідливий скрипт зберігається на сервері і починає свою діяльність при завантаженні сторінки сайту в браузері клієнта. При другому виді атак скрипт не зберігається на сервері і шкідливий вплив починає виконуватися тільки в разі будь-якого дії користувача, наприклад, при натисканні на сформоване посилання.

З метою реалізації радикальних заходів безпеки, які запобігають XSS-атаки, ми повинні пам'ятати про перевірку даних, санітарної обробки даних, і екранування.

Способи боротьби з даним видом атак:

1) заборонити включення безпосередньо параметрів $ _GET, $ _POST, $ _COOKIE в генеруєму HTML-сторінку;

2) заборонити завантаження довільних файлів на сервер, щоб уникнути завантаження шкідливих скриптів. Всі завантажені файли зберігати в базі даних, а не в файлової системі;

3) перевірка коректності. Перевірка даних це процес забезпечення того, щоб ваш додаток працював з правильними даними. Якщо ваш PHP скрипт очікує ціле число, для введення даних користувачем, то будь-який інший тип даних буде відхилений і користувач отримає повідомлення про це. Кожна частина призначених для користувача даних повинна бути перевірена при отриманні. Перевіряйте дані як на стороні клієнта, так і на стороні сервера, оскільки перевірку на стороні клієнта надзвичайно легко перехитрити. Дотримуйтесь послідовної стратегії захищеності додатка, грунтуючись на передовому досвіді розробки захищених додатків;

4) екранування даних. Для того, щоб захистити цілісність відображення вихідних даних, ви повинні екранувати їх. Це запобіжить спробі браузера ненавмисно спотворити зміст спеціальних послідовностей символів, які можуть бути знайдені їм;

5) можна використовувати для перевірки вразливостей цілеспрямовано ресурси, наприклад, https://metascan.ru

(ПЕРЕВІРКА 0-65535 ПОРТОВ

ПОШУК експлойтів та CVE

Підбір пароля

ПОШУК XSS, SQLI, RCE)

З усього написаного вище, можна зробити висновок:

1. Існує досить багато варіантів реалізації подібного роду атак, в багатьох випадках ключову роль відіграє саме людський фактор, а не продумані дії зловмисника.

2. Атака, пов'язана з межсайтовою підробкою запиту досить проста в реалізації, а, отже, часто зустрічається.

3. Атаки такого роду можуть завдати серйозної шкоди сайту або ж конкретному користувачу.

4. Проблема є актуальною з моменту появи Інтернету і до цього дня, це пов'язано з великими темпами зростання числа веб-ресурсів.

Список бібліографічних посилань

1. Шахгильдянц А. Т. Разработка способа защиты веб-приложений от межсайтовой подделки запросов : выпускная квалификационная работа по специальности 10.05.01 «Компьютерная безопасность» // Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский Федеральный университет». Ставрополь, 2018. 81 с. URL: https://dspace.ncfu.ru:443/handle/20.500.12258/57 (дата звернення: 21.10.2018).

2. Ильенко Ф.В. Безопасность web-сайтов : реферат по теме выпускной работы. URL: http://masters.donntu.org/2013/fknt/ilyenko/diss/index.htm (дата звернення: 21.10.2018).

Одержано 22.10.2018