Облудський О.А.
студент,
Національний технічний університет України
«Київський політехнічний інститут»

ЗАХИСТ ВЕБ-ДОДАТКІВ ВІД АТАК

На сьогоднішній день ми можемо спостерігати постійно зростаючі атаки на веб-додатки – до 78% випадків компрометації систем починаються з веб-додатків. Основна тема цієї статті – висвітлити найбільш розповсюджені типи сучасних атак, розглянути найбільш поширені вразливості, які активно використовують зловмисники, а також ефективні методи протидії їм за допомогою технології Web Application Firewall.

При постійному збільшенні кількості інструментів і технік атак, все складніше стає забезпечити постійну доступність сайту, захистити веб-додаток або його компоненти від злому і підміни контенту. Незважаючи на тяжкі зусилля технічних фахівців і розробників, вони традиційно займають наздоганяючу позицію, реалізовуючи захисні заходи вже після того, як веб-додаток було скомпрометовано. Веб-сайти часто піддаються атакам через публічної доступності, не завжди якісно написаному програмному коду, наявності помилок в налаштуванні серверної частини, а також відсутньому контролю з боку служби інформаційної безпеки, тим самим забезпечуючи зловмисникам доступ до даних ресурсу та користувачів.

У зв'язку з цим виникає необхідність використовувати захисні засоби, що враховують архітектуру веб-додатку, і не призводять до затримок в роботі сайту, що важливо.

Вразливість «нульового дня»

Вразливістю «нульового дня» або Zero-day – це раніше невідома уразливість, яка дуже часто експлуатується зловмисниками. Походження терміна пов'язане з тією обставиною, що уразливість або атака стає публічно відома до моменту випуску виробником ПО виправлень помилки (тобто потенційно вразливість може експлуатуватися на працюючих копіях додатків без можливості захиститися від неї).

Природа вразливостей нульового дня дозволяє зловмисникам успішно атакувати веб-додатки в період від кількох хвилин до кількох місяців. Такий великий період обумовлений безліччю факторів:

- вразливість необхідно локалізувати і усунути;
- викотити працездатний патч;
- повідомити користувачів про проблему;
- користувачам додатку запустити процес патч-менеджменту.

В цьому криється ще один важливий фактор – для нової уразливості може не існувати правил або винятків в захисній системі, а сигнатура атаки може бути не розпізнано класичними захисними засобами. В цьому випадку допоможе використання білого списку поведінкового аналізу конкретного веб-додатку для мінімізації ризиків атак нульового дня.

Як приклад можна навести хронологію атаки Struts2: CVE-2013-2251 Struts2 Prefixed Parameters OGNL Injection Vulnerability – з моменту появи «бойового» експлойту пройшло кілька днів, перш ніж багато компаній змогли встановити патч для усунення вразливості.

«Класичні» атаки»

Статистичні дослідження показали, що багато веб-додатків компрометуються також, як і роками раніше – це різного роду ін'єкції, інклуд, клієнт-сайд атаки, тому захисний засіб має вміти виявляти і блокувати атаки, спрямовані на експлуатацію наступних вразливостей:

- SQL Injection – sql ін'єкції;
- Remote Code Execution (RCE) – віддалене виконання коду;
- Cross Site Scripting (XSS) – міжсайтовий скриптинг;
- Cross Site Request Forgery (CSRF) – міжсайтова підробка запитів;
- Remote File Inclusion (RFI) – віддалений інклуд;
- Local File Inclusion (LFI) – локальний інклуд;
- Auth Bypass – обхід авторизації;
- Insecure Direct Object Reference – небезпечні прямі посилання на об'єкти;
- Bruteforce – підбір паролів.

В ідеальному веб-додатку такого роду вразливості повинні бути виявлені і зафіксовані ще на етапі розробки: повинен був проведений статичний, динамічний, інтерактивний аналіз, виявлення аномалій в логіці роботи програми. Але, найчастіше, такі моменти з тих чи інших причин не беруться до уваги, на них не залишається часу або коштів, що потім може мати фатальні наслідки.

Захист на прикладному рівні

Веб-додатки відрізняються від звичайних додатків двома речами: величезною різноманітністю і значною інтерактивністю. Це створює цілий ряд нових загроз, з якими традиційні міжмережеві екрани не справляються.

Протокол прикладного рівня – протокол верхнього (7-го) рівня мережевої моделі OSI, забезпечує взаємодію мережі й користувача. Рівень дозволяє додаткам користувача мати доступ до мережевих служб, таким, як обробник запитів до баз даних, доступ до файлів, пересилання електронних повідомлень.

Захист на прикладному рівні є найбільш надійний. Вразливості, експлуатовані зловмисниками, часто покладаються на складні сценарії введення даних користувачем, що робить їх майже невидимими для відстеження за допомогою класичних систем виявлення вторгнень. Також цей рівень є найдоступнішим ззовні. Виникає необхідність розуміти групи протоколів і залежностей, властивих для веб-додатків, які будуються над прикладними протоколами http / https.

Основний принцип захисту сайту на прикладному рівні – верифікація та фільтрація даних запитів, переданих методами GET, POST і т.д. Підміна або модифікація запиту – це базова основа практично всіх способів злому і атак на сайти.

Забезпечення захисту сайту

Найбільш оптимальним рішенням для забезпечення захисту сайту є застосування Web Application Firewall – брандмауера прикладного рівня, що дозволяє ефективно захищати сайти від атак зловмисників.

Web Application Firewall – це спеціальний механізм, який накладає певний набір правил та обмежень на те, як між собою взаємодіють сервер і клієнт, обробляючи HTTP-пакети. В основі криється той же принцип, що і в звичайних користувальницьких фаєрволах, – контроль всіх даних, які надходять ззовні та їх фільтрація. WAF спирається на набір правил, за допомогою яких виявляється факт атаки по сигнатурам – ознаками активності користувача, які можуть означати напад.

Як це працює?

Web Application Firewall працює в режимі прозорого проксірующого механізму, аналізуючи на льоту дані, що надходять від клієнта і відкидаючи нелегітимні запити.

Після установки Web Application Firewall необхідна настройка під цільовий веб-додаток – в залежності від типу і виду CMS додаються налаштування, що враховують веб-додаток, фільтрації і правила, потім захисний засіб переводиться в режим навчання, для збору еталонних моделей комунікації з веб-додатком, ідентифікаторів і т.д.

Після етапу машинного навчання включається так званий «бойовий режим», який оперує як готовими правилами фільтрації, так і напрацюваннями, зібраними на етапі навчання для виявлення і блокування атак.

Ефективність застосування Web Application Firewall складається з декількох чинників:

- Проста інтеграція в інфраструктуру;
- Гнучка система адаптації з веб-додатком;
- Блокування загроз OWASP Top 10;
- Аналіз і блокування аномалій протоколу або даних;
- Виявлення та блокування підробки ідентифікаторів сесій;
- Виявлення та блокування підбору паролів;
- Інспекція відповідей сервера на наявність критичних даних;
- Динамічне оновлення сигнатур атак;
- Низька кількість помилкових спрацьовувань;
- Самозахист WAF;
- Зручний сервіс інформування про атаки;
- Статистика та регламентна звітність.

Список використаних джерел:

1. Джоел Скрембрей, Майк Шема, Йєн-Мінг Чен, Девід Вонг Секрети хакерів. Безпека web-додатків – готові рішення // Москва, 2003 – 384 с.
2. Жуков Ю. В. Основи веб-хакінгу // Санкт-Петербург, 2011 – 176 с.