Захист інформації

УДК 004.056.53

І.В. Василенко

Таврійський державний агротехнологічний університет, Мелітополь

УНІВЕРСАЛЬНІЙ МЕТОД ЗАХИСТУ ВЕБ-ДОДАТКІВ

Проводиться аналіз існуючих систем захисту веб-додатків, описані їх основні переваги та недоліки, розглянуто типи загроз та запропоновано універсальний метод захисту веб-додатків.

Ключові слова: *брандмауер, WAF, веб-додаток, проксі-сервер.*

Вступ

Постановка проблеми. Кількість некваліфікованих веб-програмістів стрімко зростає. Разом з тим, високими темпами розвиваються загрози безпеки веб-сервісів. Актуальним завданням є знаходження нових форм та методів захисту веб-додатків від існуючих типів загроз.

Аналіз останніх досліджень. За даними статистики WASC (Web Application Security Consortium), більше 13% сайтів можуть бути скомпроматовані повністю автоматично, 80 – 96% з яких мають високий ступінь вразливості, 86% – середній ступінь вразливості, 37% – низьку.

Мета роботи. Провести аналіз методів захисту веб-сервісів, типів загроз та запропонувати новий метод захисту веб-додатків.

Основна частина

На сьогоднішній день поріг входження в сферу створення веб-сайтів мінімальний, завдяки спрощеним мовам веб-програмування та технологіям, що розвиваються, які роблять процес створення сайту простим, але ефективним з точки зору досягнення мети замовником. Не дивно, що поряд з бурхливим розвитком сфери Інтернет, тими ж темпами розвиваються і загрози безпеці працюючих у ній сервісів.

У той же час, роль сайтів та їх вплив на бізнес постійно зростає, а перенасичений ринок некваліфікованих веб-програмістів, часто роль яких виконують студенти, згубно впливає на якість програмних продуктів і сайтів зокрема. Проблема безпеки у таких виконавців, на жаль, стоїть далеко не на першому місці. Становище ускладнюється і тим, що замовник деколи залишається в невіданні, що його сайт і всі розташовані там дані є слабко захищеними або незахищеними взагалі. У даній статті хотілося б поговорити про частину Інтернету, що є його безпосереднім обличчям, і що стосується практично кожного користувача – це веб-сайти і їх безпеку. Веб-сайти і додатки локальних мереж дозволяють користувачам отримувати доступ до важливої бізнес інформації та сервісів. Щоб захистити ці важливі ресурси, Інтернет-додатки вимагають підвищеного захисту від хакинга і шахрайства. Актуальність проблеми безпеки такого виду додатків зростає з кожним днем, а більшість вразливостей, що існують на даний момент в цій сфері, пов'язані з помилками і недоліками, допущеними на етапі розробки сайту.

Таким чином, ми підійшли до питання про необхідність вирішення зазначеної проблеми. Можливих варіантів кілька. Перший – навчити всіх веб-програмістів основам безпеки при створенні сайтів, але даний спосіб не масштабується і важко реалізуємий з урахуванням темпів зростання кількості програмістів. Найбільш оптимальним варіантом компенсації людського фактора, недоліків програміста в процесі створення веб-сайтів, на сьогоднішній день є технологія WAF (Web Application Firewall).

WAF – Брандмауер веб-додатків

WAF – це міжмережевий екран, який накладає певний набір правил на те, як відбувається взаємодія сервера і клієнта, обробляючи HTTP-пакети. В основі лежить той же принцип, що й у звичайних фаєрволів – контроль і аналіз всіх пакетів, що надходять від клієнта. WAF спирається на набір правил, за допомогою якого виявляється факт атаки по сигнатурам – ознаками активності користувача, які можуть означати напад. Брандмауер інтернет-додатків ще називають третьою лінією оборони. У такій парадигмі першою лінією оборони є міжмережеві екрани, другий – системи IPS, і, нарешті третій – WAF.

Типи WAF

Web Application Firewall поділяють на 2 типи: апаратний і програмний. Найбільшого поширення отримав другий зважаючи на більш просту реалізацію. За принципом дії WAF можна розділити на три типи:

1. Реалізовані у вигляді зворотного проксі-сервера.
2. Працюючі в режимі маршрутизації / моста.
3. Вбудовані в веб-додатки.

Зворотний проксі-сервер

У даному типі WAF всі дані спочатку обробляються проксі-сервером, який вже вирішує пропускати пакети або блокувати. У разі позитивного ре-

зультату дані перенаправляються до веб-сервера без зміни, або з частковою правкою.

До цього типу належать: mod_security [3], Barracuda [4], nevisProxy [5].

Режим маршрутизації / моста

До цього типу найчастіше відносять апаратні WAF. У даного типу реалізації є як плюси, так і мінуси. До першого можна віднести приріст продуктивності, до других більш складне і тонке налаштування.

Прикладом даного типу WAF є Impreva SecureSphere [2].

Вбудовані в веб-додатки

Даний тип WAF вбудовується безпосередньо у веб-додаток в якості додаткового функціоналу і працює на програмному рівні.

Обробка правил в WAF може здійснюватися за принципом чорного списку (проводиться зіставлення зі списком неприпустимих умов), білий список (приймаються тільки дозволені дії) або змішано.

Типи загроз

На сьогоднішній день, майже всі брандмауери веб-додатків покликані захистити від основних типів загроз властивих веб-сайтам. А саме, це такі загрози:

– SQL ін'єкція;

– міжсайтовий скриптинг (XSS);

– міжсайтова підробки запитів (CSRF);

– спам в коментарях;

– розподілена відмова в обслуговуванні (DDoS-атаки,);

– відсутність таймаута сесії;

– зворотний шлях в директоріях.

Загрозам піддаються і WEB-сервери. Класифікація атак на WEB-сервера має ієрархічну структуру та розділяється на шість основних класів.

А саме:

– атаки на засоби аутентифікації;

– атаки на засоби авторизації;

– атаки на клієнтів;

– атаки направлені на виконання коду;

– атаки направлені на розголошення інформації;

– логічні атаки.

Атаки на засоби аутентифікації

Атаки цього класу направлені на обхід чи експлуатацію вразливостей в механізмах реалізації аутентифікації WEB-серверів.

Підбір

Підбір представляє собою автоматизований процес спроб на похибок, основною метою якого є вгадування імені користувача, пароля, номера кредитної картки, ключа шифрування і так далі. Багато систем дозволяють використовувати слабкі паролі або ключі шифрування, і користувачі часто вибирають легко вгадувані або такі, що містяться в словниках парольні фрази. Користувачі навмисно вибирають прості паролі, оскільки складні окрім часу введення, незручні ще і тим, що легко забуваються. Скориставшись цією ситуацією, зловмисник може застосувати електронний словник і спробувати використовувати усю потужність комбінацій символів, що містяться в словнику, як пароль. Подібна техніка спроб і помилок може бути з успіхом використана для підбору ключів шифрування. У разі використання сервером ключів недостатньої довжини зловмисник може отримати використовуваний ключ, протестувавши усі можливі комбінації. Незважаючи на популярність і високу ефективність, підбір може займати декілька годин, днів або років. Цей вид атак широко використовується переважно там, де відсутнє блокування у разі невірного поєднання.

Недостатня аутентифікація

Ця уразливість виникає тоді, коли WEB-сервер дозволяє зловмиснику діставати доступ до важливої інформації або функцій сервера без належної аутентифікації. Атаки подібного роду дуже часто реалізуються за допомогою інтерфейсу адміністрування через WEB. Щоб не використовувати аутентифікацію, деякі ресурси по дефолту використовують певну адресу, яка не вказана на основних сторінках сервера або інших загальнодоступних ресурсах. Необхідний URL може бути знайдений шляхом перебору типових файлів і директорій (таких, як /admin/) з використанням повідомлень про помилки журналів перехресних посилань або шляхом простого читання документації. Подібні ресурси мають бути захищені адекватно важливості їх вмісту і функціональних можливостей.

Виконання команд ОС

Атаки цього класу спрямовані на виконання команд операційної системи на WEB-сервері шляхом маніпуляції вхідними даними. Якщо інформація, отримана від клієнта, належним чином не верифікується, то зловмисник дістає можливість виконати команди ОС. Вони виконуватимуться з тим 2 же рівнем привілеїв, з яким працює компонент ПЗ, виконуючий запит (сервер СКБД, WEB-сервер і т.д.). Програмні WEB забезпечення часто використовують параметри, які вказують на те, який файл відображувати або використовувати як шаблон. Якщо цей параметр не перевіряється досить ретельно, то зловмисник може підставити свої команди ОС до запиту. Більшість мов сценаріїв дозволяють запускати команди ОС під час виконання, використовуючи варіанти функції exec. Якщо дані, отримані від користувача, передаються цій функції без перевірки, зловмисник може виконати команди ОС на відстані.

Впровадження операторів SQL

Ці атаки спрямовані на WEB-сервери, які створюють SQL-запити до серверів СКБД на основі даних, що вводяться користувачем. Мова запитів SQL є спеціалізованою мовою програмування, що дозволяє створювати запити до серверів СКБД. Більшість серверів підтримують цю мову у варіантах, стандартизованих ISO і ANSI. У більшості сучасних СКБД присутні розширення діалекту SQL, специфічні для цієї реалізації (T-SQL в Microsoft SQL Server, -PL SQL в Oracle і т.д.). Багато програмного WEB забезпечення використовує дані, передані користувачем,

для створення динамічних WEB-сторінок. Якщо інформація, отримана від клієнта, належним чином не верифікується, то зловмисник дістає можливість модифікувати запит до SQL-серверу, що відправляється ПЗ. Запит виконуватиметься з тим же рівнем привілегій, з яким працює компонент ПЗ, виконуючий запит (сервер СКБД, WEB-сервер і т.д). В результаті зловмисник може отримати повний контроль над сервером СКБД і навіть його операційною системою. Зазвичай виділяють два методи експлуатації впровадження операторів SQL: звичайна атака і атака всліпу. У першому випадку зловмисник підбирає параметри запиту, використовуючи інформацію про помилки, які згенеровані програмним WEB забезпеченням. У другому випадку стандартні повідомлення про помилки модифіковані, і сервер повертає зрозумілу для користувача інформацію про неправильне введення. Здійснення SQL Injection можливо і в цій ситуації, проте виявлення уразливості ускладнене. Найбільш поширений метод перевірки наявності проблеми – додавання виразів, що повертають істинне і помилкове значення.

Недоліки технології WAF

Основною проблемою, яка існує на даний момент, є обмежені можливості існуючої технології WAF у забезпеченні захисту від широкого спектру загроз. А також можливість обходу існуючих на даний момент брандмауерів. Кожен брандмауер має відмінну особливість і залишає за собою слід. Для виявлення того чи іншого брандмауера використовується метод розпізнавання "fingerprint", що в перекладі означає "відбиток пальця". Наприклад:

– спеціальні коди відповіді при передачі особливих даних або виклику помилок;

– спеціальні змінні, збережені в Cookie;

– зміна HTTP-заголовків, зокрема дані, що передаються в сервер;

– негайне завершення з'єднання при спрацьовуванні неприпустимого умови;

– вбудований набір базових правил, піддається розкриттю.

Після того як WAF виявлений залишається тільки знайти його відповідну вразливість і використовувати її. 100% захисту не існує і WAF в цьому не виняток. На сьогоднішній день існує безліч варіантів обходу WAF і цей список постійно поповнюється. Як приклад можна взяти дослідження компанії Positive Technologies, які знайшли більше 30 можливостей обходу існуючих WAF.

Висновки

Якщо говорити простою мовою, WAF – це універсальний спосіб мінімізувати загрози, пов'язані з людським фактором, при створенні веб-додатків. Як і будь-який універсальний метод, WAF має ряд недоліків. Основна проблема сучасних WAF криється в їх архітектурі, заснованій на загальному принципі. Всі вони використовують сигнатурний аналіз для визначення типу загроз.

Недолік такого підходу очевидний – його легка виявленість і відносно легкий спосіб обходу.

Один з можливих варіантів вирішення цієї проблеми ми бачимо в застосуванні методів поведінкового аналізу. Принцип такого підходу в корені відрізняється від сигнатурного. За основу береться нормальна поведінка, скажімо, в скрипті С читання з таблиці А - нормально, якщо відбувається читання з таблиці Б, це вважається аномальним. Даний підхід в теорії може закрити вразливості пов'язані з сигнатурним аналізом. Даний напрямок я бачу найбільш перспективним у вирішенні проблем безпеки веб-сайтів.

Список літератури

1. Захист веб-додатків [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: http://www.e-reading.club/bookreader.php/1012355/DJ-Andrey-sXe_-_Zaschita_veb-prilozheniy.html.

2. Євтєєв Д. Методи обходу Web Application Firewall [Електронний ресурс] / Дмитро Євтєєв. – Режим доступу до ресурсу: http://www.ptsecurity.ru/download/PT-devteev-CC-WAF.pdf.

3. Основні методи тестування безпеки веб-додатків [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: http://uastudent.com/osnovni-metody-testuvannja-bezpeky-veb-dodatkiv/.

4. Седерхольм Д. Пуленепробиваемый Web-дизайн. Повышение гибкости сайта и защита от потенциальных неприятностей с помощью XHTML и CSS / Ден Седерхольм, 2006. – 256 с. – (Школа Web-мастерства).

5. Жуков Ю.В. Основы веб-хакинга. Нападение и защита / Юрий Викторович Жуков, 2012. – 206 с.

Надійшла до редколегії 6.11.2015

Рецензент: д-р техн. наук, проф. О.М. Леженкін, Таврійський державний агротехнологічний університет, Мелітополь.

УНИВЕРСАЛЬНЫЙ МЕТОД ЗАЩИТЫ ВЕБ-ПРИЛОЖЕНИЙ

И.В. Василенко

Проводится анализ существующих систем защиты веб-приложений, описаны их основные преимущества и недостатки, рассмотрены типы угроз и предложены универсальный метод защиты веб-приложений.

Ключевые слова: *брандмауэр, WAF, веб-приложение, прокси-сервер.*

A UNIVERSAL METHOD OF WEB APPLICATION PROTECTION

I.V. Vasilenko

The analysis of existing systems, web application protection, describes their advantages and disadvantages, discussed the types of threats and proposed a universal method for protecting Web applications.

Keywords*: firewall, WAF, a web application proxy.*