УДК 004.738

АНАЛІЗ ЗАСОБІВ ЗАХИСТУ WEB-СЕРВЕРІВ ВІД АВТОМАТИЗОВАНОГО ВИКОНАННЯ ЗЛОВМИСНИХ ДІЙ

Руденко Сергій Василійович, Баранов Анатолій Анатолійович
Державний вищий навчальний заклад «Національний гірничий університет»
sergey_rud@i.ua, tocea@yandex.ru

Аналіз засобів захисту WEB-серверів від автоматизованого виконання зловмисних дій та розробка системи тестування користувачів на основі зворотного тесту Тюрінга.

ВСТУП

CAPTCHA, (Повністю автоматичний публічний тест Тьюрінга для розрізнення комп'ютерів і людей), була створена для того, що б переконатися, що введені дані не були згенеровані комп'ютером. Ці своєрідні тести зазвичай використовуються в Інтернеті для захисту форм реєстрації та коментування від спаму. Якщо бути чесним, я відчуваю змішані почуття щодо CAPTCHA. Вона в більшості випадків дратує мене, але не дивлячись на це я використав CAPTCHA для захисту на деяких сайтах.

ПРЕДМЕТ ДОСЛІДЖЕННЯ

Предметом дослідження є засоби захисту WEB-серверів від автоматизованого виконання зловмисних дій на основі технології CAPTCHA.

Задачами дослідження буде:

- аналіз загроз WEB-серверів;
- аналіз засобів захисту від WEB-роботів;
- огляд способів обходу зворотного тесту Тюрінга;

Класифікація атак на WEB-сервера

Класифікація атак на WEB-сервера має ієрархічну структуру та розділяється на шість основних класів.

- 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 до

вжини зловмисник може отримати використовуваний ключ, протестувавши усі можливі комбінації. Існує два види підбору: прямий і зворотний. При прямому підборі використовуються різні варіанти пароля для одного імені користувача.

При зворотному перебираються різні імена користувачів, а пароль залишається незмінним. У системах з мільйонами облікових записів вірогідність використання різними користувачами одного пароля досить висока. 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.

Атака на функції форматування рядків

При використанні цих атак шлях виконання програми модифікується методом перезапису областей пам'яті за допомогою функцій форматування символьних змінних. Уразливість виникає, коли призначені для користувача дані застосовуються як аргументи функцій форматування рядків - таких, як fprintf, printf, sprintf, setproctitle, syslog і так далі. Якщо зловмисник передає додатку рядок, що містить символи форматування ("%f", "%p", "%n" і так далі), то у нього з'являється можливість:

виконати довільний код на сервері;

прочитати значення із стека;

викликати помилки в програмі/відмову в обслуговуванні.

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

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.

ВИСНОВКИ

Засоби, які не вимагають від користувача ніяких дій, в більшій мірі відносяться до додаткового до зворотного тесту Тюрінга, захисту від WEB-роботів.

Отже, розробка нової системи тестування повинна підвищити рівень захисту WEB-серверів від автоматизованого виконання зловмисних дій, виключити нині існуючі способи обходу, надати можливість проходження тесту користувачам з порушенням зору.