УДК 004.056.53

О.В. Сєвєрінов, А.Г. Хрєнов

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АТАК НА ЕЛЕКТРОННІ РЕСУРСИ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

У даній статті розглянуто сучасні методи атак на електронні ресурси органів військового управління. Проведено аналіз методів атак, на основі аналізу виявлено основні найбільш поширені методи та такі, що можна передбачити при розробці архітектури електронного ресурсу.

Ключові слова: *аналіз сучасних методів атак, сучасні методи атак, електронні ресурси, атаки на електронні ресурси.*

Вступ

Інформаційна зброя - сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій і служб інформаційної інфраструктури в цілому або окремих її елементів [1]. Розглядаючи стратегію ведення інформаційної війни в мережі Інтернет неабияку роль відіграє об'єктивна інформація, що надходить з місця подій. Засоби масової інформації, як правило по різному висвітлюють події, чим впливають на політичні погляди суспільства.

Блискуча інформаційна війна розгортається задовго до початку бойових дій. Один з основних напрямів, якої є атака хакерів на сайти парламенту, уряду, міністерств та органів військового управління. Такі атаки являються організованими та масовими, основною метою яких є блокада достовірної інформації та розміщення матеріалу, що спроможний деморалізувати суспільство, налаштувати його на підтримку основних ідей країни-агресора.

Звертаючи увагу на тенденції розвитку інформаційних систем та використання електронних ресурсів у повсякденній життєдіяльності органів військового управління. Необхідно забезпечити стабільність їх використання та спроможність оперативно реагувати на різноманітні методи атак на інформаційні системи та електронні ресурси з боку ймовірного супротивника.

Метою статті є аналіз сучасних методів атак на електронні ресурси органів військового управління.

Автентифікація (Authentication)

Атаки, що використовують процедуру автентифіцації спрямовані на використання інформаційним ресурсом ідентифікатора користувача, служби або додатків. Атака спрямована на обхід або експлуатацію уразливостей в механізмі реалізації автентифікації Web-сервера [2].

До даного типу атак входять наступні методи реалізації:

1. Метод «грубої сили» (Brute Force)

Автоматизований процес перебору ймовірних варіантів ключових фраз, що використовується з метою підбору імені користувача, паролю, номера кредитної картки, ключа шифрування, тощо.

Web-сервери та електронні ресурси, які дають змогу користувачу обирати слабкі паролі або використовують слабкі ключі шифрування, найчастіше схильні до успішного завершення даного методу атаки.

Існує декілька видів підбору: прямий та зворотній. При прямому підборі використовуються різні варіанти пароля для одного імені користувача. При зворотному - перебираються різні імена користувачів , а пароль залишається незмінним.

2. Недостатня автентифікація (Insufficient Authentication)

Ця вразливість виникає, коли Web-сервер дозволяє атакуючому отримувати доступ до важливої інформації або функцій сервера без належної автентифікації.

Щоб не використовувати автентифікацію деякі ресурси розміщують сторінки за певною адресою, яка не вказана на основних сторінках сервера або інших загальнодоступних ресурсах.

Не дивлячись на те , що зловмисник не знає адреси сторінки, вона все одно доступна через Web.

3. Небезпечне відновлення паролів (Weak Password Recovery Validation)

Ця вразливість виникає, коли Web-сервер дозволяє атакуючому не санкціоновано отримувати, модифікувати або відновлювати паролі інших користувачів через функцію відновлення забутого пароля.

Уразливості пов'язані з недостатньою перевіркою при відновленні пароля виникають, коли атакуючий отримує можливість використовувати механізм відновлення для входу в систему. Це трапляється, коли інформацію, що використовується для перевірки користувача, легко вгадати або сам процес підтвердження можна обійти. Система віднов-

лення пароля може бути скомпрометована шляхом використання підбору, вразливостей системи або через підбор відповіді на секретне питання .

Авторизація (Authorization)

Атаки, що базуються на уразливості авторизації спрямовані на методи, які використовуються Web-сервером для визначення того, чи має користувач, служба або додаток дозвіл, необхідний для вчинення протиправної дії. Використовуючи різні техніки, зловмисник може підвищити свої привілеї і отримати доступ до захищених ресурсів.

До атак, що базуються на уразливості авторизації електронного ресурсу відносяться:

1. Передбачуване значення ідентифікатора сесії (Credential/Session Prediction)

Передбачуване значення ідентифікатора сесії дозволяє перехоплювати сесії інших користувачів. Подібні атаки виконуються шляхом передбачення або вгадування унікального ідентифікатора сесії користувача. Ця атака також, як і перехоплення сесії (Session Hijacking), у разі успіху дозволяє зловмисникові надіслати запит Web-сервера з правами скомпрометованого користувача.

Дизайн багатьох серверів припускає автентифікацію користувача при першому зверненні і подальше відстеження його сесії. Для цього користувач вказує комбінацію імені та пароля. Замість повторної передачі імені користувача і пароля при кожній транзакції, Web-сервер генерує унікальний ідентифікатор, який присвоюється сесії користувача. Наступні запити користувача до сервера містять ідентифікатор сесії як доказ того, що аутентифікація була успішно пройдена. Якщо атакуючий може передбачити або вгадати значення ідентифікатора іншого користувача, це може бути використано для проведення атаки [3].

2. Недостатня авторизація (Insufficient Authorization)

Недостатня авторизація виникає, коли Web-сервер дозволяє атакуючому отримувати доступ до важливої інформації або функцій, доступ до яких повинен бути обмежений. Те, що користувач пройшов автентифікацію не означає, що він повинен отримати доступ до всіх функцій і вмісту сервера. Крім автентифікації має бути реалізовано розмежування доступу.

Процедура авторизації визначає, які дії може здійснювати користувач, служба або додаток. Правильно побудовані правила доступу повинні обмежувати дії користувача згідно політики безпеки. Доступ до важливих ресурсів сайту повинен бути дозволений тільки адміністраторам.

3. Відсутність таймауту сесії (Insufficient Session Expiration)

Зловмисник спроможний скористуватися застарілими даними для авторизації у разі, якщо ідентифікатор сесії не передбачує таймаут або його значення занадто велике.

Це підвищує уразливість сервера для атак, пов'язаних з крадіжкою ідентифікаційних даних.

Конфіденційність кожного ідентифікатора повинна бути забезпечена, щоб запобігти множинний доступ користувачів з одним обліковим записом. Викрадений ідентифікатор може використовуватися для доступу до даних користувача або здійснення шахрайських транзакцій.

4. Фіксація сесії (Session Fixation)

Використовуючи даний клас атак, зловмисник присвоює ідентифікатору сесії користувача задане значення. Залежно від функціональних можливостей сервера, існує кілька способів "зафіксувати" значення ідентифікатора сесії. Для цього можуть використовуватися атаки типу міжсайтового виконання сценаріїв або підготовка сайту з допомогою попереднього HTTP запиту. Після фіксації значення ідентифікатора сесії атакуючий очікує моменту, коли користувач увійде в систему. Після входу користувача, зловмисник використовує ідентифікатор сесії для отримання доступу до системи від імені користувача.

На відміну від крадіжки ідентифікатора, фіксація сесії надає зловмисникові набагато більший простір для творчості. Це пов'язано з тим, що активна фаза атаки відбувається до входу користувача в систему.

Атаки на клієнтів (Client-side Attacks)

Під час відвідування сайту, між користувачем і веб-сервером встановлюються довірчі відносини, як в технологічному, так і в психологічному аспектах. Користувач очікує, що сайт надасть йому легітимну інформацію. Крім того, користувач не очікує атак з боку сайту. Експлуатуючи цю довіру, зловмисник може використовувати наступні методи для проведення атак:

1. Підміна вмісту (Content Spoofing)

Використовуючи цю техніку, зловмисник змушує користувача повірити, що сторінки згенеровані Web-сервером, а не передані з зовнішнього джерела. Деякі Web-сторінки створюються з використанням динамічних джерел HTML-коду. Наприклад, розташування фрейму () може передаватися в параметрі URL (http: //foo.example/page? Frame_src = http: //foo.example/file.html). Атакуючий може замінити значення параметра "frame_src" на "frame_src = http: //attacker.example/spoof.html". Коли буде відображатися результуюча сторінка, у рядку адреси браузера користувача відображатиметься адреса сервера (foo.example), але так само на сторінці буде присутній зовнішній вміст, завантажений з сервера атакуючого (attacker.example), замаскований під легальний контент [4].

Таким чином, відбудеться "дефейс" сайту http://foo.example на стороні користувача, оскільки вміст сервера буде завантажено з сервера http://attacker.example. Ця атака так само може використовуватися для створення помилкових сторінок, таких як форми введення пароля, прес-релізи і т.д.

2. Міжсайтового виконання сценаріїв (Cross-site Scripting, XSS)

Наявність уразливості Cross-site Scripting дозволяє атакуючому передати Web-серверу шкідливий код, який буде перенаправлений браузеру користувача. Цей код зазвичай створюється на мовах HTML / JavaScript, але можуть бути використані VBScript, ActiveX, Java, Flash, або інші підтримувані браузером технології.

Переданий код виконується в безпечній зоні уразливого сервера. Використовуючи ці привілеї, код отримує можливість читати, модифікувати або передавати важливі дані, доступні за допомогою браузера.

У атакованого користувача може бути скомпрометований аккакунт (крадіжка cookie), його браузер може бути перенаправлений на інший сервер або здійснена підміна вмісту сервера. У результаті ретельно спланованої атаки зловмисник може використовувати браузер жертви для перегляду сторінок сайту від імені користувача.

Виконання коду (Command Execution)

Всі сервери використовують дані, віддані користувачем при обробці запитів. Часто ці дані використовуються при складанні команд, що застосовуються для генерації динамічного вмісту. Якщо при розробці не враховуються вимоги безпеки, зловмисник отримує можливість модифікувати виконувані команди з допомогою наступних методів реалізації атаки на електронний ресурс:

1. Переповнення буфера (Buffer Overflow)

Експлуатація переповнення буфера дозволяє зловмисникові змінити шлях виконання програми шляхом перезапису даних в пам'яті системи. Переповнення буфера є найбільш поширеною причиною помилок в програмах. Воно виникає, коли обсяг даних перевищує розмір виділеного під них буфера. Коли буфер переповнюється, дані переписують інші області пам'яті, що призводить до виникнення помилки.

Якщо зловмисник має можливість управляти процесом переповнення, це може викликати ряд серйозних проблем.

Переповнення буфера може викликати відмови в обслуговуванні, приводячи до пошкодження пам'яті і викликаючи помилки в програмах. Більш серйозні ситуації дозволяють змінити шлях виконання програми і виконати в її контексті різні дії.

Використовуючи переповнювання буфера, можна перезаписувати службові області пам'яті, наприклад, адресу повернення з функцій в стек. Також, при переповненні можуть бути переписані значення змінних в програмі.

2. Впровадження операторів SQL (SQL Injection)

Ці атаки спрямовані на Web-сервери, що створюють SQL запити до серверів СУБД на основі даних, що вводяться користувачем.

Мова запитів Structured Query Language (SQL) являє собою спеціалізовану мову програмування, що дозволяє створювати запити до серверів СУБД. Більшість серверів підтримують цю мову у варіантах, стандартизованих ISO і ANSI. У більшості сучасних СУБД присутні розширення діалекту SQL, специфічні для даної реалізації (T-SQL в Microsoft SQL Server, --PL SQL в Oracle і т.д.). Багато Web-додатків використовують дані, передані користувачем, для створення динамічних Web-сторінок.

Якщо інформація, отримана від клієнта, належним чином не перевіряється, атакуючий отримує можливість модифікувати запит до SQL-сервера, що відправляється додатком. Запит буде виконуватися з тим же рівнем привілеїв, з яким працює компонент програми, що виконує запит (сервер СУБД, Web-сервер і т.д).

У результаті зловмисник може отримати повний контроль на сервером СУБД і навіть його операційною системою.

3. Впровадження серверних сценаріїв (SSI Injection)

Атаки даного класу дозволяють зловмиснику передати шкідливий код, який надалі буде виконаний на Web-сервері. Уразливості, що призводять до можливості здійснення даних атак, зазвичай полягають у відсутності перевірки даних, наданих користувачем, перед збереженням їх у інтерпретованому сервером файлі.

Перед генерацією HTML сторінки сервер може виконувати сценарії, наприклад Server-site Includes (SSI). У деяких ситуаціях вихідний код сторінок генерується на основі даних, наданих користувачем.

Якщо атакуючий передає серверу оператори SSI, він може отримати можливість виконання команд операційної системи або включити в неї заборонений вміст при наступному відображенні [4].

Логічні атаки (Logical Attacks)

Логіка додатка являє собою очікуваний процес функціонування програми при виконанні певних дій. В якості прикладів можна навести відновлення пролів, реєстрацію облікових записів, аукціонні торги, транзакції в системах електронної комерції. Додаток може вимагати від користувача коректного виконання кількох послідовних дій для виконання певного завдання.

Зловмисник може обійти або використовувати ці механізми в своїх цілях.

Методи реалізації логічних атак на електронні ресурси:

1. Відмова в обслуговуванні (Denial of Service)

Даний клас атак спрямований на порушення доступності Web-сервера. Зазвичай атаки, спрямовані на відмову в обслуговуванні реалізуються на мережевому рівні, проте вони можуть бути спрямовані і на прикладний рівень. Використовуючи функції Web-додатків, зловмисник може вичерпати критичні ресурси системи, або скористатися вразливістю, що приводить до припинення функціонування системи.

Зазвичай DoS атаки спрямовані на вичерпання критичних системних ресурсів, таких як обчислювальні потужності, оперативна пам'ять, дисковий простір або пропускна спроможність каналів зв'язку. Атаки можуть бути спрямовані на будь-який з компонентів Web-додатків, наприклад, такі як сервер СУБД, сервер автентифікації і т.д. На відміну від атак на мережевому рівні, що вимагають значних ресурсів зловмисника, атаки на прикладному рівні зазвичай легше реалізувати [4].

2. Зловживання функціональними можливостями (Abuse of Functionality)

Дані атаки спрямовані на використання функцій Web-додатків з метою обходу механізмів розмежування доступу. Деякі механізми Web-додатків, включаючи функції забезпечення безпеки, можуть бути використані для цих цілей. Наявність уразливості в одному з, можливо, другорядних компонентів додатка може призвести до компрометації всієї програми.

Рівень ризику і потенційні можливості зловмисника у разі проведення атаки дуже сильно залежать від конкретного додатка.

Зловживання функціональними можливостями дуже часто використовується спільно з іншими атаками, такими як зворотний шлях в директоріях і т.д. Приміром, при наявності уразливості типу міжсайтового виконання сценаріїв в HTML-чаті зловмисник може використовувати функції чату для розсилки URL, який експлуатує уразливість, всім поточним користувачам.

Висновки

Сучасні методи реалізації атак на електронні ресурси є різновидом інформаційної зброї, за допомогою якої розгортається інформаційна війна на цифровому полі бою. Методи ведення інформаційної війни різноманітні, один з найефективніших методів є атака на електронні ресурси військових органів управління та державної влади з метою дезінформації та донесення недостовірної інформації, що відображає погляди супротивника до суспільства з авторитетних державних ресурсів.

Атаки, що базуються на методі використання уразливостей автентифікації та авторизації можна завжди попередити, якщо приділяти при розробці електронного ресурсу значну увагу безпеці даної зони. Як правило, такі методи атаки на електронні ресурси мають успіх, якщо система захисту не була чітко спланована та реалізована з боку програміста.

Результати проведеного аналізу свідчать, що найбільш поширеними та найбільш небезпечними методами атак на електронні ресурси є DoS атаки (denial-of-service) та SQL ін'єкції (SQL injection). За допомогою цих методів найчастіше зупиняється робота електронних ресурсів та висвітлюється необхідна інформація на цільових електронних ресурсах.

Список літератури

1. Сайт http://ru.wikipedia.org/ [Електронний ресурс]. – Режим доступу до матеріалу сайту: http://ru.wikipedia.org/wiki/Інформаційна_зброя.

2. Сайт http://ru.wikipedia.org/ [Електронний ресурс]. – Режим доступу до матеріалу сайту: http://ru.wikipedia.org/wiki/Аутентификация.

3. Сайт http://projects.webappsec.org [Електронний ресурс]. – Режим доступу до матеріалу сайту: http://projects.webappsec.org/w/page/13246918/Credential%20and%20Session%20Prediction.

4. Stuart McClure, Saumil Shah, Shreeraj Shah. Web Hacking: Attacks and Defense First Edition. ISBN 5-8459-0439-0.

Надійшла до редколегії 5.08.2015

Рецензент*:* д-р техн. наук проф. І.В. Рубан, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

АНАЛІЗ СУЧАСНИХ МЕТОДІВ АТАК НА ЕЛЕКТРОННІ РЕСУРСИ ОРГАНІВ ВІЙСЬКОВОГО УПРАВЛІННЯ

А.В. Северинов, А.Г. Хренов

У даній статті розглянуто сучасні методи атак на електронні ресурси органів військового управління. Проведено аналіз методів атак, на основі аналізу виявлено основні найбільш поширені методи та такі, що можна передбачити при розробці архітектури електронного ресурсу.

Ключові слова: *аналіз сучасних методів атак, сучасні методи атак, електронні ресурси, атаки на електронні ресурси.*

ANALYSIS OF ATTACKS MODERN METHODS ON MILITARY CONTROL ELECTRONIC RESOURCES

A.V. Severinov, A.G. Khrenov

This article deals with modern methods of attacks on electronic resources of command and control. The analysis of attacks and techniques based on analysis revealed the main advantages and disadvantages of each most-common methods attacks and those that can predict the development of architecture electronic resource.

Keywords: *Analysis of modern methods of attacks, modern methods of attack, electronic resources, attacks on electronic resources.*