УДК 004.056.53

ІДЕНТИФІКАЦІЯ ВРАЗЛИВОСТЕЙ ПРОЦЕСІВ АВТЕНТИФІКАЦІЇ

Мілінчук Ю.А., Жукова О.А.

НТУ «Дніпровська політехніка»

Анотація. В роботі проведена ідентифікація вразливостей процесів автентифікації. Розглянуті деякі специфічні ознаки систем автентифікації, що можуть наражати їх на загрози. Систематизовані найбільш актуальні вразливості систем автентифікації та проведена оцінка рівня критичності згідно систематики Bugcrowd's Vulnerability Rating Taxonomy.

Ключові слова: ІДЕНТИФІКАЦІЯ, АВТЕНТИФІКАЦІЯ, ВРАЗЛИВІСТЬ, СИСТЕМА АВТЕНТИФІКАЦІЇ, КРИТИЧНІСТЬ.

Вступ. Метою автентифікації є формування необхідної впевненості в тому, максимально ускладнити використання чужих (вкрадених, підібраних) облікових даних. Атаки на системи автентифікації, на жаль, не рідкісне явище в наш час, тому захист систем автентифікації має спиратися на аналіз основних можливих вразливостей

Автентифікація – це процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності. Іншими словами, автентифікація полягає в перевірці: чи є суб'єкт, що хоче підключитися, тим, за кого себе видає.

Вразливість представляє собою слабке місце активу чи засобу управління, яке може бути використано однією та більше загрозою.

Вразливості для систем автентифікації мають деякі специфічні ознаки.

Системи, що мають наступні ознаки, можуть наражатись на загрозу заповнення облікових даних:

– дозволяють багаторазово вводити неправильний логін без тимчасового блокування;

– користувачі використовують один й той самий пароль у декількох системах.

Системи, що мають наступні ознаки, можуть наражатись на загрозу захоплення облікового запису:

– приймають слабкі паролі;

– дозволяють багаторазово вводити неправильний логін без тимчасового блокування;

– легко обійти параметри зміни паролю облікового записку. [1]

Помилки розмежування прав доступу до бази даних (БД). Критичні помилки вбудованих механізмів автентифікації системи управління базою даних (СУБД) або помилки розробки сайтів, при певних умовах, можуть прирівняти звичайних користувачів до адміністратора або контент менеджера. Такий злам реалізується вкрай просто. У випадку з сайтом, атакуючий реєструється на сайті (або форумі) як звичайний користувач, а потім, використовуючи свій обліковий запис проходить в адміністративний розділ сайту.

Недостатня автентифікація (Insufficient Authentication) – виникає коли сервер дозволяє отримувати доступ до важливої інформації чи функціям без належної автентифікації. Наприклад, отримати доступ до елементів управління адміністратора, лише з переходом до каталогу / admin без необхідності входу в систему. Багато веб-додатків за замовчуванням використовують для адміністративного доступу посилання в кореневій директорії серверу (/ admin /). Зазвичай посилання на цю сторінку не фігурує у вмісті сервера, проте сторінка доступна за допомогою стандартного браузера. Оскільки користувач або розробник припускає, що ніхто не скористається цією сторінкою, так як посилання на неї відсутні, часто реалізацією автентифікації нехтують. В результаті для отримання контролю над сервером зловмиснику достатньо зайти на цю сторінку.

Небезпечне відновлення паролів (Weak Password Recovery Validation) – веб-сервер дозволяє несанкціоновано відновлювати, модифікувати та отримувати паролі інших користувачів. Наприклад, багато веб-сайтів вимагають від користувача лише вказати свою електронну адресу в поєднанні з домашньою адресою та номером телефону. Цю інформацію можна легко отримати, і як результат, інформація перевірки автентичності користувача не є дуже секретною. Система відновлення пароля може бути скомпрометована шляхом використання підбору, секретних питань, що легко вгадати або через вразливості системи.

Недостатня протидія автоматизації (Insufficient Anti-automation) – вразливість виникає, якщо сервер дозволяє автоматично виконувати ручні операції. Система просто не визначає коли частота запитів виходить за межі нормального, прийнятного використання. Дозвіл зловмисникам використовувати автоматизацію, щоб спробувати обійти безпеку, може бути небезпечним. Причина, через яку атаки типу автоматизації зберігалися з перших днів роботи з комп'ютерами й до тепер, полягає в тому, що вони можуть бути дуже ефективними. Якщо дати програмі автоматизації необмежену кількість часу на відправку паролів без наслідків блокування, вона в кінцевому підсумку знайде правильний.

Вразливість до розщеплення HTTP-запиту виникає, коли серверні скрипти впроваджують призначені для користувача дані в заголовки HTTP-відповідей, наприклад, в URL перенаправлення, а також коли програми формують кукі на основі введених користувачем даних. Атака, що використовує дану вразливість, може бути реалізована наступним чином: на сервер надходить спеціально сформований запит, відповідь на який інтерпретується як дві різні відповіді. Таким чином, жертва, замість запитаного ресурсу, отримує інформацію, яку сформував атакуючий.

Відсутність тайм-ауту сеансу (Insufficient Session Expiration). Якщо для ідентифікатора сеансу чи облікових даних не передбачено тайм-ауту чи його значення занадто велике, то зловмисник може використати старі дані у процедурі автентифікації. Це збільшує вразливість серверу до атак, пов’язаних із крадіжкою ідентифікаційних даних. Викрадений ідентифікатор може використовуватися для доступу до даних користувача або для здійснення шахрайських транзакцій. Хоча короткий час для тайм-ауту сеансу не допомагає при негайному використанні ідентифікатора, це захищає від повторного відтворення ідентифікатора сеансу.

Неправильне зберігання автентифікаторів. Ця вразливість виникає в разі недбалого зберігання інформації автентифікації зі сторони користувачів та за відсутності політик зберігання автентифікаторів. При цьому, користувачі можуть зберігати свої паролі у записаному вигляді на робочому місці, розкривати їх стороннім особам як у розмові з колегами та іншими особами, так і при використанні зловмисниками методів соціальної інженерії на користувачах. Також, ця вразливість може бути проявлена так і у відношенні до

системи автентифікації. Наприклад, паролі та одноразові паролі OTP не повинні зберігатись на пристрої і повинні бути очищені з оперативної пам'яті, та не передаються методом GET в query параметрах HTTP запиту, а замість цього повинні використовуватись POST запити.

Оцінку вразливостей можна провести за значенням їх критичності. Дана оцінка приведена в таблиці 1. При цьому ранжування проводиться згідно систематики оцінки вразливостей Bugcrowd's Vulnerability Rating Taxonomy [2]:

1 – малий рівень критичності;

2 – середня критичність;

3 – високий рівень критичності;

4 – дуже критична вразливість.

Таблиця 1 – Оцінка критичності вразливостей

№	Умовне позначення	Вразливість	Критичність вразливості
1	B1	Недостатня автентифікація	4
2	B2	Небезпечне відновлення паролів	3
3	B3	Вразливість до розщеплення HTTP-запиту	2
4	B4	Помилки розмежування прав доступу до БД	3
5	B5	Система приймає слабкі паролі	2
6	B6	Користувачі використовують один й той самий пароль у декількох системах	3
7	B7	Система дозволяє багаторазово вводити неправильний логін без тимчасового блокування	3
8	B8	Недостатня протидія автоматизації	3
9	B9	Відсутність тайм-ауту сеансу	3
10	B10	Неправильне збереження автентифікаторів	3

Висновки. Наявність самої вразливості не завдає шкоди системі автентифікації. Для цього повинна бути загроза, що представляє можливість експлуатувати її. Вразливість без відповідної загрози, може не потребувати

реалізації контролю, але повинна бути ідентифікована та повинна піддаватись моніторингу на предмет змін.

References

1. NIST SPECIAL PUBLICATION 1800-17. Retrieved from https://www.nccoe.nist.gov/publication/1800-17

2. Bugcrowd's Vulnerability Rating Taxonomy. Retrieved from https://bugcrowd.com/vulnerability-rating-taxonomy.

AUTHENTICATION PROCESS VULNERABILITY IDENTIFICATION

Milinchuk Yuliia, Zhukova Olena

Abstract. The work identifies vulnerabilities in authentication processes. Some specific features of authentication systems that may expose them to the threat of completing credentials or the threat of account capture are discussed.

The most current vulnerabilities of authentication systems are systematized. The selected vulnerabilities were assessed for criticality, using the Bugcrowd's Vulnerability Rating Taxonomy vulnerability rating system, with the following criticality levels: low criticality, medium criticality, high criticality, very critical vulnerability.

It is obvious that having the most vulnerability does not hurt the authentication system. There must be a threat to this, which is an opportunity to exploit it. Vulnerability without appropriate threat may not require control but must be identified and monitored for change.

Keywords: IDENTIFICATION, AUTHENTICATION, SENSITIVITY, AUTHENTICATION SYSTEM, CRITICITY.