Authentication Credentials Handling

By authentication credentials handling, we mean how an application operates on passwords (password reset, password recovery, or password change). A password reset, for example, could be an easy but loud way to bypass authentication.

Speaking about typical web applications, users who forget their password can get a new one in three ways when no external authentication factor is used.

1. By requesting a new one that will be sent via email by the application
2. By requesting a URL that will allow them to set a new one
3. By answering prefilled questions as proof of identity and then setting a new one

As penetration testers, we should always look for logic flaws in "forgot password" and "password change" functionalities, as they may allow us to bypass authentication.

Previous Next Mark Complete & Next

Cheat Sheet

Resources

Table of Contents

Broken Authentication

What is Authentication

Overview of Authentication Methods

Overview of Attacks Against Authentication

Login Bruteforcing

Default Credentials

Weak Bruteforce Protections

Bruteforcing Usernames

Bruteforcing Passwords

Predictable Reset Token

Password Attacks

Authentication Credentials Handling

Guessable Answers

Username Injection

Session Attacks

Bruteforcing Cookies

Insecure Token Handling

Skill Assessment

Skill Assessment - Broken Authentication

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Powered by HACKTHEBOX