Authentication Vulnerabilities

# Definition of Authentication

**Authentication** is the process of verifying the identity of a user or client. Websites are potentially exposed to anyone who is connected to the internet. This makes robust authentication mechanisms integral to effective web security.

There are three main types of authentication:

* Something you **know**, such as a password or the answer to a security question. These are sometimes called "knowledge factors".
* Something you **have**, This is a physical object such as a mobile phone or security token. These are sometimes called "possession factors".
* Something you **are** or do. For example, your biometrics or patterns of behavior. These are sometimes called "inherence factors".

# What is Authentication Vulnerability

An **authentication vulnerability** is a security flaw that allows an attacker to bypass or weaken the authentication process, enabling unauthorized access to a system or user account. This is some of the most common vulnerabilities in authentication:

* Vulnerabilities in password-based login
* Vulnerabilities in multi-factor authentication
* Vulnerabilities in other authentication mechanisms

# Write-up labs

## Username enumeration via response timing

* Payload: username=?&password=’a’\*100 , if a username in database, response time will longer than others.

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

Ảnh có chứa văn bản, ảnh chụp màn hình, hàng, Sơ đồ

Nội dung do AI tạo ra có thể không chính xác.

* Server implemented rate-limit to incorrect login attempts, so I tried to use header X-Forwarded-For to bypass

Ảnh có chứa văn bản, số, hàng, Phông chữ

Nội dung do AI tạo ra có thể không chính xác.

* With username= ftp, we brute-force password and get password=jennifer

## Broken brute-force protection, IP block

* After 3 or more fail attempts, server will block your IP. But after a true login, your IP will be enabled
* While brute-forcing password, after a trial attempt we send a true attempt

## Username enumeration via account block

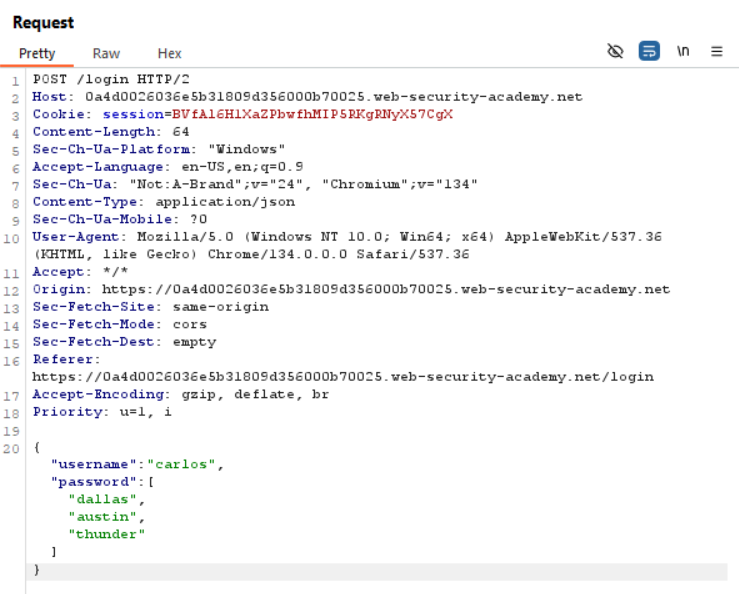
* An account will be blocked after few fail requests. With each username we send with a random password, then base on error message in response we can know if that username exists

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, thiết kế

Nội dung do AI tạo ra có thể không chính xác.

## Broken brute-force protection, multiple credentials per request

* We see that format of sent data in json format. So I try to set parameter password as a list of passwords



* Applying binary search algorithm, we can find the correct password.

## 2FA simple bypass

* After provide valid username and password, we can access other routes successfully without enter correct code sent to that user’s email address