Authentication vulnerabilities

1. Định nghĩa

Xác thực là quá trình xác minh danh tính của người dùng.

1. Sự khác biệt giữa Authen & Author?

**Authen** là quá trình xác thực người dùng

* Đăng nhập bằng tk & mk
* Basic Authentication
* Đăng nhập bằng sinh trắc học
* OTP
* API Keys
* OAuth

**Author** liên quan đến việc xác minh xem người dùng có được phép làm điều gì đó hay ko, kiểm soát truy cập (Access Control), Kiểm soát đặc quyền (Privilege Control)

* Role – Based Access Control (RBAC)
* Attribute – Based Access Control (ABAC)

1. Sự phát sinh của Authen vulnerabilities

* Các cơ chế xác thực yếu vì chúng ko bảo vệ đầy đủ trước các cuộc tấn công
* Lỗi logic or mã hóa kém trong quá trình triển khai cho phép kẻ tấn công bỏ qua hoàn toàn các cơ chế xác thực. Điều này đôi khi còn gọi là “broken Authentication”

1. Lỗ hổng trong cơ chế xác thực
   1. **Username & Password Enumeration**
2. **Username Enumeration**

* **Username Enumeration via Login**

A diagram of a login logic

Description automatically generated

* **Username Enumeration via Register**

A diagram of a register logic

Description automatically generated

* **Username Enumeration via Forgot Password**

A diagram of a computer program

Description automatically generated

* **Username Enumeration via Profile**

A diagram of a profile

Description automatically generated

* **Wordpress User Enumeration**

A screenshot of a computer

Description automatically generated

1. Password Enumeration

* **Common Password**
* Thu thập danh sách mật khẩu wifi từ các ứng dụng chia sẻ mật khẩu
* Thu thập danh sách mật khẩu phổ biến Việt Nam
* Thu thập danh sách username từ các diễn đàn tiếng việt
* Github
* **Common User Passwords Profiler**
* Thu thập thông tin cá nhân (tên, năm sinh, sđt, …) của mục tiêu
* Sử dụng công cụ CUPP để tạo danh sách mật khẩu
* **Compromised Password**
* <https://www.dehashed.com>

[**Lab: Username enumeration via different responses**](https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses)

# [Lab: Username enumeration via subtly different responses](https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-subtly-different-responses) (app/geogre)

# [Lab: Username enumeration via response timing](https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-response-timing)

Đăng nhập một tài khoản bất kì sau đó gửi yêu cầu POST/login tới Burp Repeter. Thử nghiệm với tên người dùng và mật khẩu khác nhau.

Nhận thấy khi thực hiện nhiều lần đăng nhập thì hệ thống sẽ chặn địa chỉ IP của mk

Chúng ta nghĩ đến cần 1 cái j đó để giả mạo địa chỉ IP đánh lừa máy 🡪 **X-Forwarded-For.** Sau đó gửi yêu cầu POST/login tới Burp Intruder.

**i.**Đầu tiên mk sẽ bruteforce cái X-Forwarded-For và cái username trước

* Kiểu tấn công: Pitchfork: đủ payload thì dừng lại
* Thêm X-Forwarded-For Header

Note: là phải để password thật dài chứ mk để ngắn thì chạy nó ko ra

A screenshot of a computer program

Description automatically generated

* Payload 1

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* Payload 2

A screenshot of a computer

Description automatically generated

Start 🡪Vào cột Columns chọn **Respone received** và **Response complete**.

A screenshot of a computer

Description automatically generated

Đặc biệt chú ý đến thời gian phản hồi. Lưu ý rằng khi tên người dùng không hợp lệ, thời gian phản hồi gần như giống nhau. Tuy nhiên, khi bạn nhập tên người dùng hợp lệ (của riêng bạn), thời gian **phản hồi sẽ tăng lên tùy thuộc vào độ dài của mật khẩu bạn đã nhập**.

Chọn username có thời gian phản hồi dài nhất là **administracion**

**ii.** Bây giờ mk sẽ làm tương tự như trên nhưng thay username bằng password

A screenshot of a computer

Description automatically generated

Khi kết thúc thấy status là 302 thì pass: princess

A screenshot of a phone

Description automatically generated

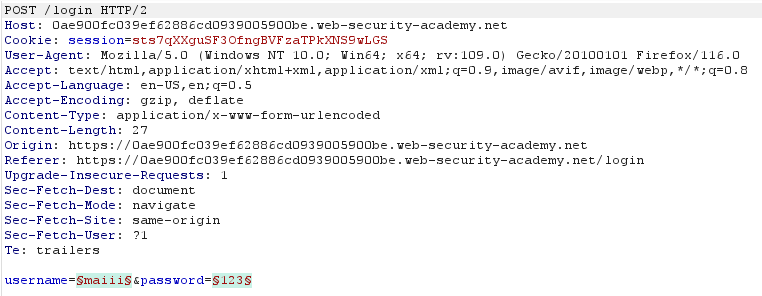
# [Lab: Broken brute-force protection, IP block](https://portswigger.net/web-security/authentication/password-based/lab-broken-bruteforce-protection-ip-block)A screenshot of a login form Description automatically generatedSau khi đăng nhập 3 lần bằng tài khoản – mk bất kỳ thì hệ thống sẽ block IP của mình.

Tạo 1 file username (tối thiểu là 100 username) với các user là user của mình (wiener), và carlos xen kẽ nhau với username đầu tiên là wiener

**File username**: "E:\username.txt"

**File pass:** "E:\password.txt"

Send Post /login to Burp Intruder



Với A screenshot of a computer

Description automatically generated : đủ payload thì dừng

Tại tab **Resource Pool**

Bằng cách chỉ gửi 1 yêu cầu tại một thời điểm, bạn có thể đảm bảo rằng các nỗ lực đăng nhập của mình được gửi đến máy chủ theo đúng thứ tự.

A screenshot of a computer

Description automatically generated

Khi status của tài khoản carlos là 200 mà có xuất hiện một trường hợp 302 🡪 mật khẩu của carlos

# [Lab: Username enumeration via account lock](https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-account-lock)

* Đầu tiên mình brutforce tên người dùng trước

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated

Payload đầu tiên là danh sách tên người dùng, và payloads thứ 2 là payload trống

A screenshot of a payout

Description automatically generated

Chọn tùy chọn tạo 5 payloads. Điều này sẽ khiến mỗi tên người dùng được lặp lại 5 lần một cách hiệu quả.

Bắt đầu cuộc tấn công.

Để ý kĩ thì thấy username là alterwind có độ dài length khác với các user còn lại nên mình ghi lại user này để thử

A screenshot of a computer

Description automatically generated

Nhận thấy chỉ có thông báo của alterwind là trả về “You have made too many incorrect login attempts”.

A screenshot of a computer

Description automatically generated

Còn những username khác sẽ thông báo là “Invalid username or password.”

* Tiếp theo mình sẽ BF mật khẩu

Kiểu tấn công: A screenshot of a computer

Description automatically generated

Tại Payloads Position thì thay username bằng tên mình vừa xác định được ở bên trên nhé, và vị trí cần test là password

A close-up of a logo

Description automatically generated

Tải danh sách password lên và bắt đầu test

A screenshot of a computer

Description automatically generated

Trong kết quả, lưu ý rằng có một số thông báo lỗi khác nhau nhưng một trong các phản hồi không chứa bất kỳ thông báo lỗi nào. Hãy ghi lại mật khẩu này.

A screenshot of a computer

Description automatically generated

Có 3 mật khẩu không hiện lỗi “You have too many…”

Trong 3 mật khẩu kia thì có password=123456789 là không có thông báo lỗi gì cả 🡪 Ghi lại mật khẩu này

Tiếp theo đăng nhập bằng username và password mình vừa xác định được

A screenshot of a computer

Description automatically generated

* 1. **Authentication Attacks**

1. **Brute-force Attack**

* Không cần biết username
* Không cần biết mật khẩu
* Đoán tất cả các trường hợp có thể xảy ra
* Mất nhiều thời gian để dò đoán
* Dễ bị phát hiện
* Các tk dễ bị khóa do các cơ chế phòng vệ. Ví dụ nhập sai mk 3 lần thì xóa tk

1. **Sparing Attack**

* Cần chuẩn bị kỹ danh sách tài khoản
* Cần chuẩn bị kỹ danh sách mk phổ biến
* Mất ít thời gian để dò đoán
* Ít bị phát hiện