

# Authentication

- Allows to gain access to sensitive data and functionality

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".

Authentication - verifies identity ==they claim to be

Authorization - verifies entity if ==allowed to do access resource

- permissions

Problems with Authentication

1. Poor Logic
2. Brute forceable

## Attacks

### 1. Password-based Auth

#### 1.1 Brute Force Attacks (Credential Trial and Error)

Protections: Account Locking, Request Rate limiting

#### A. Lab: Username enumeration via different responses(Diff might be the answer)

1. proxy username and password > right click > send to intruder > highlight username then add
2. Sniper Attack Position,, simple list and paste the wordlist on payload tab
3. Attack, Check the unique different response length (it might be correct)
4. repeat but this time with correct username and repeat but with password

#### B. Lab: Username enumeration via subtly different responses (New Column)

- Same steps above (Lab A) but adds a new column for selected text response (-warning column)
- On intruder, go to settings > ==Grep and extract ==> add > select the "Invalid username or password" as this might change if its correct.

- Attack

Positions Payloads Resource pool **Settings**

These settings can be used to extract useful information from responses

☒ Extract the following items from responses:

Add

Edit From [-warning>] to [</p>\n ...

Remove

```

action>
<p class=is-warning>Invalid username or password.</p>
<form class=login-form method=POST action="/login">
  <label>Username</label>
  <input required type=username name="username" auto
  <label>Password</label>

```

1

OK

Attack Save Columns 5. Intruder attack of https://0a1d00020339843880d735cd009800db.web-security-a...

Results Positions Payloads Resource pool Settings

Filter: Showing all items

might be correct username

no period, diff response (unique)

Request	Payload	Status code	Error	Timeout	Length	-warning> ^
21	access	200	<input type="checkbox"/>	<input type="checkbox"/>	3360	Invalid username or password
0		200	<input type="checkbox"/>	<input type="checkbox"/>	3343	Invalid username or password.
1	carlos	200	<input type="checkbox"/>	<input type="checkbox"/>	3359	Invalid username or password.
2	root	200	<input type="checkbox"/>	<input type="checkbox"/>	3339	Invalid username or password.
3	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	3360	Invalid username or password.
4	test	200	<input type="checkbox"/>	<input type="checkbox"/>	3356	Invalid username or password.
5	guest	200	<input type="checkbox"/>	<input type="checkbox"/>	3343	Invalid username or password.

### C. Lab: Username enum via response timing (IP spoof to bypass IP block)

- POST request limits after 3 consecutive attempts
  - Solution: exploit the X-Forwarded-For header if exist in http request with increasing number to bypass the IP-based brute-force protection
  - when you enter a valid username (your own), the response time is increased depending on the length of the password you entered. So we are checking if the response time is long it might be the username. if both wrong time response is same.
- Send to intruder

- On attack type, use pitch fork (more then one variable/payload to brute force)

Dashboard

Target

Proxy

Intruder

1 x

2 x

+

Positions

Payloads

Resource pool

Settings

?

Choose an attack type

Attack type: Pitchfork

?

Payload positions

Configure the positions where payloads will be inserted

Target: https://0acb0078048ddf2f80a612

20 Accept-Language: en-US,en;q=0.9

21 Priority: u=0, i

22 X-Forwarded-For: \$\$

23

24 username=\$test\$password=

daskdalscdfrandardr anrdna: dddddddd

rdlasndllknasllkndlakkkkkkkkkkkkkkkkk



## Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of ways.

Payload set: 1

Payload count: 100

Payload type: Numbers

Request count: 100



## Payload settings [Numbers]

This payload type generates numeric payloads within a given range and

Number range

Type: ☒ Sequential ☐ Random

From: 1

To: 100

Step: 1

Positions

**Payloads**

Resource pool

Settings



## Payload sets

You can define one or more payload sets. The number of payload sets depends on the number of ways.

Payload set: 2

Payload count: 101

Payload type: Simple list

Request count: 100



## Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as

Paste	
Load ...	carlos
Remove	root
Clear	admin
Deduplicate	test
	guest
	info
	adm
	...

find longest response time for username it might be the password

Attack - 2025 - Columns

5. Internal attack of https://our.com/047118200000110000002020web-security-04

Results

Positions

Payloads

Resource pool

Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response rece...	Response compl...
60	60	americas	200	440	440

repeat the process of pitchfork for password but with correct username, must see 302

Results	Positions	Payloads	Resource pool	Settings
Filter: Showing all items				
Request	Payload 1	Payload 2	Status c... ▾	Respons...
2	92	taylor	302	251

D. Lab: Broken brute-force protection, IP block

1.2 HTTP Auth Exploitation

2. Multi Factor Auth