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

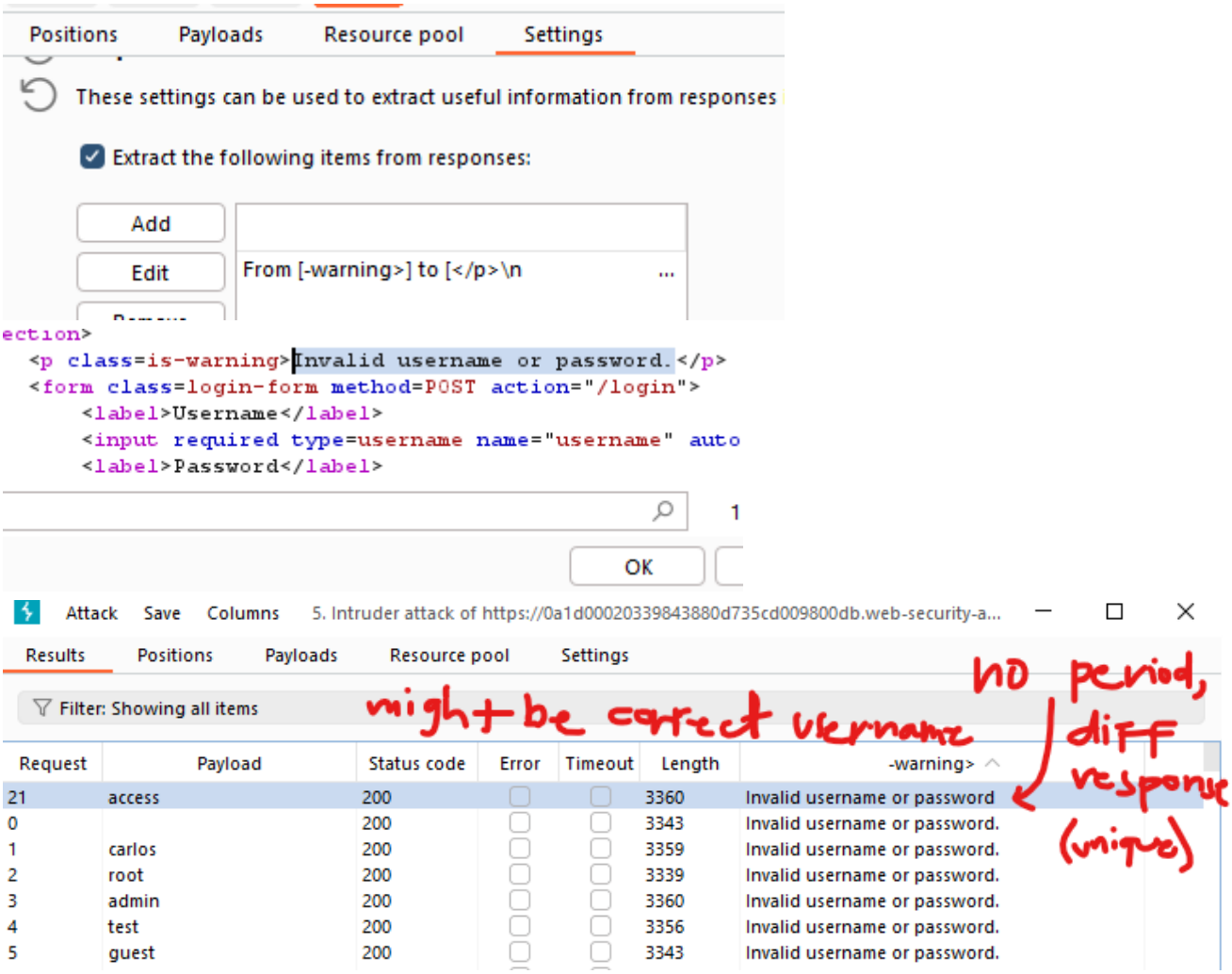
A. Lab: Username enumeration via different responses(Diff might be the answer)

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.

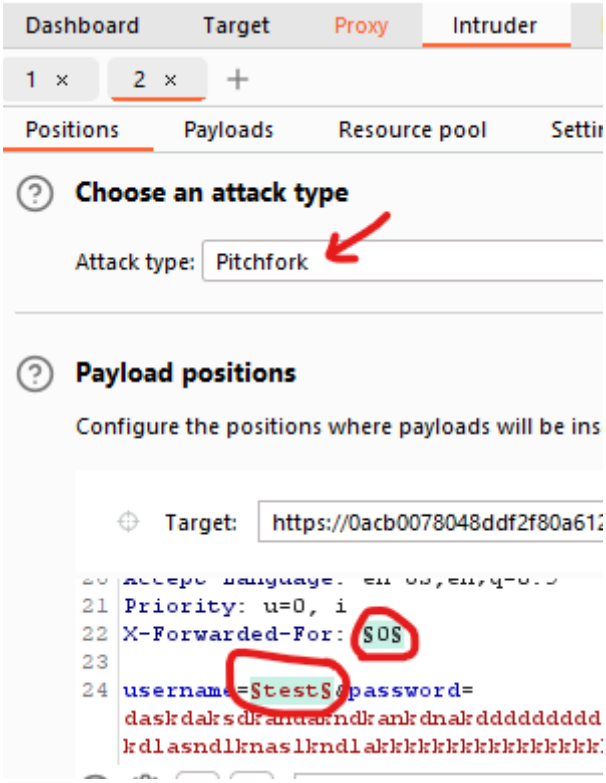
- Attack

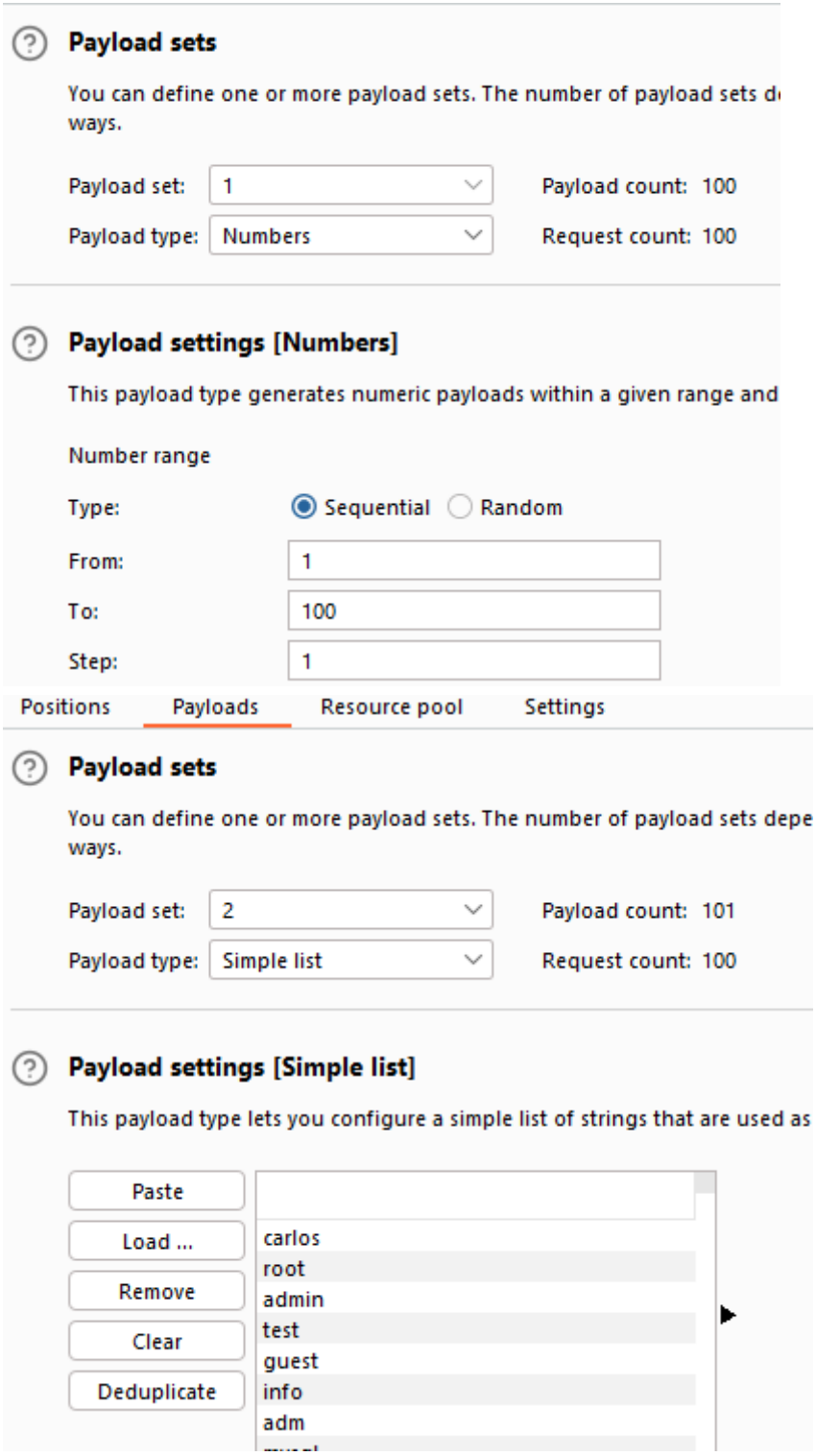


C. Lab: Username enum via response timing (IP spoof to bypass IP block)

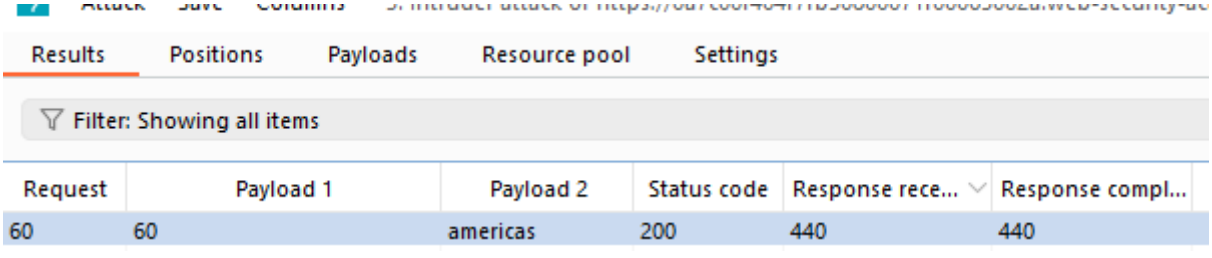
- POST request limits after 3 consecutive attempts
  - Solution: exploit the `X-Forwarded-For` header if exist in http request with increasing number to bypass the IP-based brute-force protection
  when you enter a valid username (your own), the response time is increased depending on the length of the 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)

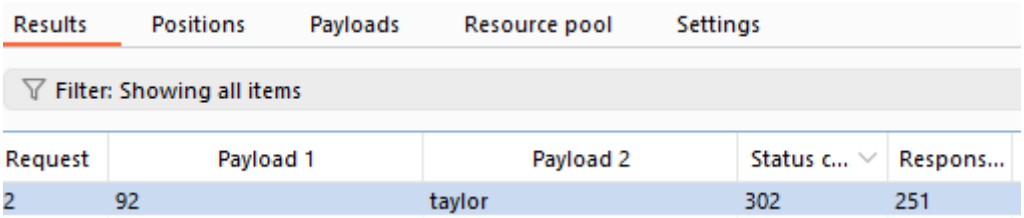




find longest response time for username it might be the password



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



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

1.2 HTTP Auth Exploitation

2. Multi Factor Auth