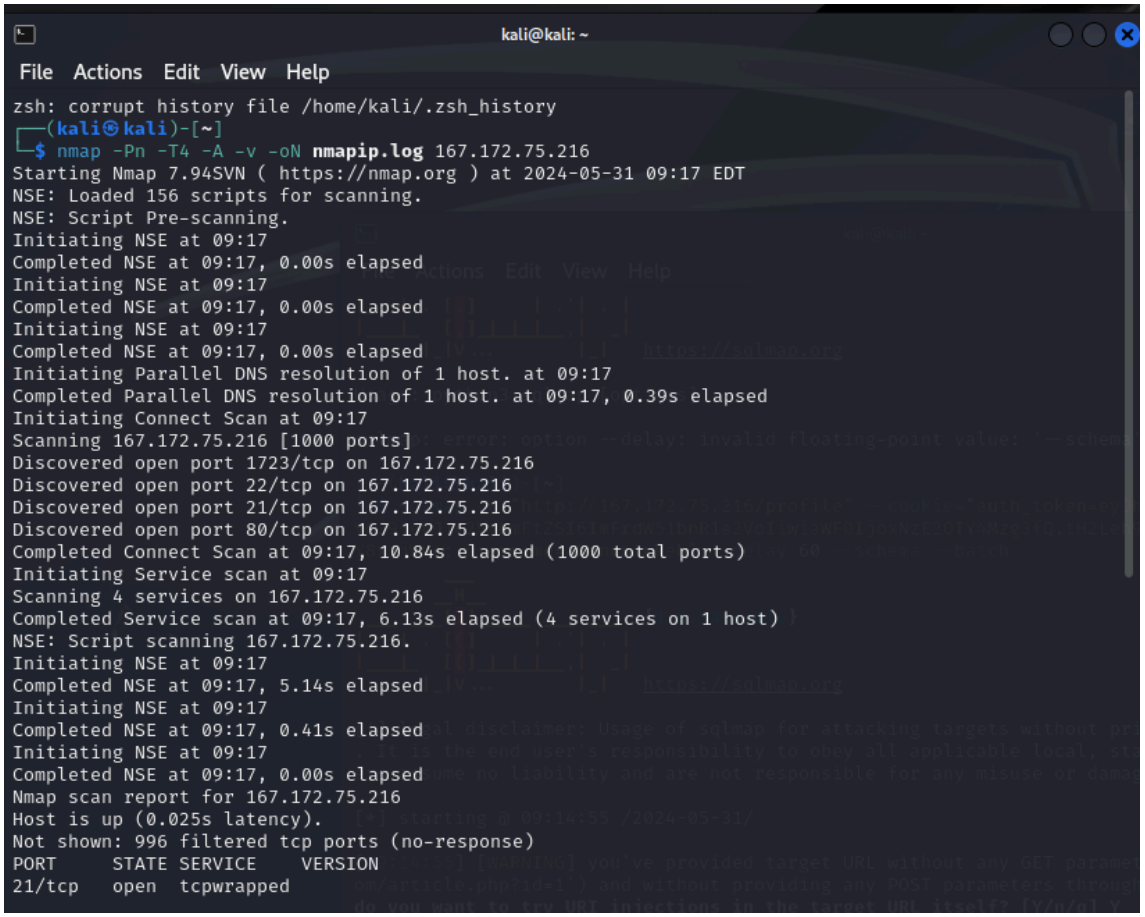
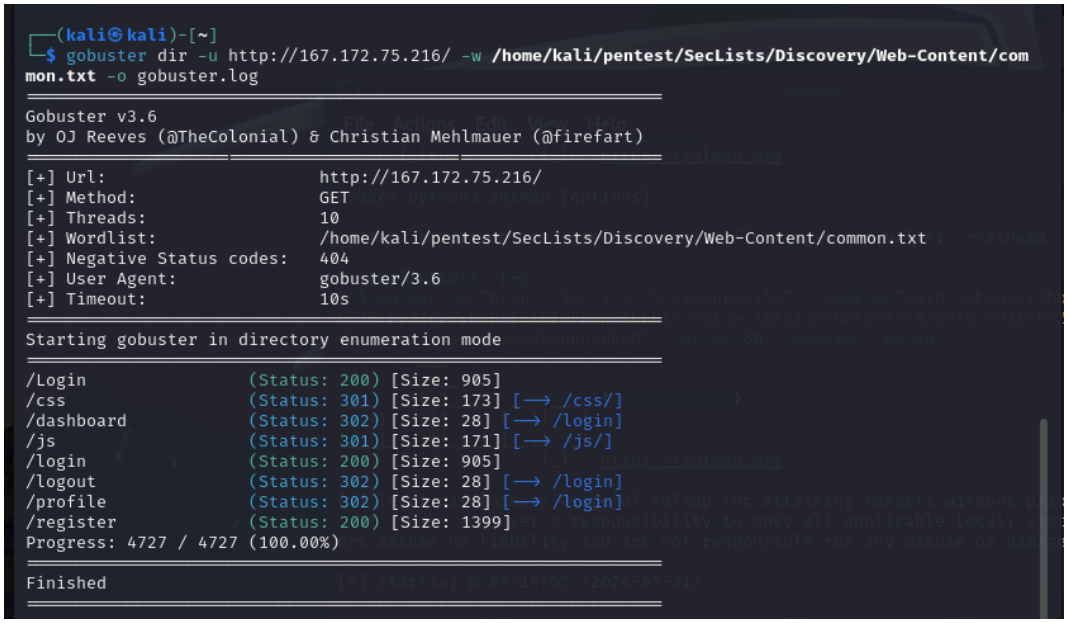
Tahap Reconnaissance and Digital Footprinting

Target IP: 167.172.75.216

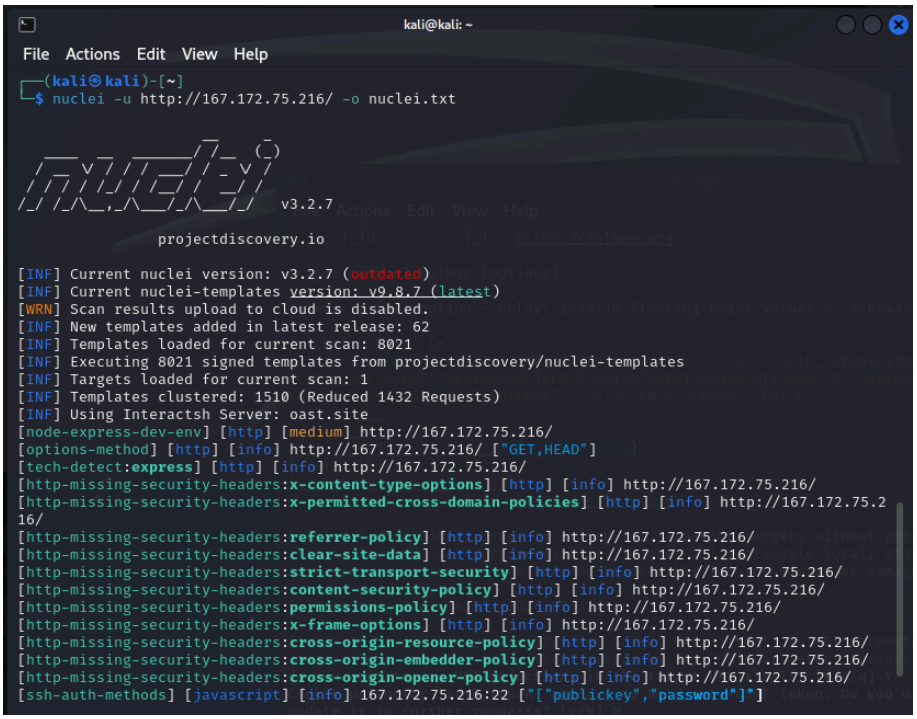
nmap



Gobuster

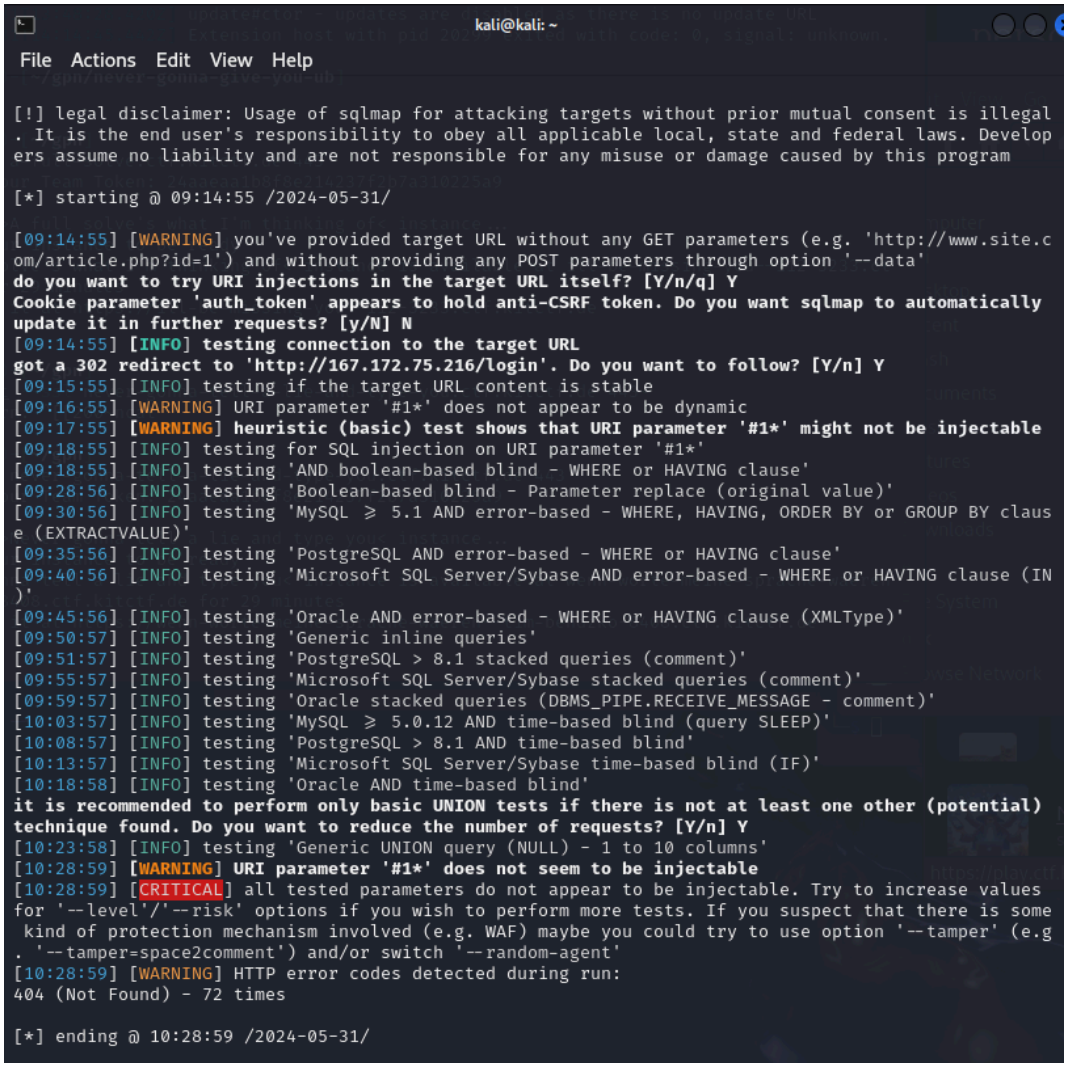


Nuclei


kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nuclei -u http://167.172.75.216/ -o nuclei.txt
v3.2.7
projectdiscovery.io
[INF] Current nuclei version: v3.2.7 (outdated)
[INF] Current nuclei-templates version: v9.8.7 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 62
[INF] Templates loaded for current scan: 8021
[INF] Executing 8021 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1510 (Reduced 1432 Requests)
[INF] Using Interactsh Server: oast.site
[node-express-dev-env] [http] [medium] http://167.172.75.216/
[options-method] [http] [info] http://167.172.75.216/ ["GET,HEAD"]
[tech-detect:express] [http] [info] http://167.172.75.216/
[http-missing-security-headers:x-content-type-options] [http] [info] http://167.172.75.216/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://167.172.75.216/
[http-missing-security-headers:referrer-policy] [http] [info] http://167.172.75.216/
[http-missing-security-headers:clear-site-data] [http] [info] http://167.172.75.216/
[http-missing-security-headers:strict-transport-security] [http] [info] http://167.172.75.216/
[http-missing-security-headers:content-security-policy] [http] [info] http://167.172.75.216/
[http-missing-security-headers:permissions-policy] [http] [info] http://167.172.75.216/
[http-missing-security-headers:x-frame-options] [http] [info] http://167.172.75.216/
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://167.172.75.216/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://167.172.75.216/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://167.172.75.216/
[ssh-auth-methods] [javascript] [info] 167.172.75.216:22 ["["publickey","password"]"]

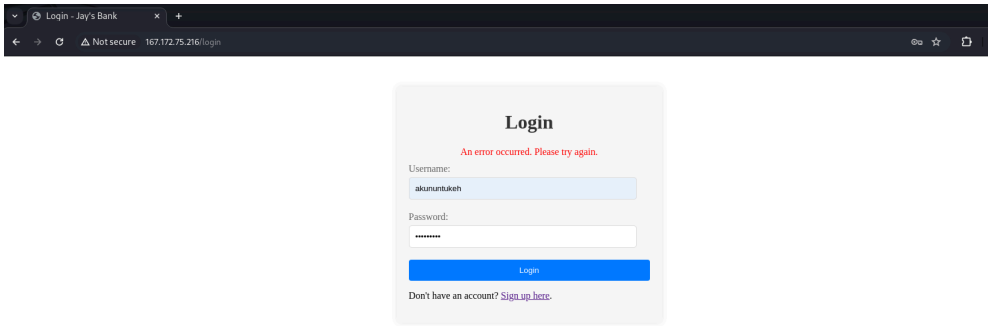
Uji SQLI

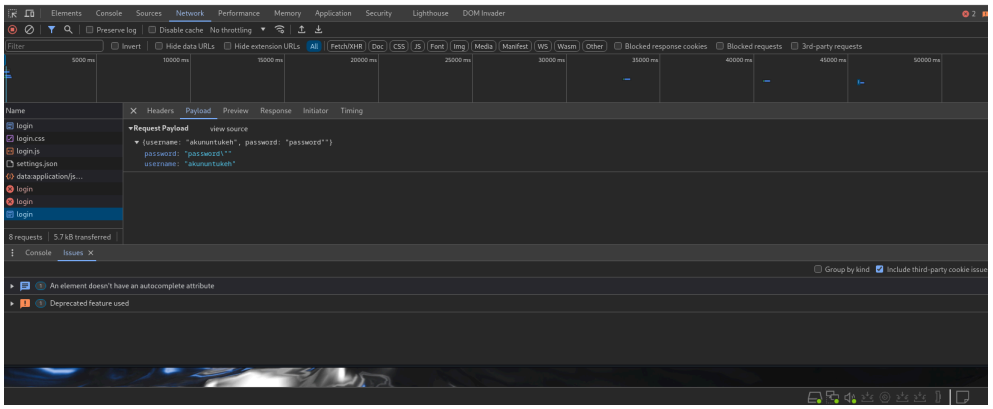
sqlmap -u "http://167.172.75.216/profile" --cookie="auth_token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFrdW51bnR1a2VoIiwiaWF0IjoxNzE2OTY4Mzg3fQ.tH2Leh9Z08TtUU2t-7UGZ-0iVk4Dvax0QXTY8xjjWuc; username=akununtukeh" --delay 60 --schema --batch



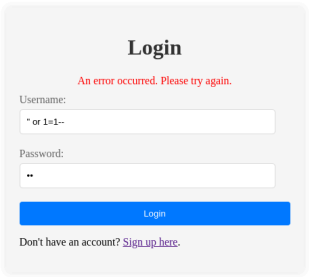
Uji XSS

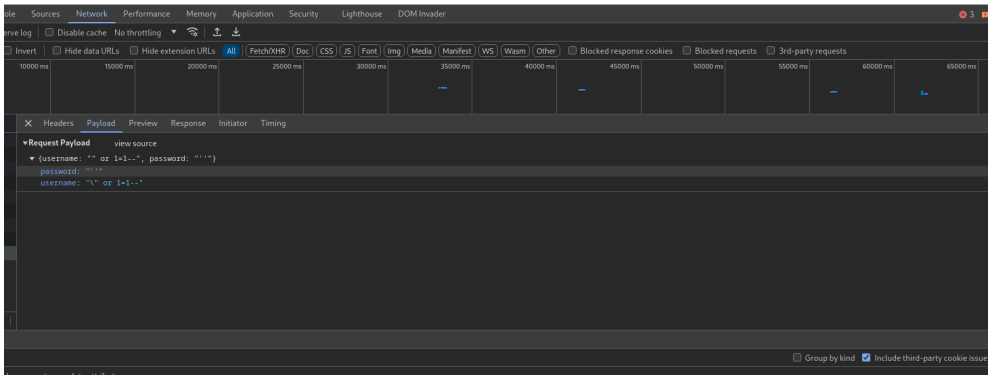
terjadi error ketika password ada petik





terjadi error ketika username ada petik





ada error ketika memberikan input simbol