Vulnerability Scan Report

SQLmap Output

```
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.5#stable}
|_ -| . [(]     | .'| . |
|___|_  ["]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:28:14 /2024-07-12/

 [?1049h [22;0;0t [1;24r (B [m [4l [?7h [24;1H [?1049l [23;0;0tÐ
 [?1l >[1/1] URL:
GET http://testphp.vulnweb.com
do you want to test this URL? [Y/n/q]
> Y
[15:28:14] [INFO] testing URL 'http://testphp.vulnweb.com'
[15:28:14] [INFO] using '/home/kali/.local/share/sqlmap/output/
results-07122024_0328pm.csv' as the CSV results file in multiple targets mode
[15:28:14] [INFO] testing connection to the target URL
[15:28:18] [INFO] testing if the target URL content is stable
[15:28:18] [INFO] target URL content is stable
[15:28:18] [ERROR] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent', skipping to the next target
[15:28:18] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/kali/.local/share/sqlmap/output/results-07122024_0328pm.csv'
```

[*] ending @ 15:28:18 /2024-07-12/

Nmap Output

Nuclei Output