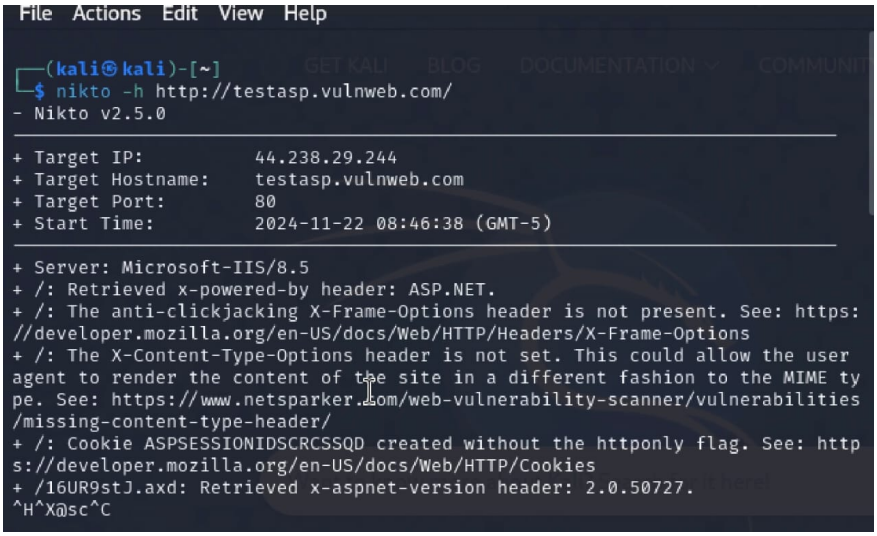
Task 3:

Report & Screenshots:

1. Steps of Nikto:

1. **Open Terminal**: Ensure you are in the Kali Linux terminal.
2. **Run the Nikto Command**:bash
   `nikto -h http://testasp.vulnweb.com`



```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nikto -h http://testasp.vulnweb.com/
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          44.238.29.244
+ Target Hostname:    testasp.vulnweb.com
+ Target Port:        80
+ Start Time:         2024-11-22 08:46:38 (GMT-5)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ /: Retrieved x-powered-by header: ASP.NET.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user
agent to render the content of the site in a different fashion to the MIME ty
pe. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities
/missing-content-type-header/
+ /: Cookie ASPSESSIONIDSCRCSSQD created without the httponly flag. See: http
s://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /16UR9stJ.axd: Retrieved x-aspnet-version header: 2.0.50727.
^H^X@sc^C
```

2. Scanning the Website Using SQLMap

SQLMap is a tool for identifying and exploiting SQL injection vulnerabilities.

Steps to Use SQLMap:

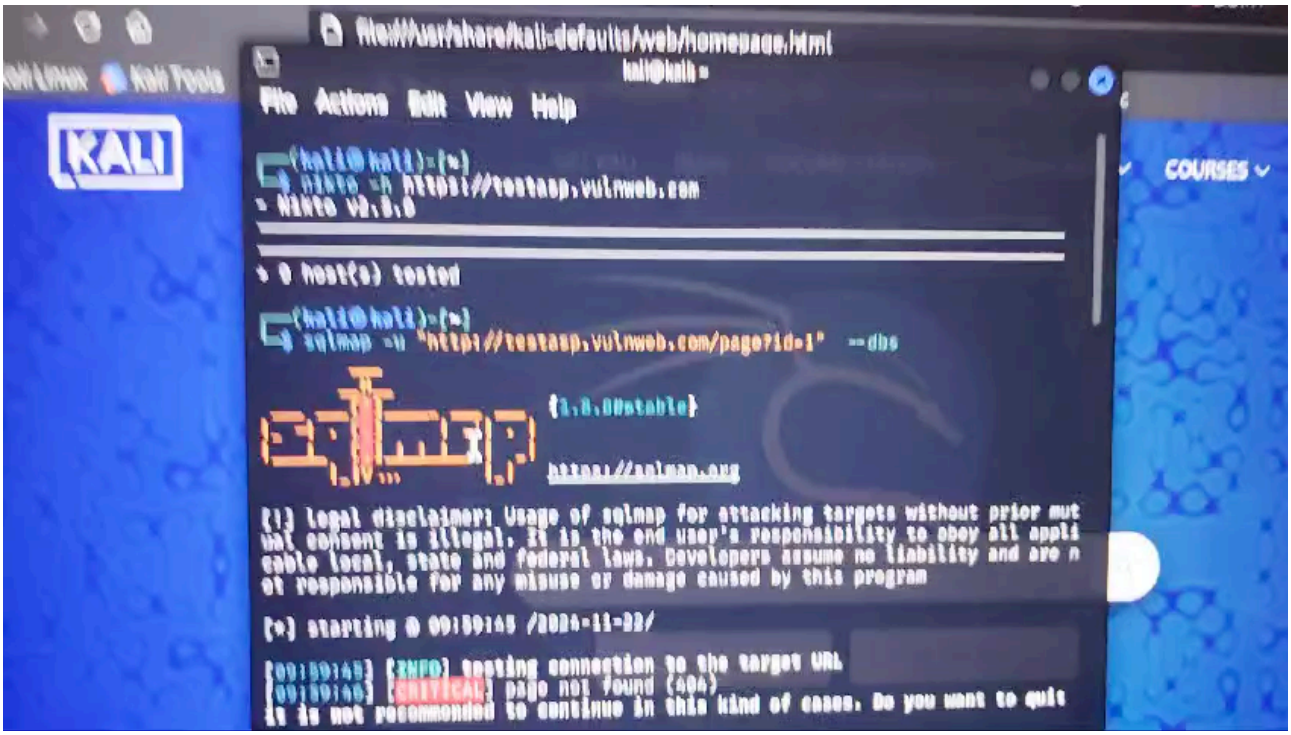
1. **Identify an Input Point**:
   - Visit the website and identify input fields (e.g., login, search) that accept user data.

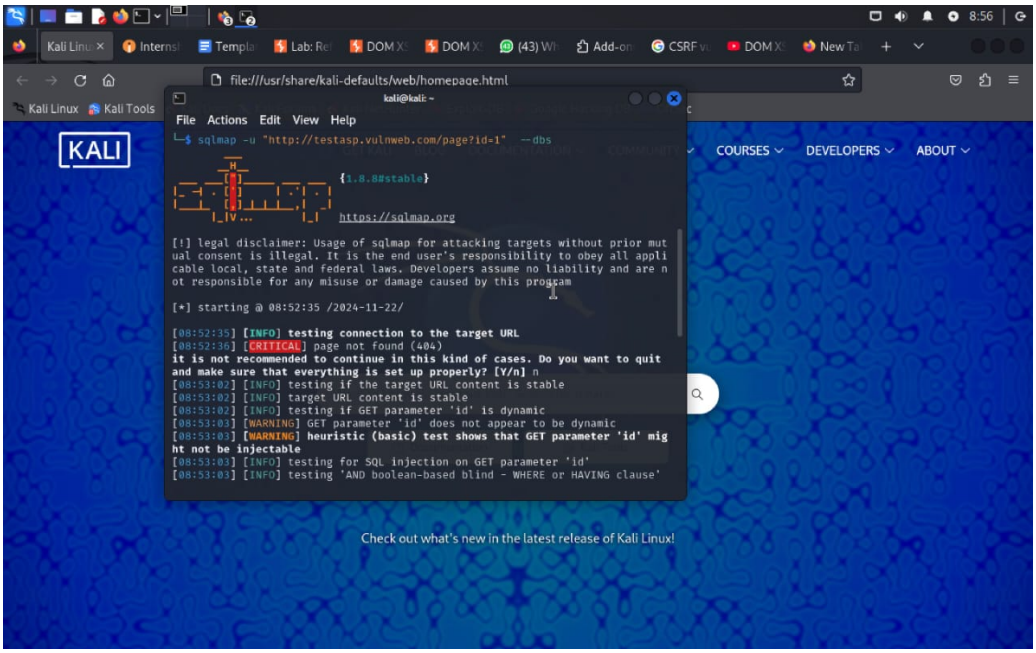
   http://testasp.vulnweb.com/search?id=1

2. Run a Basic SQL Injection Test:

   sqlmap -u "http://testasp.vulnweb.com/search?id=1"

Video:


file:///usr/share/kali-defaults/web/homepage.html
File Actions Edit View Help
KALI
COURSES
sqlmap -u "http://testasp.vulnweb.com/page?id=1" --dbs
{1.8.8#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program
[*] starting @ 08:59:45 /2024-11-22/
[08:59:45] [INFO] testing connection to the target URL
[08:59:46] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit


file:///usr/share/kali-defaults/web/homepage.html
File Actions Edit View Help
KALI
COURSES
DEVELOPERS
ABOUT
sqlmap -u "http://testasp.vulnweb.com/page?id=1" --dbs
{1.8.8#stable}
https://sqlmap.org
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program
[*] starting @ 08:52:35 /2024-11-22/
[08:52:35] [INFO] testing connection to the target URL
[08:52:36] [CRITICAL] page not found (404)
it is not recommended to continue in this kind of cases. Do you want to quit
and make sure that everything is set up properly? [Y/n] n
[08:53:02] [INFO] testing if the target URL content is stable
[08:53:02] [INFO] target URL content is stable
[08:53:02] [INFO] testing if GET parameter 'id' is dynamic
[08:53:03] [WARNING] GET parameter 'id' does not appear to be dynamic
[08:53:03] [WARNING] heuristic (basic) test shows that GET parameter 'id' mig
ht not be injectable
[08:53:03] [INFO] testing for SQL injection on GET parameter 'id'
[08:53:03] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
Check out what's new in the latest release of Kali Linux!