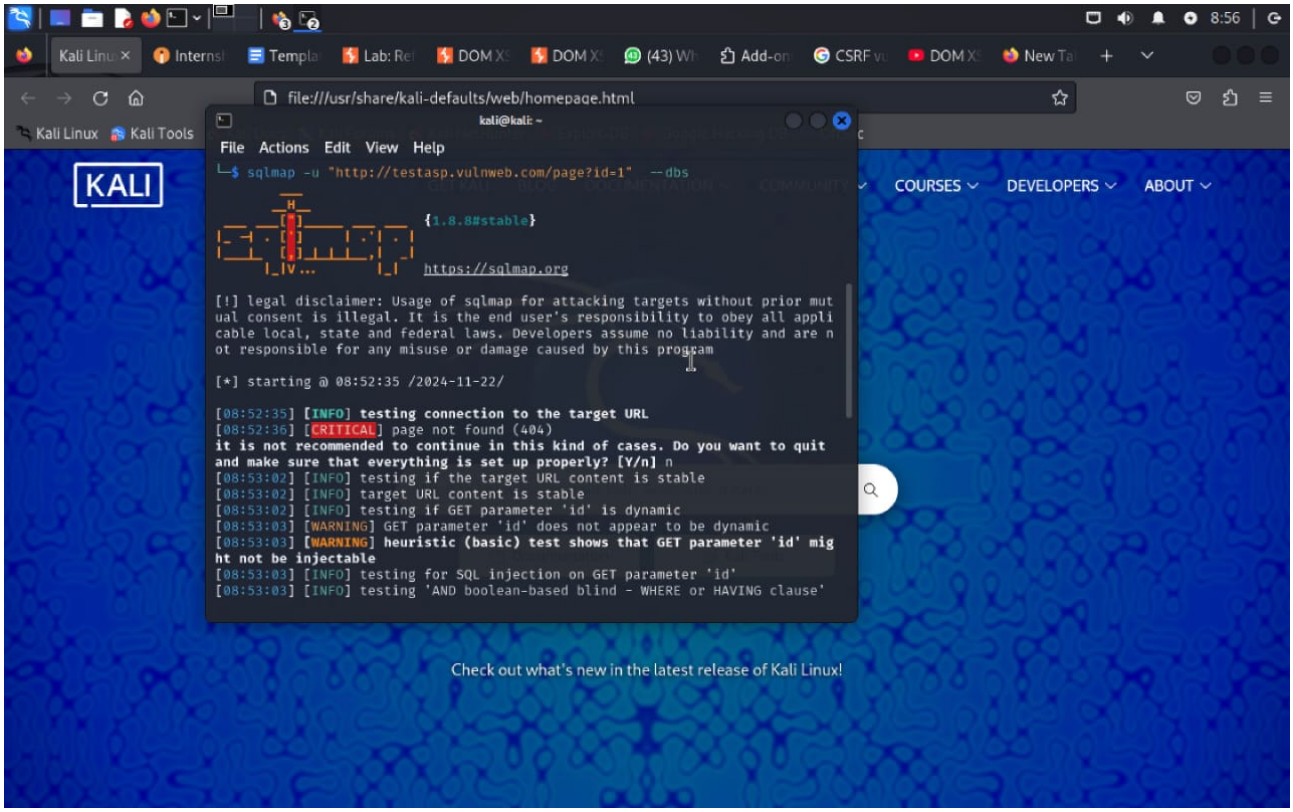
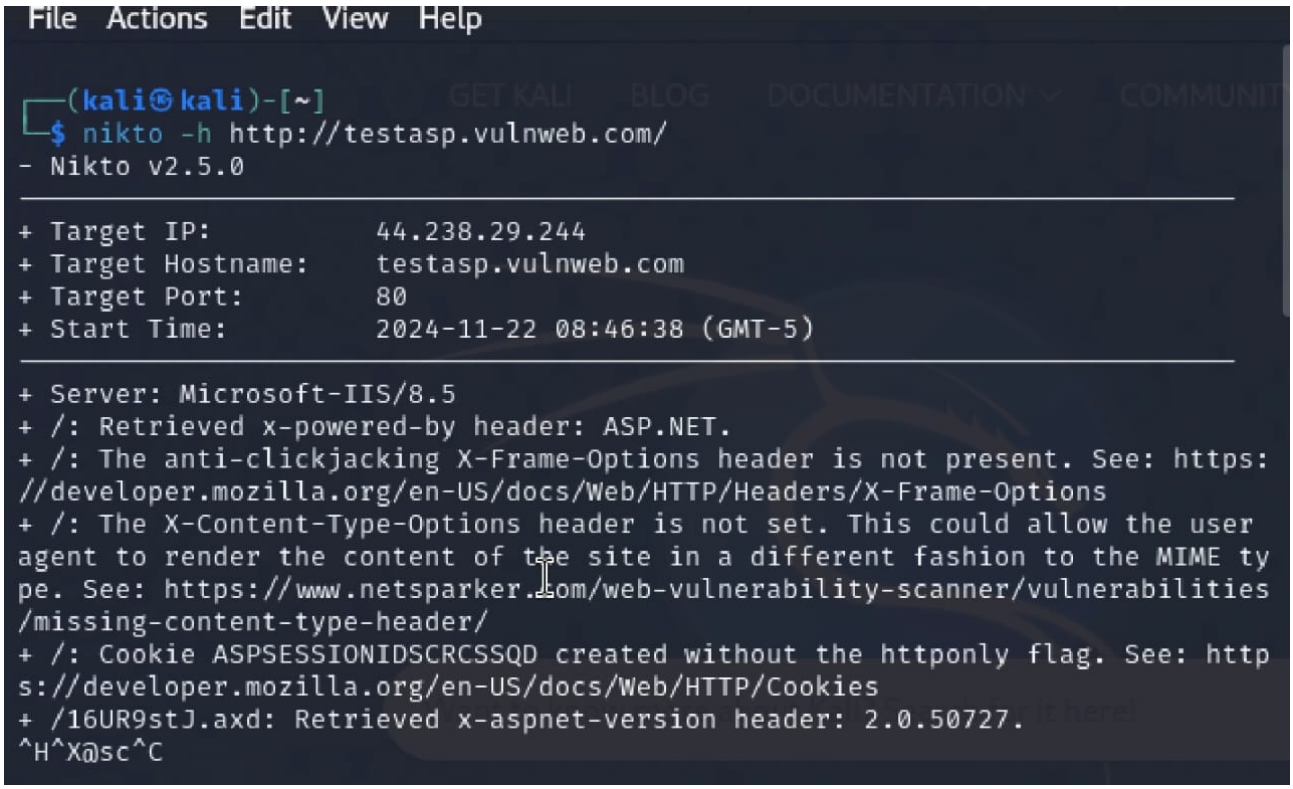
TASK-2:


file:///usr/share/kali-defaults/web/homepage.html
kali@kali: ~
File Actions Edit View Help
└─$ 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 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 @ 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' might 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'
KALI
COURSES
DEVELOPERS
ABOUT
Check out what's new in the latest release of Kali Linux!


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 type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie ASPSESSIONIDSCRCSSQD created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /16UR9stJ.axd: Retrieved x-aspnet-version header: 2.0.50727.
^H^X@sc^C

Personal report on the website:

Custom Findings and Analysis

1. Lack of Anti-Clickjacking Measures

- **Extended Analysis**:
  The absence of `X-Frame-Options` is a significant security gap. This allows attackers to load the website into an iframe, overlay malicious content, and deceive users into interacting with it. Modern browsers support `Content-Security-Policy` (CSP), which can enhance the defense against clickjacking.

2. Missing MIME Type Protection

- **Extended Analysis**:
  Without the `X-Content-Type-Options` header, the website is prone to **content sniffing attacks**. This can lead to browsers interpreting scripts, media, or other files in unintended ways, potentially executing malicious content.

3. Weak Cookie Security

- **Extended Analysis**:
  The cookie flagged in the scan lacks `HttpOnly`, which means it can be accessed by JavaScript, making it a prime target for **Cross-Site Scripting (XSS)**. Additionally, the cookie also appears to lack the `Secure` flag, meaning it could be transmitted over an unencrypted connection (HTTP). This doubles the attack vector.

4. Information Disclosure (ASP.NET Version)

- **Extended Analysis**:
  Disclosing the ASP.NET version (`2.0.50727`) indicates outdated software, as newer frameworks offer enhanced performance and security. Running an unsupported version poses additional risks, as attackers can exploit known vulnerabilities.

Manual Observations

In addition to the tool-based analysis, here are manually identified best practices that can enhance the website's security posture:

1. **SSL/TLS Configuration**:
   The report does not specify whether HTTPS is enforced. It's critical to:
   - Ensure all traffic is redirected to HTTPS.
   - Configure SSL certificates properly using tools like **SSL Labs** for analysis.

2. **Regular Patching and Updates**:
   Ensure all software components, including the server (IIS 8.5), application frameworks, and plugins, are regularly updated to their latest versions.

3. **Input Validation**:
   Harden all input fields to defend against injection attacks such as **SQL Injection** and **Cross-Site Scripting**.

Vulnerability	Impact	Severity	Recommendation
Missing Anti-Clickjacking Header	Clickjacking attacks	Medium	Add `X-Frame-Options` header with `DENY` or `SAMEORIGIN`.
Missing X-Content-Type-Options	MIME type sniffing leading to potential exploits	Medium	Add `X-Content-Type-Options: nosniff` header.
Cookie Without HttpOnly Flag	Cookie theft through XSS	High	Add `HttpOnly` and `Secure` flags to sensitive cookies.
ASP.NET Version Header Disclosure	Information disclosure aiding targeted attacks	Low	Disable the `X-AspNet-Version` header in the web application settings.