Description and the demonstration of the use of Nikto vulnerability scanning tool

Nikto is an open-source web server vulnerability scanner designed to identify potential security issues in web servers, applications, and configurations. It performs comprehensive tests against HTTP/HTTPS servers to detect known vulnerabilities, outdated software, dangerous files, insecure configurations, and other security weaknesses that could be exploited by attackers.

Nikto is widely used by **penetration testers, cybersecurity analysts, system administrators, and students** as part of security assessments and routine security audits. It does not attempt to exploit vulnerabilities; instead, it focuses on **detection, reporting, and visibility**, making it a safe and effective tool for defensive security practices.

Key Uses of Nikto

1. **Web Server Vulnerability Detection**
   Nikto scans web servers for thousands of known vulnerabilities
2. **Version Identification:** Checks for outdated server software (Apache, Nginx, etc.) and version-specific vulnerabilities.
3. **Configuration Auditing:** Identifies misconfigured server options, such as the presence of multiple index files or insecure HTTP methods (e.g., `PUT` or `TRACE`).
4. **Software Fingerprinting:** Detects installed web applications and server components through headers, favicons, and specific file paths.
5. **IDS Testing:** Because it generates thousands of HTTP GET requests, it is a perfect "stress test" for seeing if your firewall or IDS correctly triggers alerts.

Strengths of Nikto

- Open-source and actively maintained
- Simple command-line interface
- Extensive vulnerability database
- Supports multiple output formats (TXT, HTML, CSV, JSON)
- Cross-platform (Linux, Windows, macOS)

Limitations

- Generates noisy scans (easily detectable)
- Not stealthy (not suitable for covert testing)
- Does not exploit vulnerabilities
- Results may require manual verification

✓ Purpose of This Repository

The goal of this project is to:

- Demonstrate how Nikto is used in real-world security assessments
- Provide clear documentation and examples for beginners and practitioners
- Support ethical hacking and defensive security practices
- Serve as a reference for students, SOC analysts, and system administrators

Nikto **does not exploit vulnerabilities** — it focuses on detection and reporting.

Setup

Tool: Nikto

Target: scanme.nmap.org, 172.17.0.2, iplist (10.6.6.14, 10.6.6.13, 172.17.0.2, 10.6.6.23)

List of commands used

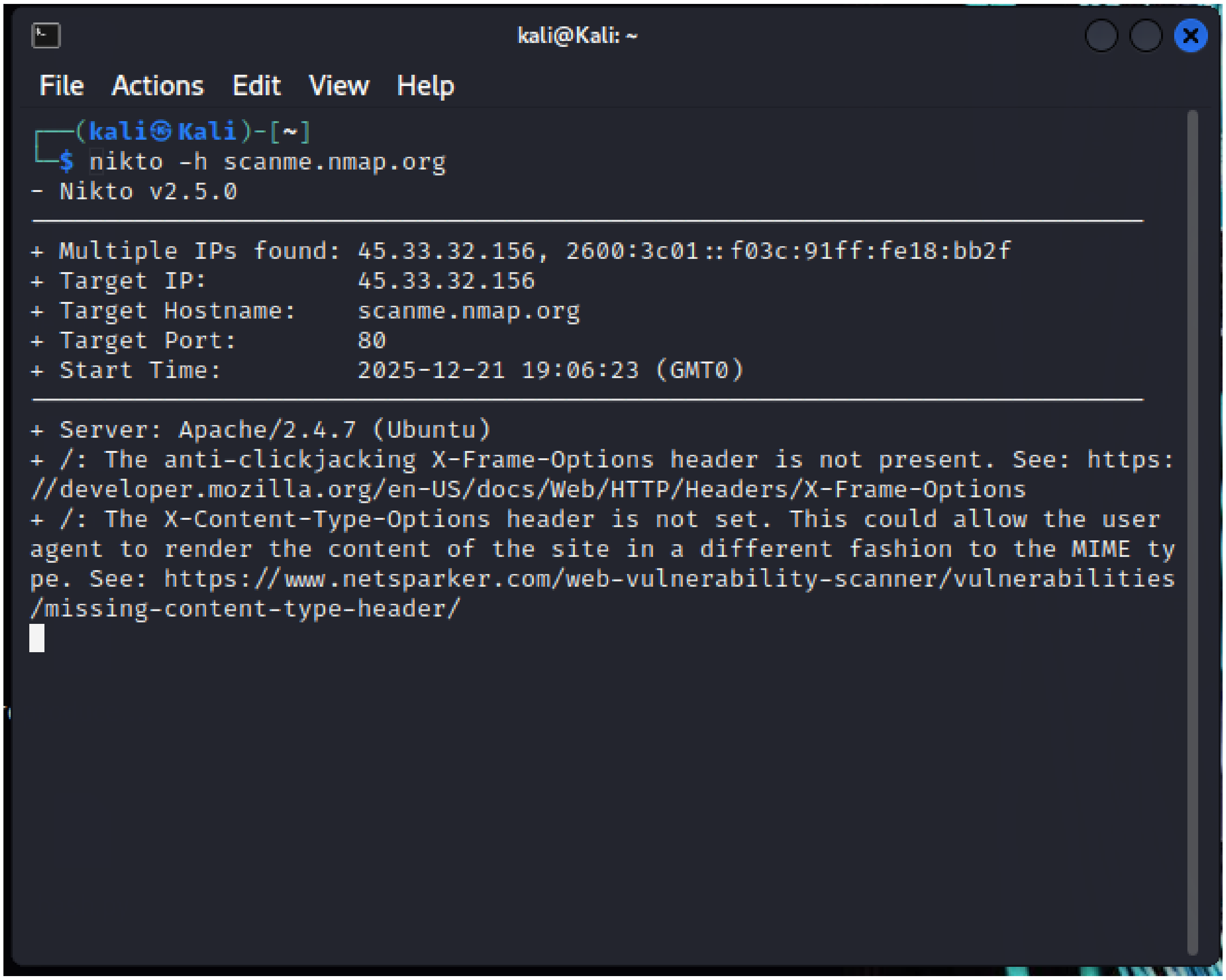
```
nikto -h scanme.nmap.org
```

`nikto -h iplist.txt` (note: the text file include list of ip addresses for nikto to scan individually)

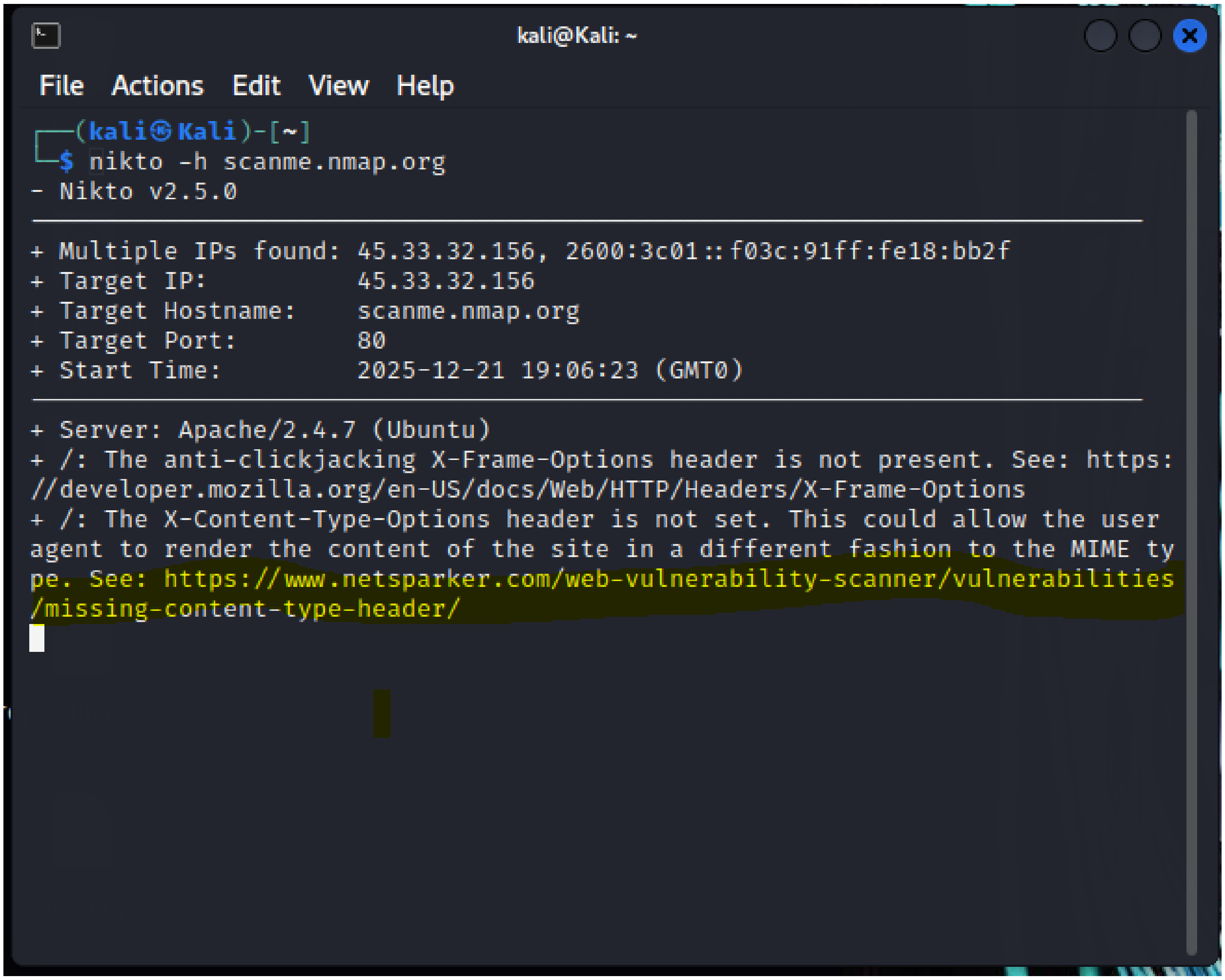
`nikto -h 172.17.0.2 -o paroscan.html` (this specific that the scan result to be saved in that file)

Screenshot of the Lab demonstration

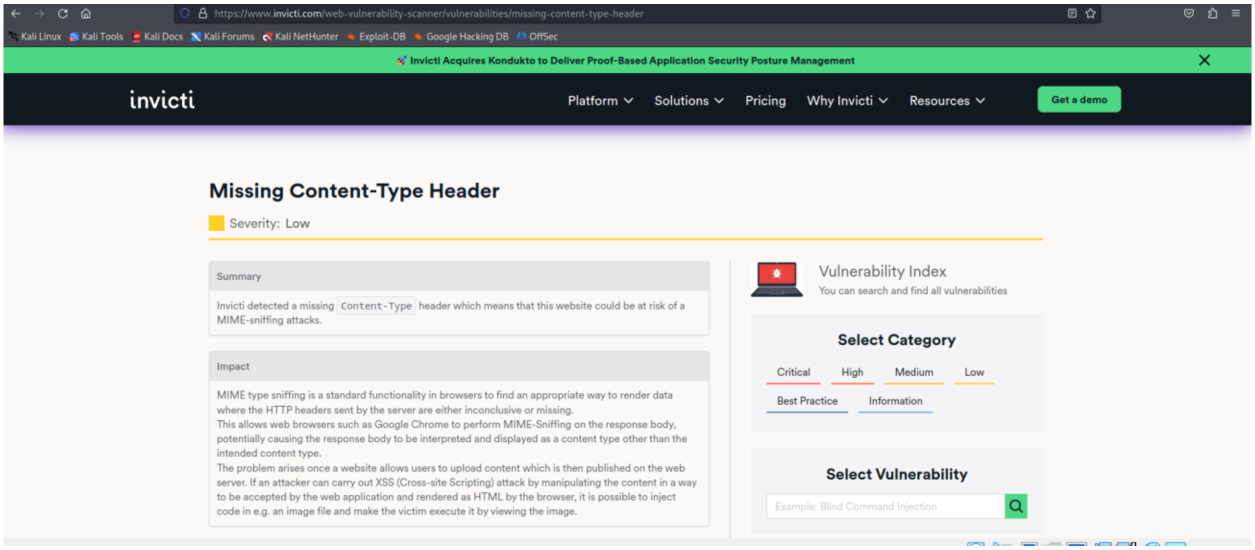
This is the screenshot of a basic nikto scan of scanme.nmap.org, which shows a list of various vulnerabilities. You need to click the website address link to view and read more about the type of vulnerability found



```
┌──(kali㉿Kali)-[~]
└─$ nikto -h scanme.nmap.org
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-21 19:06:23 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: 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/
```



```
┌──(kali㉿Kali)-[~]
└─$ nikto -h scanme.nmap.org
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2025-12-21 19:06:23 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ /: 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/
```


https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Invicti Acquires Kondukto to Deliver Proof-Based Application Security Posture Management
invicti
Platform
Solutions
Pricing
Why Invicti
Resources
Get a demo

Missing Content-Type Header

🟨 Severity: Low

Summary

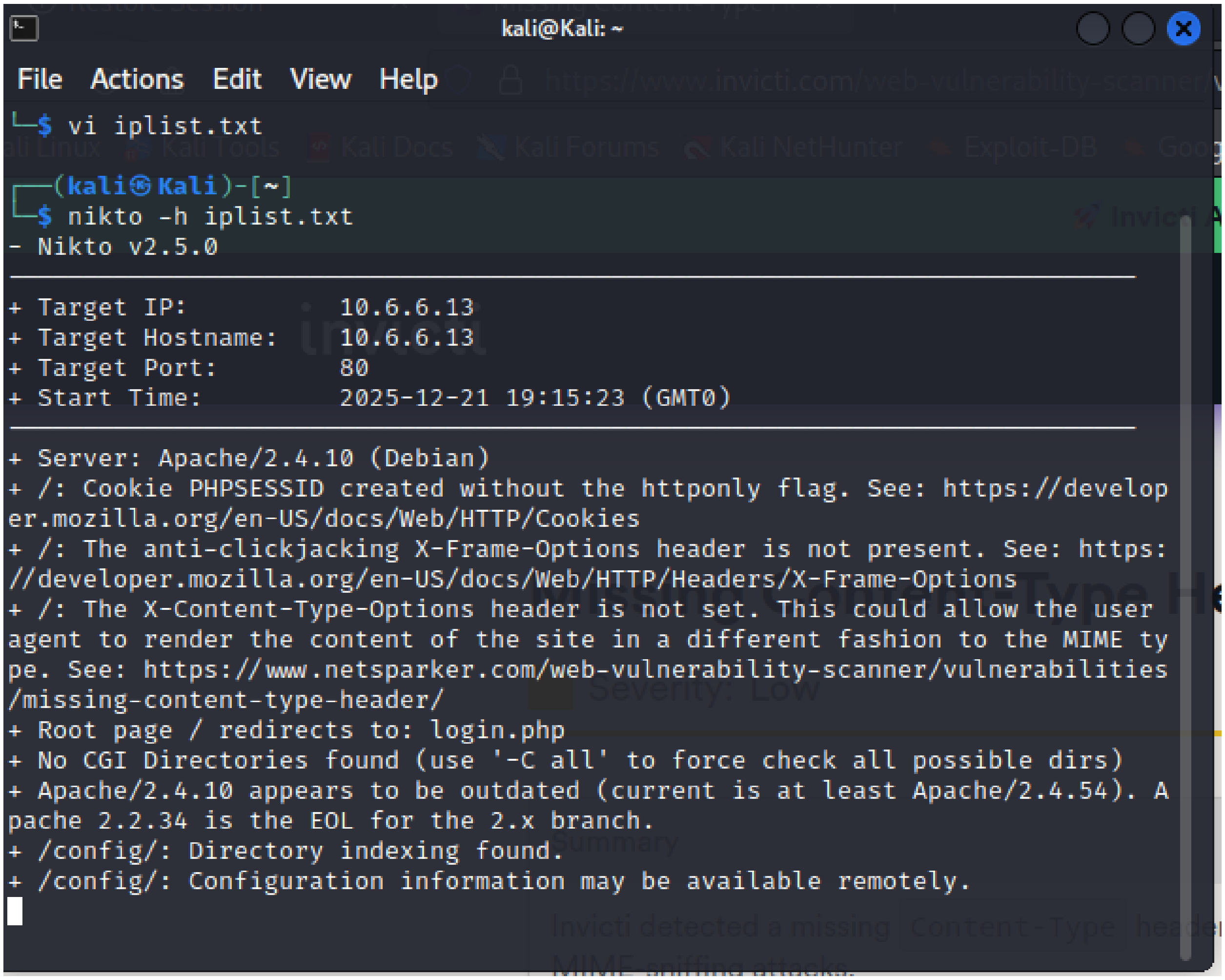
Invicti detected a missing `Content-Type` header which means that this website could be at risk of a MIME-sniffing attacks.

Impact

MIME type sniffing is a standard functionality in browsers to find an appropriate way to render data where the HTTP headers sent by the server are either inconclusive or missing.
This allows web browsers such as Google Chrome to perform MIME-Sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the intended content type.
The problem arises once a website allows users to upload content which is then published on the web server. If an attacker can carry out XSS (Cross-site Scripting) attack by manipulating the content in a way to be accepted by the web application and rendered as HTML by the browser, it is possible to inject code in e.g. an image file and make the victim execute it by viewing the image.

How to use nikto to scan vulnerabilities for a list of Ip addresses

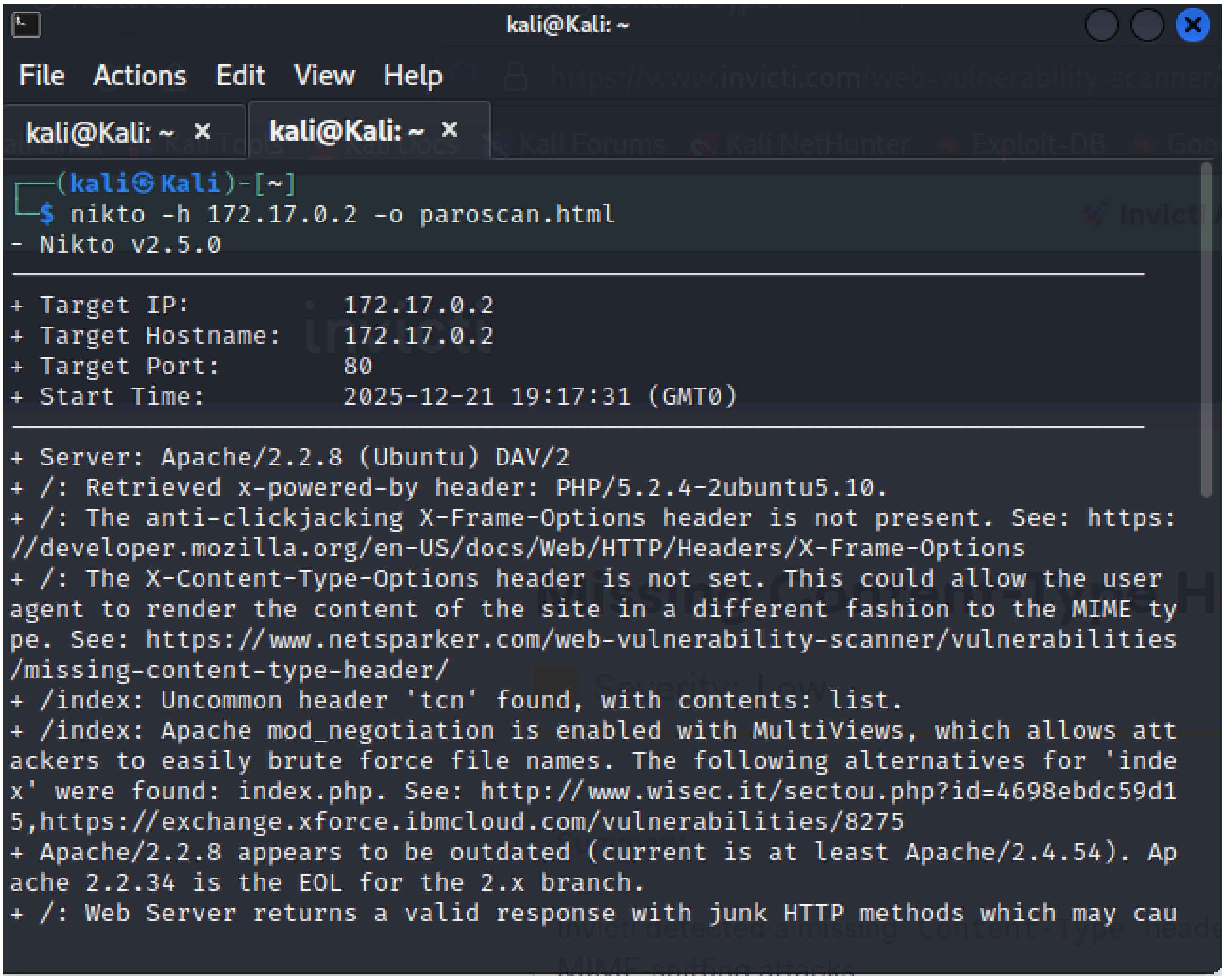
1) Create a text file with the list of ip addresses you wish to scan



```
└─$ vi iplist.txt

┌──(kali㉿Kali)-[~]
└─$ nikto -h iplist.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          10.6.6.13
+ Target Hostname:    10.6.6.13
+ Target Port:        80
+ Start Time:         2025-12-21 19:15:23 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://develop
er.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: 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/
+ Root page / redirects to: login.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.54). A
pache 2.2.34 is the EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
```

how to save the output of nikto scan to a file



```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 172.17.0.2 -o paroscan.html
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          172.17.0.2
+ Target Hostname:    172.17.0.2
+ Target Port:        80
+ Start Time:         2025-12-21 19:17:31 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ /: Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10.
+ /: 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/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows att
ackers to easily brute force file names. The following alternatives for 'inde
x' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d1
5,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Ap
ache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cau
```