

## **Lab - Web Vulnerability Scanning**

# **Objectives**

In this lab, you will complete the following objectives:

- Part 1: Launch Nikto and Perform a Basic Scan
- Part 2: Use Nikto to Scan Multiple Web Servers
- Part 3: Investigate Web Site Vulnerabilities
- Part 4: Export Nikto Results to a File

# **Background / Scenario**

Nikto is a popular web vulnerability scanner that can find SQL injection, XSS, and other common vulnerabilities in websites. It can identify installed software using page headers and files. Nikto supports both HTTP and HTTPS protocols.

# **Required Resources**

- Kali VM customized for the Ethical Hacker course
- Internet access

# **Instructions**

## **Part 1: Launch Nikto and Perform a Basic Scan**

### **Step 1: Launch Nikto on Kali Linux.**

- a. Log into the Kali system with the username **kali** and the password **kali**.
- b. Nikto is preinstalled on Kali Linux. It is a command line tool that can be launched using the **Application -> Vulnerability Analysis -> nikto** choice on the menu, or directly from the command line. To view the help file, use the **nikto --help** command.

```

(kali㉿Kali)-[~]
$ nikto --help
Unknown option: help

Options:
  -ask+           Whether to ask about submitting updates
                  yes  Ask about each (default)
                  no   Don't ask, don't send
                  s    Don't ask, just send
  -check6         Check if IPv6 is working (connects to ipv6.google.com or value set in nikto.conf)
  -cgidirs+       Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
  -config+        Use this config file
  -Display+       Turn on/off display outputs:
                  1 Show redirects
                  2 Show cookies received
                  3 Show all 200/OK responses
                  4 Show URLs which require authentication
  -D              Debug output
  -E              Display all HTTP errors
  -P              Print progress to STDOUT
  -S              Scan multiple IPs and hostnames
  -V              Verbose output
  -dbcheck        Check database and other key files for syntax errors
  -evasion+       Encoding technique:
                  1 Random URL encoding (non-UTF8)
                  2 Double slash reference (//.)
                  3 Premature URL randomization
                  4 Prepend long random string
                  5 Fake parameter
                  6 TAB as request spacer
                  7 Change the case of the URL
                  8 Use double quote separator (\")
                  9 Use carriage return (\r\n) as a request spacer
                  A Use a carriage return (\r\n\r\n) as a request spacer
                  B Use binary value \x0B as a request spacer
  -followredirects Follow 3xx redirects to new location
  -Format+        Save file (-o) format:
                  csv CSV-separated-value
                  json JSON format
                  htm HTML Format
                  nbe Nessus NBE format
                  sql Generic SQL (see docs for schema)
                  txt Plain text
                  xml XML format
                  (if not specified the format will be taken from the file extension passed to -output)
  -Help            This help information
  -host+          Target host/URL
  -id+            Host authentication to use, format is id:pass or id:pass:realm
  -ipv4           IPv4 Only
  -ipv6           IPv6 Only
  -key+           Client certificate key file
  -list-plugins  List all available plugins, perform no testing
  -maxtime+      Maximum testing time per host (e.g., 1h, 60m, 3600s)
  -mutate+        Guess additional file names:

```

What command option will uncover SQL injection vulnerabilities only? **-Tuning+9**

## Step 2: Perform a basic scan on scanme.nmap.org.

- Nmap.org has a website set up to test Nmap scans. You will use this web server to perform your first vulnerability scan. Launch Firefox and navigate to the <http://scanme.nmap.org> website. Read the description of the server and the restrictions that are placed on it.

What limitations does Nmap.org suggest for use of their server?**Fewer than 100 scans per day, no SSH brute-force password cracking tools**

- Use Nikto to perform a basic scan on the scanme.nmap.org website.

**Note:** Nikto scans against an internet server can take a few minutes to complete. Wait until the CLI prompt is returned to continue to the next steps. To terminate a running scan, enter **CTRL-C**.

```

(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: 2026-01-22 20:07:47 (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 type. See: https://www.netsparker.co
ssing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: ht
tts://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /images/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ ERROR: Error limit (20) reached for host, giving up. last error: error reading HTTP response
+ Scan terminated: 1 error(s) and 8 item(s) reported on remote host
+ End Time: 2026-01-22 20:57:32 (GMT0) (2985 seconds)

+ 1 host(s) tested

(kali㉿Kali)-[~]
$ 

```

c. Explore the link for **The X-Content-Type-Options header is not set**. vulnerability that was found. Open Firefox and navigate to the link:

<https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/>.

d. Scroll down to view the summary, impact, remediation advice, and the associated vulnerability classification links.

The screenshot shows a Firefox browser window with the URL <https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header>. The page title is "Missing Content-Type Header". The severity is listed as "Low". The "Summary" section states: "Invicti detected a missing [Content-Type] header which means that this website could be at risk of a MIME-sniffing attacks." The "Impact" section explains: "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 some 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 "Remediation" section provides two steps: 1. When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served. For example, if you are serving an HTML page, you should send the HTTP header Content-Type: text/html. 2. Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.X-Content-Type-Options: nosniff. The "Classifications" section lists: CVE-16, ISO27001-A.14.12, OWASP 2013-A5, OWASP 2017-A6, PCI v3.2-6.5.7, WASC-15. To the right, there's a "Vulnerability Index" section with a search bar, a "Select Category" section with tabs for Critical, High, Medium, Low, Best Practice, and Information, and a "Select Vulnerability" section with a search bar and a list of related vulnerabilities: Out-of-date Version (GSAP), GraphQL Library Detected (GraphQL API for Wordpress), Source Code Disclosure (Python), Out-of-date Version (XOOPS), and WordPress Theme Rozy Out Of Date.

What is the recommended remediation for this vulnerability?

- **When serving resources, make sure you send the content-type header to appropriately match the type of the resource being served.**
- **Add the X-Content-Type-Options header with a value of "nosniff" to inform the browser to trust what the site has sent is the appropriate content-type, and to not attempt "sniffing" the real content-type.X-Content-Type-Options: nosniff**

e. Nikto scans for port 80 web services. To scan domains with HTTPS enabled, you must specify the **-ssl** flag to scan port 443: **NOTE: This scan can take a good amount of time before it finishes.**

```
(kali㉿Kali)-[~]
$ nikto -h https://nmap.org -ssl
- Nikto v2.5.0

+ Multiple IPs found: 50.116.1.184, 2600:3c01:e000:3e6::6d4e:7061
+ Target IP: 50.116.1.184
+ Target Hostname: nmap.org
+ Target Port: 443

+ SSL Info: Subject: /CN=insecure.com
             Ciphers: ECDHE-RSA-AES128-GCM-SHA256
             Issuer: /C=US/O=Let's Encrypt/CN=Root
+ Start Time: 2026-01-23 18:46:20 (GMT0)

+ Server: Apache/2.4.6 (CentOS)
+ /: 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/ssing-content-type-header/
+ /robots.txt: Entry '/search/?*/*' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/search/*?' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: Entry '/mailman/listinfo/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 5 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Hostname 'nmap.org' does not match certificate's names: insecure.com. See: https://cwe.mitre.org/data/definitions/297.html
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.html. See: https://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.4.6 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[[A'[+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /mailman/listinfo: Mailman was found on the server. See: CWE-552
+ /css/: Directory indexing found.
+ /css/: This might be interesting.
+ /data/: Directory indexing found.
+ /data/: This might be interesting.
+ /misc/: Directory indexing found.
+ /misc/: This might be interesting.
+ /images/: Directory indexing found.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-icongsreadme/
^[[B^[[B^[[B+ 8777 requests: 0 error(s) and 22 item(s) reported on remote host
+ End Time: 2026-01-23 22:50:28 (GMT0) (14648 seconds)

+ 1 host(s) tested

(kali㉿Kali)-[~]
$
```

## Part 2: Use Nikto to Scan Multiple Web Servers

In this part, you will use Nikto to scan servers on the internal virtual networks to look for vulnerable web servers. You will first create a text file to list the IP addresses that you want to scan. In real-life reconnaissance, you can obtain the IP addresses of the servers by doing a DNS lookup of the server name from the URL.

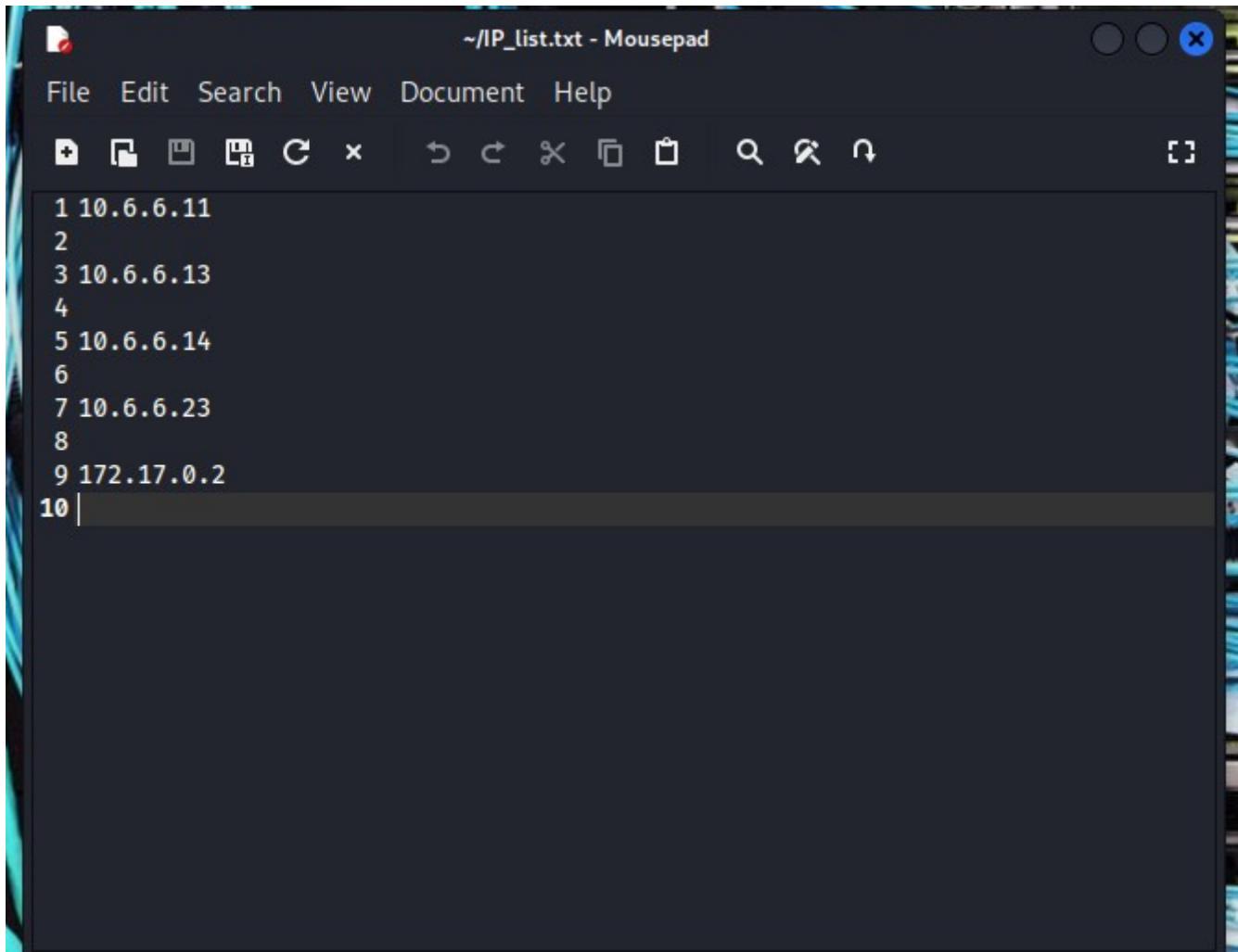
- a. First, create a text file listing the IP addresses of the web servers to be scanned. Use the built-in MousePad application in Kali to create the file. Click **Applications -> Favorites->Text Editor**. Copy and paste this list of IP addresses into your document. Save the document to the home directory as **IP\_list.txt**.

10.6.6.11  
10.6.6.13

10.6.6.14

10.6.6.23

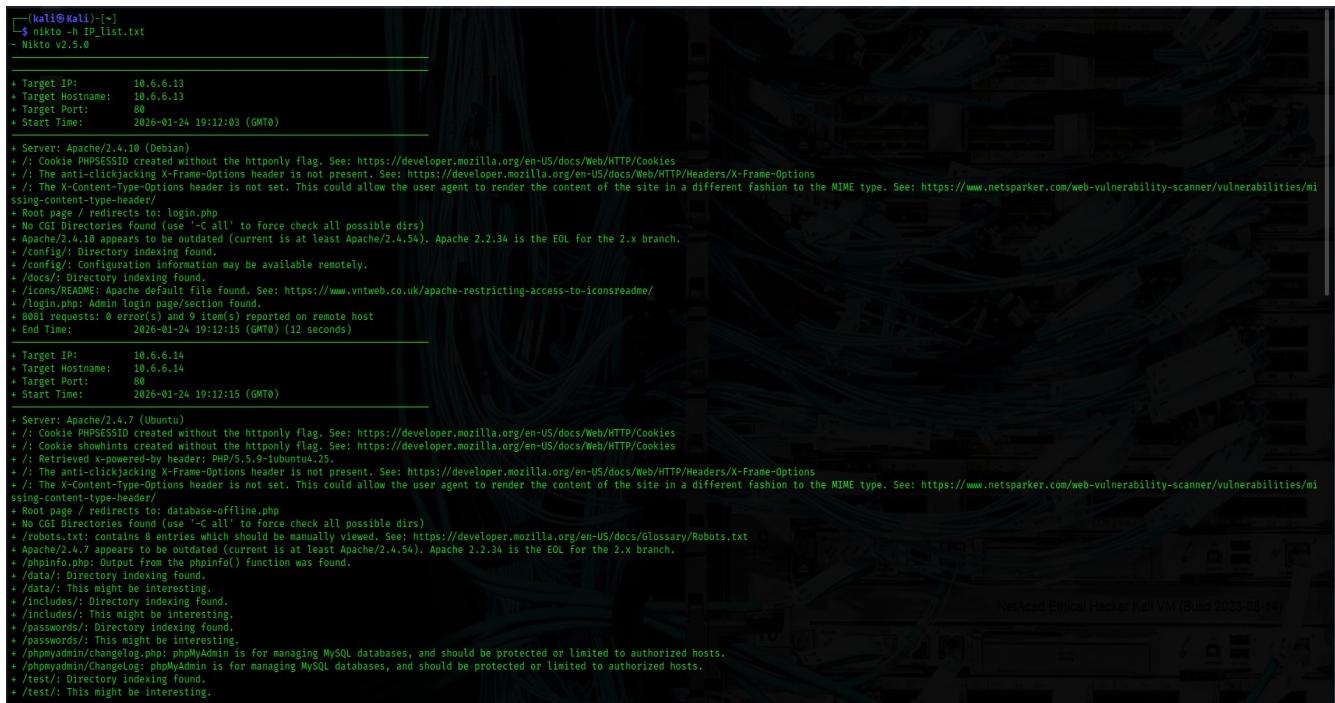
172.17.0.2



The screenshot shows a terminal window titled "~/IP\_list.txt - Mousepad". The window has a dark theme with white text. The menu bar includes "File", "Edit", "Search", "View", "Document", and "Help". Below the menu is a toolbar with icons for file operations like Open, Save, Print, Copy, Paste, Cut, Undo, Redo, Find, Replace, and others. The main text area contains the following list of IP addresses:

```
1 10.6.6.11
2
3 10.6.6.13
4
5 10.6.6.14
6
7 10.6.6.23
8
9 172.17.0.2
10 |
```

b. Run the scan using the **nikto -h IP\_list.txt** command.



The screenshot shows a terminal window displaying the output of the nikto command. The output is a multi-host report with the following details:

```
(kali㉿Kali)-[~]
$ nikto -h IP_list.txt
- Nikto v2.5.0

+ Target IP:      10.6.6.11
+ Target Hostname: 10.6.6.11
+ Target Port:    80
+ Start Time:   2026-01-24 19:12:03 (GMT0)

+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.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 type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misssing-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). Apache 2.2.34 is the EOL for the 2.x branch.
+ /config/: Directory indexing found.
+ /config/: Configuration information may be available remotely.
+ /docs/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /login.php: Admin login page/section found.
+ 8001 requests: 0 error(s) and 9 item(s) reported on remote host
+ End Time:     2026-01-24 19:12:15 (GMT0) (12 seconds)

+ Target IP:      10.6.6.13
+ Target Hostname: 10.6.6.13
+ Target Port:    80
+ Start Time:   2026-01-24 19:12:15 (GMT0)

+ Server: Apache/2.4.10 (Debian)
+ /: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie showhints created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Retrieved x-powered-by header: PHP/5.5.9-ubuntu4.25.
+ /: 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/misssing-content-type-header/
+ Root page / redirects to: database-offline.php
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: contains 8 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /data/: Directory indexing found.
+ /data/: This might be interesting.
+ /includes/: Directory indexing found.
+ /includes/: This might be interesting.
+ /passwords/: Directory indexing found.
+ /passwords/: This might be interesting.
+ /phpmyadmin/: Manager for MySQL databases, and should be protected or limited to authorized hosts.
+ /phpmyadmin/ChangeLog: MySQLAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
```

How many of the targets are hosting web servers? How many servers are running Apache?

**4 targets are hosting web servers**

**3 servers are running Apache**

```
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
+ /styles/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /.git/index: Git index file may contain directory listing information.
+ /.git/HEAD: Git HEAD file found. Full repo details may be present.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /webservers/: Directory indexing found.
+ /wp-admin/: Directory indexing found.
+ /wp-login/: Directory indexing found.
+ /wp-config/: Git config file found. Infos about repo details may be present.
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ 16141 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time: 2026-01-24 19:12:31 (GMT0) (10 seconds)

+ Target IP: 10.6.6.23
+ Target Hostname: 10.6.6.23
+ Target Port: 80
+ Start Time: 2026-01-24 19:12:31 (GMT0)

+ Server: nginx/1.14.2
+: 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/misusing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /admin/: This might be interesting.
+ /admin/index.html: Admin login page/section found.
+ /wp-admin/: Admin login page/section found.
+ /wp-login/: Admin login page/section found.
+ /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 24194 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2026-01-24 19:12:43 (GMT0) (12 seconds)

+ Target IP: 172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port: 80
+ Start Time: 2026-01-24 19:12:43 (GMT0)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+: 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/misusing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Multiple index files found: /index.html, /index.php
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,hhttps://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+/: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+/: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /*=HP8885FA0-3C92-11d3-A3A9-4C7B80C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /*=HPHE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184

NetAcad Ethical Hacker Kali VM (Build 2023-08-14)
Right Ctrl
```

```
Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
+ misusing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /admin/: This might be interesting.
+ /admin/index.html: Admin login page/section found.
+ /wp-admin/: Admin login page/section found.
+ /wp-login/: Admin login page/section found.
+ /wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 24194 requests: 0 error(s) and 7 item(s) reported on remote host
+ End Time: 2026-01-24 19:12:43 (GMT0) (12 seconds)

+ Target IP: 172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port: 80
+ Start Time: 2026-01-24 19:12:43 (GMT0)

+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+: 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/misusing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Multiple index files found: /index.html, /index.php
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sectou.php?id=4698ebdc59d15,hhttps://exchange.xforce.ibmcloud.com/vulnerabilities/8275
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+/: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+/: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /doc/: Directory indexing found.
+ /doc/: The /doc/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /*=HP8885FA0-3C92-11d3-A3A9-4C7B80C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /*=HPHE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /*=HPHE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-12184
+ /phpMyAdmin/changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/Changelog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 111938, size: 40540, mtime: Tue Dec 9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ /phpMyAdmin/Changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory indexing found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/ChangeLog: Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 111938, size: 40540, mtime: Tue Dec 9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ 4 hosts(s) tested

NetAcad Ethical Hacker Kali VM (Build 2023-08-14)
Right Ctrl
```



The screenshot shows a web browser window with the title "Ethical-Hacker-Kali [Running] - Oracle VirtualBox". The address bar displays the URL <https://www.cve.org/CVERecord?id=CVE-1999-0678>. The page content is for CVE-1999-0678, which is listed as "PUBLISHED". The main section contains "Required CVE Record Information" for CNA: MITRE Corporation. It includes details like "Published: 2000-03-22" and "Updated: 2005-11-02". The "Description" section notes that a default configuration of Apache on Debian GNU/Linux sets the ServerRoot to /usr/doc, allowing remote users to read documentation files. The "Product Status" section indicates "Information not provided". The "References" section lists one entry from securityfocus.com. A sidebar on the right titled "On This Page" includes sections for "Required CVE Record Information", "CNA: MITRE Corporation", and "CVE Program".

## CVE-2003-1418

The screenshot shows a web browser window with the title "Ethical-Hacker-Kali [Running] - Oracle VirtualBox". The address bar displays the URL <https://www.cve.org/CVERecord?id=CVE-2003-1418>. The page content is for CVE-2003-1418, which is listed as "PUBLISHED". The main section contains "Required CVE Record Information" for CNA: MITRE Corporation. It includes details like "Published: 2007-10-20" and "Updated: 2017-10-19". The "Description" section notes that Apache HTTP Server 1.3.22 through 1.3.27 on OpenBSD allows remote attackers to obtain sensitive information via the ETag header or multipart MIME boundary. The "Product Status" section indicates "Information not provided". The "References" section lists five entries, including links to oracle.com, openbsd.org, securityfocus.com, and exchange.xforce.ibmcloud.com. A sidebar on the right titled "On This Page" includes sections for "Required CVE Record Information", "CNA: MITRE Corporation", and "CVE Program".

What vulnerabilities are described by the two CVEs listed?

**CVE-1999-0678 refers to the default configuration on some Apache versions that sets the ServerRoot to /usr/doc. This allows remote users to read documentation files for the entire server.**  
**CVE-2003-1418 allows remote attackers to obtain sensitive information via the ETag header or the multipart MIME boundary.**

b. Use the National Vulnerability Database (<https://nvd.nist.gov>) to find additional information on the CVEs. In the References to Advisories, Solutions, and Tools section, follow the links to find the remediation measures needed to close each vulnerability.

What is the solution provided for CVE-2003-1418? A source code patch exists which fixes this issue

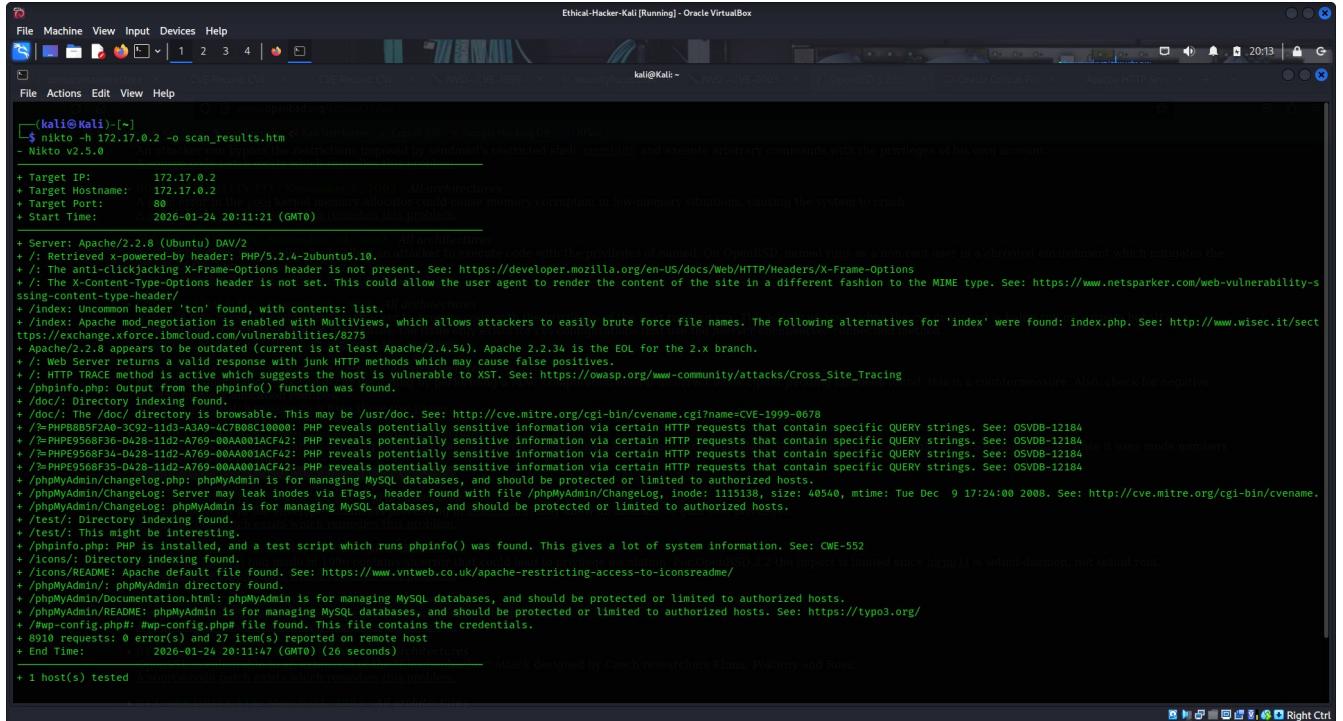
An attacker can bypass the restrictions imposed by sendmail's restricted shell, `smrsh(8)`, and execute arbitrary commands with the privileges of his own account.  
A source code patch exists which remedies this problem.

- **004: RELIABILITY FIX: November 6, 2002 All architectures**  
A logic error in the pool kernel memory allocator could cause memory corruption in low-memory situations, causing the system to crash.  
A source code patch exists which remedies this problem.
- **005: SECURITY FIX: November 14, 2002 All architectures**  
A buffer overflow in `named(8)` could allow an attacker to execute code with the privileges of named. On OpenBSD, named runs as a non-root user in a chrooted environment which mitigates the effects of this bug.  
A source code patch exists which remedies this problem.
- **006: SECURITY FIX: January 20, 2003 All architectures**  
A double free in `cvs(1)` could allow an attacker to execute code with the privileges of the user running cvs. This is only an issue when the cvs command is being run on a user's behalf as a different user. This means that, in most cases, the issue only exists for cvs configurations that use the `pserver` client/server connection method.  
A source code patch exists which remedies this problem.
- **007: SECURITY FIX: February 22, 2003 All architectures**  
In `ssl(8)` an information leak can occur via timing by performing a MAC computation even if incorrect block cipher padding has been found, this is a countermeasure. Also, check for negative sizes in memory allocation routines.  
A source code patch exists which fixes these two issues.
- **008: SECURITY FIX: February 25, 2003 All architectures**  
`httpd(8)` leaks file mode numbers via Etag header as well as child PIDs in multipart MIME boundary generation. This could lead, for example, to NFS exploitation because it uses inode numbers as part of the file handle.  
A source code patch exists which fixes these two issues.
- **009: SECURITY FIX: March 3, 2003 All architectures**  
A buffer overflow in the envelope comments processing in `sendmail(8)` may allow an attacker to gain root privileges.  
A source code patch exists which remedies this problem.
- **010: SECURITY FIX: March 5, 2003 All architectures**  
A fix for an `lprm(1)` bug made in 1996 contains an error that could lead to privilege escalation. For OpenBSD 3.2 the impact is limited since `lprm(1)` is setuid daemon, not setuid root.  
A source code patch exists which remedies this problem.
- **011: SECURITY FIX: March 18, 2003 All architectures**  
Various SSL and TLS operations in OpenSSL are vulnerable to timing attacks.  
A source code patch exists which remedies this problem.
- **012: SECURITY FIX: March 19, 2003 All architectures**  
OpenSSL is vulnerable to an extension of the "Bleichenbacher" attack designed by Czech researchers Klima, Pokorny and Rosa.  
A source code patch exists which remedies this problem.

## Part 4: Export Nikto Results to a File

Nikto can output the results of a scan in various formats including CSV, HTML, SQL, txt, and XML. In addition, Nikto can be paired with Metasploit to launch exploits against the vulnerabilities that you uncover.

- a. To export a scan result, use the `-o` flag followed by the file name. Export the results of a scan to an HTML report file named **scan\_results.htm**. The output file type is determined from the file extension.

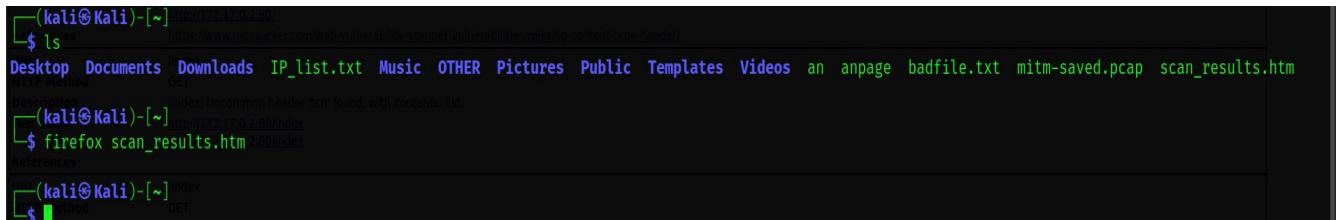


```
(kali㉿Kali)-[~] $ nikto -h 172.17.0.2 -o scan_results.htm
- Nikto v2.5.0
  An attacker can bypass the restrictions imposed by suidman's restricted shell, unshash, and execute arbitrary commands with the privileges of his own account.

+ Target IP: 172.17.0.2
+ Target Hostname: 172.17.0.2
+ Target Port: 80
+ Start Time: 2026-01-24 20:11:21 (GMT)
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ OS: Linux 4.15.0-163-generic #19-Ubuntu SMP Mon Aug 21 10:13:43 UTC 2017 x86_64
+ CPU Architecture: All architectures
+ 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 type. See: https://www.netsparker.com/web-vulnerability-s-sing-content-type-header/
+ /index: Uncommon header 'tcn' found, with contents: list.
+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found: index.php. See: http://www.wisec.it/sect
+ /index: Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross_Site_Tracing
+ /phpinfo.php: Output from the phpinfo() function was found.
+ /icons/: Directory indexing found.
+ /docs/: /docs/ directory is browsable. This may be /usr/doc. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0678
+ /etc/PHP80S/F24B-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-1218A
+ /etc/PHP9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-1218A
+ /etc/PHP9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-1218A
+ /etc/PHP9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. See: OSVDB-1218A
+ /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/changelog: Server may leak inodes via ETags, header found with file /phpMyAdmin/Changelog, inode: 1115138, size: 40540, mtime: Tue Dec 9 17:24:00 2008. See: http://cve.mitre.org/cgi-bin/cvename.
+ /phpMyAdmin/changelog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /test/: Directory index found.
+ /test/: This might be interesting.
+ /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /icons/: Directory indexing found.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpMyAdmin/: phpMyAdmin directory found.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ /httpd.conf.php#: /etc/httpd/conf.d/httpd.conf.php file found. This file contains the credentials.
+ 8910 requests: 0 error(s) and 27 items(s) reported on remote host
+ End Time: 2026-01-24 20:11:47 (GMT) (26 seconds)

+ 1 host(s) tested
A source code with a exploit which consumes this problem.
```

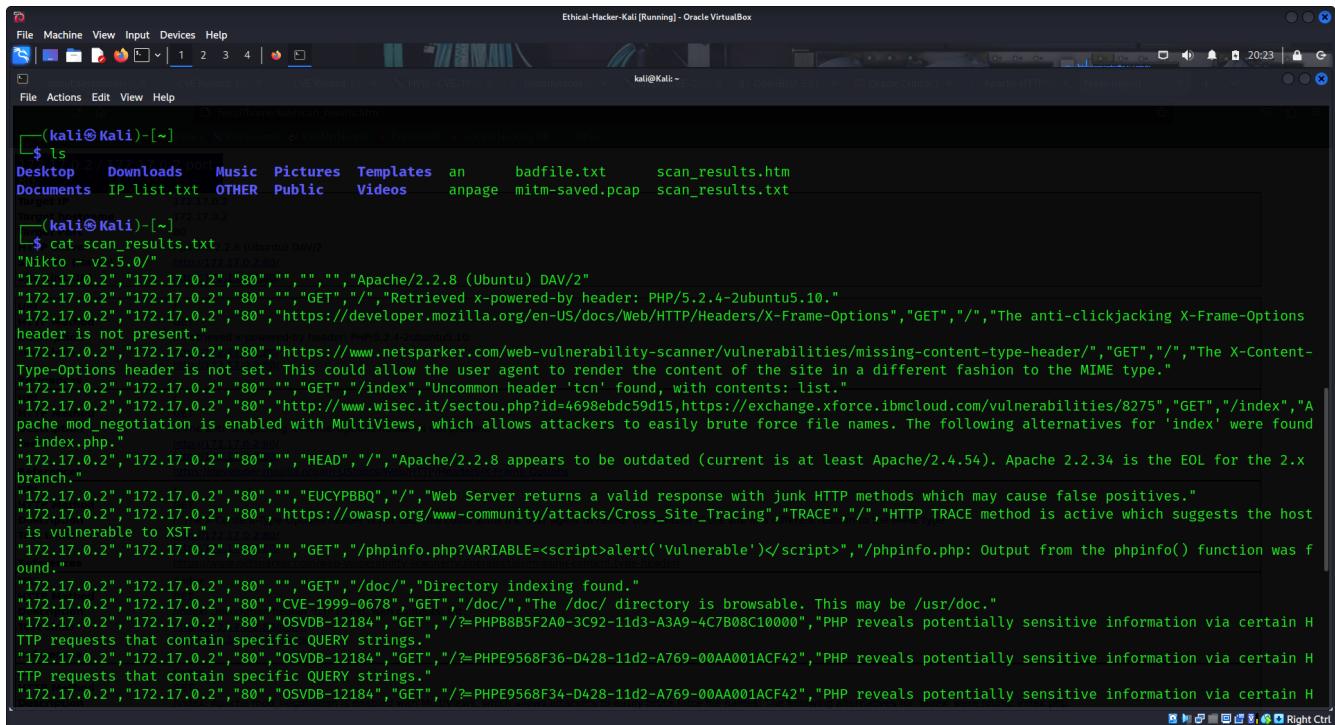
b. Locate the file in the /home/kali directory and open it in your browser to view the report format.



```
(kali㉿Kali)-[~] $ ls
Desktop Documents Downloads IP_list.txt Music OTHER Pictures Public Templates Videos an anpage badfile.txt mitm-saved.pcap scan_results.htm
HTTP Method GET
Description: index: Uncommon header 'tcn' found, with contents: list.
(kali㉿Kali)-[~] $ firefox scan_results.htm
HTTP Method GET
References
(kali㉿Kali)-[~] $
```

Firefox:





The screenshot shows a terminal window titled "Ethical-Hacker-Kali [Running] - Oracle VirtualBox". The terminal displays the output of a "ls" command, followed by the contents of a file named "scan\_results.txt". The file contains numerous lines of text, each representing a discovered vulnerability or configuration issue on a target host at "172.17.0.2". The text is color-coded in green and yellow for readability.

```
(kali㉿Kali)-[~]
$ ls
Desktop  Downloads  Music  Pictures  Templates  an      badfile.txt      scan_results.htm
Documents  IP_list.txt  OTHER  Public    Videos     anpage  mitm-saved.pcap  scan_results.txt

(kali㉿Kali)-[~]
└─$ cat scan_results.txt
"Nikto ~ v2.5.0/" 2016-07-29 00:00
"172.17.0.2","172.17.0.2","80","","","","Apache/2.2.8 (Ubuntu) DAV/2"
"172.17.0.2","172.17.0.2","80","","GET","/",Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10."
"172.17.0.2","172.17.0.2","80","https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options","GET","/",The anti-clickjacking X-Frame-Options header is not present."
"172.17.0.2","172.17.0.2","80","https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/","GET","/",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."
"172.17.0.2","172.17.0.2","80","","GET","/index","Uncommon header 'tcn' found, with contents: list."
"172.17.0.2","172.17.0.2","80","http://www.wisec.it/sectou.php?id=4698ebdc59d15,https://exchange.xforce.ibmcloud.com/vulnerabilities/8275","GET","/index",A
pache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for 'index' were found
: index.php."
"172.17.0.2","172.17.0.2","80","","HEAD","/",Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x
branch."
"172.17.0.2","172.17.0.2","80","","EUCYPBBQ","/",Web Server returns a valid response with junk HTTP methods which may cause false positives."
"172.17.0.2","172.17.0.2","80","https://owasp.org/www-community/attacks/Cross_Site_Tracing","TRACE","/",HTTP TRACE method is active which suggests the host
is vulnerable to XST."
"172.17.0.2","172.17.0.2","80","","GET","/phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>","/phpinfo.php: Output from the phpinfo() function was f
ound."
"172.17.0.2","172.17.0.2","80","","GET","/doc/","Directory indexing found."
"172.17.0.2","172.17.0.2","80","CVE-1999-0678","GET","/doc/","The /doc/ directory is browsable. This may be /usr/doc."
"172.17.0.2","172.17.0.2","80","OSVDB-12184","GET","/?=PHPE9568F36-D428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain H
TTP requests that contain specific QUERY strings."
"172.17.0.2","172.17.0.2","80","OSVDB-12184","GET","/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain H
TTP requests that contain specific QUERY strings."
"172.17.0.2","172.17.0.2","80","OSVDB-12184","GET","/?=PHPE9568F34-D428-11d2-A769-00AA001ACF42","PHP reveals potentially sensitive information via certain H
```

How does the saved file differ from the output shown on the screen? **In the saved file, each field is separated by a comma.**