CyberLawPioneers.org

Internal Web Application VAPT Report

Conducted By:

CyberLaw Pioneers Pvt. Ltd. / Yash Vardhan Dwivedi, Security Engineer

Document	*CLP VAPT Consolidated Report*
Prepared By	*Yash Vardhan Dwivedi*
Target	*https://cyberlawpioneers.org/#/home*
Report Content	*CLP Application Consolidated VAPT Report*
Classification	*Confidential*
Status	*VAPT Report*
Version	*V1*
Date	*08-04-2025*
Security Team	*CLP Security Team*

S.No	***Vulnerability***
1	*Deprecated TLS 1.1 Protocol Enabled*
2	*Weak Cipher Suites over TLS 1.1*
3	*Missing Security Headers*
4	*Insecure DNS – DNSSEC Not Enabled*
5	*Misconfigured SPF Records*
6	*Weak DMARC Policy*
7	*SMTP Command Enumeration & STARTTLS Disclosure*
8	*Mail Server Fingerprinting*
9	*OTP Bypass – Registration*
10	*OTP Bypass – Forgot Password*

1. Deprecated TLS 1.1 Enabled

Component	Details
Vulnerability Name	Deprecated TLS 1.1 Protocol Enabled
Description	The server supports the outdated TLS 1.1 protocol which is considered insecure and deprecated by major browsers and organizations. This exposes the server to various cryptographic attacks.
Severity	Medium
Mitigation	Disable support for TLS 1.0 and 1.1. Only support TLS 1.2 and TLS 1.3. Update server configuration accordingly.
CWE/CVE	CWE-326: Inadequate Encryption Strength
Steps to Reproduce	1. Use `nmap` or `openssl s_client -connect cyberlawpioneers.org:443 -tls1_1` to confirm support. 2. Observe the successful handshake.
PoC	`openssl s_client -connect cyberlawpioneers.org:443 -tls1_1` Successful connection confirms the protocol is enabled.

2. Weak Cipher Suites Over TLS 1.1

Component	Details
Vulnerability Name	Weak Cipher Suites over TLS 1.1
Description	The server supports weak cipher suites with TLS 1.1 that offer insufficient security, making the encrypted traffic susceptible to brute-force and downgrade attacks.
Severity	Low
Mitigation	Disable all weak ciphers in the server configuration and enforce strong cipher suites.
CWE/CVE	CWE-326: Inadequate Encryption Strength
Steps to Reproduce	1. Use SSL Labs or `nmap --script ssl-enum-ciphers -p 443 cyberlawpioneers.org` 2. Check listed ciphers under TLS 1.1
PoC	Nuclei log shows: `[weak-cipher-suites:tls-1.1] [ssl] [low] cyberlawpioneers.org:443 ["[tls11 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA]"]`

3. Missing Security Headers

Component	Details
Vulnerability Name	Missing Security Headers
Description	The website is missing multiple essential HTTP security headers which help protect against clickjacking, XSS, content sniffing, and data leakage.
Severity	Medium
Mitigation	Add the following headers to web server or application config: - `Strict-Transport-Security` - `Content-Security-Policy` - `Permissions-Policy` - `X-Content-Type-Options` - `X-Frame-Options` - `Referrer-Policy` - `Cross-Origin-Embedder-Policy` - `Cross-Origin-Opener-Policy` - `Cross-Origin-Resource-Policy`
CWE/CVE	CWE-693: Protection Mechanism Failure
Steps to Reproduce	1. Visit the site in browser. 2. Use browser dev tools → Network → Headers. 3. Observe absence of key headers.

PoC	From Nuclei:
	`[http-missing-security-headers:strict-transport-security]`
	`[http] [info] https://cyberlawpioneers.org/#/home`
	`...and multiple others`

4. Insecure DNS Configuration – Missing DNSSEC

Component	Details
Vulnerability Name	Insecure DNS – DNSSEC Not Enabled
Description	DNSSEC (Domain Name System Security Extensions) is not enabled, making DNS responses vulnerable to spoofing or man-in-the-middle attacks.
Severity	Low
Mitigation	Enable DNSSEC on the domain through your domain registrar or DNS provider.
CWE/CVE	CWE-345: Insufficient Verification of Data Authenticity
Steps to Reproduce	1. Use `dig +dnssec cyberlawpioneers.org` 2. Observe absence of `ad` (Authenticated Data) flag in response.
PoC	Nuclei shows: `[rdap-whois:secureDNS] [http] [info] ... ["false"]`

5. Misconfigured SPF Records

Component	Details
Vulnerability Name	Misconfigured SPF Records
Description	The domain has multiple SPF records (`"v=spf1"`), which is a violation of the SPF specification. This can lead to failures in email authentication, making the domain more susceptible to email spoofing.
Severity	Medium
Mitigation	Consolidate all SPF entries into a single record. Ensure only one valid `v=spf1` record exists. Test with SPF validation tools after updating DNS.
CWE/CVE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
Steps to Reproduce	1. Run `dig txt cyberlawpioneers.org` or use MXToolbox SPF lookup. 2. Note multiple `v=spf1` records in response.
PoC	`[spf-record-detect] [dns] [info] cyberlawpioneers.org ["v=spf1 include:webhostbox.net ~all", "v=spf1 a mx -all"]`

6. Weak DMARC Policy (p=quarantine)

Component	Details
Vulnerability Name	Weak DMARC Policy
Description	The DMARC policy for the domain is set to `quarantine`, which allows spoofed emails to reach spam folders. A `reject` policy provides stricter enforcement to prevent spoofing.
Severity	Low
Mitigation	Update the DMARC policy to `p=reject` once SPF and DKIM are fully configured and verified. Monitor reports to ensure deliverability.
CWE/CVE	CWE-285: Improper Authorization
Steps to Reproduce	1. Run `dig TXT _dmarc.cyberlawpioneers.org` 2. Observe policy is `p=quarantine`
PoC	`[dmarc-detect] [dns] [info] _dmarc.cyberlawpioneers.org ["v=DMARC1; p=quarantine; rua=mailto:admin@cyberlawpioneers.org"]`

7. SMTP Command Enumeration and STARTTLS Disclosure

Component	Details
Vulnerability Name	SMTP Command Enumeration & STARTTLS Disclosure
Description	The SMTP server exposes a variety of commands (`VRFY`, `ETRN`, `AUTH`) and allows STARTTLS. While STARTTLS is recommended, enumeration of SMTP capabilities can help attackers craft brute-force or social engineering attacks.
Severity	Medium
Mitigation	Disable unnecessary SMTP commands (`VRFY`, `ETRN`) via mail server configuration. Limit EHLO responses. Enable authentication and logging for abuse.
CWE/CVE	CWE-319: Cleartext Transmission of Sensitive Information
Steps to Reproduce	1. Connect to mail server using `telnet cyberlawpioneers.org 587`. 2. Type `EHLO test.com`. 3. Observe supported commands.
PoC	`[smtp-commands-enum:ehlo] [tcp] [info] cyberlawpioneers.org:587 ["PIPELINING", "SIZE 102400000", "ENHANCEDSTATUSCODES", "8BITMIME", "SMTPUTF8", "CHUNKING", "VRFY", "ETRN", "STARTTLS", "DSN"]`

8. Mail Server Fingerprinting via DNS

Component	Details
Vulnerability Name	Mail Server Fingerprinting
Description	The domain's mail server is publicly exposed and easily identifiable (`mail.cyberlawpioneers.org`). While not inherently a vulnerability, this increases the attack surface for spamming, spoofing, or direct attacks.
Severity	Low
Mitigation	Ensure proper hardening of the mail server (rate-limiting, brute-force protection, etc.). Avoid using predictable subdomains if possible. Monitor mail logs for abuse.
CWE/CVE	CWE-200: Information Exposure
Steps to Reproduce	1. Use `dig mx cyberlawpioneers.org`. 2. Observe record pointing to `mail.cyberlawpioneers.org`.
PoC	`[mx-fingerprint] [dns] [info] cyberlawpioneers.org ["10 mail.cyberlawpioneers.org."]`

9. OTP Bypass – Registration

Component	Details
Vulnerability Name	**OTP Bypass via Brute Force during Registration**
Description	**The OTP verification endpoint allows automated brute-force attempts without rate-limiting or account lockout. An attacker can rapidly test OTPs until the correct one is found, bypassing verification.**
Severity	**High**
CWE/CVE	**CWE-307: Improper Restriction of Excessive Authentication Attempts**
Steps to Reproduce	**1. Navigate to: https://cyberlawpioneers.org/#/register** **2. Trigger OTP generation** **3. Use a tool like Burp Suite Intruder to brute-force OTP values (as seen in the screenshot)** **4. When the response length changes (e.g., to 3964433), OTP is correct.**
PoC	**OTP Payload: 420207** **Response: "msg": "Data Matched" and success:true with user details**
Mitigation	**- Implement rate-limiting per IP or user** **- Lock account or invalidate OTP after few failed attempts** **- Add CAPTCHA after N attempts** **- Use OTP expiration logic**

10. OTP Bypass – Forgot Password

Component	Details
Vulnerability Name	**OTP Bypass via Brute Force during Forgot Password**
Description	**Similar to the registration flow, the OTP verification endpoint in the forgot password workflow is vulnerable to brute-force attacks, allowing attackers to reset passwords of arbitrary users.**
Severity	**High**
CWE/CVE	**CWE-640: Weak Password Recovery Mechanism for Forgotten Password**
Steps to Reproduce	**1. Navigate to: https://cyberlawpioneers.org/#/forget-password** **2. Enter known user info** **3. Use a brute-force tool to iterate OTPs** **4. Observe response changes on correct OTP (e.g., Data Matched)**
PoC	**OTP Payload: 287460** **Response contains matching email/mobile with success:true and Data Matched**
Mitigation	**- Enforce OTP retry limits** **- Invalidate OTP after incorrect attempts** **- Log and alert unusual activity** **- Strengthen OTP generation (longer, less predictable)**

3. Intruder attack of https://cyberlawpioneers.org

Results Positions

Capture filter: Capturing all items

View filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length
61	287460	200	43			396
0		200	43			296
1	287400	200	47			296
2	287401	200	49			296
3	287402	200	44			296
4	287403	200	44			296
5	287404	200	51			296
6	287405	200	52			296
7	287406	200	44			296

OTP

Request Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Server: nginx
Date: Tue, 15 Apr 2025 06:20:44 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 139
X-Powered-By: Express
Access-Control-Allow-Origin: *
Etag: W/"8b-GqEQYJTsoFLAluesX54Nt2UXIJ0"
Vary: Accept-Encoding

{"success":true,"data":[{"_id":"67f3f6aaeed33fc42648b1f7","email":"yashvardhan2810@gmail.com","mobile":"9975063337"}],"msg":"Data Matched"}
```

1 × +

Send Cancel

Request

Pretty Raw Hex

```
POST /auth/getOtpVerification HTTP/2
Host: cyberlawpioneers.org
Content-Length: 106
Sec-Ch-Ua-Platform: "Windows"
Authorization: Bearer
eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYXQi0jE3NDQ20Tc2MzcsImV4cCI6MTc0NzI40T
YzNywiYXVkIjoiNjdmM2Y2YWFlZWQzM2ZjNDI2NDhiMWY3IiwiaXNzIjoibG9jYWxob3N0In0.zZst-
xp7kGlhTRIJvUU_mnWsKovalJo4xd7CcRb2wfA
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="135", "Not-A.Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
Accept: application/json, text/plain, */*
Content-Type: application/json
Origin: https://cyberlawpioneers.org
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://cyberlawpioneers.org/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i

{
  "id":"67f3f6aaeed33fc42648b1f7",
  "email":"yashvardhan2810@gmail.com",
  "mobile":"9975063337",
  "otp":"287460"
}
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Server: nginx
Date: Tue, 15 Apr 2025 06:25:16 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 139
X-Powered-By: Express
Access-Control-Allow-Origin: *
Etag: W/"8b-GqEQYJTsoFLAluesX54Nt2UXIJ0"
Vary: Accept-Encoding

{
  "success":true,
  "data":[
    {
      "_id":"67f3f6aaeed33fc42648b1f7",
      "email":"yashvardhan2810@gmail.com",
      "mobile":"9975063337"
    }
  ],
  "msg":"Data Matched"
}
```

✔ Thank You

Thank you for reviewing this security assessment. The findings and recommendations outlined are intended to help improve the overall security posture of the platform. We appreciate your attention to these issues and welcome any questions or clarifications.

Contact Us

If you have any queries or require further assistance, feel free to reach out:

- **Email:** yashvardhan2810@gmail.com
- **Phone:** +91-9975063337