Reconnaissance Report

Target: upes.ac.in
Report Generated: 2025-11-08 13:09:35

Key Findings

Total Findings: 137

Endpoints (80)

Type	Severity	Value	Source
Directory	INFO	/html;	httpx, aquatone, sniper
URL	INFO	http://upes.ac.in	aquatone, whatweb
Directory	INFO	//upes.ac.in	aquatone, whatweb
Directory	INFO	/A	aquatone, sniper
Directory	INFO	/api-docs	api-discovery
Directory	INFO	/health	api-discovery
Directory	INFO	/openapi.json	api-discovery
Directory	INFO	/docs	api-discovery, feroxbuster
Directory	INFO	/clients	api-discovery
Directory	INFO	/auth	api-discovery
Directory	INFO	/swagger	api-discovery
Directory	INFO	/status	api-discovery
Directory	INFO	/oauth	api-discovery
Directory	INFO	/documentation	api-discovery
Directory	INFO	/webhook	api-discovery
Directory	INFO	/register	api-discovery
Directory	INFO	/client	api-discovery
Directory	INFO	/redoc	api-discovery
Directory	INFO	/swagger.json	api-discovery
Directory	INFO	/rest	api-discovery
Directory	INFO	/version	api-discovery

Directory	INFO	/graphql	api-discovery
Directory	INFO	/swagger-ui	api-discovery
Directory	INFO	/api	api-discovery, feroxbuster
Directory	INFO	/sdk	api-discovery
Directory	INFO	/api/v2	api-discovery
Directory	INFO	/callback	api-discovery
Directory	INFO	/login	api-discovery, feroxbuster
Directory	INFO	/developers	api-discovery
Directory	INFO	/ping	api-discovery
Directory	INFO	/api/v1	api-discovery
Directory	INFO	/help	api-discovery
Directory	INFO	/developer	api-discovery
Directory	INFO	/Hosting:	tech-profiling
Directory	INFO	/Framework:	tech-profiling
Directory	INFO	/admin.html	nikto
Directory	INFO	/phpmyadmin	nikto, feroxbuster
Directory	INFO	/wp-admin	nikto, feroxbuster
Directory	INFO	/admin.php	nikto
Directory	INFO	/administrator	nikto
Directory	INFO	/admin	nikto, feroxbuster
URL	INFO	https://www.facebook.com/upes.ac.in	social-intel
URL	INFO	https://www.reddit.com/r/upes.ac.in	social-intel
URL	INFO	https://twitter.com/upes.ac.in	social-intel
URL	INFO	https://www.instagram.com/upes.ac.in	social-intel
Directory	INFO	//www.instagram.com/upes.ac.in	social-intel
Directory	INFO	//twitter.com/upes.ac.in	social-intel
Directory	INFO	//www.reddit.com/r/upes.ac.in	social-intel
Directory	INFO	//www.facebook.com/upes.ac.in	social-intel
Directory	INFO	/Kolkata	geo-intel
Directory	INFO	/lib	feroxbuster
Directory	INFO	/dev	feroxbuster
Directory	INFO	/downloads	feroxbuster
Directory	INFO	/cache	feroxbuster
Directory	INFO	/bin	feroxbuster
Directory	INFO	/config	feroxbuster

Directory	INFO	/src	feroxbuster
Directory	INFO	/beta	feroxbuster
Directory	INFO	/archive	feroxbuster
Directory	INFO	/js	feroxbuster
Directory	INFO	/css	feroxbuster
Directory	INFO	/old	feroxbuster
Directory	INFO	/uploads	feroxbuster
Directory	INFO	/images	feroxbuster
Directory	INFO	/test	feroxbuster
Directory	INFO	/var	feroxbuster
Directory	INFO	/files	feroxbuster
Directory	INFO	/includes	feroxbuster
Directory	INFO	/stage	feroxbuster
Directory	INFO	/temp	feroxbuster
Directory	INFO	/logs	feroxbuster
Directory	INFO	/etc	feroxbuster
Directory	INFO	/backup	feroxbuster
Directory	INFO	/mobile	mobile-analysis
Directory	INFO	/app	mobile-analysis
Directory	INFO	/.well-known/apple-app-site-association	mobile-analysis
Directory	INFO	/.well-known/assetlinks.json	mobile-analysis
Directory	INFO	/mobile-app	mobile-analysis
Directory	INFO	/android	mobile-analysis
Directory	INFO	/ios	mobile-analysis

Network (11)

Type	Severity	Value	Source
Open Port	INFO	Port 2	api-discovery
Open Port	INFO	Port 1	api-discovery
Open Port	INFO	Port 80	sniper, naabu, masscan, nmap
Open Port	INFO	Port 443	sniper, naabu, masscan, nmap
Open Port	INFO	Port 8443	sniper, naabu
IP Address	INFO	4.186.33.78	sniper, geo-intel

Open Port	INFO	Port 00	ssl-analysis
Open Port	INFO	Port 59	ssl-analysis
DNS A Record	INFO	4.186.33.78	DNS
DNS MX Record	INFO	10 mx2.hc223-81.ap.iphmx.com.	DNS
DNS MX Record	INFO	5 mx1.hc223-81.ap.iphmx.com.	DNS

Vulnerabilities (2)

Type	Severity	Value	Source
Vulnerability	MEDIUM	web vulnerabilities found: backup file accessible: index.bak admin panel accessible: /admin admin panel access	hackertarget
Vulnerability	MEDIUM	vulnerabilities found: potential open redirect vulnerability robots.txt accessible	wapiti

Information (2)

Type	Severity	Value	Source
Email Address	INFO	international.admissions@upes.ac.in	theHarvester
Email Address	INFO	enrollments@upes.ac.in	theHarvester

Subdomains (42)

Type	Severity	Value	Source
Subdomain	INFO	upes.ac.in	CT Logs
Subdomain	INFO	apply.upes.ac.in www.apply.upes.ac.in	CT Logs
Subdomain	INFO	lms.upes.ac.in	CT Logs
Subdomain	INFO	myupes-beta.upes.ac.in	CT Logs
Subdomain	INFO	www.upes.ac.in	CT Logs
Subdomain	INFO	partners.upes.ac.in	CT Logs
Subdomain	INFO	admission.upes.ac.in	CT Logs
Subdomain	INFO	capig.upes.ac.in	CT Logs
Subdomain	INFO	helpdesk.delhi.upes.ac.in	CT Logs
Subdomain	INFO	*.upes.ac.in upes.ac.in	CT Logs

Subdomain	INFO	survey.delhi.upes.ac.in	CT Logs
Subdomain	INFO	image.team.upes.ac.in	CT Logs
Subdomain	INFO	www.vf.upes.ac.in	CT Logs
Subdomain	INFO	online.upes.ac.in	CT Logs
Subdomain	INFO	www.uat.upes.ac.in	CT Logs
Subdomain	INFO	dr.ddn.upes.ac.in	CT Logs
Subdomain	INFO	*.ddn.upes.ac.in ddn.upes.ac.in	CT Logs
Subdomain	INFO	*.cce.upes.ac.in cce.upes.ac.in	CT Logs
Subdomain	INFO	learn.cce.upes.ac.in learn.phd.upes.ac.in learn.upes.ac.in	CT Logs
Subdomain	INFO	alumni.upes.ac.in	CT Logs
Subdomain	INFO	uat.upes.ac.in www.uat.upes.ac.in	CT Logs
Subdomain	INFO	click.team.upes.ac.in	CT Logs
Subdomain	INFO	cloud.team.upes.ac.in	CT Logs
Subdomain	INFO	view.team.upes.ac.in	CT Logs
Subdomain	INFO	*.delhi.upes.ac.in delhi.upes.ac.in	CT Logs
Subdomain	INFO	blog.cce.upes.ac.in	CT Logs
Subdomain	INFO	cce.upes.ac.in www.cce.upes.ac.in	CT Logs
Subdomain	INFO	cpanel.uat.upes.ac.in cpcalendars.uat.upes.ac.in cpcontacts.uat.upes.ac.in mail.uat.upes.ac.in uat.upes.ac.in webdisk.uat.upes.ac.in webmail.uat.upes.ac.in www.uat.upes.ac.in	CT Logs
Subdomain	INFO	sappro.delhi.upes.ac.in	CT Logs
Subdomain	INFO	sapep.delhi.upes.ac.in	CT Logs
Subdomain	INFO	learn.cce.upes.ac.in learn.upes.ac.in	CT Logs
Subdomain	INFO	cpanel.uat.upes.ac.in mail.uat.upes.ac.in uat.upes.ac.in webdisk.uat.upes.ac.in webmail.uat.upes.ac.in www.uat.upes.ac.in	CT Logs

Subdomain	INFO	sapep.delhi.upes.ac.in www.sapep.delhi.upes.ac.in	CT Logs
Subdomain	INFO	sappro.delhi.upes.ac.in www.sappro.delhi.upes.ac.in	CT Logs
Subdomain	INFO	upes-hd.ddn.upes.ac.in	CT Logs
Subdomain	INFO	learn.upes.ac.in	CT Logs
Subdomain	INFO	maildel.upes.ac.in upes.ac.in upesmail.ddn.upes.ac.in www.maildel.upes.ac.in	CT Logs
Subdomain	INFO	lms.ddn.upes.ac.in	CT Logs
Subdomain	INFO	academics.ddn.upes.ac.in	CT Logs
Subdomain	INFO	academics.ddn.upes.ac.in admission.upes.ac.in intranet.ddn.upes.ac.in mailddn.ddn.upes.ac.in maildel.upes.ac.in www.maildel.upes.ac.in	CT Logs
Subdomain	INFO	academics.ddn.upes.ac.in intranet.ddn.upes.ac.in mailddn.ddn.upes.ac.in maildel.upes.ac.in upes.ac.in www.maildel.upes.ac.in	CT Logs
Subdomain	INFO	academics.ddn.upes.ac.in mailddn.ddn.upes.ac.in maildel.upes.ac.in upes.ac.in www.maildel.upes.ac.in	CT Logs

Passive Reconnaissance

DNS Records

{'AAAA_error': 'The DNS response does not contain an answer to the question: upes.ac.in. IN AAAA', 'MX': ['10 mx2.hc223-81.ap.iphmx.com.', '5 mx1.hc223-81.ap.iphmx.com.'], 'A': ['4.186.33.78'], 'NS': ['ns-1394.awsdns-46.org.', 'ns-1590.awsdns-06.co.uk.', 'ns-67.awsdns-08.com.', 'ns-684.awsdns-21.net.'], 'TXT_error': 'The resolution lifetime expired after 5.001 seconds: Server Do53:172.20.10.1@53 answered The DNS operation timed out.; Server Do53:192.168.1.1@53 answered ; Server Do53:192.168.1.1@53 answered The DNS operation timed out.; Server Do53:172.20.10.1@53 answered The DNS operation timed out.'}

WHOIS Information

{'error': '[Errno 11001] getaddrinfo failed'}

SSL Information

{'subject': [[['commonName', '*.upes.ac.in']]], 'issuer': [[['countryName', 'GB']], [['organizationName', 'Sectigo Limited']], [['commonName', 'Sectigo Public Server Authentication CA DV R36']]], 'notAfter': 'Aug 9 23:59:59 2026 GMT'}

Tool Outputs

subfinder - OK

```
Found subdomains: www.upes.ac.in mail.upes.ac.in ftp.upes.ac.in blog.upes.ac.in
dev.upes.ac.in test.upes.ac.in beta.upes.ac.in img.upes.ac.in app.upes.ac.in
```

httpx - OK

```
HTTP Probe Results: Status: 200 Content-Type: text/html; charset=utf-8 Content-Length:
145767 Server: Title: UPES: Ranked #1 in Academic Reputation
```

cloud-detect - OK

```
No obvious cloud infrastructure detected
```

wafw00f - OK

```
WAF detected: Joomla
```

aquatone - OK

```
URL: http://upes.ac.in Status: 200 Content-Type: text/html; charset=utf-8
Content-Length: 145767 Server: N/A Title: UPES: Ranked #1 in Academic Reputation Links
found: 185 Images found: 54 Forms found: 4 JavaScript detected iFrames detected
```

api-discovery - OK

```
API Endpoints Discovered: /api (301) /api/v1 (301) /api/v2 (301) /rest (301) /graphql
(301) /swagger (301) /docs (301) /openapi.json (301) /swagger.json (301) /api-docs
(301) /developer (301) /developers (301) /sdk (301) /client (301) /clients (301) /oauth
(301) /auth (301) /login (301) /register (301) /webhook (301) /callback (301) /status
(301) /health (301) /ping (301) /version (301) Documentation: /swagger-ui (301)
Documentation: /redoc (301) Documentation: /api-docs (301) Documentation:
/documentation (301) Documentation: /help (301)
```

sublist3r - OK

```
Found subdomains: mail.upes.ac.in ftp.upes.ac.in blog.upes.ac.in test.upes.ac.in
app.upes.ac.in m.upes.ac.in dashboard.upes.ac.in stats.upes.ac.in old.upes.ac.in
vpn.upes.ac.in
```

sniper - OK

=== SNIPER SCAN RESULTS FOR upes.ac.in === Open ports: 80 (http), 443 (https), 8443 (unknown) Web server: 200 Server: N/A Content-Type: text/html; charset=utf-8 Error messages found DNS A records: 4.186.33.78

js-analysis - OK

JavaScript Analysis: JavaScript files found: 12 Inline JavaScript blocks: 31 External JavaScript libraries: 2

tech-profiling - OK

Technology Stack Profile: Language/Framework: PHP Language/Framework: Node.js Language/Framework: Java Language/Framework: Go Frontend: Bootstrap Frontend: jQuery Frontend: Angular Frontend: Vue.js Database: Oracle Cloud/Hosting: AWS Cloud/Hosting: Azure Cloud/Hosting: Google Cloud Cloud/Hosting: DigitalOcean Analytics: Google Analytics Analytics: Google Tag Manager Analytics: Facebook Pixel

nikto - OK

Web vulnerabilities found: Backup file accessible: index.bak Admin panel accessible: /admin Admin panel accessible: /administrator Admin panel accessible: /admin.php Admin panel accessible: /admin.html Admin panel accessible: /wp-admin Admin panel accessible: /phpmyadmin

naabu - OK

Open ports found: 80 (http) 443 (https) 8443 (unknown)

social-intel - OK

Social Media Profiles Found: Facebook: https://www.facebook.com/upes.ac.in Twitter: https://twitter.com/upes.ac.in Instagram: https://www.instagram.com/upes.ac.in Reddit: https://www.reddit.com/r/upes.ac.in

ssl-analysis - OK

SSL Certificate Analysis for upes.ac.in: Subject: *.upes.ac.in Issuer: Sectigo Public Server Authentication CA DV R36 Valid From: Jul 9 00:00:00 2025 GMT Valid Until: Aug 9 23:59:59 2026 GMT Days Remaining: 274 Security Issues: None detected

gobuster-dns - OK

DNS brute force results: www.upes.ac.in mail.upes.ac.in ftp.upes.ac.in blog.upes.ac.in dev.upes.ac.in test.upes.ac.in beta.upes.ac.in img.upes.ac.in app.upes.ac.in m.upes.ac.in dashboard.upes.ac.in old.upes.ac.in

masscan - OK

Open ports found (1-1024): 80 (http) 443 (https)

theHarvester - OK

Harvested information: Email found: enrollments@upes.ac.in Subdomain found: admission.upes.ac.in Email found: international.admissions@upes.ac.in Subdomain found: www.upes.ac.in Subdomain found: refund.upes.ac.in

nmap - OK

Open ports found: 80 (http) 443 (https)

dnsx - OK

DNS Records found: MX: 10 mx2.hc223-81.ap.iphmx.com., 5 mx1.hc223-81.ap.iphmx.com. SOA: ns-67.awsdns-08.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400

email-security - OK

Email Security Analysis: No SPF record found No DKIM record found No DMARC record found MX Records: mx2.hc223-81.ap.iphmx.com. (Priority: 10), mx1.hc223-81.ap.iphmx.com. (Priority: 5)

nuclei - OK

Vulnerabilities found: Potential open redirect vulnerability Robots.txt accessible

ffuf-vhost - OK

Virtual hosts found: www.upes.ac.in (301)

geo-intel - OK

Geolocation Intelligence: IP Address: 4.186.33.78 Country: India Region: Maharashtra City: Pune ISP: Microsoft Corporation Organization: Microsoft Azure Cloud (centralindia) Timezone: Asia/Kolkata

feroxbuster - OK

Found directories: / (301) /admin (301) /login (301) /wp-admin (301) /phpmyadmin (301) /config (301) /backup (301) /api (301) /docs (301) /test (301) /dev (301) /stage (301) /beta (301) /old (301) /archive (301) /files (301) /images (301) /css (301) /js (301)

/uploads (301) /downloads (301) /temp (301) /cache (301) /logs (301) /includes (301) /lib (301) /src (301) /bin (301) /etc (301) /var (301)

amass - OK

Found subdomains: www.upes.ac.in mail.upes.ac.in ftp.upes.ac.in blog.upes.ac.in dev.upes.ac.in test.upes.ac.in beta.upes.ac.in img.upes.ac.in app.upes.ac.in m.upes.ac.in dashboard.upes.ac.in stats.upes.ac.in old.upes.ac.in

whatweb - OK

Target: http://upes.ac.in Status: 200 Technologies: Bootstrap, jQuery, Drupal, Google Analytics, Facebook Pixel

mobile-analysis - OK

Mobile App Analysis: Mobile app path: /.well-known/apple-app-site-association (301) Mobile app path: /.well-known/assetlinks.json (301) Mobile app path: /mobile (301) Mobile app path: /app (301) Mobile app path: /android (301) Mobile app path: /ios (301) Mobile app path: /mobile-app (301) Mobile indicator: viewport

builtin-tcp - OK

Open ports: 80, 443, 8443