Footprinting Report – REVA University (www.reva.edu.in)

Author: Yuvraj mahilange
Date: 2025-10-11
Engagement Type: Passive Footprinting (Open-Source Intelligence)
Scope & Authorization:

- Target domain: `www.reva.edu.in` and related subdomains discovered through passive reconnaissance.
- Tools used: crt.sh, VirusTotal, urlscan.io, Censys, SecurityHeaders.io, BuiltWith, Wayback Machine.
- Testing type: Passive only – no intrusive scanning, exploitation, or login attempts performed.

🧩 Executive Summary

The passive footprinting process for REVA University's main website revealed a well-configured system served through Amazon CloudFront and Cloudflare CDNs. The site has a strong HTTP security header posture (Grade **A** on SecurityHeaders.io), though it lacks a **Content-Security-Policy (CSP)** header. Several subdomains and third-party services were identified, including REVA's LMS, Salesforce portals, AWS S3 storage, Google analytics, and UserWay accessibility widget.

Additionally, a Censys record associated with IP `13.203.182.119` was found, showing a host on AWS India (AS16509) running **nginx/1.29.1** and **Next.js**, with SSH access enabled. This is marked as *informational* pending internal verification by REVA IT.

High-Level Findings Summary

Category	Description	Severity
HTTP Security Headers	Good (A grade) but missing CSP	Medium
Subdomains & Integrations	Multiple third-party integrations discovered	Informational

Category	Description	Severity
Host Fingerprint	nginx + Next.js server on AWS (13.203.182.119)	Informational
Server Version Disclosure	Apache/2.4.65 and nginx version exposed	Low

Risk Posture

Overall posture: **Low-to-Medium Risk** – mostly due to missing CSP and visible software versions.

🧭 Methodology

1. **crt.sh** – Checked for issued certificates and subdomains (no new entries found).
2. **VirusTotal** – Parsed URLs and scripts loaded by the main site; enumerated third-party dependencies.
3. **urlscan.io** – Retrieved resource map, IPs, and ASN data for loaded assets.
4. **Censys** – Queried host and certificate data; extracted one relevant host (13.203.182.119).
5. **SecurityHeaders.io** – Analyzed HTTP response headers for security configuration.
6. **BuiltWith** – Identified technology stack, frameworks, and analytics integrations.
7. **Wayback Machine** – Checked for historical snapshots (no sensitive legacy data found).

🗂️ Asset Inventory

Below is an expanded asset inventory compiled from the `reva_site_scan.md` and the uploaded XLSX export. (I copied the hostnames, URLs, IPs and ASNs you captured into this report.)

Hostname / URL	IP Address (observed)	Provider / ASN	Purpose	Notes / Evidence
`www.reva.edu.in`	18.66.171.114	Amazon CloudFront (AS16509)	Main website (HTTPS)	Evidence: SecurityHeaders.io report; urlscan summary. □filecite□turn1file12□turn1file5□
`files.reva.ac.in`	104.21.x.x (Cloudflare ranges)	Cloudflare (AS13335)	Static file CDN	Evidence: VirusTotal / urlscan resource list. □filecite□turn1file2□turn1file1□
`lms.reva.edu.in`	(not resolved in passive data)	(LMS provider)	Learning Management System (login)	Evidence: URL found in VirusTotal export: `https://lms.reva.edu.in/login/index.php`. □filecite□turn1file2□
`reva-university.lightning.force.com`	(Salesforce)	Salesforce Cloud	CRM / external portal	Evidence: VirusTotal / BuiltWith entries show Salesforce portals. □filecite□turn1file2□turn1file16□
`revaeduin.s3.ap-south-1.amazonaws.com`	S3 (ap-south-1)	Amazon S3 (AWS AS16509)	Public storage bucket	Evidence: VirusTotal URL list and urlscan resources. □filecite□turn1file2□turn1file5□
`13.203.182.119`	13.203.182.119	Amazon (AS16509)	EC2 host serving Next.js / nginx	Evidence: Censys host record (SSH + nginx + Next.js). □filecite□turn1file0□turn1file14□
`cdn / third-party hosts`	various	Google (AS15169), Cloudflare (AS13335), Amazon (AS16509)	Fonts, analytics, CDNs, widgets	Examples: `fonts.googleapis.com`, `cdnjs.cloudflare.com`, `unpkg.com`, `cdnjs.cloudflare.com` (see VirusTotal/urlscan). □filecite□turn1file2□turn1file1□

Collected Data (raw snippets from your scan files)

Title / Meta Evidence (from VirusTotal export):

```
Title: Top Private University in Bangalore, Karnataka | REVA University
```

Source: `reva_site_scan.md`. □filecite□turn1file6□

Security headers summary (from SecurityHeaders.io):

```
SecurityHeaders.io Grade: A – HSTS present (max-age=63072000; includeSubDomains; preload). Missing: Content-
Security-Policy.
```

Source: `reva_site_scan.md` SecurityHeaders export. □filecite□turn1file12□

Censys host banner (raw snippet):

```
Censys record for 13.203.182.119 – SSH banner: "SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.11"; HTTP Server:
"nginx/1.29.1"; X-Powered-By: "Next.js". Observed at 2025-10-10T19:34:06Z; ASN: AMAZON-02 (India region).
```

Source: `reva_site_scan.md` (Censys export). □filecite□turn1file0□

Representative URLs found (append to Appendix B):

- `https://files.reva.ac.in/assets/frontend/images/COMMON%20BROCHURE_FINAL_2021_AV1_web.pdf`
- `https://lms.reva.edu.in/login/index.php`
- `https://reva-university.lightning.force.com/lightning/page/home`
- `https://revaeduin.s3.ap-south-1.amazonaws.com`
  Source: VirusTotal / urlscan exports. □filecite□turn1file2□turn1file5□

Tech / Third-party list (from BuiltWith / urlscan):

- Cloudflare (CDN)
- Amazon CloudFront (CDN / Hosting)
- Google Fonts & Google Analytics / Tag Manager
- Salesforce portals (lightning.force.com)
- Yellow Messenger (chat)
- UserWay (accessibility widget)
  Source: BuiltWith and urlscan summaries. □filecite□turn1file16□turn1file5□

🧱 Technical Findings

Finding #1 – Missing Content Security Policy (CSP)

- **Severity:** Medium
- **Description:** The SecurityHeaders.io report for `https://www.reva.edu.in` shows a missing Content-Security-Policy header, though other headers are configured properly.
- **Evidence (copy-paste):**

  > SecurityHeaders.io Grade: A — HSTS present (max-age=63072000; includeSubDomains; preload). Missing: Content-Security-Policy.

- **Impact:** Absence of a CSP increases exposure to cross-site scripting (XSS) and injection-based attacks.
- **Recommendation:** Implement a restrictive Content-Security-Policy, e.g.:

```
Content-Security-Policy: default-src 'self'; img-src 'self' https: data:; script-src 'self' 'unsafe-inline'
https://trusted.cdn.com;
```

Finding #2 – Server Version Disclosure

- **Severity:** Low
- **Description:** Server response headers expose software versions.
  - Apache/2.4.65 (Amazon Linux)
  - nginx/1.29.1 (AWS EC2 host)
- **Evidence (copy-paste):**

> `Server: Apache/2.4.65 (Amazon Linux)`
> `Server: nginx/1.29.1`

- **Impact:** Attackers can tailor exploits for known vulnerabilities in these versions.
- **Recommendation:** Mask or remove version strings in headers (`ServerTokens Prod` and `ServerSignature Off` for Apache).

Finding #3 – Third-Party Dependencies & Subdomains

- **Severity:** Informational
- **Description:** Multiple third-party services and subdomains were identified.
- **Evidence (copy-paste):**

> Detected vendors/resources: Cloudflare (CDN), Amazon CloudFront (hosting), Google Fonts, Google Analytics/Tag Manager, Salesforce portals (reva-university.lightning.force.com), S3 bucket (revaeduin.s3.ap-south-1.amazonaws.com), Yellow Messenger (live chat), UserWay (accessibility).

- **Impact:** Third-party dependencies can introduce external risks if not regularly audited.
- **Recommendation:** Review and inventory all third-party integrations, ensure updated configurations and least-privilege API usage.

Finding #4 – Host Fingerprint (AWS India)

- **Severity:** Informational
- **Description:** Censys identified IP `13.203.182.119` associated with REVA web assets.
- **Evidence (copy-paste):**

> Censys record for 13.203.182.119 — SSH banner: "SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.11"; HTTP Server: "nginx/1.29.1"; X-Powered-By: "Next.js". Observed at 2025-10-10T19:34:06Z; ASN: AMAZON-02 (India region).

- **Impact:** Existence of SSH and a web service confirms active infrastructure; configuration and access control should be validated internally.
- **Recommendation:** Restrict SSH to trusted IPs; monitor and patch nginx/Next.js host; confirm this instance belongs to REVA.

🧰 Recommendations Summary

Area	Recommendation	Priority
Security Headers	Add CSP header	Medium
Server Hardening	Hide version info in headers	Low
Third-Party Integrations	Periodic review of external dependencies	Medium
Host Management	Verify & secure AWS EC2 host (13.203.182.119)	Medium
Cookies & Flags	Ensure Secure and SameSite flags on cookies	Low

---

📎 Appendices

- **Appendix A:** crt.sh search output (no results)
- **Appendix B:** VirusTotal URL/resource list
  - Example URLs:
    - https://files.reva.ac.in/assets/frontend/images/COMMON%20BROCHURE_FINAL_2021_AV1_web.pdf
    - https://lms.reva.edu.in/login/index.php
    - https://reva-university.lightning.force.com/lightning/page/home
    - https://revaeduin.s3.ap-south-1.amazonaws.com
- **Appendix C:** urlscan.io IP/ASN list
- **Appendix D:** SecurityHeaders.io report screenshot (Grade A)
- **Appendix E:** Censys host record JSON (13.203.182.119)
- **Appendix F:** BuiltWith technology summary

Ethical Note:
All information was obtained from publicly available sources for educational and authorized research purposes only. No intrusive or exploitative testing was performed.

End of Report