# Security Scan Report for http://skit.ac.in

## Scan Summary

Total Time: 22.54 seconds

## Subdomains Found

- www.skit.ac.in

- mail.skit.ac.in

## Hidden Content

Path: /robots.txt (Status Code: 200)

Preview: User-agent: * Disallow: Sitemap: https://www.skit.ac.in/index.php?option=com_schuweb_sitemap&view=xml&tmpl=component&id=1

Path: /sitemap.xml (Status Code: 200)

Preview: <!DOCTYPE html> <html xmlns="//www.w3.org/1999/xhtml" xml:lang="en-gb" lang="en-gb" > <head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <meta name="viewport" content="width=dev

## Security Headers Analysis

### *Detected Headers:*

Date: Thu, 12 Dec 2024 09:40:15 GMT

Content-Type: text/html; charset=utf-8

Transfer-Encoding: chunked

Connection: keep-alive

P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM"

Vary: Accept-Encoding,User-Agent

Expires: Wed, 17 Aug 2005 00:00:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

Pragma: no-cache

Set-Cookie: 23a4061cb5a30e2f39c765d2fa920db7=8e7b1db66cfdad3b8891653b408c6815; path=/; secure; HttpOnly

X-Content-Type-Options: nosniff

Last-Modified: Thu, 12 Dec 2024 09:40:15 GMT

X-XSS-Protection: 1; mode=block

CF-Cache-Status: DYNAMIC

Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=smzJevdQhJMQ5NGg0unkMakUgWtTsS3B%2F9b2SXjES%2BLz%2F1IBNLPYNNVQbDC2woZLLylS1aXTb76OC%2Bb4Yv87jeBGGzcY2LSLrq023yEhYW7BwIJoB4d0ha5F5wDBFg6CHg%3D%3D"}],"group":"cf-nel","max_age":604800}

NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}

Server: cloudflare

CF-RAY: 8f0cc077d815631f-LHR

Content-Encoding: gzip

alt-svc: h3=":443"; ma=86400

server-timing: cfL4;desc="?proto=TCP&rtt;=175024&min;_rtt=168289&rtt;_var=76580&sent;=4&recv;=6&lost;=0&retrans;=0&sent;_bytes=2836&recv;_bytes=764&delivery;_rate=13142&cwnd;=138&unsent;_bytes=0&cid;=afd6c9ab6162a351&ts;=851&x;=0"

### *Recommendations:*

- Enable HSTS: Protects against protocol downgrade attacks and cookie hijacking.

- Add Content Security Policy: Mitigates cross-site scripting (XSS) and data injection attacks.

## SQL Injection Vulnerabilities

## Discovered API Endpoints

## Custom Test Case Results

Test: Test admin login

Endpoint: /admin

Status Code: 200

Response Preview: <!DOCTYPE html> <html xmlns="//www.w3.org/1999/xhtml" xml:lang="en-gb" lang="en-gb" > <head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"> <meta name="viewport" content="width=dev