DOCUMENTATION ON CYBER SECURITY

REPORT ON PROJECT

BY
NIMMALAPUDI SREE SUNANDA
NALLAMALLI VIKAS REDDY
TANKALA VIKAS
TADI SUBHASH SAI SANDEEP REDDY

DAY -1

Bug Bounty

Task -1

Step -1

hackerone. Com

Step -2

Domain name exploring

Step -3

I choose mux.com

Domain name

Step -4

osint frame work

in another tab

Step -5

Domain name - whois records - whois

Step -6

Whois redirects to new tab

Step -7

Paste the domain name

mux.com

Step -8

I got some information of that site

Domain Name: mux.com

Registry Domain ID: 2368218_DOMAIN_COM-VRSN

Registrar WHOIS Server: whois.godaddy.com

Registrar URL: https://www.godaddy.com

Updated Date: 2023-04-17T09:03:18Z

Creation Date: 1998-04-17T23:00:00Z

Registrar Registration Expiration Date: 2024-04-16T23:00:00Z

Registrar: GoDaddy.com, LLC

Registrar IANA ID: 146

Registrar Abuse Contact Email: email@godaddy.com

Registrar Abuse Contact Phone: +1.4806242505

Domain Status: clientTransferProhibited
https://icann.org/epp#clientTransferProhibited

Domain Status: clientUpdateProhibited
https://icann.org/epp#clientUpdateProhibited

Domain Status: clientRenewProhibited
https://icann.org/epp#clientRenewProhibited

Domain Status: clientDeleteProhibited
https://icann.org/epp#clientDeleteProhibited

Registry Registrant ID: Not Available From Registry

Registrant Name: Registration Private

Registrant Organization: Domains By Proxy, LLC

Registrant Street: DomainsByProxy.com

Registrant Street: 2155 E Warner Rd

Registrant City: Tempe

Registrant State/Province: Arizona

Registrant Postal Code: 85284

Registrant Country: US

Registrant Phone: +1.4806242599

Registrant Phone Ext:

Registrant Fax: +1.4806242598

Registrant Fax Ext:

Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=mux.com

Registry Admin ID: Not Available From Registry

Admin Name: Registration Private

Admin Organization: Domains By Proxy, LLC

Admin Street: DomainsByProxy.com

Admin Street: 2155 E Warner Rd

Admin City: Tempe

Admin State/Province: Arizona

Admin Postal Code: 85284

Admin Country: US

Admin Phone: +1.4806242599

Admin Phone Ext:

Admin Fax: +1.4806242598

Admin Fax Ext:

Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=mux.com

Registry Tech ID: Not Available From Registry

Tech Name: Registration Private

Tech Organization: Domains By Proxy, LLC

Tech Street: DomainsByProxy.com

Tech Street: 2155 E Warner Rd

Tech City: Tempe

Tech State/Province: Arizona

Tech Postal Code: 85284

Tech Country: US

Tech Phone: +1.4806242599

Tech Phone Ext:

Tech Fax: +1.4806242598

Tech Fax Ext:

Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=mux.com

Name Server: NS-1600.AWSDNS-08.CO.UK

Name Server: NS-1247.AWSDNS-27.ORG

Name Server: NS-132.AWSDNS-16.COM

Name Server: NS-808.AWSDNS-37.NET

DNSSEC: unsigned

URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

>>> Last update of WHOIS database: 2023-06-23T18:10:48Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Day-1

Task -2

Finding vulnerable sites

Step -1

Securitytrails. Com

Step -2

Some sites will be shown

In contents

Step -3

Vulnerable sites

CTFlearn

bWAPP

Google Gruyere

Hellbound Hackers

OWASP Multilidae ||

HackThis!!

DAY -2

Foot printing and reconnaissance

```
[recon-ng][default] > db insert domains
domain (TEXT): https://mux.com
notes (TEXT): for learning purpose
[*] 1 rows affected.
[recon-ng][default] > show domains
+                                                  -   -                +
| rowid |       domain             |           notes           |    module      |
+                                                  -   -                +
|   1      | https://mux.com      | for learning purpose | user_defined |
+                                                  -   -                  +
[*] 1 rows returned
[recon-ng][default] > modules help
Interfaces with installed modules


Usage: modules <load|reload|search> [...]


[recon-ng][default] > modules search hack
[*] Searching installed modules for 'hack'...


  Recon
```

recon/domains-hosts/hackertarget

[recon-ng][default] > modules load recon/domains-hosts/hackertarget

[recon-ng][default][hackertarget] > options set SOURCE mux.com

SOURCE => mux.com

[recon-ng][default][hackertarget] > run

MUX.COM

[*] Country: None

[*] Host: mux.com

[*] Ip_Address: 76.76.21.21

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-east-1-dop1.mux.com

[*] Ip_Address: 34.225.13.238

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: auth.aws-us-east-1-dop1.mux.com

[*] Ip_Address: 54.237.187.223

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-east-1-dos1.mux.com

[*] Ip_Address: 3.215.41.143

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: auth.aws-us-east-1-dos1.mux.com

[*] Ip_Address: 34.228.172.221

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: admin-qa.mux.com

[*] Ip_Address: 184.72.214.149

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: static.mux.com

[*] Ip_Address: 18.160.41.128

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: o1.sendgrid.mux.com

[*] Ip_Address: 168.245.48.185

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: dashboard.mux.com

[*] Ip_Address: 108.138.64.58

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: legacy-live.mux.com

[*] Ip_Address: 34.160.204.215

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: us-east1.gcp.live.mux.com

[*] Ip_Address: 34.138.128.221

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: us-west1.gcp.live.mux.com

[*] Ip_Address: 35.230.19.118

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: europe-west4.gcp.live.mux.com

[*] Ip_Address: 34.91.174.38

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: dashboard-staging.mux.com

[*] Ip_Address: 65.8.158.48

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: live-staging.mux.com

[*] Ip_Address: 35.235.125.238

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: global-live-staging.mux.com

[*] Ip_Address: 34.95.103.84

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: us-west2.gcp.live-staging.mux.com

[*] Ip_Address: 35.235.125.238

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: admin-staging.mux.com

[*] Ip_Address: 52.203.95.190

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*] -

[*] Country: None

[*] Host: gcp-us-west1-vos1.staging.mux.com

[*] Ip_Address: 34.145.105.68

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gce-us-west1.staging.mux.com

[*] Ip_Address: 35.230.73.183

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: buildkite.gce-us-west1.staging.mux.com

[*] Ip_Address: 35.230.73.183

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: chunk.gce-us-west1.staging.mux.com

[*] Ip_Address: 34.145.105.68

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: chunked-transfer-demo.gce-us-west1.staging.mux.com

[*] Ip_Address: 35.230.73.183

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: debugger.gce-us-west1.staging.mux.com

[*] Ip_Address: 35.230.73.183

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: mediarouter.gce-us-west1.staging.mux.com

[*] Ip_Address: 35.230.73.183

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: asset.gce-us-west1.staging.mux.com

[*] Ip_Address: 35.230.73.183

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*] -

[*] Country: None

[*] Host: vault.gce-us-west1.staging.mux.com

[*] Ip_Address: 35.230.73.183

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: manifest.gce-us-west1.staging.mux.com

[*] Ip_Address: 34.145.105.68

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: api.staging.mux.com

[*] Ip_Address: 34.237.87.177

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: retool.staging.mux.com

[*] Ip_Address: 35.170.153.40

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: api.mux.com

[*] Ip_Address: 52.22.14.139

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: test-api.mux.com

[*] Ip_Address: 52.71.16.114

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: admin.mux.com

[*] Ip_Address: 54.85.215.119

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-eu-central-1-dop1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-east-1-dop1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-eu-central-1-rop1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-east-1-rop1.production.mux.com

[*] Ip_Address: 35.199.6.175

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-west-2-rop1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-east-1-top1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gcp-us-east1-vop1.production.mux.com

[*] Ip_Address: 34.148.121.217

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gcp-us-east4-vop1.production.mux.com

[*] Ip_Address: 34.86.182.0

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gce-us-east1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: chunk.gce-us-east1.production.mux.com

[*] Ip_Address: 34.148.121.217

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: debugger.gce-us-east1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: mediarouter.gce-us-east1.production.mux.com

[*] Ip_Address: 34.148.121.217

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: asset.gce-us-east1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: manifest.gce-us-east1.production.mux.com

[*] Ip_Address: 34.148.121.217

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gce-europe-west1.production.mux.com

[*] Ip_Address: 35.187.113.74

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: chunk.gce-europe-west1.production.mux.com

[*] Ip_Address: 35.187.113.74

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: debugger.gce-europe-west1.production.mux.com

[*] Ip_Address: 35.187.113.74

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: mediarouter.gce-europe-west1.production.mux.com

[*] Ip_Address: 35.187.113.74

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: asset.gce-europe-west1.production.mux.com

[*] Ip_Address: 35.187.113.74

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: manifest.gce-europe-west1.production.mux.com

[*] Ip_Address: 35.187.113.74

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-west-2.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gcp-us-west1-vep2.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gcp-europe-west4-vep2.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gce-us-east4.production.mux.com

[*] Ip_Address: 35.199.6.175

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: chunk.gce-us-east4.production.mux.com

[*] Ip_Address: 34.86.182.0

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: debugger.gce-us-east4.production.mux.com

[*] Ip_Address: 35.199.6.175

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: mediarouter.gce-us-east4.production.mux.com

[*] Ip_Address: 34.86.182.0

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: asset.gce-us-east4.production.mux.com

[*] Ip_Address: 35.199.6.175

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: manifest.gce-us-east4.production.mux.com

[*] Ip_Address: 34.86.182.0

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: asset.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: app.mux.com

[*] Ip_Address: 108.138.64.89

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: global-live-backup.mux.com

[*] Ip_Address: 34.160.204.215

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: jobs.mux.com

[*] Ip_Address: 18.165.98.120

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: api-docs.mux.com

[*] Ip_Address: 108.138.85.8

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: global-live-legacy.mux.com

[*] Ip_Address: 34.160.204.215

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: signing-keys.aws-us-east-1-dop1.mux.com

[*] Ip_Address: 34.225.27.0

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-east-1-top1.mux.com

[*] Ip_Address: 52.5.219.94

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: signing-keys.aws-us-east-1-dos1.mux.com

[*] Ip_Address: 184.72.214.149

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: stats.aws-us-east-1.production.mux.com

[*] Ip_Address: 35.199.6.175

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gcp-us-east1-vep1.production.mux.com

[*] Ip_Address: 35.199.6.175

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: gcp-us-east1.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-eu-central-1-dop2.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

[*] Country: None

[*] Host: aws-us-east-1-dop2.production.mux.com

[*] Ip_Address: 35.227.52.160

[*] Latitude: None

[*] Longitude: None

[*] Notes: None

[*] Region: None

[*]

SUMMARY

[*] 76 total (76 new) hosts found.

[recon-ng][default][hackertarget] > show hosts

rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	mux.com	76.76.21.21						hackertarget
2	aws-us-east-1-dop1.mux.com	34.225.13.238						hackertarget
3	auth.aws-us-east-1-dop1.mux.com	54.237.187.223						hackertarget
4	aws-us-east-1-dos1.mux.com	3.215.41.143						hackertarget
5	auth.aws-us-east-1-dos1.mux.com	34.228.172.221						hackertarget
6	admin-qa.mux.com	184.72.214.149						hackertarget
7	static.mux.com	18.160.41.128						hackertarget
8	o1.sendgrid.mux.com	168.245.48.185						hackertarget
9	dashboard.mux.com	108.138.64.58						hackertarget
10	legacy-live.mux.com	34.160.204.215						hackertarget
11	us-east1.gcp.live.mux.com	34.138.128.221						hackertarget
12	us-west1.gcp.live.mux.com	35.230.19.118						hackertarget
13	europe-west4.gcp.live.mux.com	34.91.174.38						hackertarget
14	dashboard-staging.mux.com	65.8.158.48						hackertarget
15	live-staging.mux.com	35.235.125.238						hackertarget
16	global-live-staging.mux.com	34.95.103.84						hackertarget
17	us-west2.gcp.live-staging.mux.com	35.235.125.238						hackertarget
18	admin-staging.mux.com	52.203.95.190						hackertarget
19	gcp-us-west1-vos1.staging.mux.com	34.145.105.68						hackertarget
20	gce-us-west1.staging.mux.com	35.230.73.183						hackertarget
21	buildkite.gce-us-west1.staging.mux.com	35.230.73.183						hackertarget
22	chunk.gce-us-west1.staging.mux.com	34.145.105.68						hackertarget
23	chunked-transfer-demo.gce-us-west1.staging.mux.com	35.230.73.183						hackertarget
24	debugger.gce-us-west1.staging.mux.com	35.230.73.183						hackertarget
25	mediarouter.gce-us-west1.staging.mux.com	35.230.73.183						hackertarget
26	asset.gce-us-west1.staging.mux.com	35.230.73.183						hackertarget
27	vault.gce-us-west1.staging.mux.com	35.230.73.183						hackertarget
28	manifest.gce-us-west1.staging.mux.com	34.145.105.68						hackertarget
29	api.staging.mux.com	34.237.87.177						hackertarget
30	retool.staging.mux.com	35.170.153.40						hackertarget
31	api.mux.com	52.22.14.139						hackertarget
32	test-api.mux.com	52.71.16.114						hackertarget
33	admin.mux.com	54.85.215.119						hackertarget
34	aws-eu-central-1-dop1.production.mux.com	35.227.52.160						hackertarget
35	aws-us-east-1-dop1.production.mux.com	35.227.52.160						hackertarget
36	aws-eu-central-1-rop1.production.mux.com	35.227.52.160						hackertarget
37	aws-us-east-1-rop1.production.mux.com	35.199.6.175						hackertarget

38	aws-us-west-2-rop1.production.mux.com	35.227.52.160						hackertarget
39	aws-us-east-1-top1.production.mux.com	35.227.52.160						hackertarget
40	gcp-us-east1-vop1.production.mux.com	34.148.121.217						hackertarget
41	gcp-us-east4-vop1.production.mux.com	34.86.182.0						hackertarget
42	gce-us-east1.production.mux.com	35.227.52.160						hackertarget
43	chunk.gce-us-east1.production.mux.com	34.148.121.217						hackertarget
44	debugger.gce-us-east1.production.mux.com	35.227.52.160						hackertarget
45	mediarouter.gce-us-east1.production.mux.com	34.148.121.217						hackertarget
46	asset.gce-us-east1.production.mux.com	35.227.52.160						hackertarget
47	manifest.gce-us-east1.production.mux.com	34.148.121.217						hackertarget
48	gce-europe-west1.production.mux.com	35.187.113.74						hackertarget
49	chunk.gce-europe-west1.production.mux.com	35.187.113.74						hackertarget
50	debugger.gce-europe-west1.production.mux.com	35.187.113.74						hackertarget
51	mediarouter.gce-europe-west1.production.mux.com	35.187.113.74						hackertarget
52	asset.gce-europe-west1.production.mux.com	35.187.113.74						hackertarget
53	manifest.gce-europe-west1.production.mux.com	35.187.113.74						hackertarget
54	aws-us-west-2.production.mux.com	35.227.52.160						hackertarget
55	gcp-us-west1-vep2.production.mux.com	35.227.52.160						hackertarget
56	gcp-europe-west4-vep2.production.mux.com	35.227.52.160						hackertarget
57	gce-us-east4.production.mux.com	35.199.6.175						hackertarget
58	chunk.gce-us-east4.production.mux.com	34.86.182.0						hackertarget
59	debugger.gce-us-east4.production.mux.com	35.199.6.175						hackertarget
60	mediarouter.gce-us-east4.production.mux.com	34.86.182.0						hackertarget
61	asset.gce-us-east4.production.mux.com	35.199.6.175						hackertarget
62	manifest.gce-us-east4.production.mux.com	34.86.182.0						hackertarget
63	asset.production.mux.com	35.227.52.160						hackertarget
64	app.mux.com	108.138.64.89						hackertarget
65	global-live-backup.mux.com	34.160.204.215						hackertarget
66	jobs.mux.com	18.165.98.120						hackertarget
67	api-docs.mux.com	108.138.85.8						hackertarget
68	global-live-legacy.mux.com	34.160.204.215						hackertarget
69	signing-keys.aws-us-east-1-dop1.mux.com	34.225.27.0						hackertarget
70	aws-us-east-1-top1.mux.com	52.5.219.94						hackertarget
71	signing-keys.aws-us-east-1-dos1.mux.com	184.72.214.149						hackertarget
72	stats.aws-us-east-1.production.mux.com	35.199.6.175						hackertarget
73	gcp-us-east1-vep1.production.mux.com	35.199.6.175						hackertarget
74	gcp-us-east1.production.mux.com	35.227.52.160						hackertarget
75	aws-eu-central-1-dop2.production.mux.com	35.227.52.160						hackertarget
76	aws-us-east-1-dop2.production.mux.com	35.227.52.160						hackertarget

[*] 76 rows returned

[recon-ng][default][hackertarget] > modules search report

[*] Searching installed modules for 'report'...

Reporting

reporting/csv

reporting/html

reporting/json

reporting/list

reporting/proxifier

reporting/pushpin

reporting/xlsx

reporting/xml

DAY -3

Finding ports on - nmap

Step -1

Open kali linux

Step -2

Open terminal

Step -3

nmap mux.com

Starting Nmap 7.94 (https://nmap.org) at 2023-07-19 21:53 IST

Nmap scan report for mux.com (76.76.21.21)

Host is up (0.016s latency).

Not shown: 997 filtered tcp ports (no-response)

PORT STATE SERVICE

80/tcp open http

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 7.27 seconds

Step -4

I got 2 open ports

80/tcp open http

443/tcp open https

Step -5

Using chat gpt or google i got this information about those 2 open ports

80 HTTP, 443 HTTPS, they are used by web servers.

Can you hack something through port 80/443? It depends on the specific service that runs on

those ports (which specific web server, i.e. nginx), and on the content which is provided by the web

server. Usually it's latter which is vulnerable (sql injection, IDOR, look at OWASP top 10), even

though also the web server can be configured wrongly

It is used

Port 80 is used for unencrypted web traffic and port 443 is used for encrypted web traffic.

DAY -4

Exploitation of vulnerabilities

Step -1

php.testsparker.com

Step-2

In terminal

nmap php.testsparker.com

Starting Nmap 7.94 (https://nmap.org) at 2023-07-20 18:00 IST

Nmap scan report for php.testsparker.com (107.20.213.223)

Host is up (0.029s latency).

rDNS record for 107.20.213.223: ec2-107-20-213-223.compute-1.amazonaws.com

Not shown: 996 filtered tcp ports (no-response)

PORT STATE SERVICE

25/tcp open smtp

53/tcp open domain

80/tcp open http

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 54.01 seconds

Step -3

Take ip address of domain and

nmap -sV 107.20.213.223 -p 80

Starting Nmap 7.94 (https://nmap.org) at 2023-07-20 18:06 IST

Nmap scan report for ec2-107-20-213-223.compute-1.amazonaws.com (107.20.213.223)

Host is up (0.0013s latency).

PORT STATE SERVICE VERSION

80/tcp filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds

Step -4

Copied the version

nginx 1.19.0 and

Pasted it in google

The results is

PHuiP-FPizdaM

What's this

This is an exploit for a bug in php-fpm (CVE-2019-11043). In certain nginx + php-fpm configurations, the bug is possible to trigger from the outside. This means that a web user may get code execution if you have vulnerable config (see [below](#the-full-list-of-preconditions)).

What's vulnerable

If a webserver runs nginx + php-fpm and nginx have a configuration like

```
location ~ [^/]\.php(/|$) {
  ...
  fastcgi_split_path_info ^(.+?\.php)(/.*)$;
  fastcgi_param PATH_INFO       $fastcgi_path_info;
  fastcgi_pass   php:9000;
  ...
```

}which also lacks any script existence checks (like try_files), then you can probably hack it with this sploit.

The full list of preconditions

Nginx + php-fpm, location ~ [^/]\.php(/|$) must be forwarded to php-fpm (maybe the regexp can be stricter, see [#1](https://github.com/neex/phuip-fpizdam/issues/1)).

The fastcgi_split_path_info directive must be there and contain a regexp starting with ^ and ending with $, so we can break it with a newline character.

There must be a PATH_INFO variable assignment via statement fastcgi_param PATH_INFO $fastcgi_path_info;. At first, we thought it is always present in the fastcgi_params file, but it's not true.

No file existence checks like try_files $uri =404 or if (-f $uri). If Nginx drops requests to non-existing scripts before FastCGI forwarding, our requests never reach php-fpm. Adding this is also the easiest way to patch.

This exploit works only for PHP 7+, but the bug itself is present in earlier versions (see [below](#about-php5)).

Isn't this known to be vulnerable for years?

A long time ago php-fpm didn't restrict the extensions of the scripts, meaning that something like /avatar.png/some-fake-shit.php could execute avatar.png as a PHP script. This issue was fixed around 2010.

The current one doesn't require file upload, works in the most recent versions (until the fix has landed), and, most importantly, the exploit is much cooler.

How to run

Install it using

go get github.com/neex/phuip-fpizdam

If you get strange compilation errors, make sure you're using go >= 1.13. Run the program using phuip-fpizdam [url] (assuming you have the $GOPATH/bin inside your $PATH, otherwise specify the full path to the binary). Good output looks like this:

2019/10/01 02:46:15 Base status code is 200

2019/10/01 02:46:15 Status code 500 for qsl=1745, adding as a candidate

2019/10/01 02:46:15 The target is probably vulnerable. Possible QSLs: [1735 1740 1745]

2019/10/01 02:46:16 Attack params found: --qsl 1735 --pisos 126 --skip-detect

2019/10/01 02:46:16 Trying to set "session.auto_start=0"...

2019/10/01 02:46:16 Detect() returned attack params: --qsl 1735 --pisos 126 --skip-detect <-- REMEMBER THIS

2019/10/01 02:46:16 Performing attack using php.ini settings...

2019/10/01 02:46:40 Success! Was able to execute a command by appending "?a=/bin/sh+-c+'which+which'&" to URLs

2019/10/01 02:46:40 Trying to cleanup /tmp/a...

2019/10/01 02:46:40 Done!

`After this, you can start appending `?a=<your command>` to all PHP scripts (you may need multiple retries).

Playground environment

If you want to reproduce the issue or play with the exploit locally, do the following:

Clone this repo and go to the `reproducer` directory.

Create the docker image using `docker build -t reproduce-cve-2019-11043 .`. It takes a long time as it internally clones the php repository and builds it from the source. However, it will be easier this way if you want to debug the exploit. The revision built is the one right before the fix.

Run the docker using `docker run --rm -ti -p 8080:80 reproduce-cve-2019-11043`.

Now you have http://127.0.0.1:8080/script.php, which is an empty file.

Run the exploit using `phuip-fpizdam http://127.0.0.1:8080/script.php`

If everything is ok, you'll be able to execute commands by appending `?a=` to the script: http://127.0.0.1:8080/script.php?a=id. Try multiple times as only some of php-fpm workers are infected.

About PHP5

The buffer underflow in php-fpm is present in PHP version 5. However, this exploit makes use of an optimization used for storing FastCGI variables, [_fcgi_data_seg](https://github.com/php/php-src/blob/5d6e923/main/fastcgi.c#L186). This optimization is present only in php 7, so this particular exploit works only for php 7. There might be another exploitation technique that works in php 5.

Credits

Original anomaly discovered by [d90pwn](https://twitter.com/d90pwn) during Real World CTF. Root clause found by me (Emil Lerner) as well as the way to set php.inioptions. Final php.ini options set is found by [beched](https://twitter.com/ahack_ru).

DAY -5

Session hijacking attack

Step -1

Go to browser and search

Crosssite scripting clean sheet

Then select tags

Then copy the code

<script src=data:text/javascript;base64,%59%57%78%6c%63%6e%51%6f%4d%53%6b%3d></script>

Step -2

Then take a domain name and search it in new tab

Then paste the code in that site

<script src=data:text/javascript;base64,%59%57%78%6c%63%6e%51%6f%4d%53%6b%3d></script>

Step -3

Then you will get a popup raised and gives 1

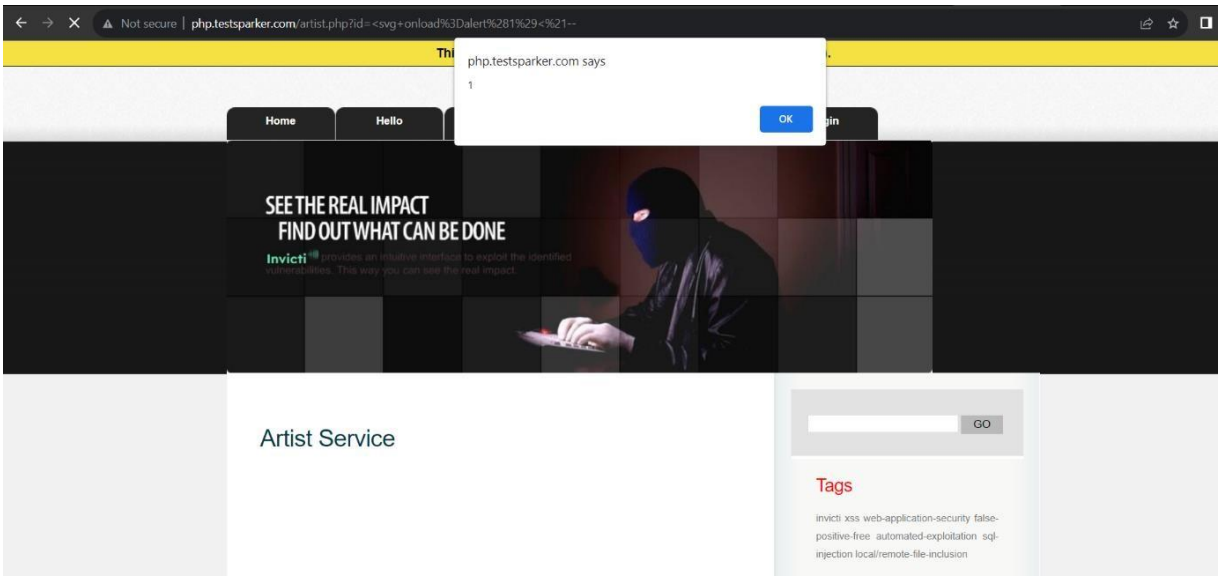
After that again search for

That code this time remove alert(1)

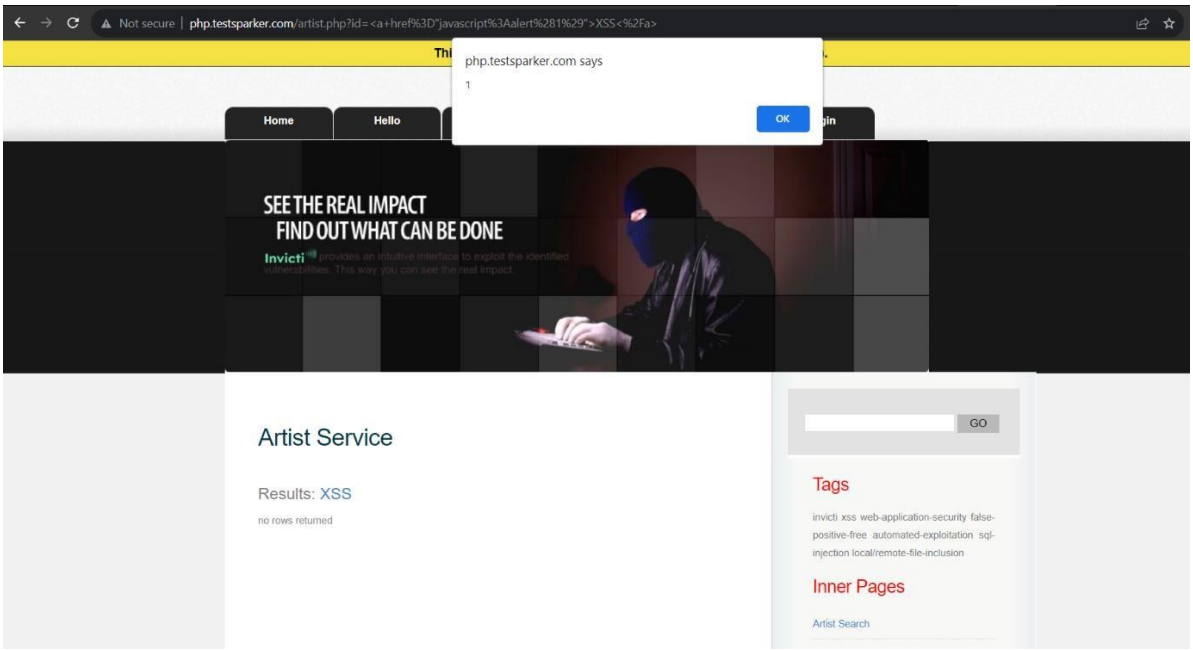
Step -4

Crosssite scripting clean sheet :

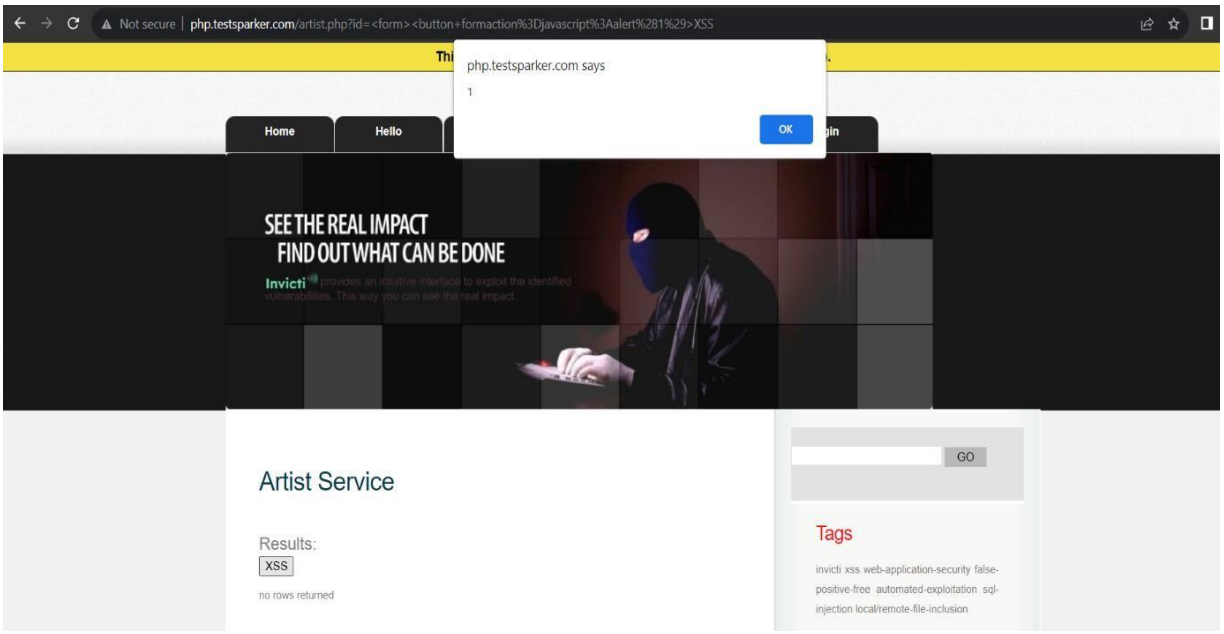
<svg onload=alert(1)<!—



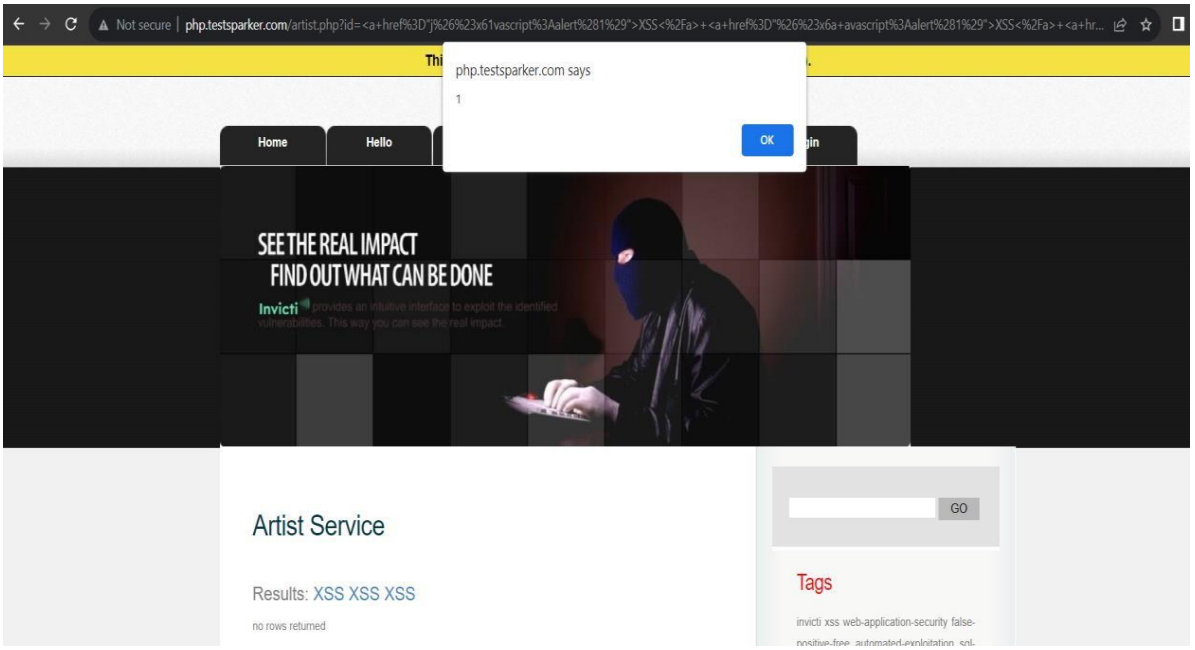
XSS



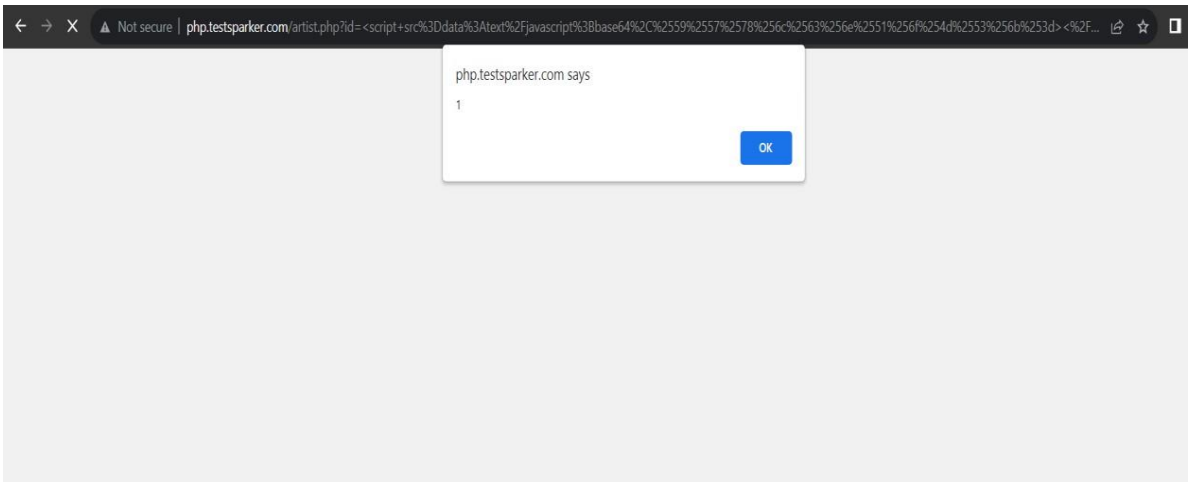
<form><button formaction=javascript:alert(1)>XSS



XSS XSS XSS



<script src=data:text/javascript;base64,%59%57%78%6c%63%6e%51%6f%4d%53%6b%3d></script>



DAY -6

Nmap checking connected devices to our network

Step -1

Open kali linux

Step -2

Open terminal and

Update sudo apt packages

Step -3

Sudo su

Step -4

Enter password

Step -5

Enter cmnd

Apt update

It updates packages

Step -6

Enter cmnd

Apt upgrade

packages are upgraded

step -7

Enter command

nmap -Pn 192.168.1.0/24

Starting Nmap 7.94 (https://nmap.org) at 2023-07-21 23:06 IST

Nmap scan report for 192.168.1.1

Host is up (0.014s latency).

Nmap scan report for 192.168.1.255

Host is up (0.0015s latency).

Nmap done: 256 IP addresses (2 hosts up) scanned in 2.78 seconds

DAY -7

Owasp to 10 vulnerabilitie understanding

Broken Access Control

During app development, access controls are applied that prohibit users from retrieving the information out of their given permission. Failure to perform efficiently can lead to unauthorized information disclosure, data modification, destruction of all data and many other damages. When an application evolves with time and numerous features are loaded to it, failure can occur and this can result in fallout for the application's security. Broken Access Control in any application or website must be prevented at all cost.

It is among the commonly faced OWASP 2023 vulnerabilities.

Cryptographic Failures

Poor use of cryptography and algorithm are responsible for a series of threats that are known as Cryptographic failures. It is important to use encrypted connections to application like SFTP, HTTPS, SSH, etc while carrying out any configuration or code changes. This vulnerability can expose sensitive data such as passwords, business records, credit card information, email addresses, patient health records, or other personal user data. To prevent this, all data should be stored with the recommended hashing algorithms.

Injection

Injection is one of the oldest vulnerability that can lead to data loss, data theft, service denial, etc and in worst scenario can compromise the full system. Injection attacks, especially SQL Injections (SQLi attacks) and Cross-site Scripting (XSS), are most dangerous and widespread weakness of any

application. Other than these, there are several other types of Injections that a web developer should look out for. Using a safe API and positive server-side input validation can help in preventing Injections.

Insecure Design

To keep application free of security gaps, it is recommended that developers use safe design patterns and securely created threat modeling while designing. A secure application can be build using secured component library, tooling and methodology. Implementation of ineffective control design can lead to different weaknesses termed as Insecure Design. It is suggested to determine the level of security design before beginning the app development to prevent Insecure Design vulnerability.

Security Misconfiguration

Inaccurately or insecurely configured security controls can cause Security Misconfiguration vulnerability and put the system and data to risk. Unnecessary features enabled or installed, outdated software, etc can also cause Security Misconfiguration. This threat can impact any layer of the application stack, cloud or network, leaving important information to expose. It can be prevented by implementing secure installation process. Using an automated process to verify the effectiveness of the configurations and settings in all environments is also recommended.

Vulnerable and Outdated Components

If the components used in the development of a website or application is outdated or is vulnerable itself, it can compromise the whole application. This is known as Vulnerable and Outdated Components vulnerability. A developer should also always know the versions of

components being used and should perform regular scan for vulnerabilities to keep problems at bay. As a protective measure, remove unnecessary features, unused dependencies, components, files and documentation from time to time.

Identification and Authentication Failures

Before accessing any protected site, the application must keep a check on user's identity, authentication, and session management. These things are important for protection against authentication-related attacks or can else lead to Identification and Authentication Failures vulnerability. With the introduction of two-factor authentication, the number of failures has reduced but is still too frequent to be listed in the OWASP Top 10 vulnerabilities 2023. Limiting failed login attempts and generating a new

random session ID at every login can further prevent the issue.

Software and Data Integrity Failures

Code and infrastructure that does not protect against integrity violations can lead to Software and data integrity failures. It is therefore important to verify the installed packages on your system and make sure that the data is from a reliable source and has not been altered at any stage. Implementing libraries and dependencies, software supply chain security tool, and review process for code and configuration changes are other ways of preventing this vulnerability.

Security Logging and Monitoring

Security logging and monitoring are vital to the maintenance of a secure infrastructure. Viewing the logs regularly can

be helpful in acting fast in case any potentially dangerous activity is noticed. On the other hand, insufficient monitoring of log activities can lead to a bunch of issues collectively termed as Security logging and monitoring vulnerability. Depending on the risk of the application, protective measures must be applied to eliminate any risk as soon as possible.

Server-Side Request Forgery

Server-Side Request Forgery (SSRF) occurs when a web application procures a distant resource without validating the URL supplied by the user. The attacker can send a crafted request to an unexpected destination, even if protected by a firewall or VPN. Both frequency and severity of this vulnerability has increased with time. To protect an application against SSRF, all the data entered should be checked carefully and each URL scheme should be checked against the allowed li