Sri Lanka Institute of Information Technology

WEB SECURITY

(IE2062)

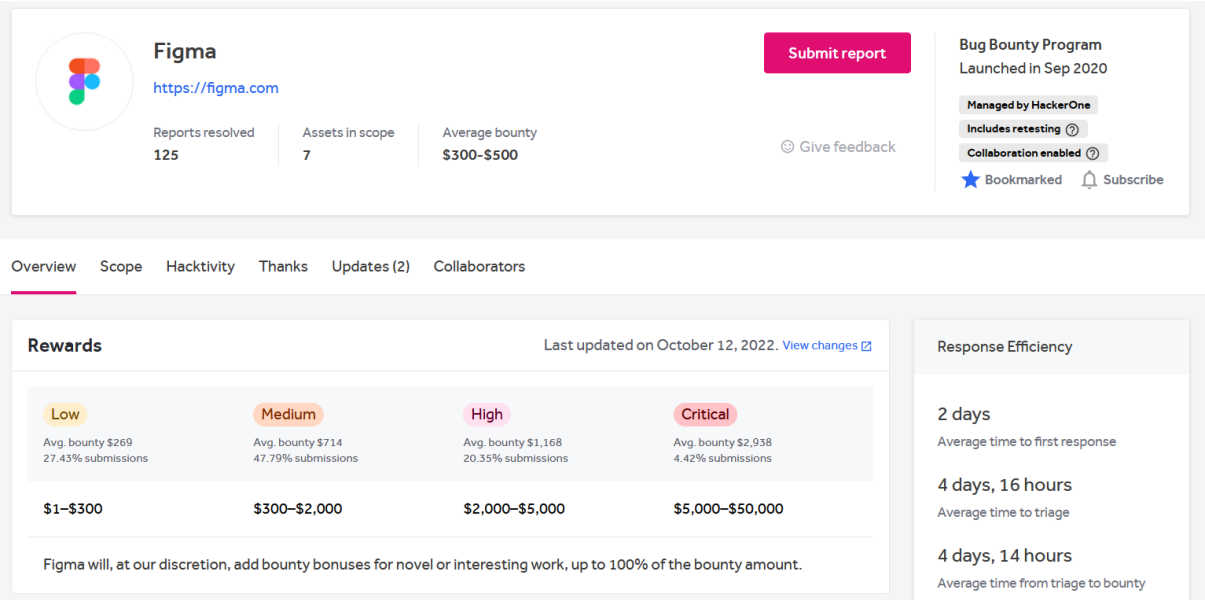
BUG BOUNTY

REPORT 2

Thilakarathna S.T.D- IT22578914

B.Sc. (Hons) in Information Technology Specializing in cyber security

Overview of the website



Design teams are transforming the way they interact and produce work with Figma, an online platform hosted by Figma.com that is a cloud-based design and prototype tool. Anyone with an internet connection may work on creative projects using Figma with ease thanks to its user-friendly browser-based interface. At its core, Figma collaborates in real-time, allowing numerous team members to work on the same project at once and quickly view each other's modifications. Without the need for additional tools, the platform allows for the production of interactive prototypes and has powerful vector editing capabilities that support component-based design. Design teams looking for speed, flexibility, and creativity in their processes will find Figma.com to be a comprehensive solution with features like version history, comments, and interfaces with well-known collaboration and project management applications.

Scope

- InScope

Figma iOS and Android apps	Other	In scope	Critical	Eligible	Sep 22, 2022	0 (0%)
Figma Slack App https://figma.slack.com/apps/A01N2QYSA81-figma-and-figjam?tab=more_info	Other	In scope	Critical	Eligible	Oct 12, 2022	0 (0%)
Figma for Microsoft Teams https://appsource.microsoft.com/en-us/product/office/wa200004521?tab=overview	Other	In scope	Critical	Eligible	Oct 12, 2022	0 (0%)
api.figma.com	Domain	In scope	Critical	Eligible	Sep 30, 2020	9 (7%)
Figma Desktop App	Other	In scope	Critical	Eligible	Sep 22, 2022	3 (2%)
Figma Atlassian App https://marketplace.atlassian.com/apps/1217865/figma-for-jira Unauthorized access via this app or the APIs that this app uses is also in scope.	Other	In scope	Critical	Eligible	Sep 30, 2020	2 (2%)
www.figma.com We are primarily looking for high/critical vulnerabilities in the system. English AmazonRDS Amazon Web Services JavaScript Rails React Ruby	Domain	In scope	Critical	Eligible	Sep 30, 2020	805 (644%)

OutScope

www.designsystems.com	Domain	Out of scope	None	Ineligible	Oct 3, 2020	0 (0%)

Information Gathering

Security researchers and ethical hackers must first gather data through bug bounty programs in order to identify vulnerabilities in a target system or application. This step's objective is to learn as much as you can about the target, including its technologies, architecture, known vulnerabilities, and potential weak points. Open-source intelligence gathering (OSINT), network scanning, fingerprinting, and asset enumeration are typically required to give a complete view of the target's attack surface.

Since it enables ethical hackers to identify potential points of entry and focus their search for system security flaws, efficient information gathering is the cornerstone of a successful bug hunting operation.

Subdomains for Hunting

The process of listing sub-domains for one or more domains is called sub-domain enumeration. This is a critical stage in the reconnaissance process. Finding vulnerabilities is made more likely by sub-domain enumeration, which can identify several domains and sub-domains that are part of a security assessment.

Seen through cryptic, abandoned sub-domains, programs may have dangerous bugs.

The same weaknesses are frequently found throughout numerous domains and applications within a single organization.

- **Knockpy**

Knoppy is a Python-based subdomain reconnaissance tool. Its major purpose is to list subdomains via passive DNS techniques. Knockpy uses multiple DNS data sources to help find subdomains associated with a given domain.

```
┌──(root㉿kali)-[/home/tharusha]
└─# knockpy figma.com

 _ __                  _
 | |/ /                | |   v6.1.0
 | ' / _ __   ___   __ | | ___ __ _  _
 |  < | '_ \ / _ \ / _| |/ / '_ \| | |
 | . \| | | | (_) | (_|   <| |_) | |_| |
 |_|\_\_| |_|\___/ \___|_|\_\ .__/ \__, |
                            | |     __/ |
                            |_|    |___/

local: 10757 | remote: 134

Wordlist: 10891 | Target: figma.com | Ip: 13.35.18.95

11:51:21

Ip address      Code Subdomain                                          Server                                  Real hostname

108.157.254.41  200  admin.staging.figma.com                            nginx
108.157.254.117 200  admin.figma.com                                    nginx
13.225.4.29     200  api.figma.com
52.84.45.113    200  api-cdn.figma.com
108.156.133.27  202  api.staging.figma.com                             CloudFront
13.35.18.104    502  bcp.figma.com                                      AmazonS3
52.74.166.77    200  brand.figma.com
108.157.254.100 200  blog.figma.com
192.28.158.138       bounce.figma.com
108.157.254.69  403  cdn.figma.com                                      AmazonS3
108.156.133.18  404  click.figma.com                                    nginx
54.80.69.53     200  compliance.figma.com                               nginx
108.157.254.69  404  cors-image-proxy.figma.com                         CloudFront
3.236.115.212   200  config.figma.com                                   nginx
13.35.18.127    403  desktop.figma.com                                  AmazonS3
54.189.201.11   200  deploys.figma.com                                  nginx
13.35.18.101    404  embed.figma.com
13.33.30.12     400  embed.bcp.figma.com                                Server
13.227.254.24   403  errors.staging.figma.com
18.155.68.79    403  errors.figma.com
151.101.194.133 403  events.figma.com                                   DataDome
104.16.53.111   403  help.figma.com                                     cloudflare
52.11.255.62    204  hello.figma.com
104.17.71.206   200  info.figma.com
108.157.254.124 200  marketing.figma.com                               AmazonS3
18.155.68.37    200  marketing.staging.figma.com                       AmazonS3
167.89.87.53         o1.email.figma.com
13.227.254.92   403  s3-alpha-sig.figma.com                            CloudFront
13.33.88.123    403  s3-figma-canvas-images-eu-production-sig.figma.com CloudFront
13.35.18.27     403  s3-alpha.figma.com                                AmazonS3
13.33.30.3      403  s3-figma-fonts-private-production-sig.figma.com   CloudFront
```

```
13.35.18.37     403  s3-figma-plugin-images-production-sig.figma.com   CloudFront
13.33.88.113    403  s3-figma-videos-production-sig.figma.com          CloudFront
13.35.18.31     403  s3-figma-hubfile-images-production.figma.com      CloudFront
13.35.18.48     403  s3-figma-file-comment-attachments-production-sig.figma.com CloudFront
108.157.254.64  403  s3-figma-file-comment-attachments-production.figma.com AmazonS3
3.248.123.157   200  schemavirtual2022.figma.com
108.157.254.123 200  schema.figma.com                                   Netlify
184.73.163.186  200  share.figma.com                                    cloudflare
13.33.30.56     404  slack.figma.com
52.84.229.113   200  sprig.figma.com
13.227.254.48   202  staging.figma.com                                 CloudFront
18.155.68.114   403  static.figma.com                                  AmazonS3
18.155.68.29    200  status.figma.com                                  AtlassianEdge
23.227.38.74    200  store-jp.figma.com                                cloudflare
23.227.38.74    200  store-eu.figma.com                                cloudflare
23.227.38.74    200  store-uk.figma.com                                cloudflare
18.161.97.62    200  staging-admin.figma.com                           nginx
23.227.38.74    200  store-ca.figma.com                                cloudflare
23.227.38.74    200  store.figma.com                                   cloudflare
50.112.128.91   404  us-west-2.figma.com                               awselb/2.0
54.213.177.196  404  us-west-2.staging.figma.com                       awselb/2.0
44.241.90.5          us-west-2.figma-for-jira.figma.com
108.157.254.94  404  verify.bcp.figma.com                              AmazonS3
18.155.68.6     404  verify.figma.com                                  AmazonS3
52.43.220.32    403  web-logger.figma.com                              awselb/2.0
13.35.18.95     200  www.figma.com
18.161.97.14    200  www.staging-admin.figma.com                       nginx
162.159.128.7   403  zendesk1.figma.com                                cloudflare
162.159.138.6   403  zendesk4.figma.com                                cloudflare

12:00:50

Ip address: 172 | Subdomain: 60 | elapsed time: 00:09:28
```

- **Amass**

A tool has been developed by the OWASP Amass Project to assist information security professionals in external asset discovery and network mapping of attack surfaces.

```
┌──(root㉿kali)-[/home/tharusha]
└─# amass enum -h

                                                                      v4.2.0
                                          OWASP Amass Project - @owaspamass
                      In-depth Attack Surface Mapping and Asset Discovery


Usage: amass enum [options] -d DOMAIN

  -active
        Attempt zone transfers and certificate name grabs
  -addr value
        IPs and ranges (192.168.1.1-254) separated by commas
  -alts
        Enable generation of altered names
  -asn value
        ASNs separated by commas (can be used multiple times)
  -aw value
        Path to a different wordlist file for alterations
  -awm value
        "hashcat-style" wordlist masks for name alterations
  -bl value
        Blacklist of subdomain names that will not be investigated
  -blf string
        Path to a file providing blacklisted subdomains
  -brute
        Execute brute forcing after searches
  -cidr value
        CIDRs separated by commas (can be used multiple times)
  -config string
        Path to the YAML configuration file. Additional details below
  -d value
        Domain names separated by commas (can be used multiple times)
  -demo
        Censor output to make it suitable for demonstrations
  -df value
        Path to a file providing root domain names
```

```
┌──(root㉿kali)-[/home/tharusha]
└─# amass enum -brute -d figma.com
figma.com (FQDN) --> mx_record --> aspmx.l.google.com (FQDN)
figma.com (FQDN) --> mx_record --> aspmx2.googlemail.com (FQDN)
figma.com (FQDN) --> mx_record --> alt1.aspmx.l.google.com (FQDN)
figma.com (FQDN) --> mx_record --> alt2.aspmx.l.google.com (FQDN)
figma.com (FQDN) --> mx_record --> aspmx3.googlemail.com (FQDN)
figma.com (FQDN) --> a_record --> 13.35.18.86 (IPAddress)
figma.com (FQDN) --> a_record --> 13.35.18.52 (IPAddress)
figma.com (FQDN) --> a_record --> 13.35.18.115 (IPAddress)
figma.com (FQDN) --> a_record --> 13.35.18.95 (IPAddress)
api-cdn.figma.com (FQDN) --> cname_record --> d38riddbjre3uu.cloudfront.net (FQDN)
share.figma.com (FQDN) --> cname_record --> custom.getcloudapp.com (FQDN)
help.figma.com (FQDN) --> cname_record --> figma.zendesk.com (FQDN)
schemavirtual2022.figma.com (FQDN) --> cname_record --> elb-1853-schemavirtual2022-figma-com.swoogo.com (FQDN)
hello.figma.com (FQDN) --> cname_record --> 1535b102-a0b5-453e-9c40-17c4e7bbd070.outrch.com (FQDN)
cdn.figma.com (FQDN) --> cname_record --> d3ltmwrtxhidg3.cloudfront.net (FQDN)
desktop.figma.com (FQDN) --> cname_record --> d330if318qxsm2.cloudfront.net (FQDN)
admin.figma.com (FQDN) --> a_record --> 108.157.254.117 (IPAddress)
admin.figma.com (FQDN) --> a_record --> 108.157.254.99 (IPAddress)
admin.figma.com (FQDN) --> a_record --> 108.157.254.38 (IPAddress)
admin.figma.com (FQDN) --> a_record --> 108.157.254.18 (IPAddress)
font-daemon.figma.com (FQDN) --> cname_record --> d2kpab8750oqko.cloudfront.net (FQDN)
bounce.figma.com (FQDN) --> a_record --> 192.28.158.138 (IPAddress)
click.figma.com (FQDN) --> cname_record --> d16kdv7zgcta6p.cloudfront.net (FQDN)
www.figma.com (FQDN) --> a_record --> 3.164.230.79 (IPAddress)
www.figma.com (FQDN) --> a_record --> 3.164.230.55 (IPAddress)
13.35.16.0/21 (Netblock) --> contains --> 13.35.18.95 (IPAddress)
13.35.16.0/21 (Netblock) --> contains --> 13.35.18.115 (IPAddress)
13.35.16.0/21 (Netblock) --> contains --> 13.35.18.86 (IPAddress)
13.35.16.0/21 (Netblock) --> contains --> 13.35.18.52 (IPAddress)
16509 (ASN) --> managed_by --> AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) --> announces --> 13.35.16.0/21 (Netblock)
aspmx.l.google.com (FQDN) --> a_record --> 64.233.170.27 (IPAddress)
aspmx.l.google.com (FQDN) --> aaaa_record --> 2404:6800:4003:c01::1b (IPAddress)
1535b102-a0b5-453e-9c40-17c4e7bbd070.outrch.com (FQDN) --> cname_record --> app1a.outrch.com (FQDN)
www.figma.com (FQDN) --> a_record --> 3.164.230.47 (IPAddress)
www.figma.com (FQDN) --> a_record --> 3.164.230.74 (IPAddress)
store-uk.figma.com (FQDN) --> cname_record --> the-figma-store-uk.myshopify.com (FQDN)
status.figma.com (FQDN) --> cname_record --> rxpksf93ynw6.stspg-customer.com (FQDN)
store-eu.figma.com (FQDN) --> cname_record --> the-figma-store-eu.myshopify.com (FQDN)
store-ca.figma.com (FQDN) --> cname_record --> the-figma-store-ca.myshopify.com (FQDN)
go.figma.com (FQDN) --> cname_record --> mkto-sj310059.com (FQDN)
store-jp.figma.com (FQDN) --> cname_record --> the-figma-store.myshopify.com (FQDN)
forms.figma.com (FQDN) --> cname_record --> figforms.netlify.app (FQDN)
info.figma.com (FQDN) --> cname_record --> figmainc.mktoweb.com (FQDN)
store.figma.com (FQDN) --> cname_record --> the-figma-store.myshopify.com (FQDN)
compliance.figma.com (FQDN) --> cname_record --> elb-conveyor-67483.aptible.in (FQDN)
events.figma.com (FQDN) --> cname_record --> figmaevents.splashthat.com (FQDN)
brand.figma.com (FQDN) --> cname_record --> peaceful-poitras-70ec83.netlify.com (FQDN)
zendesk1.figma.com (FQDN) --> cname_record --> mail1.zendesk.com (FQDN)
zendesk4.figma.com (FQDN) --> cname_record --> mail4.zendesk.com (FQDN)
```

```
static.figma.com (FQDN) ⟶ cname_record ⟶ d3otp6i141k5zo.cloudfront.net (FQDN)
friends.figma.com (FQDN) ⟶ cname_record ⟶ figma.bevylabs.com (FQDN)
108.157.252.0/22 (Netblock) ⟶ contains ⟶ 108.157.254.38 (IPAddress)
108.157.252.0/22 (Netblock) ⟶ contains ⟶ 108.157.254.18 (IPAddress)
108.157.252.0/22 (Netblock) ⟶ contains ⟶ 108.157.254.117 (IPAddress)
16509 (ASN) ⟶ announces ⟶ 108.157.252.0/22 (Netblock)
forum.figma.com (FQDN) ⟶ cname_record ⟶ figma.hosted-by-discourse.com (FQDN)
us-west-2.staging.figma.com (FQDN) ⟶ a_record ⟶ 54.213.177.196 (IPAddress)
us-west-2.staging.figma.com (FQDN) ⟶ a_record ⟶ 44.224.209.50 (IPAddress)
us-west-2.staging.figma.com (FQDN) ⟶ a_record ⟶ 54.70.145.146 (IPAddress)
108.157.252.0/22 (Netblock) ⟶ contains ⟶ 108.157.254.99 (IPAddress)
192.28.144.0/20 (Netblock) ⟶ contains ⟶ 192.28.158.138 (IPAddress)
3.164.224.0/21 (Netblock) ⟶ contains ⟶ 3.164.230.74 (IPAddress)
3.164.224.0/21 (Netblock) ⟶ contains ⟶ 3.164.230.47 (IPAddress)
3.164.224.0/21 (Netblock) ⟶ contains ⟶ 3.164.230.79 (IPAddress)
3.164.224.0/21 (Netblock) ⟶ contains ⟶ 3.164.230.55 (IPAddress)
64.233.160.0/19 (Netblock) ⟶ contains ⟶ 64.233.170.27 (IPAddress)
54.212.0.0/14 (Netblock) ⟶ contains ⟶ 54.213.177.196 (IPAddress)
44.224.0.0/11 (Netblock) ⟶ contains ⟶ 44.224.209.50 (IPAddress)
54.64.0.0/12 (Netblock) ⟶ contains ⟶ 54.70.145.146 (IPAddress)
16509 (ASN) ⟶ announces ⟶ 3.164.224.0/21 (Netblock)
16509 (ASN) ⟶ announces ⟶ 54.212.0.0/14 (Netblock)
16509 (ASN) ⟶ announces ⟶ 44.224.0.0/11 (Netblock)
16509 (ASN) ⟶ announces ⟶ 54.64.0.0/12 (Netblock)
15224 (ASN) ⟶ managed_by ⟶ OMNITURE - Adobe Systems Inc. (RIROrganization)
15224 (ASN) ⟶ announces ⟶ 192.28.144.0/20 (Netblock)
15169 (ASN) ⟶ managed_by ⟶ GOOGLE - Google LLC (RIROrganization)
15169 (ASN) ⟶ announces ⟶ 64.233.160.0/19 (Netblock)
figmainc.mktoweb.com (FQDN) ⟶ cname_record ⟶ sj31.mktossl.com (FQDN)
figma.bevylabs.com (FQDN) ⟶ cname_record ⟶ production-ingress-6.bevylabs.com (FQDN)
staging.figma.com (FQDN) ⟶ mx_record ⟶ mx.sendgrid.net (FQDN)
staging.figma.com (FQDN) ⟶ ns_record ⟶ ns-390.awsdns-48.com (FQDN)
staging.figma.com (FQDN) ⟶ ns_record ⟶ ns-816.awsdns-38.net (FQDN)
staging.figma.com (FQDN) ⟶ ns_record ⟶ ns-1268.awsdns-30.org (FQDN)
staging.figma.com (FQDN) ⟶ ns_record ⟶ ns-1921.awsdns-48.co.uk (FQDN)
```

```
figma-for-jira.figma.com (FQDN) ⟶ a_record ⟶ 3.162.112.128 (IPAddress)
figma-for-jira.figma.com (FQDN) ⟶ a_record ⟶ 3.162.112.2 (IPAddress)
figma-for-jira.figma.com (FQDN) ⟶ a_record ⟶ 3.162.112.112 (IPAddress)
s3-figma-file-comment-attachments-production-sig.figma.com (FQDN) ⟶ a_record ⟶ 18.245.31.38 (IPAddress)
s3-figma-file-comment-attachments-production-sig.figma.com (FQDN) ⟶ a_record ⟶ 18.245.31.32 (IPAddress)
s3-figma-file-comment-attachments-production-sig.figma.com (FQDN) ⟶ a_record ⟶ 18.245.31.104 (IPAddress)
s3-figma-file-comment-attachments-production-sig.figma.com (FQDN) ⟶ a_record ⟶ 18.245.31.33 (IPAddress)
3.162.112.0/21 (Netblock) ⟶ contains ⟶ 3.162.112.96 (IPAddress)
3.162.112.0/21 (Netblock) ⟶ contains ⟶ 3.162.112.128 (IPAddress)
3.162.112.0/21 (Netblock) ⟶ contains ⟶ 3.162.112.2 (IPAddress)
3.162.112.0/21 (Netblock) ⟶ contains ⟶ 3.162.112.112 (IPAddress)
18.245.28.0/22 (Netblock) ⟶ contains ⟶ 18.245.31.38 (IPAddress)
18.245.28.0/22 (Netblock) ⟶ contains ⟶ 18.245.31.32 (IPAddress)
18.245.28.0/22 (Netblock) ⟶ contains ⟶ 18.245.31.104 (IPAddress)
18.245.28.0/22 (Netblock) ⟶ contains ⟶ 18.245.31.33 (IPAddress)
16509 (ASN) ⟶ announces ⟶ 3.162.112.0/21 (Netblock)
16509 (ASN) ⟶ announces ⟶ 18.245.28.0/22 (Netblock)

The enumeration has finished
```

- **Dnsdumpster**

Block addresses, emails, domain names, and other kinds of DNS-related data can be gathered using an online passive scanning tool called DNSdumpster.

Result of figma.com

dns recon & research, find & lookup dns records

figma.com | Search

DNS Servers

ns-1239.awsdns-26.org.	205.251.196.215	AMAZON-02 United States
ns-1657.awsdns-15.co.uk.	205.251.198.121	AMAZON-02 United States
ns-326.awsdns-40.com.	205.251.193.70	AMAZON-02 United States
ns-912.awsdns-50.net.	205.251.195.144	AMAZON-02 United States

MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com.	142.251.167.26	GOOGLE United States
10 aspmx2.googlemail.com.	209.85.202.26	GOOGLE United States
10 aspmx3.googlemail.com.	64.233.184.26	GOOGLE United States
5 alt1.aspmx.l.google.com.	209.85.202.27	GOOGLE United States
5 alt2.aspmx.l.google.com.	64.233.184.26	GOOGLE United States

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"1password-site-verification=LUTCLEML6JDMHACYUXWAJAOV74"

"MS=ms23440957"

"MS=ms46247837"

"ZOOM_verify_vCQSjij2TCG8TawaqXfiMQ"

"apple-domain-verification=1IOgJXKcT9knvlrK"

"atlassian-domain-verification=oDxpYa6fakpgoavsUf0n1AppTm13MnKzy2d01eAF1xtr9jA58AKXqtjU68cCkFtJ"

"drift-domain-verification=1dcdd2801b99b27623f8d35030ff747cc591acd43ff39054869a54dd645ee0f8"

"dropbox-domain-verification=u0lztjyam5gd"

"google-site-verification=56-T7QBpEBj_eJAQEeNBiiDaKx2ylEDgBH0heMnXYkU"

"google-site-verification=A9O3cWeQxmKPiLAY-3s7WfVVpktBZCTxlIMU-eDz5Xs"

"google-site-verification=HaMs8wg-gbgQs2hFJuwU_ciNQK_YobMtJ5hizbD2BZQ"

"google-site-verification=RGkyUdk1Vglm9VUITzietBk9EpJLNF690eAPGADZAO8"

"google-site-verification=TUp2QwBcCejFVJKwyvEFK4yMNoQgQy5W0cIvuf66Mvs"

"google-site-verification=nB1tDMUrIaTGOd9dydIEsFV5x1dbAIouhQ0VutHrzlU"

"google-site-verification=rCFXO7IrgLapurW3LCjK3g10AK27Mu0dMoqL-0yW8wY"

"notion-domain-verification=geo971ObbpRnpoT5ZZ73OOXXFxDMUKS0v5PdfY2W20M"

"segment-site-verification=z2vlLwo9wlSRgpA1gJtKG7Cf7hXGU8ck"

"shopify-verification-code=W6bLm0nIDEt0NPjQ0RiAjioCy5vKJP"

"stripe-verification=60dc440f0fb540a3a80e4bb56aa675cd75849fd66b427bc012ea67e1f2f4d026"

"v=spf1 a include:mktomail.com include:_spf.google.com ip4:149.72.216.165 ip4:167.89.79.69 ip4:167.89.87.53 ip4:168.245.25.177 include:mail.zendesk.com include:mg-spf.greenhouse.io -all"

- **DNSrecon**

For DNS enumeration and reconnaissance, an open-source tool named DNSRecon is utilized. The purpose of gathering information is to assist with penetration testing and security evaluations by providing details on DNS servers, domains, subdomains, and DNS records.

```
┌──(root㉿kali)-[/home/tharusha]
└─# dnsrecon -d figma.com
[*] std: Performing General Enumeration against: figma.com...
[-] DNSSEC is not configured for figma.com
[*]     SOA ns-1657.awsdns-15.co.uk 205.251.198.121
[*]     SOA ns-1657.awsdns-15.co.uk 2600:9000:5306:7900::1
[*]     NS ns-1657.awsdns-15.co.uk 205.251.198.121
[*]     NS ns-1657.awsdns-15.co.uk 2600:9000:5306:7900::1
[*]     NS ns-1239.awsdns-26.org 205.251.196.215
[*]     NS ns-1239.awsdns-26.org 2600:9000:5304:d700::1
[*]     NS ns-326.awsdns-40.com 205.251.193.70
[*]     NS ns-326.awsdns-40.com 2600:9000:5301:4600::1
[*]     NS ns-912.awsdns-50.net 205.251.195.144
[*]     NS ns-912.awsdns-50.net 2600:9000:5303:9000::1
[*]     MX aspmx.l.google.com 74.125.68.27
[*]     MX aspmx2.googlemail.com 173.194.202.26
[*]     MX alt1.aspmx.l.google.com 173.194.202.26
[*]     MX alt2.aspmx.l.google.com 142.250.141.26
[*]     MX aspmx3.googlemail.com 142.250.141.27
[*]     MX aspmx.l.google.com 2404:6800:4003:c04::1b
[*]     MX aspmx2.googlemail.com 2607:f8b0:400e:c00::1a
[*]     MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1b
[*]     MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1b
[*]     MX aspmx3.googlemail.com 2607:f8b0:4023:c0b::1a
[*]     A figma.com 13.35.18.86
[*]     A figma.com 13.35.18.115
[*]     A figma.com 13.35.18.52
[*]     A figma.com 13.35.18.95
[*]     TXT _dmarc.figma.com v=DMARC1; p=quarantine;
[*] Enumerating SRV Records
[-] No SRV Records Found for figma.com
```

- **WHOIS**

Domain names, IP addresses, and autonomous system numbers (ASNs) can all be found via a database system or a protocol, respectively. It provides information, such as contact details, about the owner of a block of IP addresses or the person who registered a domain name.

```
┌──(root㉿kali)-[/home/tharusha]
└─# whois figma.com
   Domain Name: FIGMA.COM
   Registry Domain ID: 5176427_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.amazon.com
   Registrar URL: http://registrar.amazon.com
   Updated Date: 2024-03-07T00:07:37Z
   Creation Date: 1999-04-10T04:00:00Z
   Registry Expiry Date: 2025-04-10T04:00:00Z
   Registrar: Amazon Registrar, Inc.
   Registrar IANA ID: 468
   Registrar Abuse Contact Email: abuse@amazonaws.com
   Registrar Abuse Contact Phone: +1.2024422253
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-1239.AWSDNS-26.ORG
   Name Server: NS-1657.AWSDNS-15.CO.UK
   Name Server: NS-326.AWSDNS-40.COM
   Name Server: NS-912.AWSDNS-50.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-09T12:31:59Z <<<
Domain Name: figma.com
Registry Domain ID: 5176427_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon
Registrar URL: https://registrar.amazon.com
Updated Date: 2024-03-07T00:07:37Z
Creation Date: 1999-04-10T04:00:00Z
Registrar Registration Expiration Date: 2025-04-10T04:00:00Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: abuse@amazonaws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: On behalf of figma.com owner
Registrant Organization: Identity Protection Service
Registrant Street: PO Box 786
Registrant City: Hayes
Registrant State/Province: Middlesex
Registrant Postal Code: UB3 9TR
Registrant Country: GB
Registrant Phone: +44.1483307527
Registrant Phone Ext:
Registrant Fax: +44.1483304031
Registrant Fax Ext:
Registrant Email: 7addb415-33a9-4c81-9147-4f476f18c689@identity-protect.org
Registry Admin ID: Not Available From Registry
Admin Name: On behalf of figma.com owner
Admin Organization: Identity Protection Service
Admin Street: PO Box 786
Admin City: Hayes
Admin State/Province: Middlesex
Admin Postal Code: UB3 9TR
Admin Country: GB
Admin Phone: +44.1483307527
Admin Phone Ext:
Admin Fax: +44.1483304031
Admin Fax Ext:
Admin Email: 7addb415-33a9-4c81-9147-4f476f18c689@identity-protect.org
Registry Tech ID: Not Available From Registry
Tech Name: On behalf of figma.com owner
Tech Organization: Identity Protection Service
Tech Street: PO Box 786
Tech City: Hayes
Tech State/Province: Middlesex
Tech Postal Code: UB3 9TR
Tech Country: GB
Tech Phone: +44.1483307527
Tech Phone Ext:
Tech Fax: +44.1483304031
```

- **Whatweb**

A web application's technology stack can be discovered with this open-source research tool. It analyzes HTTP answers from a target web server to collect further information about the web server, web framework, programming language, content management system (CMS), JavaScript libraries, and other technologies that the target site may be utilizing.

```
┌──(root㉿kali)-[/home/tharusha]
└─# whatweb figma.com
http://figma.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[13.35.18.95], RedirectLocation[https://figma.com/], Title[301 Moved Permanently], UncommonHeaders[x-amz-cf-pop,alt-svc,x-amz-cf
-id], Via-Proxy[1.1 a0dab1619e09a1e6e84a759dfdfe7342.cloudfront.net (CloudFront)]
https://figma.com/ [301 Moved Permanently] Country[UNITED STATES][US], IP[13.35.18.86], RedirectLocation[https://www.figma.com/], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], UncommonHeaders[x-amz-cf-pop,alt
-svc,x-amz-cf-id], Via-Proxy[1.1 7d6cd6b1cab0712d291c301dc839b042.cloudfront.net (CloudFront)]
https://www.figma.com/ [200 OK] Country[UNITED STATES][US], HTML5, IP[13.35.18.86], Open-Graph-Protocol[website], Script, Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Figma: The Collaborative Interface
 Design Tool], UncommonHeaders[x-amz-version-id,x-content-type-options,x-amz-cf-pop,alt-svc,x-amz-cf-id], Via-Proxy[1.1 b95596d6887b20449c59c2fc9d141c4a.cloudfront.net (CloudFront)], X-Frame-Options[SAMEORIGIN]
```

- **Wafw00f**

An open-source program called Wafw00f is used to identify and fingerprint Web application firewalls (WAFs). Web application firewalls (WAFs), security solutions, defend against SQL injection, cross-site scripting (XSS), and other attacks.

We can see that Cloudfront WAF is protecting figma.com.

```
┌──(tharusha㉿kali)-[~]
└─$ wafw00f figma.com

                    ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://figma.com
[+] The site https://figma.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

- **Using nmap, open port enumeration**

Open port enumeration is a method for locating and classifying the open network ports on a target machine or network using the Nmap (Network Mapper) program. Nmap is an effective open-source tool for network scanning and host discovery that provides extensive information on the services and statuses that are running on various ports. This process involves sending specially made packets to a target system and analyzing the responses in order to determine which ports are open and what services are using them.

Nmap is a popular tool for network administrators and security specialists to assess system security, identify potential security flaws, and enhance network configurations due to its abundance of features and versatility. It's a helpful tool for enhancing security and computer network administration in general.

```
┌──(tharusha㉿kali)-[~]
└─$ sudo nmap -sS figma.com
[sudo] password for tharusha:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 07:28 EDT
Nmap scan report for figma.com (13.35.18.115)
Host is up (0.016s latency).
Other addresses for figma.com (not scanned): 13.35.18.95 13.35.18.52 13.35.18.86
rDNS record for 13.35.18.115: server-13-35-18-115.sin5.r.cloudfront.net
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.39 seconds
┌──(tharusha㉿kali)-[~]
└─$ sudo nmap --script vuln figma.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 07:29 EDT
Nmap scan report for figma.com (13.35.18.115)
Host is up (0.017s latency).
Other addresses for figma.com (not scanned): 13.35.18.52 13.35.18.86 13.35.18.95
rDNS record for 13.35.18.115: 115.18.35.13.in-addr.arpa
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
443/tcp open  https
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.

Nmap done: 1 IP address (1 host up) scanned in 244.13 seconds
```

- **Using Nikto to scan for vulnerabilities**

One method to check for vulnerabilities in Kali Linux is to use the powerful open-source tool Nikto web scanner, which is part of the popular operating system for penetration testing and

ethical hacking. Nikto is specifically designed to identify and assess server and web application vulnerabilities.

When checking target web servers for known vulnerabilities, common security issues, and misconfigurations, Nikto can be used from the Kali Linux command line. Nikto searches for issues including outdated software, possibly unsafe scripts, security headers, and other online vulnerabilities. It helps ethical hackers and security professionals understand and reduce such threats by providing comprehensive information on the vulnerabilities discovered.

```
┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h figma.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 13.35.18.86, 13.35.18.95, 13.35.18.115, 13.35.18.52
+ Target IP:          13.35.18.86
+ Target Hostname:    figma.com
+ Target Port:        80
+ Start Time:         2024-05-09 07:34:45 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: Retrieved via header: 1.1 a0dab1619e09a1e6e84a759dfdfe7342.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Optio
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://develo
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
ing-content-type-header/
+ Root page / redirects to: https://figma.com/
^C

┌──(tharusha㉿kali)-[~]
└─$ sudo nikto -h 13.35.18.86
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          13.35.18.86
+ Target Hostname:    13.35.18.86
+ Target Port:        80
+ Start Time:         2024-05-09 07:35:02 (GMT-4)
---------------------------------------------------------------------------
+ Server: CloudFront
+ /: Retrieved via header: 1.1 6744df903aaebd8a225f5410dbe17efc.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Optio
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
ing-content-type-header/
+ All CGI directories 'found', use '-C none' to test none
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response
+ Scan terminated: 20 error(s) and 3 item(s) reported on remote host
+ End Time:           2024-05-09 07:55:42 (GMT-4) (1240 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Exploitation

I employed PWNXSS and SQLMAP tools to identify cross-site and SQL injection vulnerabilities in the target web application for the exploitations.

- **PwnXSS**

PwnXSS is a free and open-source application that may be found on GitHub. This program especially detects cross-site scripting. I execute several payloads in numerous web application directories while testing my target domain for XSS vulnerabilities. After the test, I discovered that indrive.com had no XSS vulnerabilities.

```
┌──(root㉿kali)-[/home/tharusha/PwnXSS]
└─# python3 pwnxss.py -u https://www.figma.com
{v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<<<< STARTING >>>>>>>

[12:18:44] [INFO] Starting PwnXSS ...
***************
[12:18:44] [INFO] Checking connection to: https://www.figma.com
[12:18:48] [INFO] Connection estabilished 200
[12:18:48] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:18:48] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>console.log(5000/3000)</script>
[12:18:48] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Econsole.log%285000%2F3000%29%3C%2Fscript%3E
[12:18:50] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:18:50] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:18:50] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>console.log(5000/3000)</script>
[12:18:50] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Econsole.log%285000%2F3000%29%3C%2Fscript%3E
[12:18:52] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:18:52] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:18:52] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>console.log(5000/3000)</script>
[12:18:52] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Econsole.log%285000%2F3000%29%3C%2Fscript%3E
[12:18:54] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:18:54] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:18:54] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>console.log(5000/3000)</script>
[12:18:54] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Econsole.log%285000%2F3000%29%3C%2Fscript%3E
[12:18:55] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:18:55] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:18:55] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>console.log(5000/3000)</script>
[12:18:55] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Econsole.log%285000%2F3000%29%3C%2Fscript%3E
[12:18:57] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:18:57] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:18:57] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>console.log(5000/3000)</script>
[12:18:57] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Econsole.log%285000%2F3000%29%3C%2Fscript%3E
[12:18:59] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:18:59] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:18:59] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>console.log(5000/3000)</script>
[12:18:59] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Econsole.log%285000%2F3000%29%3C%2Fscript%3E
[12:19:01] [INFO] Parameter page using (GET) payloads but not 100% yet ...
```

```
***************
[12:19:03] [INFO] Checking connection to: https://www.figma.com#main
[12:19:08] [INFO] Connection estabilished 200
[12:19:08] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:08] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>prompt(document.cookie)</script>
[12:19:08] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:10] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:10] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:10] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:10] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:12] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:12] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:12] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:12] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:14] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:14] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:14] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:14] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:15] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:15] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:15] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>prompt(document.cookie)</script>
[12:19:15] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:16] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:16] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:16] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:16] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:18] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:18] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:18] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:18] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:21] [INFO] Parameter page using (GET) payloads but not 100% yet ...
***************
[12:19:24] [INFO] Checking connection to: https://www.figma.com/
[12:19:28] [INFO] Connection estabilished 200
[12:19:28] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:28] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>prompt(document.cookie)</script>
[12:19:28] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:30] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:30] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:30] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:30] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:36] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:36] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:36] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:36] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:38] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:38] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:38] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:38] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
```

```
[12:19:36] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:36] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:36] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:38] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:38] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:38] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:38] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:39] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:39] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:39] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>prompt(document.cookie)</script>
[12:19:39] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:41] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:41] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:41] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:41] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:42] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:42] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:42] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:42] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:44] [INFO] Parameter page using (GET) payloads but not 100% yet ...
***************
[12:19:46] [INFO] Checking connection to: https://www.figma.com/#main
[12:19:49] [INFO] Connection estabilished 200
[12:19:49] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:49] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>prompt(document.cookie)</script>
[12:19:49] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:51] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:51] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:51] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:51] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:53] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:53] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:53] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:53] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:55] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:55] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:55] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:55] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:57] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:57] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:57] [INFO] Query (GET) : https://www.figma.com/login?locale=<script>prompt(document.cookie)</script>
[12:19:57] [INFO] Query (GET) : https://www.figma.com/login?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:19:59] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:19:59] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:19:59] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:19:59] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:20:00] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[12:20:00] [WARNING] Found link with query: locale=en-us Maybe a vuln XSS point
[12:20:00] [INFO] Query (GET) : https://www.figma.com/signup?locale=<script>prompt(document.cookie)</script>
[12:20:00] [INFO] Query (GET) : https://www.figma.com/signup?locale=%3Cscript%3Eprompt%28document.cookie%29%3C%2Fscript%3E
[12:20:02] [INFO] Parameter page using (GET) payloads but not 100% yet ...
```

- **SQLmap**

An open-source penetration testing tool called SQL Map automatically locates and takes advantage of SQL injection vulnerabilities to take over databases.

In an attempt to locate any web application injection points, I experimented with various payloads and parameters. I tested this application and discovered that it is not injectable.

```
┌──(root㉿kali)-[/home/tharusha]
└─# sqlmap -u https://www.figma.com/login?locale=en-us
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.2#stable}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
esponsible for any misuse or damage caused by this program

[*] starting @ 10:53:47 /2024-05-09/

[10:53:47] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('__Host-figma.did=MTcxNTI2NjQ...1T319FAf2Y;figma.session=BAh7B0kiD3N...71689bae4c'). Do you want to use those [Y/n] y
[10:53:53] [INFO] checking if the target is protected by some kind of WAF/IPS
[10:53:54] [INFO] testing if the target URL content is stable
[10:53:55] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected,
 manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] y
[10:53:58] [INFO] testing if GET parameter 'locale' is dynamic
[10:53:59] [WARNING] GET parameter 'locale' does not appear to be dynamic
[10:54:00] [WARNING] heuristic (basic) test shows that GET parameter 'locale' might not be injectable
[10:54:02] [INFO] testing for SQL injection on GET parameter 'locale'
[10:54:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[10:54:14] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[10:54:17] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[10:54:21] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[10:54:27] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[10:54:31] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[10:54:36] [INFO] testing 'Generic inline queries'
[10:54:37] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[10:54:40] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[10:54:43] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[10:54:47] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[10:54:51] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[10:54:55] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[10:54:59] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[10:55:06] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[10:55:14] [WARNING] GET parameter 'locale' does not seem to be injectable
[10:55:14] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there
d (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 10:55:14 /2024-05-09/
```

Vulnerabilities detect when Scanning

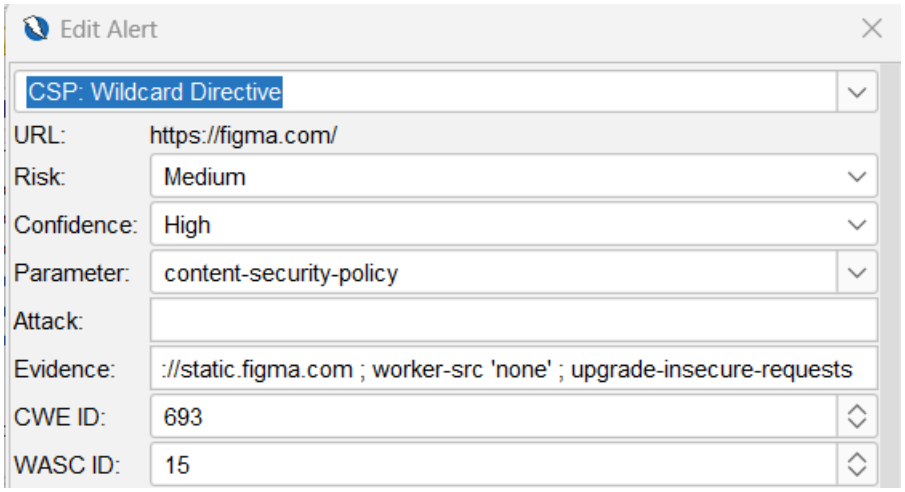
In order to process and find problems and vulnerabilities that are based on the OWASP top 10, I used tools like sub404, OWASP ZAP.

Sub 404 is used to test for attempted subdomain takeovers.

```
┌──(root㉿kali)-[/home/tharusha/PwnXSS/sub404]
└─# python3 sub404.py -d figma.com
                                    - By r3curs1v3_pr0xy

[-] Default http [use -p https]
[-] Gathering Information...
[-] Enumerating subdomains for figma.com
|[INF] Detected old /root/.config/subfinder/config.yaml config file, trying to migrate providers to /root/.config/subfinder/provider-config.yaml
[INF] Migration successful from /root/.config/subfinder/config.yaml to /root/.config/subfinder/provider-config.yaml.
[-] Total Unique Subdomain Found:  57
|[-] Getting URL's of 404 status code...
\[-] URL Checked: 57
[-] Checking CNAME records...

/home/tharusha/PwnXSS/sub404/sub404.py:246: DeprecationWarning: please use dns.resolver.resolve() instead
  resolve = dns.resolver.query(data.strip(), 'CNAME')

[-] verify.figma.com
    Not Vulnerable

[-] embed.figma.com
    Not Vulnerable

[-] us-west-2.staging.figma.com
    Not Vulnerable

[-] cors-image-proxy.figma.com
    Not Vulnerable

[-] slack.figma.com
    Not Vulnerable

[-] us-west-2.figma.com
    Not Vulnerable

[-] Vulnerability Possible on: click.figma.com
    CNAME: d16kdv7zgcta6p.cloudfront.net.
[*] Task Completed :)
```

OWASP ZAP is a testing tool that may be used to identify potential security gaps in internet applications. OWASP ZAP can be used to find common vulnerabilities such as SQL injection and cross-site scripting (XSS).

1. Vulnerability Title



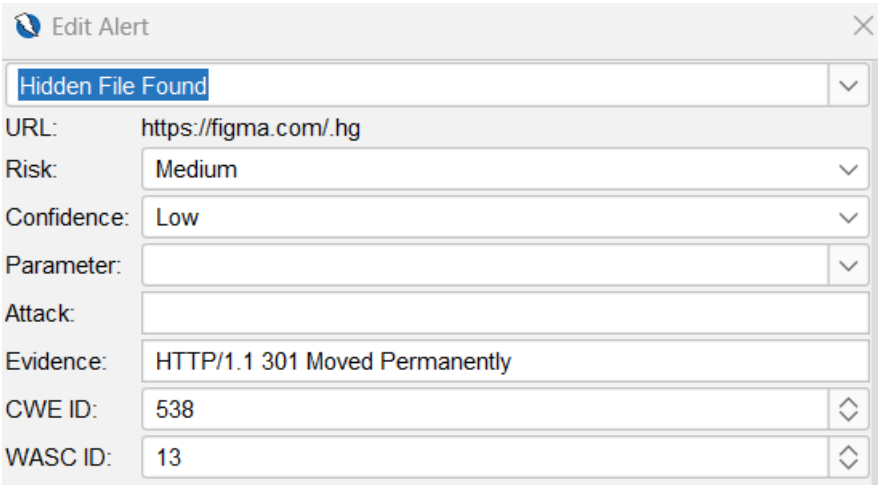
Vulnerability Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

How to mitigate

Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

2. Vulnerability Title



Vulnerability Description

A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.

How to mitigate

Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensuring access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.