Sri Lanka Institute of Information Technology

IE2062-Web Security

IT Number	Name
IT22581402	C.D.Aluthge

Information gathering and reconnaissance phase

a. Subdomain enumeration
    i. Recon-ng

b. Getting alive subdomains
    i. Nslookup
    ii. Sublist3r

c. DNS enumeration
    i. Dnsrecon
    ii. Nikto
    iii. Dnsdumper

d. Public devices enumeration
    i. Censys
    ii. Whois
    iii. Whatweb

e. Find WAF (web application firewall) protection.
    i. Wafwoof

f. Find open ports.
    i. Nmap

g. Exploitation
    i. sqlmap

vulnerability analysis phase

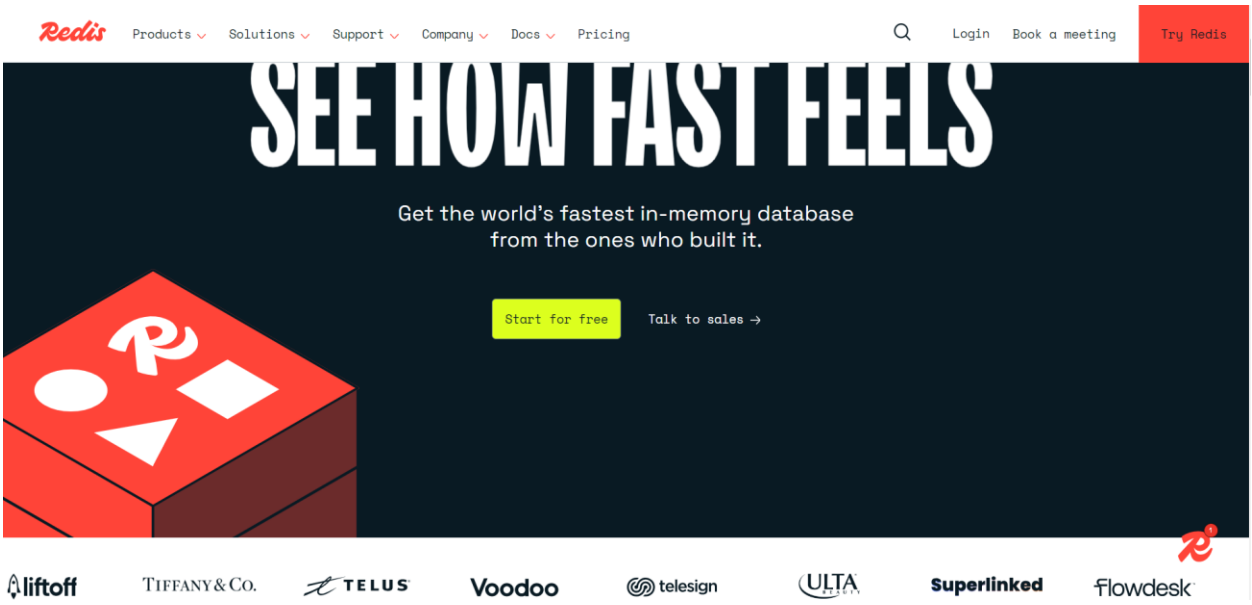
1. Target domain: http://redis.com

    a. Weak Ciphers Enabled (Confirmed)
    b. [Possible] Phishing by Navigating Browser Tabs
    c. Web Application Firewall Detected
    d. Unexpected Redirect Response Body (Too Large)
    e. Forbidden Resource
    f. Missing X-XSS-Protection Header

Conclusion

Scope:

Redis is the world’s fastest in-memory database. It provides cloud and on-prem solutions for caching, vector search, and NoSQL databases that seamlessly fit into any tech stack—making it simple for digital customers to build, scale, and deploy the fast apps our world runs on.



In Scope:

Asset name	Type	Coverage	Max. severity	Bounty	Last update	Resolved Reports
api.redislabs.com Amazon Web Services	Domain	In scope	Critical	Ineligible	Jan 25, 2022	0 (0%)
www.redislabs.com Imperva Incapsula WAF	Domain	In scope	Critical	Ineligible	Jan 25, 2022	3 (38%)
www.redis.com Imperva Incapsula WAF	Domain	In scope	Critical	Ineligible	Jan 25, 2022	2 (25%)
app.redislabs.com Imperva Incapsula WAF	Domain	In scope	Critical	Ineligible	Jan 25, 2022	4 (50%)

OWASP top 10 vulnerabilities

- Broken Access Control
- Cryptographic Failures

- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

Broken Access Control

When users are unable to adequately impose limitations on what they can access or do within a system, this is known as broken access control. This vulnerability makes it possible for unauthorized individuals to access private data or carry out tasks that shouldn't be permitted. Insecure references to objects, improperly configured permissions, and a lack of authentication checks are the causes of it. Because it can result in illegal data exposure, manipulation, or system penetration, it's a major problem.

Cryptographic Failures

Cryptographic collapses are the result of poor algorithms, incorrect implementations, or improper management of encryption keys, which compromise the security of information encrypted via encryption techniques. Undermining security safeguards and perhaps leading in data breaches, this can lead to unauthorized access to or exposure of sensitive data.

Injection

Injection: it is a type of security vulnerability in which untrusted data is sent to an interpreter as part of a command or query. Most often, attackers use this to inject malicious code into input fields, for example, login forms or search boxes. The interpreter then executes this code, which can give the attacker unauthorized access to data, alter the application's behavior, or gain full control over the system. There are many types of injections, such as SQL injection, where the attackers manipulate database queries, or cross-site scripting, where the malicious script is injected into a web page that other users view.

Insecure Design

Insecure design means the security flaws within the fundamental system or application design born out of insufficient attention to security at the design time. Consequently, systems have vulnerabilities that enable unauthorized system access or breaches. Examples are poor user authentication or no network segmentation. To fix insecure design, significant changes to the architecture are needed to develop the designs securely.

Security Misconfiguration

Imagine you accidentally leave your front door closed but not locked. That's what a security misconfiguration is like. Essentially, it's not properly securing your software systems, servers, or web applications. This can include default settings, shipped insecurely, or unnecessary features. Unauthorized users might target such

vulnerabilities to access your info or disrupt the operation. Therefore, one should monitor and update security measures continuously to avoid misconfiguration.

Vulnerable and Outdated Components

Vulnerable components are software elements that are known to contain security flaws that could be exploited by hackers. However, software components that have not received an upgrade in a long time are known as outdated components, and they may not include important security updates and bug fixes. In order to maintain a secure system environment, both sorts of components present security concerns and should be routinely updated and monitored.

Identification and Authentication Failures

When systems are unable to accurately confirm user identities or authenticate their access credentials, identification and authentication failures take place. Whereas authentication failures are caused by an inability to verify user identities, identification failures are the consequence of incorrect user recognition. In order to identify and fix system vulnerabilities, strong authentication procedures and frequent security assessments are essential. These failures might result in unauthorized access and security breaches.

Software and Data Integrity Failures

Software code or data accuracy, consistency, and reliability are jeopardized in software and data integrity issues. Data integrity problems are caused by mistakes, unauthorized access, or cyberattacks, whereas programming errors, malicious code, or unauthorized alterations are the causes of software integrity problems. To reduce risks and guarantee system security and dependability, preventive measures include backups, data encryption, access controls, and regular updates.

Security Logging and Monitoring Failures

Failed security logging and monitoring systems result in a delayed detection of security incidents and higher risks since they are unable to reliably capture and evaluate security-related events. Monitoring failures are caused by insufficient tools or response protocols, whereas logging failures are caused by misconfigurations or deactivated logging systems. Organizations should establish strong response protocols, use comprehensive logging practices, deploy efficient monitoring tools like SIEM tools, train security teams, and continuously improve logging and monitoring configurations in light of best practices and emerging threats in order to address these failures. By taking these steps, cybersecurity defenses are strengthened and the effects of security events are lessened.

Server-Side Request Forgery

A security flaw known as server-side request forgery (SSRF) allows attackers to take control of a susceptible server and send unwanted requests, usually to external or internal systems. Unauthorized access, data loss, and more exploitation may result from this. Input validation, whitelisting authorized resources, network segmentation, and access controls are all part of prevention. Frequent security testing improves overall system security by assisting in the identification and mitigation of SSRF threats.

Information gathering and reconnaissance phase.

The objective is to gather as much pertinent data as you can about the intended system or organization. Understanding the target's infrastructure, seeing potential vulnerabilities, and organizing additional security testing operations are all made easier with the aid of this information.

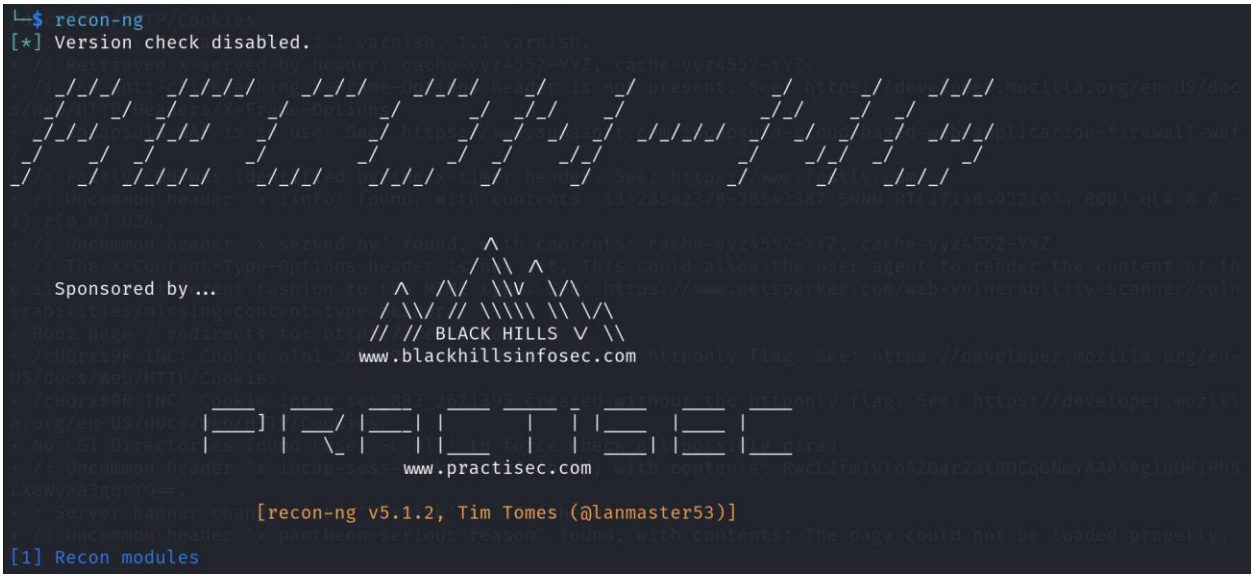
Domain: http://redis.com

Subdomain enumeration

- Recon-ng

Recon-ng is an open-source reconnaissance tool with Python foundation that is used for penetration testing and security evaluations. It collects data from domains, IPs, emails, and social media platforms using a modular framework with different modules. The advantages of recon-ng are its flexibility for scripting and automation, integration with many data sources, and data enrichment capabilities. It is used by security experts to gather and evaluate intelligence, spot possible weaknesses, and improve overall security posture during the first reconnaissance phase. Its vibrant community guarantees continuous upgrades and support, which makes it an invaluable addition to cybersecurity toolkits.

Proof of concept:



- To get google website give this command.

```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ...
+---------------------------------------------------------------------------------------+
|                Path                | Version |   Status  |  Updated   | D | K |
+---------------------------------------------------------------------------------------+
| recon/domains-hosts/google_site_web | 1.0     | installed | 2019-06-24 |   |   |
+---------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > show info
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|re
positories|vulnerabilities>
```

- You can see it’s not installed yet. We must download installation path.

```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ...
+---------------------------------------------------------------------------------------+
|                Path                | Version |   Status  |  Updated   | D | K |
+---------------------------------------------------------------------------------------+
| recon/domains-hosts/google_site_web | 1.0     | installed | 2019-06-24 |   |   |
+---------------------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

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

- After installing path using show info to see its download or not
- Load the installed module path and use info see options.
- Go to options and set source to our targeted domain indrive.com and run it.

```
[recon-ng][default][google_site_web] > info

    Name: Google Hostname Enumerator
  Author: Tim Tomes (@lanmaster53)
 Version: 1.0

Description:
  Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
  the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  clubhouse.com  yes       source of input (see 'info' for details)

Source Options:
  default       SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>      string representing a single input
  <path>        path to a file containing a list of inputs
  query <sql>   database query returning one column of inputs

[recon-ng][default][google_site_web] > options set source redis.com
SOURCE => redis.com
[recon-ng][default][google_site_web] > run
```

Proof of concept:

```
----------
REDIS.COM
----------
[*] Searching Google for: site:redis.com
[*] Country: None
[*] Host: oss.redis.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------
[*] Country: None
[*] Host: developer.redis.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------
```

```
[*] ---------------------------------------------------------
[*] Country: None
[*] Host: trust.redis.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------------
[*] Country: None
[*] Host: university.redis.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------------
[*] Country: None
[*] Host: docs.redis.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------------
```

Proof of concept:

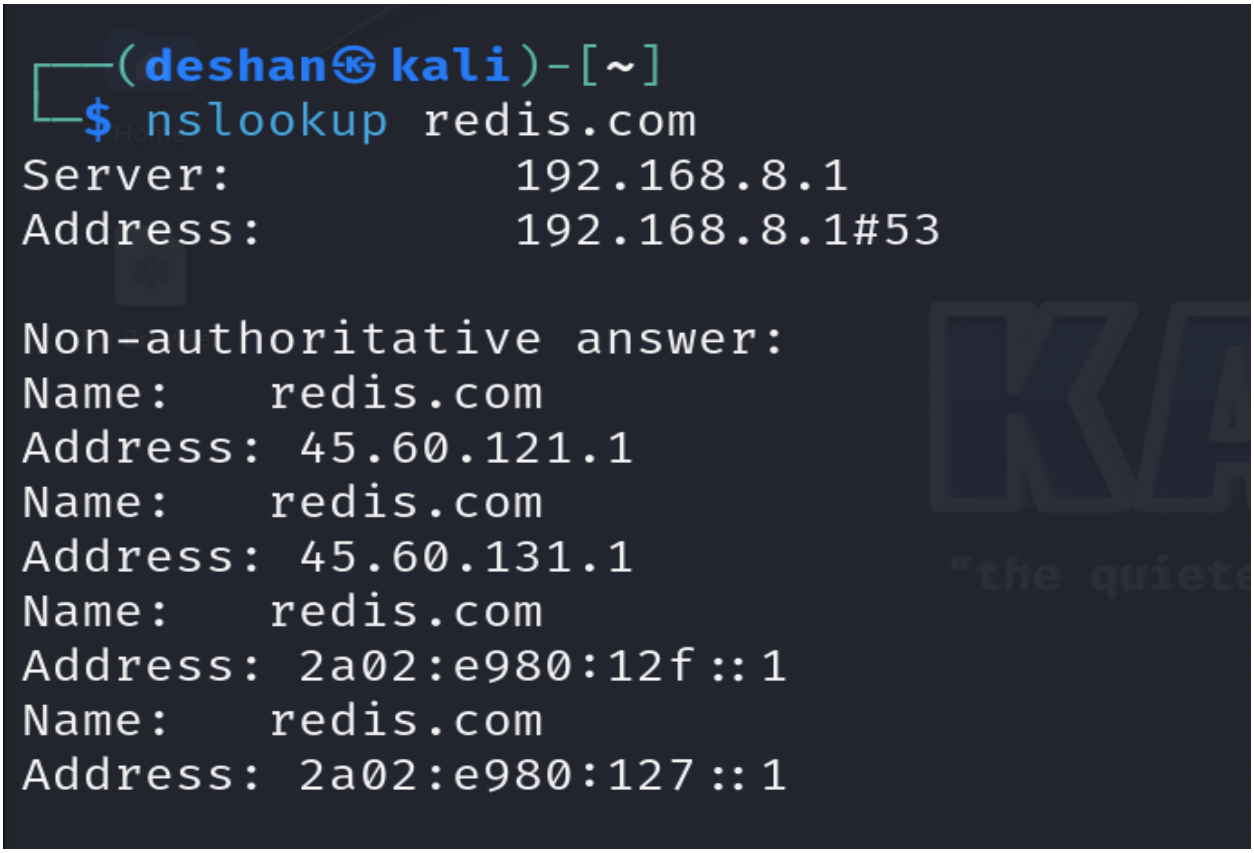
```
---------
SUMMARY
---------
[*] 6 total (6 new) hosts found.
[recon-ng][default][google_site_web] >
```

Getting alive subdomains

- Nslookup

A command-line utility called `nslookup` is used to query DNS (Domain Name System) servers and get DNS-related data. In addition to performing reverse DNS lookups and retrieving other DNS records like A, AAAA, MX, NS, PTR, and TXT records, it resolves domain names to IP addresses. It is flexible for diagnosing DNS problems, validating DNS configurations, and testing DNS servers because it may be used in both interactive and non-interactive modes. Network administrators and cybersecurity experts frequently utilize `nslookup`, which runs on several platforms, for DNS-related activities and diagnostics.

Proof of concept:

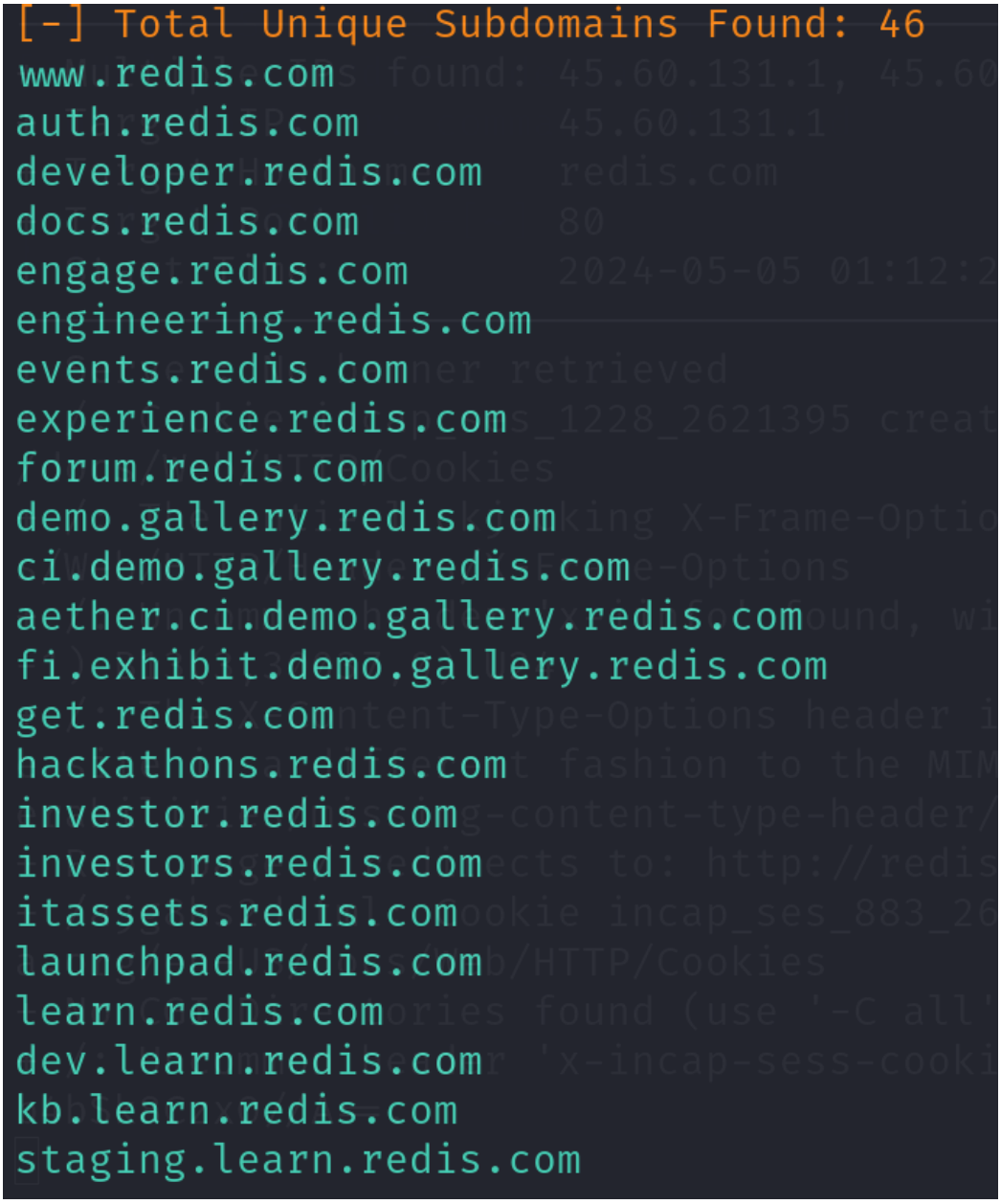


- Sublist3r

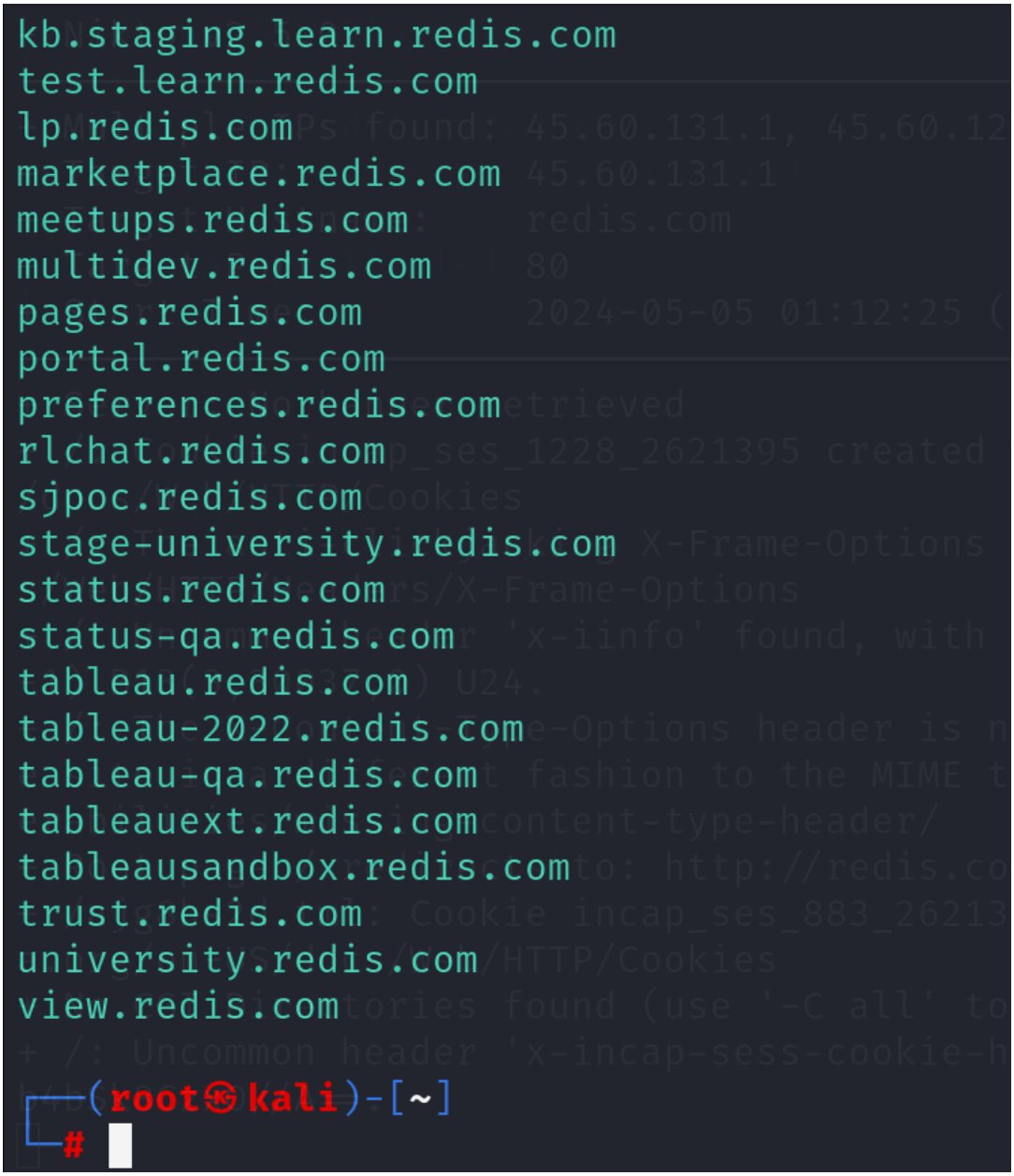
Sublist3r is an open-source subdomain enumeration tool used in cybersecurity for reconnaissance purposes. It assists security professionals, penetration testers, and researchers in identifying valid subdomains associated with a target domain. The tool employs various methods including passive search through search engine results, active search via DNS queries, and brute-force techniques using wordlists to enumerate subdomains. Sublist3r supports output in multiple formats, making it versatile for integration with other tools and workflows. It is valuable in expanding the attack surface during security assessments but should be used responsibly and with proper authorization.

Proof of concept:

Proof of concept:



Proof of concept:

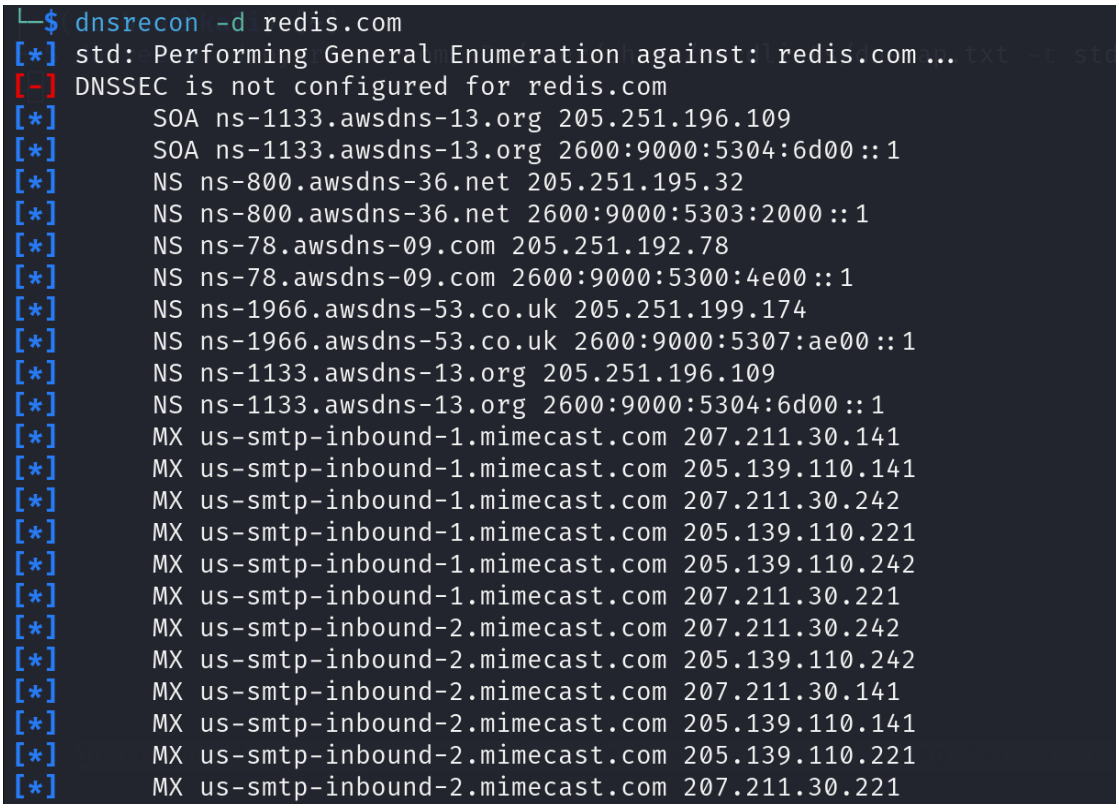


DNS enumeration

- Dnsrecon

For security evaluations and penetration tests, DNSRecon is a powerful open-source tool for DNS reconnaissance that finds and counts DNS information. It is particularly good at finding subdomains, enumerating DNS records (A, AAAA, MX, NS, SOA, TXT), transferring DNS zones, and it can handle wordlist-based and brute-force attacks. With its automation, customization, and integration features, it's a useful tool for figuring out possible attack points, comprehending target infrastructure, and raising security awareness in general. DNSRecon is still a dependable option for DNS reconnaissance operations because of its community support and frequent updates.

Proof of concept:



Proof of concept:

```
[*] A redis.com 45.60.121.1
[*] A redis.com 45.60.131.1
[*] AAAA redis.com 2a02:e980:127::1
[*] AAAA redis.com 2a02:e980:12f::1
[*] TXT redis.com adobe-idp-site-verification=9a542dfe12f7fa2f32e48f82d1f3102c8f0480593d7c4e86de87400ee28
a68ad
[*] TXT redis.com wiz-domain-verification=5b6d27936dad4ce78788e70551307cffb3bdd77439291e76f154d3ddb41889f
7
[*] TXT redis.com status-page-domain-verification=t0y77fhm0qxl
[*] TXT redis.com OSSRH-72625
[*] TXT redis.com cisco-ci-domain-verification=14ec584a2413dd46b812e40bc3e923f2e122e69ccbaeaa0f0fe72fa91b
0d8094
[*] TXT redis.com docker-verification=1af20237-aacc-4c0a-8407-63a631301dc6
[*] TXT redis.com google-site-verification=hBCBFPG_4AWxXoFNVwkDZXklO3H6JrJba_lQKUl7sWc
[*] TXT redis.com globalsign-domain-verification=146F0FB14B2DFCFFF0C36E1E38EA38BF
[*] TXT redis.com google-site-verification=qLAgvo7_FSyHKTVHzvdtIfPDy7h8UVNb7HEWwnMXO7g
[*] TXT redis.com cloudflare-verify=419497658-446892919
[*] TXT redis.com docusign=3bad2123-5e60-4d30-b251-86624093ab85
[*] TXT redis.com 0ed1fe018a613ced461c7a4efeb808271b5a3b8a28
[*] TXT redis.com 11685988
[*] TXT redis.com 65A45059C6
[*] TXT redis.com h1-domain-verification=Gips7g7xihVrM51jVnDiRSTQsYPtMvNsiJzFQQhbNSU2AJTK
[*] TXT redis.com pendo-domain-verification=01cf7947-b3c9-41c6-b549-d076113c33e5
```

Proof of concept:

```
[*] TXT redis.com ZOOM_verify_tjfgNVoFwP3m9yW0EhW0ok
[*] TXT redis.com MS=ms98161846
[*] TXT redis.com airtable-verification=afa3201f7f4d3fdfda5c37c212c75d22
[*] TXT redis.com h1-domain-verification=Da7tCSAXUU3pYzU13h1MrcHbA7fGeV2qHGMNZKHKddDXtuPg
[*] TXT redis.com canva-site-verification=VqW-oHHgEUICHFnx7uXsKQ
[*] TXT redis.com atlassian-domain-verification=l9AJIQnEUwoU3JUWAChOYu3jc+gW8Yb3eltC+BW8M2s5UK5hsURpwkrFZ
NL6pUSu
[*] TXT redis.com google-site-verification=XPtqNr9exy_762P70-2pt43U9918KUzRPmG6wVqxoNQ
[*] TXT redis.com drift-domain-verification=5fafa5e7d17f555701539cf2d20c40bebd5a3f37aa5b09fa6fda785fd2f9f
bf9
[*] TXT redis.com v=spf1 include:_spf.google.com include:mktomail.com include:sendgrid.net include:us._ne
tblocks.mimecast.com include:stspg-customer.com include:spf.mandrillapp.com ~all
[*] TXT _dmarc.redis.com v=DMARC1; p=quarantine; rua=mailto:0a0e5042@mxtoolbox.dmarc-report.com,mailto:dm
arc-rua@redis.com; ruf=mailto:0a0e5042@forensics.dmarc-report.com,mailto:dmarc-ruf@redis.com; adkim=r; aspf=r;
 fo=0:1:d:s; pct=100
[*] Enumerating SRV Records
[-] No SRV Records Found for redis.com
```

- Dnsdumper

DNSDumpster is an online tool focused on DNS information gathering for a target domain. It assists in discovering subdomains, viewing DNS records (A, AAAA, MX, NS, SOA, TXT), mapping domain names to IP addresses, and providing visual representations of DNS-related data. Security professionals and penetration testers use DNSDumpster during reconnaissance to understand a domain's infrastructure,

identify potential vulnerabilities, and aid in security assessments. While it offers valuable insights, users should supplement its findings with other tools for a comprehensive analysis, considering that its data may not always be the most current or complete.

- **Proof of concept:**

- **Proof of concept:**

DNS Servers

ns-1133.awsdns-13.org.	205.251.196.109	AMAZON-02 United States
ns-1966.awsdns-53.co.uk.	205.251.199.174	AMAZON-02 United States
ns-78.awsdns-09.com.	205.251.192.78	AMAZON-02 United States
ns-800.awsdns-36.net.	205.251.195.32	AMAZON-02 United States

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

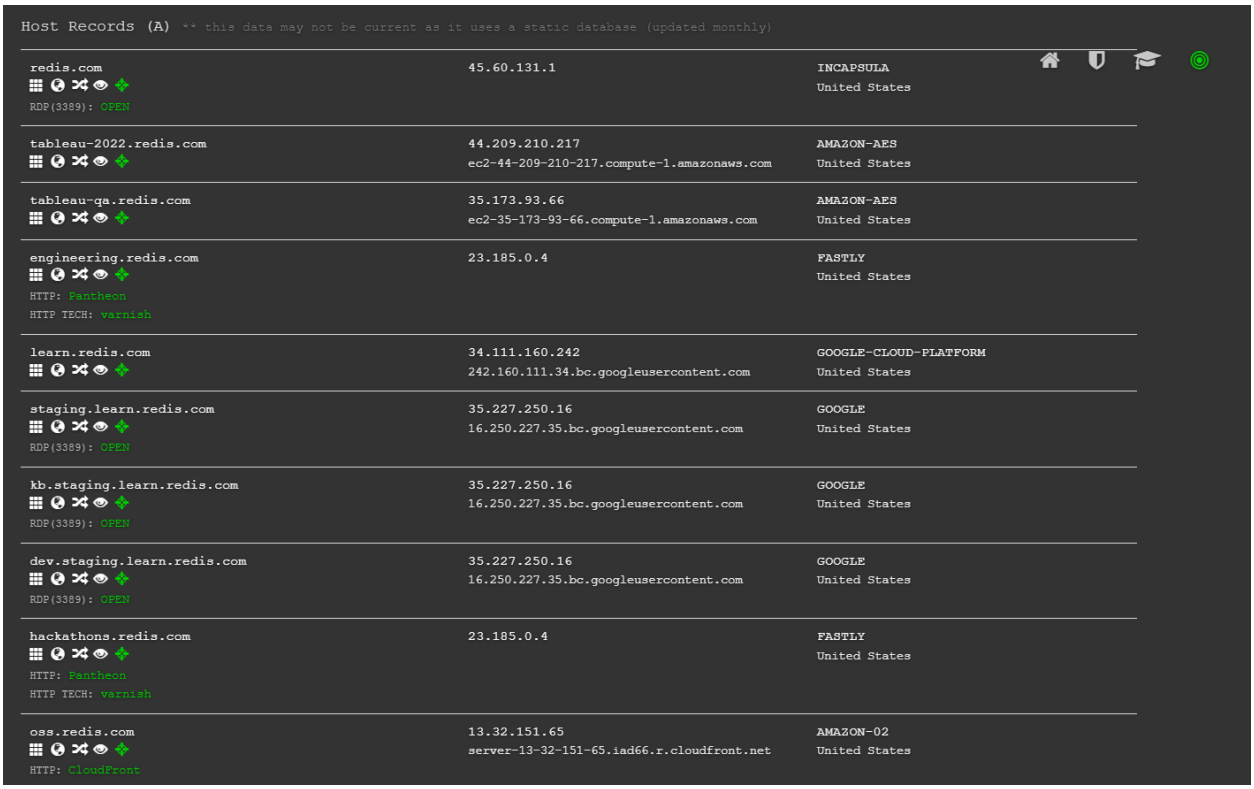
10 us-smtp-inbound-1.mimecast.com.	205.139.110.242	MIMECAST- United States
10 us-smtp-inbound-2.mimecast.com.	205.139.110.242	MIMECAST- United States

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

```
"0ed1fe018a613ced461c7a4efeb808271b5a3b8a28"
"11685988"
"65A45059C6"
"MS=ms98161846"
"OSSRH-72625"
"ZOOM_verify_tjfgNVoFwP3m9yW0EhW0ok"
"adobe-idp-site-verification=9a542dfe12f7fa2f32e48f82d1f3102c8f0480593d7c4e86de87400ee28a68ad"
"airtable-verification=afa3201f7f4d3fdfda5c37c212c75d22"
"atlassian-domain-verification=l9AJIQnEUwoU3JUWAChOYu3jc+gW8Yb3eltC+BW8M2s5UK5hsURpwkrF2NL6pUSu"
"canva-site-verification=VqW-oHHgEUICHFnx7uXsKQ"
"cisco-ci-domain-verification=14ec584a2413dd46b812e40bc3e923f2e122e69ccbaeaa0f0fe72fa91b0d8094"
"cloudflare-verify=419497658-446892919"
"docker-verification=1af20237-aacc-4c0a-8407-63a631301dc6"
"docusign=3bad2123-5e60-4d30-b251-86624093ab85"
"drift-domain-verification=5fafa5e7d17f555701539cf2d20c40bebd5a3f37aa5b09fa6fda785fd2f9fbf9"
"globalsign-domain-verification=146F0FB14B2DFCFFF0C36E1E38EA38BF"
"google-site-verification=XPtqNr9exy_762P70-2pt43U9918KUzRPmG6wVqxoNQ"
"google-site-verification=hBCBFPG_4AWxXoFNVwkD2XklO3H6JrJba_lQKUl7sWc"
"google-site-verification=qLAgvo7_FSyHKTVHzvdtIfPDy7h8UVNb7HEWwnMXO7g"
```

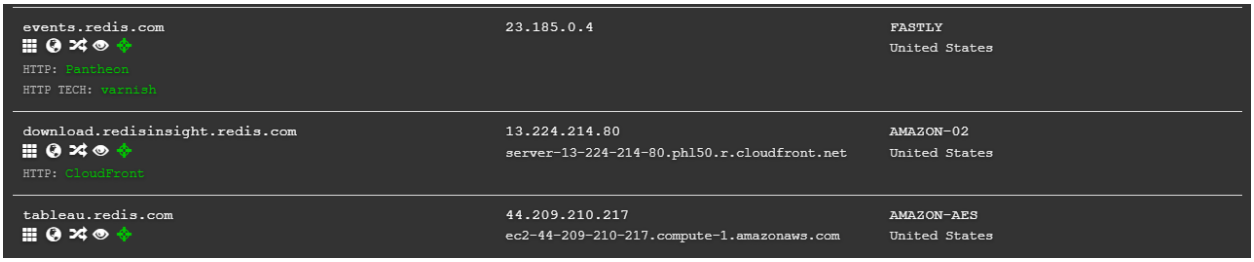
- **Proof of concept:**

```
"h1-domain-verification=Gips7g7xihVrM51jVnDiRSTQsYPtMwNsiJzFQQhbNSU2AJTK"
"pendo-domain-verification=01cf7947-b3c9-41c6-b549-d076113c33e5"
"status-page-domain-verification=t0y77fhm0qxl"
"v=spf1 include:_spf.google.com include:mktomail.com include:sendgrid.net include:us._netblocks.mimecast.com include:stspg-customer.com
include:spf.mandrillapp.com ~all "
"wiz-domain-verification=5b6d27936dad4ce78788e70551307cffb3bdd77439291e76f154d3ddb41889f7"
```



Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

redis.com RDP(3389): OPEN	45.60.131.1	INCAPSULA United States
tableau-2022.redis.com	44.209.210.217 ec2-44-209-210-217.compute-1.amazonaws.com	AMAZON-AES United States
tableau-qa.redis.com	35.173.93.66 ec2-35-173-93-66.compute-1.amazonaws.com	AMAZON-AES United States
engineering.redis.com HTTP: Pantheon HTTP TECH: varnish	23.185.0.4	FASTLY United States
learn.redis.com	34.111.160.242 242.160.111.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM United States
staging.learn.redis.com RDP(3389): OPEN	35.227.250.16 16.250.227.35.bc.googleusercontent.com	GOOGLE United States
kb.staging.learn.redis.com RDP(3389): OPEN	35.227.250.16 16.250.227.35.bc.googleusercontent.com	GOOGLE United States
dev.staging.learn.redis.com RDP(3389): OPEN	35.227.250.16 16.250.227.35.bc.googleusercontent.com	GOOGLE United States
hackathons.redis.com HTTP: Pantheon HTTP TECH: varnish	23.185.0.4	FASTLY United States
oss.redis.com HTTP: CloudFront	13.32.151.65 server-13-32-151-65.iad66.r.cloudfront.net	AMAZON-02 United States



events.redis.com HTTP: Pantheon HTTP TECH: varnish	23.185.0.4	FASTLY United States
download.redisinsight.redis.com HTTP: CloudFront	13.224.214.80 server-13-224-214-80.phl50.r.cloudfront.net	AMAZON-02 United States
tableau.redis.com	44.209.210.217 ec2-44-209-210-217.compute-1.amazonaws.com	AMAZON-AES United States

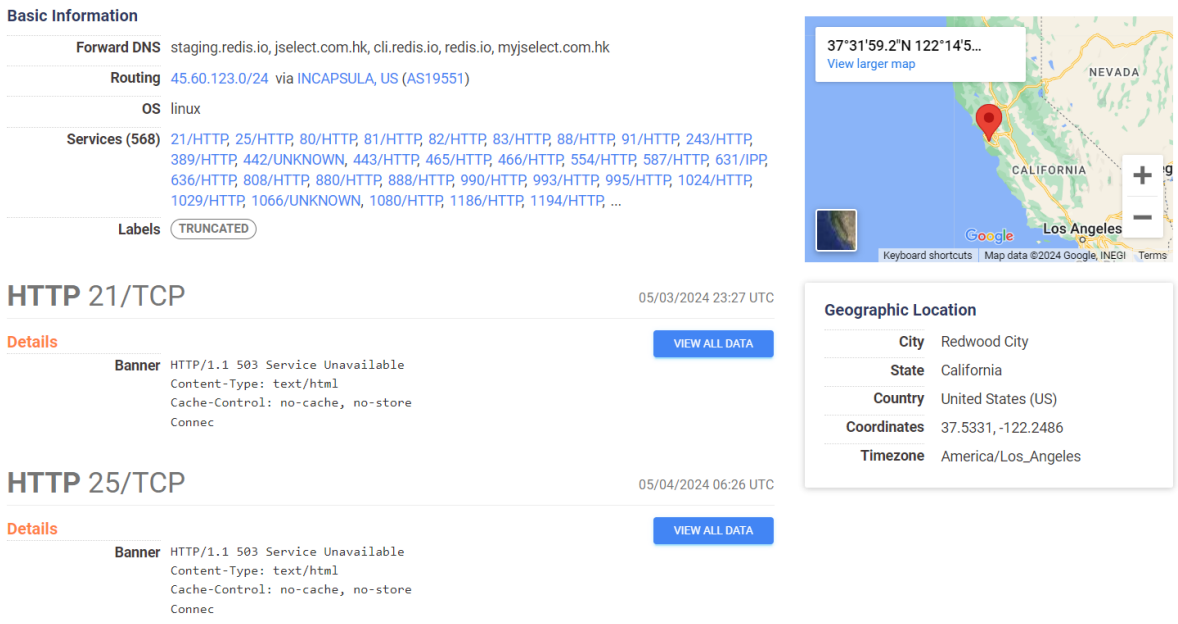
Public devices enumeration

- Censys

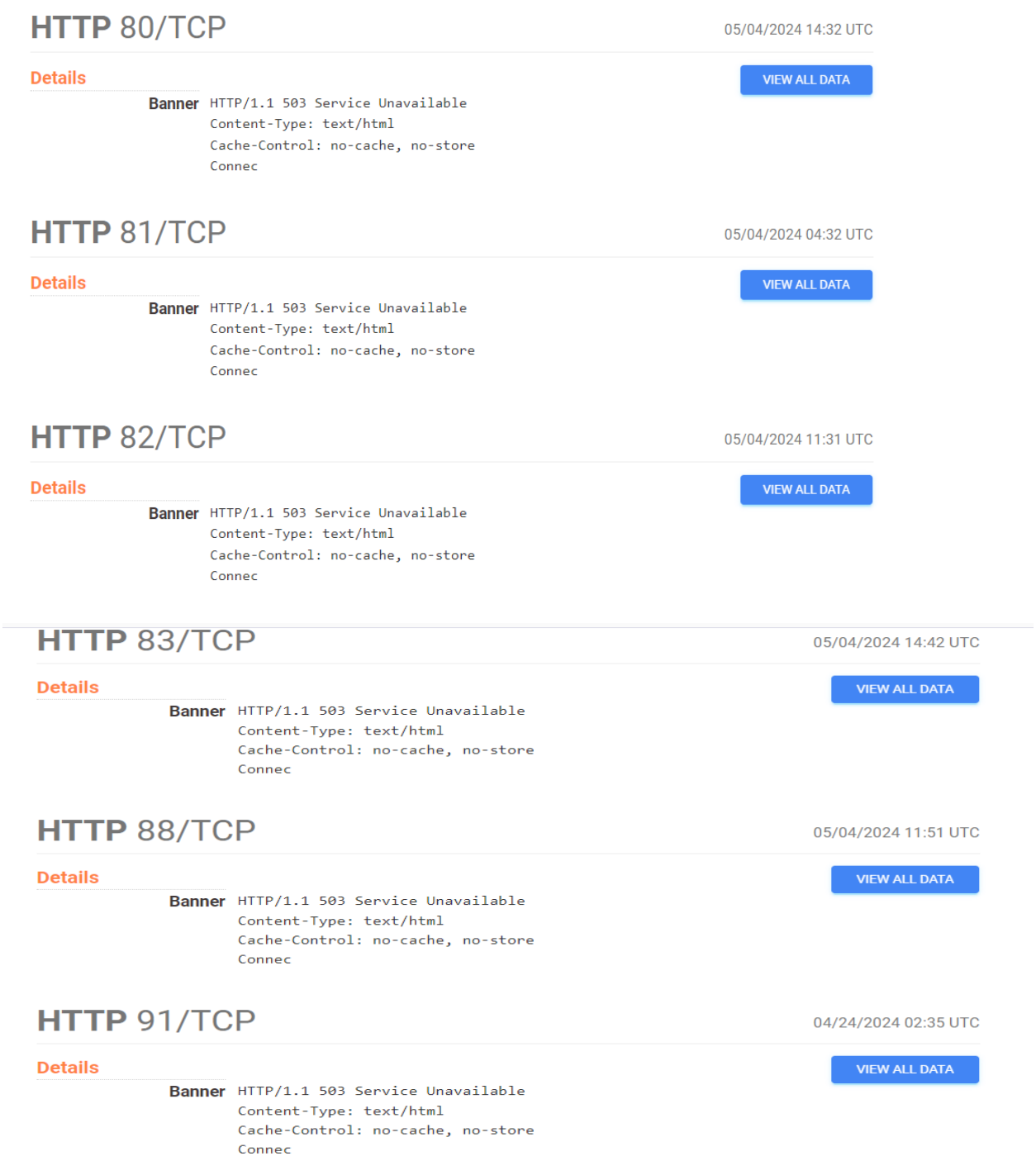
Censys is a potent internet scanning tool that scans and monitors devices, networks, and services online all the time. It performs thorough scans, keeps track of SSL/TLS certificates, keeps an eye on attack surfaces, finds vulnerabilities, and offers threat information. Large volumes of data may

be searched and analyzed, processes can be automated with the help of the API, and Censys can be integrated into security workflows. In the connected digital world of today, Censys is useful for asset discovery, vulnerability management, compliance monitoring, and proactive risk reduction.

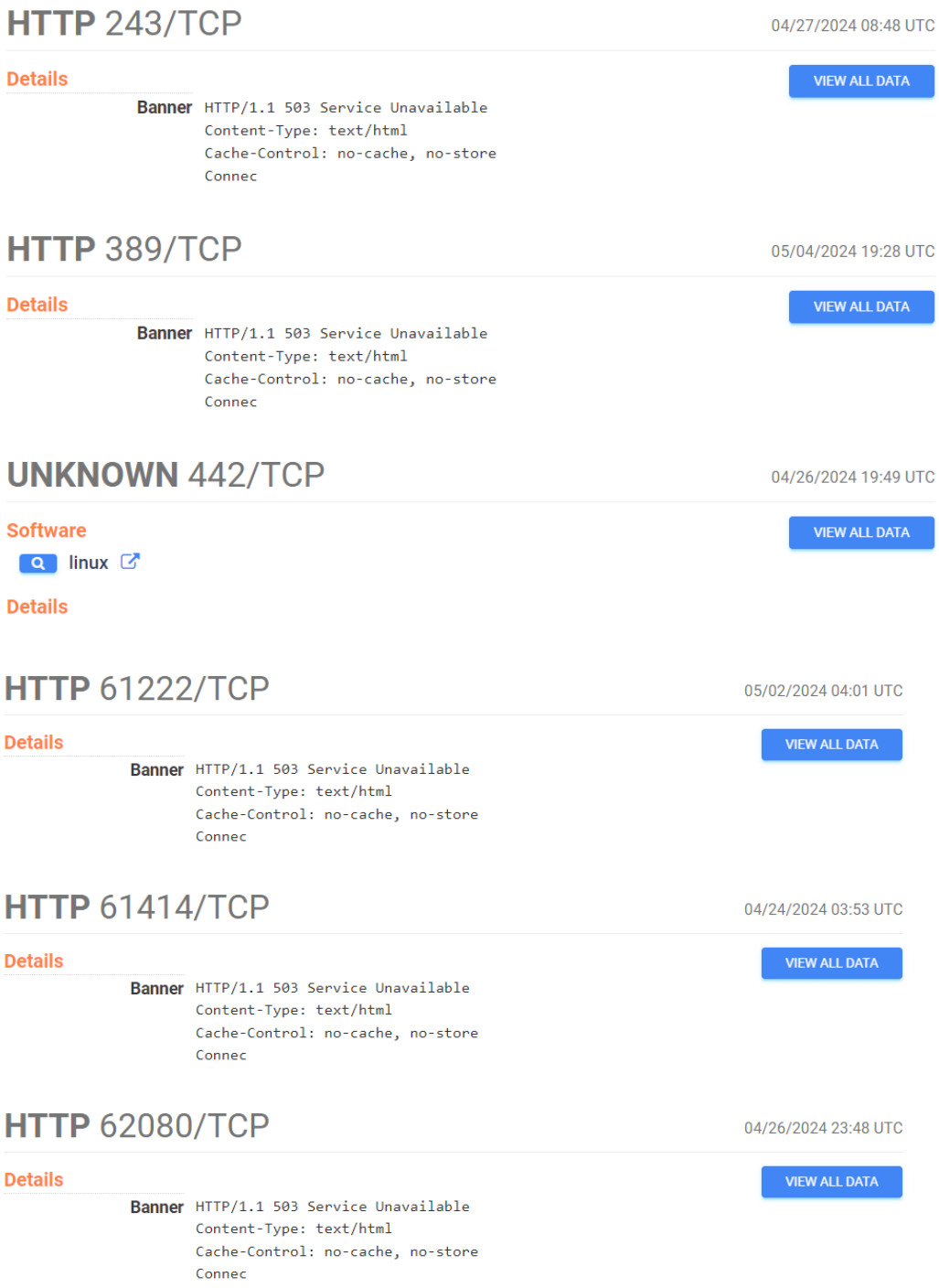
- **Proof of concept:**



- **Proof of concept:**



- **Proof of concept:**



- Whois

A key networking tool and protocol, whois is used to query databases and obtain data on IP addresses, domain names, and autonomous system numbers (ASNs). It offers information about domain registration, owner contact details, DNS

information, IP address allocation, and ASN ownership. Whois is frequently used for domain research, network problems, IP geolocation, abuse investigations, and domain registration questions by network administrators, cybersecurity experts, domain registrars, and law enforcement organizations. Due to privacy concerns, registrars have started offering privacy services that conceal personal information from view in public Whois data. While Whois provides insightful information, users should be aware of potential limits across multiple Whois servers, privacy concerns, and data accuracy.

- **Proof of concept:**

```
└─# whois redis.com
   Domain Name: REDIS.COM
   Registry Domain ID: 2888963_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.name.com
   Registrar URL: http://www.name.com
   Updated Date: 2024-02-03T19:20:22Z
   Creation Date: 1996-02-24T05:00:00Z
   Registry Expiry Date: 2025-02-25T05:00:00Z
   Registrar: Name.com, Inc.
   Registrar IANA ID: 625
   Registrar Abuse Contact Email: abuse@name.com
   Registrar Abuse Contact Phone: 7202492374
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Name Server: NS-1133.AWSDNS-13.ORG
   Name Server: NS-1966.AWSDNS-53.CO.UK
   Name Server: NS-78.AWSDNS-09.COM
   Name Server: NS-800.AWSDNS-36.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-04T20:28:45Z <<<
```

- **Proof of concept:**

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

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
```

```
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.
```

- **Proof of concept:**

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: REDIS.COM
Registry Domain ID: 2888963_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.name.com
Registrar URL: http://www.name.com
Updated Date: 2024-02-03T19:20:22Z
Creation Date: 1996-02-24T05:00:00Z
Registrar Registration Expiration Date: 2025-02-25T05:00:00Z
Registrar: Name.com, Inc.
Registrar IANA ID: 625
Reseller:
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Redacted For Privacy
Registrant Organization: Domain Protection Services, Inc.
Registrant Street: PO Box 1769
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072
```

```
Registrant Fax: +1.7209758725
Registrant Email: https://www.name.com/contact-domain-whois/redis.com
Registry Admin ID: Not Available From Registry
Admin Name: Redacted For Privacy
Admin Organization: Domain Protection Services, Inc.
Admin Street: PO Box 1769
Admin City: Denver
Admin State/Province: CO
Admin Postal Code: 80201
Admin Country: US
Admin Phone: +1.7208009072
Admin Fax: +1.7209758725
Admin Email: https://www.name.com/contact-domain-whois/redis.com
Registry Tech ID: Not Available From Registry
Tech Name: Redacted For Privacy
Tech Organization: Domain Protection Services, Inc.
Tech Street: PO Box 1769
Tech City: Denver
Tech State/Province: CO
Tech Postal Code: 80201
Tech Country: US
Tech Phone: +1.7208009072
Tech Fax: +1.7209758725
Tech Email: https://www.name.com/contact-domain-whois/redis.com
```

- **Proof of concept:**

```
Tech Email: https://www.name.com/contact-domain-whois/redis.com
Name Server: ns-1133.awsdns-13.org
Name Server: ns-78.awsdns-09.com
Name Server: ns-1966.awsdns-53.co.uk
Name Server: ns-800.awsdns-36.net
DNSSEC: unSigned
Registrar Abuse Contact Email: abuse@name.com
Registrar Abuse Contact Phone: +1.7203101849
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-05-04T20:29:07Z <<<

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

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

The data in the Name.com, Inc. WHOIS database is provided by Name.com, Inc. for information purposes, and to a
ssist persons in obtaining information about or related to a domain name registration record. Name.com, Inc. d
oes not guarantee its accuracy.  Users accessing the Name.com, Inc. WHOIS service agree to use the data only f
or lawful purposes, and under no circumstances may this data be used to: a) allow, enable, or otherwise suppor
t the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitat
ions to entities other than the registrar's own existing customers and b) enable high volume, automated, elect
ronic processes that send queries or data to the systems of Name.com, Inc., except as reasonably necessary to
register domain names or modify existing registrations. When using the Name.com, Inc. WHOIS service, please co
nsider the following: the WHOIS service is not a replacement for standard EPP commands to the SRS service. WHO
IS is not considered authoritative for registered domain objects. The WHOIS service may be scheduled for downt
ime during production or OT&E maintenance periods. Where applicable, the presence of a [Non-Public Data] tag i
ndicates that such data is not made publicly available due to applicable data privacy laws or requirements.  A
ccess to non-public data may be provided, upon request, where it can be reasonably confirmed that the requeste
r holds a specific legitimate interest and a proper legal basis, for accessing the withheld data. Access to th
is data can be requested by submitting a request via the form found at https://www.name.com/layered-access-req
uest . Name.com, Inc. reserves the right to modify these terms at any time. By submitting this query, you agre
e to abide by this policy.
```

- Whatweb

WhatWeb is a powerful open-source website scanner that specializes in identifying the technologies utilized by websites. It excels in detecting web servers, frameworks, content management systems (CMS), programming languages, and more through its fingerprinting and HTTP header analysis capabilities. Security professionals leverage WhatWeb during reconnaissance and vulnerability assessments to gather insights into target websites' technology stacks, assess security risks associated with detected technologies, and identify potential vulnerabilities or outdated components. Its scriptable and customizable nature, along with integration options, makes it a valuable tool for automating scanning workflows and enhancing security assessments.

- **Proof of concept:**

```
┌──(root㉿kali)-[~]
└─# whatweb redis.com
http://redis.com [302 Found] Cookies[incap_ses_883_2621395,visid_incap_2621395], Country[RESERVED][ZZ], HttpOn
ly[visid_incap_2621395], IP[45.60.131.1], Incapsula-WAF, RedirectLocation[http://redis.com/], Title[Loading],
UncommonHeaders[x-iinfo]
```

Find WAF (web application firewall) protection.

- Wafwoof

Wafw00f is an open-source program that uses content patterns, HTTP responses, and header analysis to detect and fingerprint web application firewalls (WAFs). It gives testers and security experts information about the particular WAF technology or vendor being used as well as assists them in determining whether a web application is protected by a WAF. In addition to being user-friendly and seamlessly integrating with automated testing workflows, Wafw00f also keeps an updated database of WAF signatures and offers community support. It is a useful tool for security assessment and reconnaissance jobs, supporting the creation of efficient testing plans and workarounds.

Proof of concept:

```
┌──(root㉿kali)-[~]
└─# wafw00f redis.com
                    ______
                   /      \
                  (  Woof!  )
                   \  ____/
                   ,,
              .-.  |
             ()``; |==|  _______)
             /  ('  /|\
            /  )   / | \
           /_)_))    /  |  \

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

[*] Checking https://redis.com
[+] The site https://redis.com is behind Incapsula (Imperva Inc.) WAF.
[~] Number of requests: 2
```

Find open ports.

- Nmap

Nmap, sometimes known as "Network Mapper," is a potent open-source network scanning program used for vulnerability analysis, security audits, and network discovery. It is particularly good at operating system detection, host discovery, port scanning, and service version detection. Because it supports custom scripting and automation, Nmap's scripting engine (NSE) is adaptable to a wide range of security activities and integration requirements. Because of its dependability, adaptability, and large feature set, network administrators, security experts, and penetration testers frequently use it for network reconnaissance, security audits, and network monitoring.

Proof of concept:

Proof of concept:

```
|   X-Iinfo: 2-14024673-0 0NNN RT(1714855501322 685) q(0 -1 -1 -1) r(0 -1)
|   <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=27&xinfo=2-14024673-0%200NNN%20RT%281714855501322%20685%29%20q%280%20-1%20-1%20-1%29%20r%
280%20-1%29&incident_id=0-67600006475679954&edet=9&cinfo=ffffffff&rpinfo=0&mth=GET" frameborder=0 width="100%"
height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-6760000647567
7954</iframe></body></html>
|   HTTPOptions:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
|     Content-Length: 691
|     X-Iinfo: 3-17209138-0 0NNN RT(1714855502739 505) q(0 -1 -1 -1) r(0 -1)
|_    <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=27&xinfo=3-17209138-0%200NNN%20RT%281714855502739%20505%29%20q%280%20-1%20-1%20-1%29%20r%
280%20-1%29&incident_id=0-8130172094906339&edet=9&cinfo=ffffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="10
0%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-813017209
49063939</iframe></body></html>
```

```
25/tcp    open  smtp?
|_smtp-commands: SMTP EHLO redis.com: failed to receive data: connection closed
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
|     452 syntax error (connecting)
|     many errors
|   Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|_    452 syntax error (connecting)
37/tcp    open  ssl/time?
| ssl-cert: Subject: commonName=imperva.com
| Subject Alternative Name: DNS:app-gcp.redislabs.com, DNS:cli.redis.io, DNS:www.redis.com, DNS:*.redis.com, DN
S:redis.io, DNS:staging.redis.io, DNS:redis.com, DNS:try.redis.io, DNS:*.redislabs.com, DNS:download.redis.io,
DNS:imperva.com, DNS:www.redis.io
| Not valid before: 2024-04-22T21:11:57
|_Not valid after:  2024-10-19T21:11:57
| tls-nextprotoneg:
|_  http/1.1
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
```

Proof of concept:

```
25/tcp    open  smtp?
|_smtp-commands: SMTP EHLO redis.com: failed to receive data: connection closed
| fingerprint-strings:
|   FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
|     452 syntax error (connecting)
|     many errors
|   Hello, Help, Kerberos, LPDString, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
|_    452 syntax error (connecting)
37/tcp    open  ssl/time?
| ssl-cert: Subject: commonName=imperva.com
| Subject Alternative Name: DNS:app-gcp.redislabs.com, DNS:cli.redis.io, DNS:www.redis.com, DNS:*.redis.com, DN
S:redis.io, DNS:staging.redis.io, DNS:redis.com, DNS:try.redis.io, DNS:*.redislabs.com, DNS:download.redis.io,
DNS:imperva.com, DNS:www.redis.io
| Not valid before: 2024-04-22T21:11:57
|_Not valid after:  2024-10-19T21:11:57
| tls-nextprotoneg:
|_  http/1.1
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
```

```
|     Content-Length: 690
|     X-Iinfo: 14-24435125-0 0NNN RT(1714855501537 443) q(0 -1 -1 -1) r(0 -1)
|     <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=27&xinfo=14-24435125-0%200NNN%20RT%281714855501537%20443%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29&incident_id=0-114090879971229966&edet=9&cinfo=ffffffff&rpinfo=0&mth=GET" frameborder=0 width="100%
" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-11409087997
1229966</iframe></body></html>
|   HTTPOptions:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
|     Content-Length: 694
|     X-Iinfo: 12-24348054-0 0NNN RT(1714855502669 559) q(0 -1 -1 -1) r(0 -1)
|_    <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=27&xinfo=12-24348054-0%200NNN%20RT%281714855502669%20559%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29&incident_id=0-114512379471724812&edet=9&cinfo=ffffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="
100%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-1145123
79471724812</iframe></body></ht
|_ssl-date: TLS randomness does not represent time
```

Proof of concept:

```
53/tcp    open  domain?
| fingerprint-strings:
|   DNSStatusRequestTCP:
|     4jjom9f
|     incapdns
|     hostmaster incapsula
|     incapdns
|     '\x94
|     bgdfa8q6ge51ee59rilcc71nv83oe1hc
|     \x1a
|     incapdns
|     =l1'
|     3DXY
|     y{iuh
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp    open  ssl/http
| ssl-cert: Subject: commonName=imperva.com
| Subject Alternative Name: DNS:app-gcp.redislabs.com, DNS:cli.redis.io, DNS:www.redis.com, DNS:*.redis.com, DN
S:redis.io, DNS:staging.redis.io, DNS:redis.com, DNS:try.redis.io, DNS:*.redislabs.com, DNS:download.redis.io,
DNS:imperva.com, DNS:www.redis.io
| Not valid before: 2024-04-22T21:11:57
|_Not valid after:  2024-10-19T21:11:57
```

```
|   HTTPOptions:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
|     Content-Length: 692
|     X-Iinfo: 10-14108208-0 0NNN RT(1714855504198 576) q(0 -1 -1 -1) r(0 -1)
|_    <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=27&xinfo=10-14108208-0%200NNN%20RT%281714855504198%20576%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29&incident_id=0-68377279592136970&edet=9&cinfo=ffffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="1
00%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-68377279
592136970</iframe></body></html
|_ssl-date: TLS randomness does not represent time
|_http-title: Did not follow redirect to https://redis.io/
| tls-nextprotoneg:
|_  http/1.1
```

Proof of concept:

```
|  Connection: close
|  Content-Length: 691
|  X-Iinfo: 4-18874066-0 0NNN RT(1714855503376 364) q(0 -1 -1 -1) r(0 -1)
|_ <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=27&xinfo=4-18874066-0%200NNN%20RT%281714855503376%20364%29%20q%280%20-1%20-1%20-1%29%20r%
280%20-1%29&incident_id=0-904652398335101488edet=9&cinfo=ffffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="10
0%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-904652398
33510148</iframe></body></html>
| tls-nextprotoneg:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=imperva.com
| Subject Alternative Name: DNS:app-gcp.redislabs.com, DNS:cli.redis.io, DNS:www.redis.com, DNS:*.redis.com, DN
S:redis.io, DNS:staging.redis.io, DNS:redis.com, DNS:try.redis.io, DNS:*.redislabs.com, DNS:download.redis.io,
DNS:imperva.com, DNS:www.redis.io
| Not valid before: 2024-04-22T21:11:57
|_Not valid after:  2024-10-19T21:11:57
84/tcp    open  ssl/ctf?
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=imperva.com
| Subject Alternative Name: DNS:app-gcp.redislabs.com, DNS:cli.redis.io, DNS:www.redis.com, DNS:*.redis.com, DN
S:redis.io, DNS:staging.redis.io, DNS:redis.com, DNS:try.redis.io, DNS:*.redislabs.com, DNS:download.redis.io,
DNS:imperva.com, DNS:www.redis.io
```

```
88/tcp    open  ssl/kerberos-sec?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
|     Content-Length: 688
|     X-Iinfo: 10-14108147-0 0NNN RT(1714855503379 339) q(0 -1 -1 -1) r(0 -1)
|     <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=27&xinfo=10-14108147-0%200NNN%20RT%281714855503379%20339%29%20q%280%20-1%20-1%20-1%29%20r
%280%20-1%29&incident_id=0-68377013304164618&edet=9&cinfo=ffffffff&rpinfo=0&mth=GET" frameborder=0 width="100%"
 height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-683770133041
64618</iframe></body></html>
|   HTTPOptions:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
|     Content-Length: 693
|     X-Iinfo: 5-21162614-0 0NNN RT(1714855504343 723) q(0 -1 -1 -1) r(0 -1)
|_    <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
```

Proof of concept:

```
|   HTTP/1.1 503 Service Unavailable
|   Content-Type: text/html
|   Cache-Control: no-cache, no-store
|   Connection: close
|   Content-Length: 691
|   X-Iinfo: 7-24060388-0 0NNN RT(1714855484131 21) q(0 -1 -1 -1) r(0 -1)
|_  <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
ula_Resource?CWUDNSAI=5&xinfo=7-24060388-0%200NNN%20RT%281714855484131%2021%29%20q%280%20-1%20-1%20-1%29%20r%28
0%20-1%29&incident_id=0-11294880521755059 9&edet=9&cinfo=ffffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="100
%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-1129488052
17550599</iframe></body></html>
211/tcp   open  914c-g?
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 503 Service Unavailable
|     Content-Type: text/html
|     Cache-Control: no-cache, no-store
|     Connection: close
|     Content-Length: 688
|     X-Iinfo: 12-24345724-0 0NNN RT(1714855483478 16) q(0 -1 -1 -1) r(0 -1)
|     <html style="height:100%"><head><META NAME="ROBOTS" CONTENT="NOINDEX, NOFOLLOW"><meta name="format-detect
ion" content="telephone=no"><meta name="viewport" content="initial-scale=1.0"><meta http-equiv="X-UA-Compatible
" content="IE=edge,chrome=1"></head><body style="margin:0px;height:100%"><iframe id="main-iframe" src="/_Incaps
```

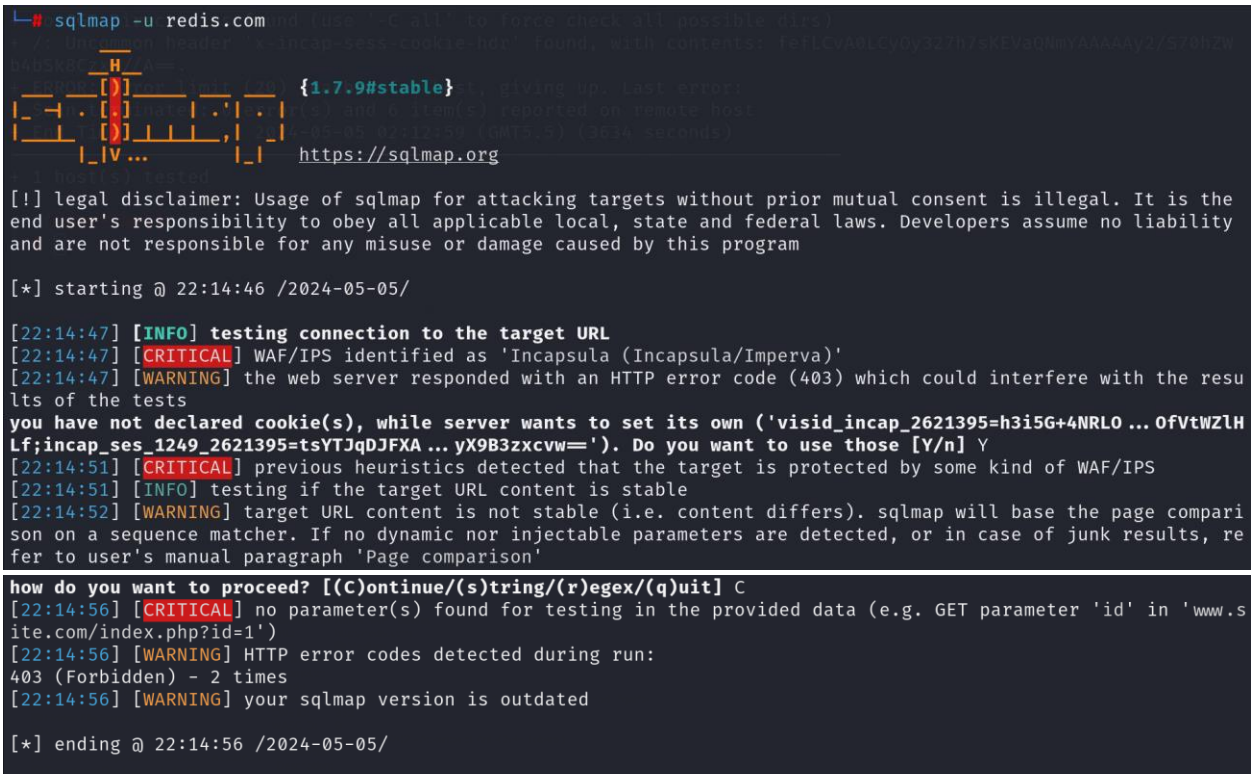
```
SF:%2817148555023 54%20420%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29&inc
SF:ident_id=0-10190210638256563 8&edet=9&cinfo=ffffffff&rpinfo=0&mth=OPTION
SF:S\"\x20frameborder=0\x20width=\"100%\"\x20height=\"100%\"\x20marginheig
SF:ht=\"0px\"\x20marginwidth=\"0px\">Request\x20unsuccessful\.\x20Incapsul
SF:a\x20incident\x20ID:\x200-10190210638256563 8</iframe></body></html");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: VoIP phone|specialized|firewall|general purpose
Running (JUST GUESSING): Grandstream embedded (91%), 2N embedded (88%), Cisco ASA 9.X (87%), Philips embedded (
85%), lwIP 1.4.X (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:2n:helios cpe:/a:cisco:adaptive_security_appliance_software:9.2 cpe:/
h:philips:hue_bridge cpe:/a:lwip_project:lwip:1.4
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (91%), 2N Helios IP VoIP doorbell (88%), Cisco Adaptive S
ecurity Appliance (ASA 9.2) (87%), Philips Hue Bridge (lwIP stack v1.4.0) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.50 ms 45.60.131.1

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1040.61 seconds
```

Exploitation

Sqlmap

Web applications with SQL injection vulnerabilities can be automatically found and exploited with SQLMap, an open-source penetration testing tool. It employs a number of detecting methods, supports a number of database management systems, and provides customization choices. Security experts and penetration testers find SQLMap useful as it automates testing, enumeration, data extraction, and reporting procedures during security assessments. It should, therefore, be utilized sensibly, morally, and with the appropriate authorization to test programs and systems.

Proof of concept:



Vulnerability analysis phase

I used tool like ZAP (zed attack proxy) to process and catch bugs and vulnerabilities are based on OWASP top 10.

Targeted Domain: - http://redis.com

- ZAP (zed attack proxy)

OWASP created the open-source Zed Attack Proxy (ZAP) tool for online application security testing. Users can examine and alter HTTP/HTTPS communication between web browsers and programs by using it as an intercepting proxy. ZAP provides spidering to map application structures in addition to active and passive scanning for vulnerabilities like SQL injection and XSS. It facilitates input validation testing with fuzzing, controls sessions for authentication verification, and offers automation via scripting and APIs. ZAP helps with risk management and safe application development by providing thorough reports on vulnerabilities that have been found.

Vulnerability title

Absence of Anti-CSRF Tokens

- Vulnerability description

Users are vulnerable to Cross-Site Request Forgery (CSRF) attacks due to web apps' lack of Anti-CSRF (Cross-Site Request Forgery) tokens. Cybercriminals employ cross-site request forgeries (CSRF) to gain unauthorized access to a website by manipulating a user's authenticated session. By requiring distinct tokens for every request and validating them on the server side, anti-CSRF tokens are security measures intended to lessen the impact of these attacks.

The risks associated with the absence of Anti-CSRF tokens include unauthorized actions, data manipulation, and account compromise. To mitigate this risk, web developers must implement Anti-CSRF measures such as generating and validating unique tokens per session or request. Security best practices like secure cookie handling and regular security assessments are also crucial in maintaining a secure web application environment

Addressing the absence of Anti-CSRF tokens strengthens the security posture of web applications, protecting users from CSRF attacks and ensuring the integrity of sensitive actions and data.

- Impact assessment

In the absence of Anti-CSRF Tokens, impact assessment focuses on evaluating the potential repercussions of CSRF attacks on web applications. Key considerations include financial risks such as unauthorized transactions, reputational damage from compromised user

trust, operational disruptions, and legal liabilities due to regulatory non-compliance.

Impact assessment drives the implementation of mitigation strategies like Anti-CSRF Tokens, secure coding practices, and continuous monitoring to reduce the likelihood and impact of CSRF attacks, bolstering overall cybersecurity posture and regulatory adherence.

- Affected components

In the absence of Anti-CSRF Tokens, several critical components within a web application become vulnerable to exploitation. These include user authentication mechanisms, sensitive transaction operations, data integrity controls, session management protocols, regulatory compliance standards, application reputation, and operational continuity. Mitigating these risks involves implementing Anti-CSRF Tokens or alternative protection mechanisms, securing session handling processes, conducting thorough input validation checks, and adhering to security best practices throughout the application's lifecycle. Regular security assessments and monitoring are essential to detect and remediate CSRF vulnerabilities promptly, safeguarding the application and its users from potential threats and unauthorized activities.

How to mitigate?

Mitigating the absence of Anti-CSRF Tokens involves implementing robust security measures to protect web applications from CSRF attacks. Here are key strategies to mitigate this risk:

1. Implement Anti-CSRF Tokens-Generate and include unique, unpredictable tokens in HTML forms or headers for each user session. Validate these tokens on the server side for every sensitive or state-changing request.

2. Use SameSite Cookies-Set cookies with the SameSite attribute to "Strict" or "Lax" mode to prevent cross-origin requests, reducing the risk of CSRF attacks originating from other sites.

3. Token Validation-Ensure that Anti-CSRF Tokens are securely generated, unique per session, and cryptographically strong to resist token prediction or brute-force attacks.

4. Secure Session Management- Employ secure session handling practices, such as using HTTP cookies with secure and HttpOnly attributes, implementing session expiration mechanisms, and re-authenticating sensitive actions.

5. Implement Referer Checks-Validate HTTP Referer headers to ensure that requests originate from trusted domains. However, note that this method may not be foolproof due to Referer header limitations.

6. Use Content Security Policy (CSP)-Leverage CSP headers to restrict the sources from which content can be loaded, reducing the risk of executing malicious scripts injected via CSRF attacks.

7. Input Validation- Validate and sanitize all user inputs on the server side to prevent injection attacks, including those that could be leveraged in CSRF exploits.

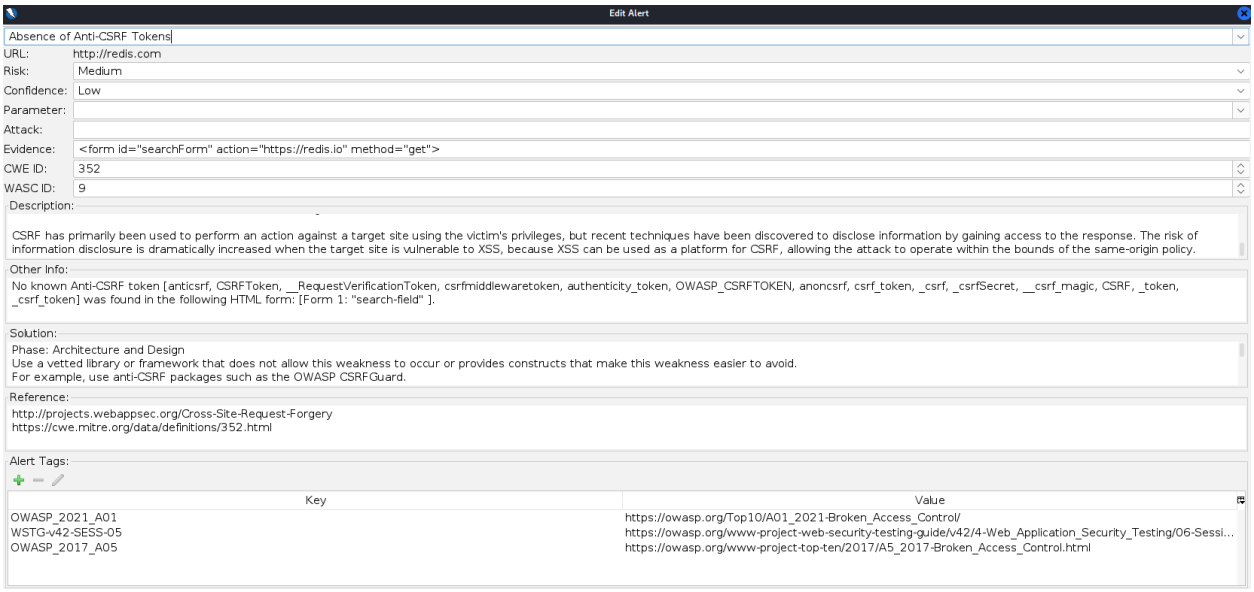
8. Security Awareness Training- Educate developers, administrators, and users about CSRF vulnerabilities, best practices for secure coding, and recognizing and reporting suspicious activities.

9. Regular Security Audits-Conduct regular security assessments, code reviews, and penetration testing to identify and remediate CSRF vulnerabilities and other security weaknesses proactively.

10. Update Security Practices- Stay updated with the latest security standards, frameworks, and practices to adapt mitigation strategies according to evolving threats and attack vectors.

By implementing these mitigation strategies, organizations can significantly reduce the risk of CSRF attacks and enhance the overall security posture of their web applications.

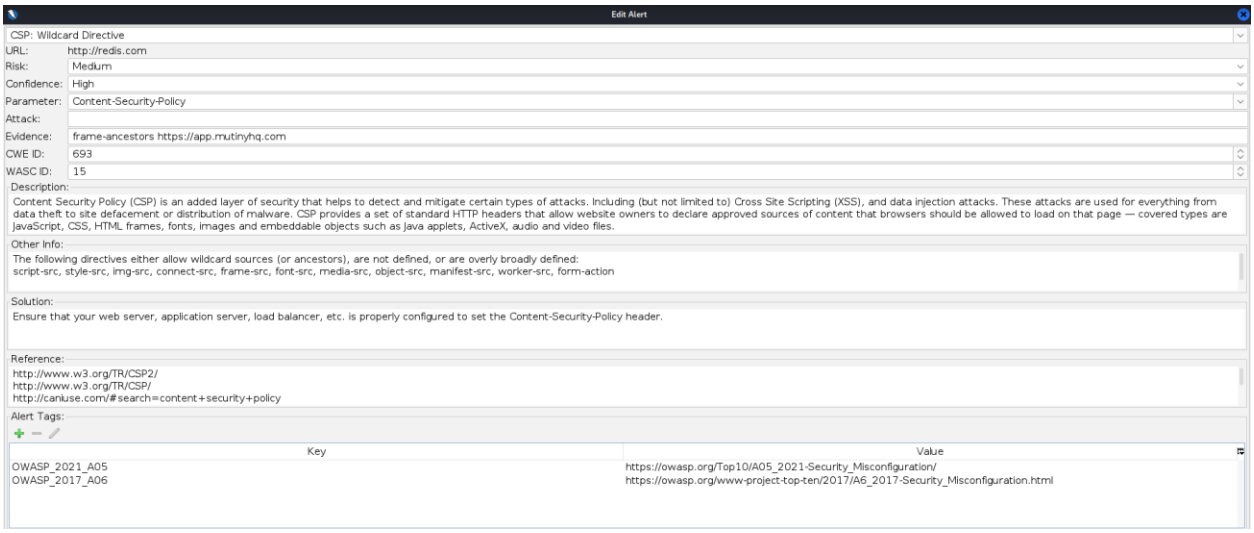
Proof of concept:



Other vulnerabilities were identified during the scan

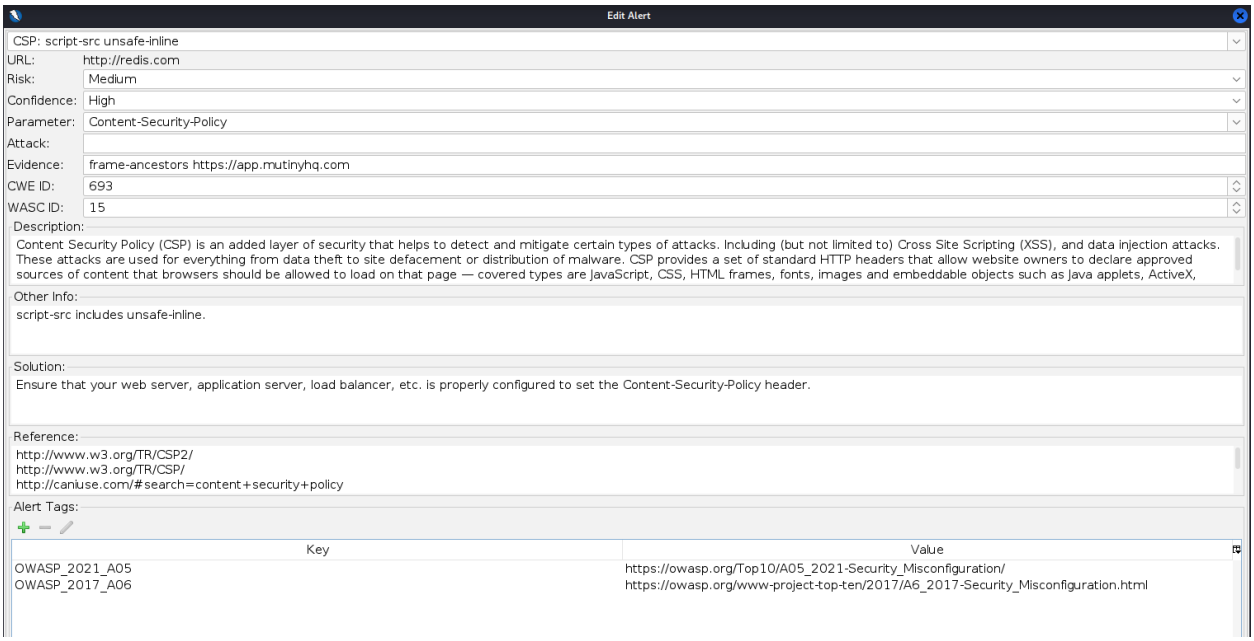
- CSP: Wildcard Directive

Proof of concept:



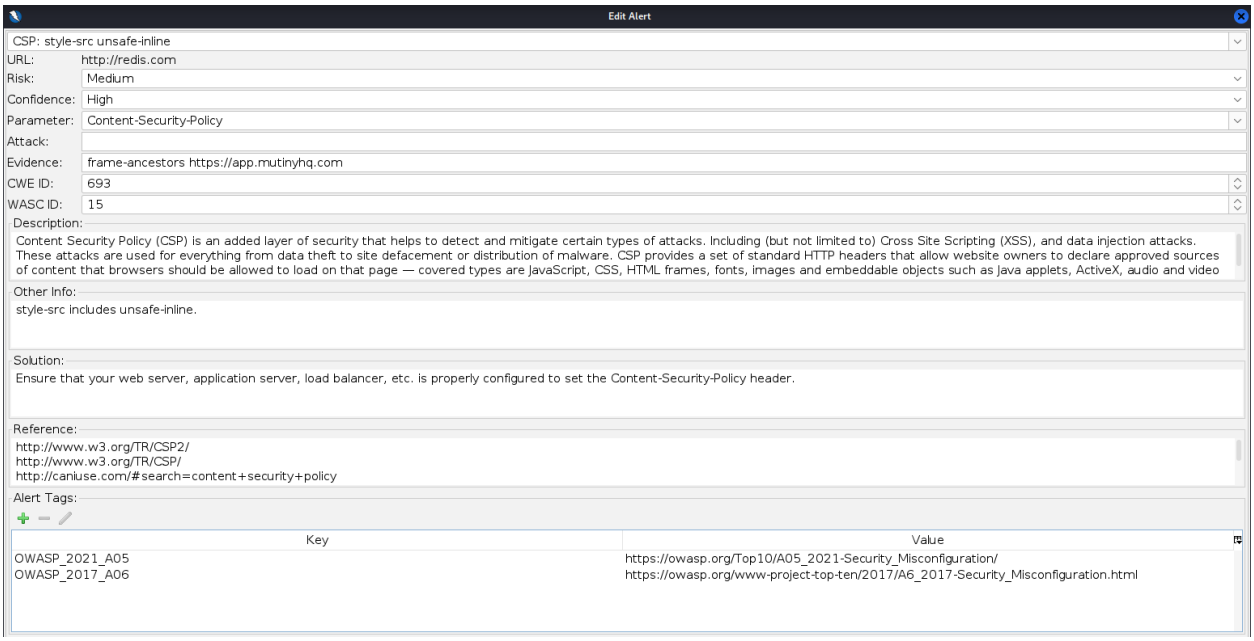
- CSP: script-src unsafe-inline

Proof of concept:



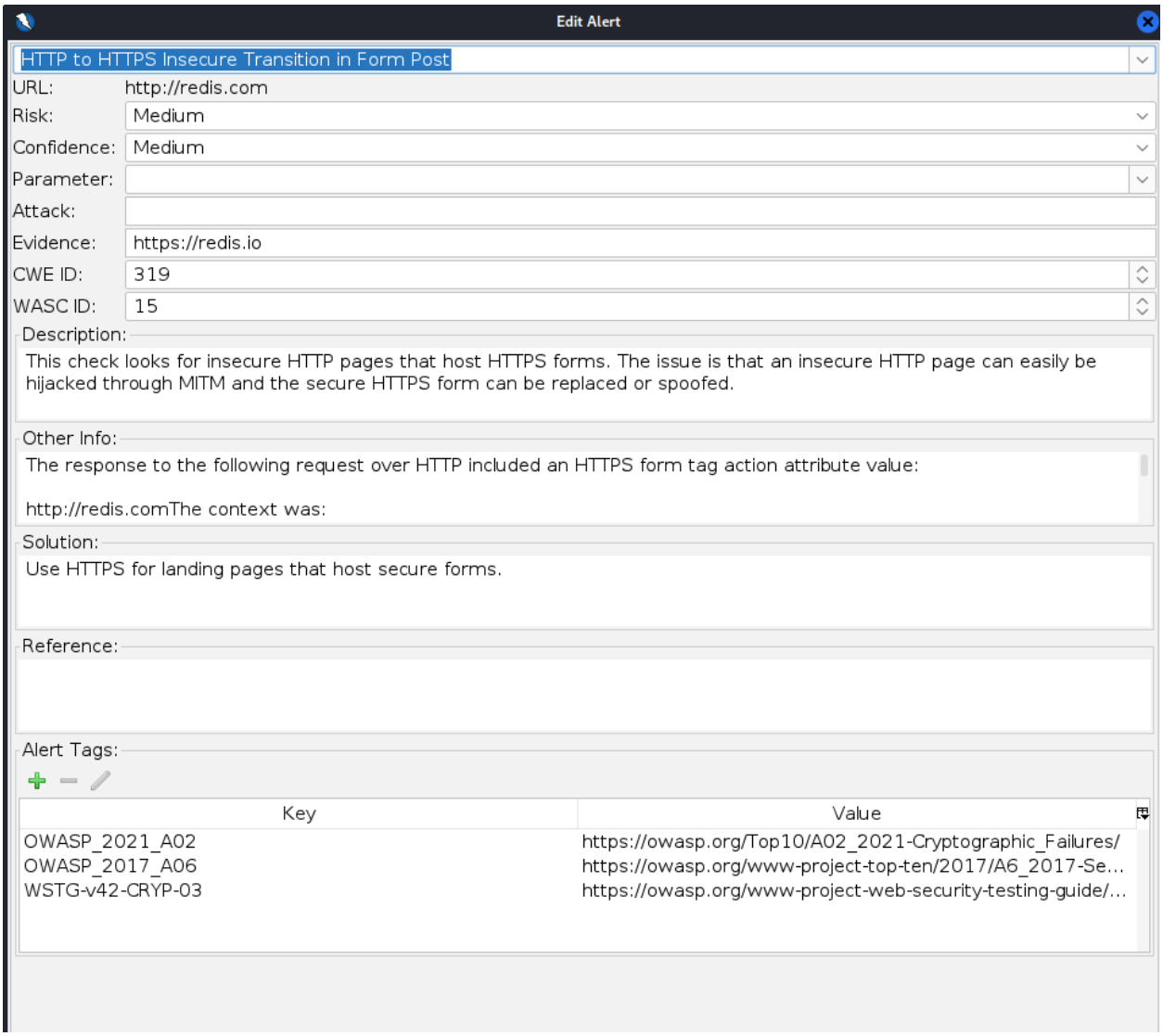
CSP: style-src unsafe-inline

Proof of concept:



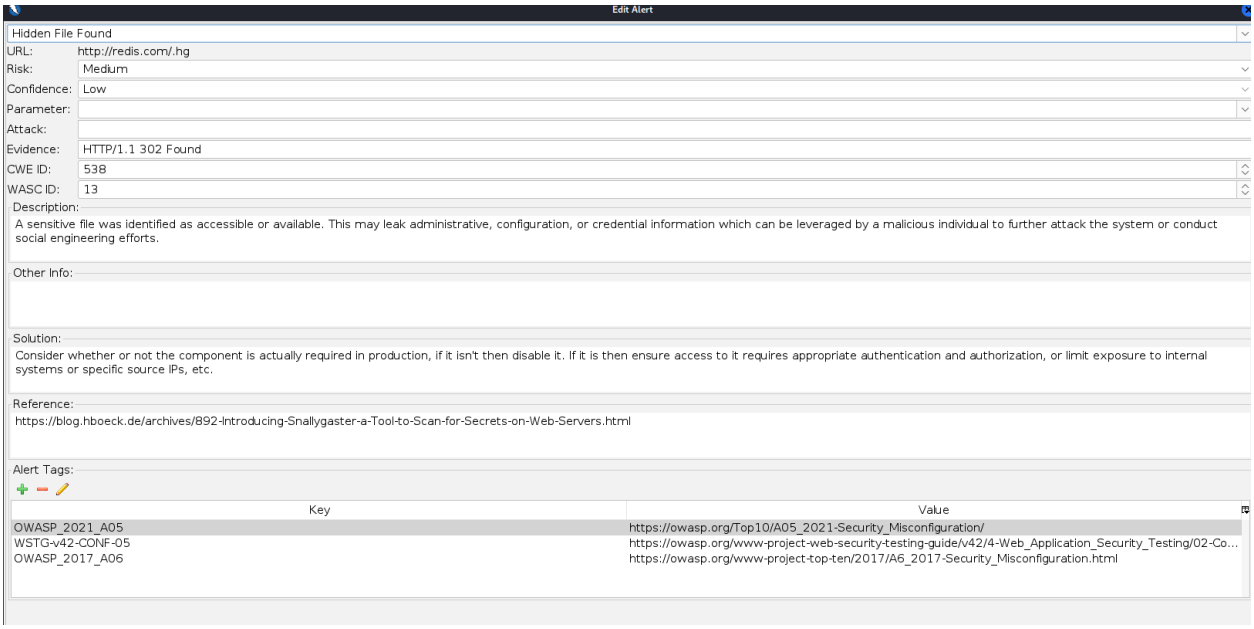
- HTTP to HTTPS Insecure Transition in Form Post

Proof of concept:



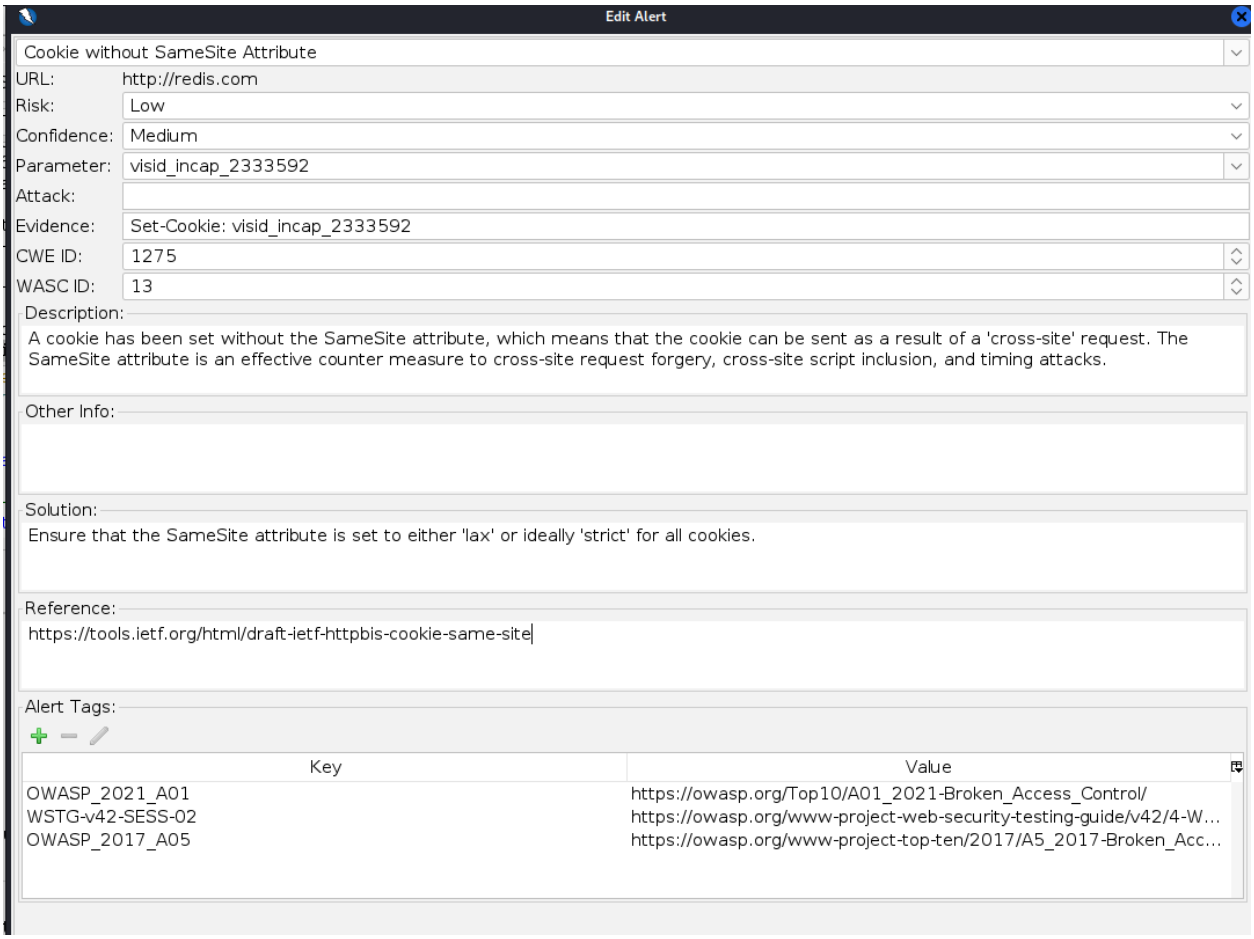
- Hidden File Found

Proof of concept:



- Cookie without SameSite Attribute

Proof of concept:



Conclusion

The security assessment conducted on the Redis website has identified several critical vulnerabilities that pose significant risks to the security and integrity of the platform. These vulnerabilities include weak ciphers, potential phishing risks through browser tabs, the presence of a Web Application Firewall (WAF) indicating potential attack prevention measures, unexpected redirect response body issues, forbidden resource

access, and missing X-XSS-Protection headers that help prevent cross-site scripting attacks.

To address these vulnerabilities, it is crucial to implement robust security measures such as Anti-CSRF tokens to prevent unauthorized actions, secure cookie handling with SameSite attributes to mitigate cross-origin risks, strict token validation procedures, secure session management practices, Referer header checks, and Content Security Policy (CSP) implementations to restrict malicious script executions.

Furthermore, regular security audits, updates to security practices, vulnerability assessments, and security awareness training for developers and users are essential to maintain a strong security posture and protect against evolving threats. By addressing these vulnerabilities and implementing comprehensive security measures, the Redis website can significantly enhance its security resilience and safeguard against potential exploits and data breaches.