



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. Sublist*3r*
- 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. Waf*woof*
- 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.

The screenshot shows the Redis homepage. At the top, there is a navigation bar with links for Products, Solutions, Support, Company, Docs, Pricing, a search icon, Login, Book a meeting, and a prominent red 'Try Redis' button. The main heading 'SEE HOW FAST FEELS' is displayed in large, bold, white letters against a dark background. Below the heading, a subtext reads 'Get the world's fastest in-memory database from the ones who built it.' There are two buttons: 'Start for free' (yellow) and 'Talk to sales →'. To the left of the heading is a stylized graphic of a red cube with white geometric shapes (circle, triangle, square) on its faces. Below the main section are logos for various Redis customers: Allitoff, TIFFANY & CO., TELUS, Voodoo, telesign, ULTA, Superlinked, and Flowdesk. A small Redis logo is also visible in the bottom right corner of the page area.

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:

```

└$ recon-ng t3/Cookies
[*] Version check disabled.
+ /: Retrieved 'x-served-by' header: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
+ /: Uncommon header 'x-content-options' found, with contents: no-store, max-age=0, must-revalidate. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Options
+ /: Uncommon header 'x-forwarded-for' found, with contents: 172.16.1.1. See: https://www.troyhunt.com/forwarded-ip-headers-in-application-firewall-waf/
+ /: Uncommon header 'x-iinfo' found, with contents: 13-28542328-28542387-SNNN-RT(1716849221034 800) q(0 0 0 -) r(0 0 0) U24.
+ /: Uncommon header 'x-served-by' found, ^th contents: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
+ /: The X-Content-Type-Options header is \n \t. This could allow the user agent to render the content of the sponsored by ... site in a fashion to \n \t \n \t \n \t https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type/\n\n\n\n\n\n\n\n
+ Root page / redirects to: http://BLACK HILLS V
+ /HQrxs9R.INC: Cookie nmbi_26 www.blackhillsinfosec.com httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /HQrxs9R.INC: Cookie inран се_883_2621305 created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/HTTP-only
+ No CGI Directories found (see -c to follow the headers in possible dirs)
+ /: Uncommon header 'x-incap-sess-www.practisec.com' with contents: RwclZfmIVloA2Gar2wtBDCqGNmYAAAAAgJnUH1Ph8LX8Wya3gqrYQ=.
+ : Server banner char [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
+ /: Uncommon header 'x-pantheon-serious-reason' found, with contents: The page could not be loaded properly.
[1] Recon modules

```

- To get google website give this command.

```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ... 1 varnish.
+ /: Retrieved x-served-by header: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
+-----+-----+-----+-----+-----+
| s/eb/HTTP/Headers/XPathme-Options | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/domains-hosts/google_site_web | 1.0 | installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+
+ /: Uncommon header 'x-iiinfo' found, with contents: 13-28542378-28542387 SNNN RT(1714849221034 800) q(0 0 0 - D = Has dependencies. See info for details.
K = Requires keys. See info for details.
with contents: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of th
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web.com/web-vulnerability-scanner/vuln
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > show info 1395 created without the httponly flag. See: https://developer.mozilla.org/en-
Shows various framework items
+ /CHOXxSRJNC> Cookie incap_ses_883_2621395 created without the httponly flag. See: https://developer.mozilla.org/en-
Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|re
positories|vulnerabilities> use '-C all' to force check all possible dirs
```

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

```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ... 1 varnish.
+ /: Retrieved x-served-by header: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
+-----+-----+-----+-----+-----+
| s/eb/HTTP/Headers/XPathme-Options | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/domains-hosts/google_site_web | 1.0 | installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+
+ /: Uncommon header 'x-iiinfo' found, with contents: 13-28542378-28542387 SNNN RT(1714849221034 80
D = Has dependencies. See info for details.
K = Requires keys. See info for details.
with contents: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the c
[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 varnish
[+] Retrieved x-served-by header: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
[+] Name: Google Hostname Enumeratorions header is not present. See: https://developer.mozilla.org/en-US/doc
[+] Author: Tim Tomes (@lanmaster53)
[+] Version: 1.0
[+] WAF is in use. See: https://www.sumasoft.com/incapsula-cloud-based-web-application-firewall-waf

Description: DN was identified by the x-timer header. See: https://www.fastly.com/
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with q(0.0 - the results.
[+] Uncommon header 'x-served-by' found, with contents: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
Options:
  Name | Current Value | Required | Description | See: https://www.netsparker.com/web-vulnerability-scanner/vuln
  _____|_____|_____|
  SOURCE | clubhouse.com | yes | https | source of input (see 'info' for details)
Source Options:
  default | SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL | ag | See: https://developer.mozilla.org/en-US/docs/Web/API/Database/SELECT
  <string> | string representing a single input |
  <path> | Directs to a file containing a list of inputs possible dirs |
  query <sql> | database query returning one column of inputs | t: RwcLZfmiVloAzbgar2wtBDCqgNmYAAAAGliUhiPh5
[recon-ng][default][google_site_web] > options set source redis.com
SOURCE => redis.com <span>no serious reason</span> found, with contents: The page could not be loaded properly.
[recon-ng][default][google_site_web] > run
```

Proof of concept:

```
[-] Retrieved x-served-by header: cache-yyz4552-YYZ, cache-yyz4552-YYZ
REDIS.COManti-clickjacking X-Frame-Options header is not present. See: https://www.netsparker.com/web-vulnerability-scanner/vuln
  _____|_____|
  Headers | X-Frame-Options |
  _____|_____|
  [*] Searching Google for: site:redis.com://www.sumasoft.com/incapsula-c
  [*] Country: None
  [*] Host: oss.redis.com <span>identified by the x-timer header. See: https://www.sumasoft.com/incapsula-c</span>
  [*] Ip_Address: None <span>'x-iinfo' found, with contents: 13-28542378-28542378</span>
  [*] Latitude: None
  [*] Longitude: None <span>'x-served-by' found, with contents: cache-yyz4552-YYZ</span>
  [*] Notes: None <span>'x-content-type-options' header is not set. This could allow the user agent to render the content in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vuln
  [*] Region: None <span>'x-content-type-options' header is not set. This could allow the user agent to render the content in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vuln
  [*] browser/missing_content_type_header/
  [*] Country: None <span>Directs to: https://redis.com/</span>
  [*] Host: developer.redis.com <span>2621395 created without the httponly flag.</span>
  [*] Ip_Address: None <span>cookies</span>
  [*] Latitude: None <span>Cookie incap_sess_883_2621395 created without the httponly flag.</span>
  [*] Longitude: None <span>HTTP/Cookies</span>
  [*] Notes: None <span>No entries found (use '-C all' to force check all possible domains).</span>
  [*] Region: None <span>'x-incap-sess-cookie-hdr' found, with contents: RwcLZfmiVloAzbgar2wtBDCqgNmYAAAAGliUhiPh5</span>
  [*] WyduSg41TQ
```

```
[*] -- /Web/HTTP/Cookies
[*] Country: None header: 1.1 varnish, 1.1 varnish.
[*] Host: trust.redis.com header: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
[*] Ip_Address: None lacking X-Frame-Options header is not present. See: https://
[*] Latitude: None X-Frame-Options
[*] Longitude: None is in use. See: https://www.sumasoft.com/incapsula-cloud-bas
[*] Notes: None
[*] Region: None was identified by the x-timer header. See: https://www.fastly.c
[*] _____ common header 'x-timer' found, with contents: 13-28542378-28542387 SNNN
[*] Country: None
[*] Host: university.redis.com header 'x-timer' found, with contents: cache-yyz4552-YYZ, cache-yyz4552-YYZ
[*] Ip_Address: None type=Options header is not set. This could allow the user ag
[*] Latitude: None ent fashion to the MIME type. See: https://www.netsparker.com
[*] Longitude: None content-type-header/
[*] Notes: None edirects to: https://redis.com/
[*] Region: None Cookie nlbi_2621395 created without the httponly flag. See: ht
[*] _____
[*] Country: None cookie incap_ses_883_2621395 created without the httponly flag
[*] Host: docs.redis.com P/Cookies
[*] Ip_Address: None found (use '-C all' to force check all possible dirs)
[*] Latitude: None er 'x-incap-sess-cookie-hdr' found, with contents: RwcLZfmIVI
[*] Longitude: None
[*] Notes: None er changed from 'Varnish' to 'Pantheon'.
[*] Region: None header 'x-pantheon-serious-reason' found, with contents: The page
```

Proof of concept:

```
-----common header 'x-incap-sess-cookie-hdr'
SUMMARY 3gqrYQ==.
----- Server banner changed from 'Varnish' to 'P
[*]:6Utotal(6new)hostsafound.x-pantheon-serious-reaso
[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:

```
(deshan㉿kali)-[~]
$ nslookup redis.com
Server:      192.168.8.1
Address:     192.168.8.1#53

Non-authoritative answer:
Name:   redis.com
Address: 45.60.121.1
Name:   redis.com
Address: 45.60.131.1
Name:   redis.com
Address: 2a02:e980:12f::1
Name:   redis.com
Address: 2a02:e980:127::1
```

- 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:

```
└─# sublist3r -d redis.com

+ Multiple IPs found: 45.60.131.1, 45.60.121.1, 2a02:e980:127::1, 2a02:e980:127::2
+ Target IP: 45.60.131.1
+ Target Hostname: redis.com
+ Target Port: 80
+ Start Time: 2024-01-12T12:25:00Z

+ Server: No ban#eCodedBy Ahmed Aboul-Ela - @aboul3la
+ /: Cookie incap_ses_1228_2621395 created without the httponly flag
[-] Enumerating subdomains now for redis.com
[-] Searching now in Baidu.. -Frame-Options header is not present. See https://www.w3.org/TR/CSP3/#frame-options
[-] Searching now in Yahoo..options
[-] Searching now in Google.. found, with contents: 1-11918667-0 0
[-] Searching now in Bing..
[-] Searching now in Ask..options header is not set. This could allow
[-] Searching now in Netcraft..o the MIME type. See: https://www.netcraft.com/
[-] Searching now in DNSdumpster..header/
[-] Searching now in Virustotal..//redis.com/
[-] Searching now in ThreatCrowd..883_2621395 created without the h
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS .. -C all' to force check all possible
[!] Error: Virustotal probably now is blocking our requests contents
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration ...
```

Proof of concept:

```
[+] Total Unique Subdomains Found: 46
www.redis.com found: 45.60.131.1, 45.60
auth.redis.com      45.60.131.1
developer.redis.com redis.com
docs.redis.com      80
engage.redis.com    2024-05-05 01:12:2
engineering.redis.com
events.redis.com
experience.redis.com_1228_2621395 created
forum.redis.com
demo.gallery.redis.com X-Frame-Options
ci.demo.gallery.redis.com e-Options
aether.ci.demo.gallery.redis.comound, wi
fi.exhibit.demo.gallery.redis.com
get.redis.com Content-Type-Options header i
hackathons.redis.com fashion to the MIM
investor.redis.com g-content-type-header/
investors.redis.com connects to: http://redis
itassets.redis.com cookie incap_ses_883_26
launchpad.redis.comb/HTTP/Cookies
learn.redis.com mories found (use '-C all'
dev.learn.redis.comr 'x-incap-sess-cooki
kb.learn.redis.com
staging.learn.redis.com
```

Proof of concept:

```
kb.staging.learn.redis.com
test.learn.redis.com
lp.redis.comPs found: 45.60.131.1, 45.60.12
marketplace.redis.com 45.60.131.1
meetups.redis.com:     redis.com
multidev.redis.com    80
pages.redis.com        2024-05-05 01:12:25 (
portal.redis.com
preferences.redis.com retrieved
rlchat.redis.comp_ses_1228_2621395 created
sjpoc.redis.comCookies
stage-university.redis.com X-Frame-Options
status.redis.comrs/X-Frame-Options
status-qa.redis.comr 'x-iinfo' found, with
tableau.redis.com) U24.
tableau-2022.redis.come-Options header is n
tableau-qa.redis.comt fashion to the MIME t
tableauext.redis.comcontent-type-header/
tableausandbox.redis.comto: http://redis.co
trust.redis.com: Cookie incap_ses_883_26213
university.redis.com/HTTP/Cookies
view.redis.comories found (use '-C all' to
+ /: Uncommon header 'x-incap-sess-cookie-h
└─(root㉿kali)-[~]
└─#
```

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:

```
└$ dnsrecon -d redis.com
[*] std: Performing General Enumeration against: redis.com...txt -t st
[-] DNSSEC is not configured for redis.com
[*]      SOA ns-1133.awsdns-13.org 205.251.196.109
[*]      SOA ns-1133.awsdns-13.org 2600:9000:5304:6d00::1
[*]      NS ns-800.awsdns-36.net 205.251.195.32
[*]      NS ns-800.awsdns-36.net 2600:9000:5303:2000::1
[*]      NS ns-78.awsdns-09.com 205.251.192.78
[*]      NS ns-78.awsdns-09.com 2600:9000:5300:4e00::1
[*]      NS ns-1966.awsdns-53.co.uk 205.251.199.174
[*]      NS ns-1966.awsdns-53.co.uk 2600:9000:5307:ae00::1
[*]      NS ns-1133.awsdns-13.org 205.251.196.109
[*]      NS ns-1133.awsdns-13.org 2600:9000:5304:6d00::1
[*]      MX us-smtp-inbound-1.mimecast.com 207.211.30.141
[*]      MX us-smtp-inbound-1.mimecast.com 205.139.110.141
[*]      MX us-smtp-inbound-1.mimecast.com 207.211.30.242
[*]      MX us-smtp-inbound-1.mimecast.com 205.139.110.221
[*]      MX us-smtp-inbound-1.mimecast.com 205.139.110.242
[*]      MX us-smtp-inbound-1.mimecast.com 207.211.30.221
[*]      MX us-smtp-inbound-2.mimecast.com 207.211.30.242
[*]      MX us-smtp-inbound-2.mimecast.com 205.139.110.242
[*]      MX us-smtp-inbound-2.mimecast.com 207.211.30.141
[*]      MX us-smtp-inbound-2.mimecast.com 205.139.110.141
[*]      MX us-smtp-inbound-2.mimecast.com 205.139.110.221
[*]      MX us-smtp-inbound-2.mimecast.com 207.211.30.221
```

Proof of concept:

```

[*] A redis.com 45.60.121.1 user/share/wordlists/dnsmap.txt -l std --xml oyorooms.xml
[*] 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=14ec584a2413dd46b812e40bc3e923f2e122e69ccbaeaaf0fe72fa91b
0d8094
[*] TXT redis.com docker-verification=1af20237-aacc-4c0a-8407-63a631301dc6
[*] TXT redis.com google-site-verification=hBCBFPNG_4AWxXoFNVwkDZXk1o3H6JrJba_lQKUl7sWc
[*] TXT redis.com globalsign-domain-verification=146F0FB14B2DFCFFF0C36E1E38EA38BF
[*] TXT redis.com google-site-verification=qLAGvo7_FSyHKTvhzvdtIfPDy7h8UVNb7HEWwnMX07g
[*] TXT redis.com cloudflare-verify=419497658-446892919
[*] TXT redis.com docusign=3bad2123-5e60-4d30-b251-86624093ab85
[*] TXT redis.com 0edife018a613ced461c7a4efeb808271b5a3b8a28
[*] 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=5fafae7d17f555701539cf2d20c40bebd5a3f37aa5b09fa6fd785fd2f9f
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		
"0edife018a613ced461c7a4efeb808271b5a3b8a28"		  
"11685988"		
"65A45059C6"		
"MS=ms98161846"		
"OSRRH-72625"		
"ZOOM_verify_tjfgNVoPwP3m9yW0EhW0ok"		
"adobe-idp-site-verification=9a542dfe12f7fa2f32e48f82d1f3102c8f0480593d7c4e86de87400ee28a68ad"		
"airtable-verification=afa3201f7f4d3fdfda5c37c212c75d2"		
"atlassian-domain-verification=l9AJIQnEuwoU3JUWACHoYu3jc+gW8Yb3eltC+BW8M2a5UR5hsURpwkrFZNL6pUSu"		
"canva-site-verification=VqW-oHHgEUICHFnx7uXsKQ"		
"cisco-ci-domain-verification=14ec584a2413dd46b812e40bc3e923f2e122e69ccbaea0f0fe72fa91b0d8094"		
"cloudflare-verify=419497658-446892919"		
"docker-verification=1af20237-aacc-4c0a-8407-63a631301dc6"		
"docsign=3bad2123-5e60-4d30-b251-86624093ab85"		
"drift-domain-verification=5fafaf5e7d17f555701539cf2d20c40beb5a3f37aa5b09fa6fd785fd2f9fbf9"		
"globalsign-domain-verification=146F0FB14B2DFCF0C36E1E38EA38BF"		
"google-site-verification=XPtqN9exy_762B70-2pt43U9918KUzRPmG6wVqxoNQ"		
"google-site-verification=hBCBFPG_4AWxXoFNVwkDZXklo3H6JrJba_lQRU17sWc"		
"google-site-verification=qLAgvo7_FSyHKTWhzvdtIfFDy7h8UVNb7HEWwnMK07g"		

• Proof of concept:

"h1-domain-verification=Gips7g7xihvRm51jVnDirSTQsYPtMvNsijzFQQhbNSU2AJTK"
"pendo-domain-verification=01cf7947-b3c9-41c6-b549-d076113c33e5"
"status-page-domain-verification=t0y77fhm0qx1"
"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	45.60.131.1	INCAPSULA	United States
■			
RDP (3389): OPEN			
tableau-2022.redis.com	44.209.210.217	AMAZON-AES	United States
■	ec2-44-209-210-217.compute-1.amazonaws.com		
tableau-qa.redis.com	35.173.93.66	AMAZON-AES	United States
■	ec2-35-173-93-66.compute-1.amazonaws.com		
engineering.redis.com	23.185.0.4	FASTLY	United States
■			
HTTP: Pantheon			
HTTP TECH: varnish			
learn.redis.com	34.111.160.242	GOOGLE-CLOUD-PLATFORM	United States
■	242.160.111.34.bc.googleusercontent.com		
staging.learn.redis.com	35.227.250.16	GOOGLE	United States
■	16.250.227.35.bc.googleusercontent.com		
RDP (3389): OPEN			
kb.staging.learn.redis.com	35.227.250.16	GOOGLE	United States
■	16.250.227.35.bc.googleusercontent.com		
RDP (3389): OPEN			
dev.staging.learn.redis.com	35.227.250.16	GOOGLE	United States
■	16.250.227.35.bc.googleusercontent.com		
RDP (3389): OPEN			
hackathons.redis.com	23.185.0.4	FASTLY	United States
■			
HTTP: Pantheon			
HTTP TECH: varnish			
oss.redis.com	13.32.151.65	AMAZON-02	United States
■	server-13-32-151-65.iad66.r.cloudfront.net		
HTTP: CloudFront			
events.redis.com	23.185.0.4	FASTLY	United States
■			
HTTP: Pantheon			
HTTP TECH: varnish			
download.redisinsight.redis.com	13.224.214.80	AMAZON-02	United States
■	server-13-224-214-80.phl50.r.cloudfront.net		
HTTP: CloudFront			
tableau.redis.com	44.209.210.217	AMAZON-AES	United States
■	ec2-44-209-210-217.compute-1.amazonaws.com		

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:**

Basic Information

Forward DNS	staging.redis.io, jselect.com.hk, cli.redis.io, redis.io, myselect.com.hk
Routing	45.60.123.0/24 via INCAPSULA, US (AS19551)
OS	linux
Services (568)	21/HTTP, 25/HTTP, 80/HTTP, 81/HTTP, 82/HTTP, 83/HTTP, 88/HTTP, 91/HTTP, 243/HTTP, 389/HTTP, 442/UNKNOWN, 443/HTTP, 465/HTTP, 466/HTTP, 554/HTTP, 587/HTTP, 631/IPP, 636/HTTP, 808/HTTP, 880/HTTP, 888/HTTP, 990/HTTP, 993/HTTP, 995/HTTP, 1024/HTTP, 1029/HTTP, 1066/UNKNOWN, 1080/HTTP, 1186/HTTP, 1194/HTTP, ...
Labels	TRUNCATED

HTTP 21/TCP 05/03/2024 23:27 UTC

Details

Banner	HTTP/1.1 503 Service Unavailable Content-Type: text/html Cache-Control: no-cache, no-store Connec
--------	--

VIEW ALL DATA

HTTP 25/TCP 05/04/2024 06:26 UTC

Details

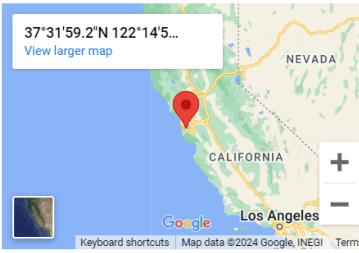
Banner	HTTP/1.1 503 Service Unavailable Content-Type: text/html Cache-Control: no-cache, no-store Connec
--------	--

VIEW ALL DATA

Geographic Location

City	Redwood City
State	California
Country	United States (US)
Coordinates	37.5331, -122.2486
Timezone	America/Los_Angeles

37°31'59.2"N 122°14'5"E
[View larger map](#)



Keyboard shortcuts | Map data ©2024 Google, INEGI | Terms

- **Proof of concept:**

HTTP 80/TCP

05/04/2024 14:32 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 81/TCP

05/04/2024 04:32 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 82/TCP

05/04/2024 11:31 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 83/TCP

05/04/2024 14:42 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 88/TCP

05/04/2024 11:51 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 91/TCP

04/24/2024 02:35 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

- **Proof of concept:**

HTTP 243/TCP

04/27/2024 08:48 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 389/TCP

05/04/2024 19:28 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

UNKNOWN 442/TCP

04/26/2024 19:49 UTC

Software

[VIEW ALL DATA](#)



Details

HTTP 61222/TCP

05/02/2024 04:01 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 61414/TCP

04/24/2024 03:53 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

HTTP 62080/TCP

04/26/2024 23:48 UTC

Details

[VIEW ALL DATA](#)

Banner HTTP/1.1 503 Service Unavailable
Content-Type: text/html
Cache-Control: no-cache, no-store
Connec

• 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:**

```
L# whois redis.com
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ Domain Name: REDIS.COM info' found, with contents: 13-28542378-28542387 SNNN RT(17148492210
1) Registry Domain ID: 2888963_DOMAIN_COM-VRSN
+ Registrar WHOIS Server: whois.name.com with contents: cache-yyz4552-YYZ, cache-yyz4552-YYZ
+ Registrar URL: http://www.name.com is not set. This could allow the user agent to render
+ Updated Date: 2024-02-03T19:20:22Z MIME type. See: https://www.netsparker.com/web-vulnerabi
+ Creation Date: 1996-02-24T05:00:00Z
+ Registry Expiry Date: 2025-02-25T05:00:00Z
+ Registrar: Name.com, Inc. 2621395 created without the httponly flag. See: https://develop
+ Registrar IANA ID: 625
+ Registrar Abuse Contact Email: abuse@name.com created without the httponly flag. See: https://
+ 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' to 'Pantheon'.
+ Name Server: NS-78.AWSDNS-09.COM 'ious-reason' found, with contents: The page could not be
+ Name Server: NS-800.AWSDNS-36.NET item(s) reported on remote host
+ DNSSEC: unsigned 2024-05-05 01:58:53 (GMT5.5) (5314 seconds)
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. See: <https://us/docs/Web/HTTP/Cookies>

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 28542387 SNNN RT(1714849221
Registrars.24.
Domain Name: REDIS.COM -served-by' found, with contents: cache-yyz4552-YYZ, cache-yyz4552-YY
Registry Domain ID: T2888963_DOMAIN_COM-VRSN not set. This could allow the user agent to render
Registrar WHOIS Server: whois.name.com MIME type. See: https://www.netsparker.com/web-vulnerab
Registrar URL: http://www.name.com reader/
Updated Date: 2024-02-03T19:20:22Z //redis.com/
Creation Date: 1996-02-24T05:00:00Z created without the httponly flag. See: https://develop
Registrar Registration Expiration Date: 2025-02-25T05:00:00Z
Registrar: Name.com, Inc. ncap_ses_883_2621395 created without the httponly flag. See: https:
Registrar IANA ID: e625 TTP/Cookies
Reseller: Directories found (use '-C all' to force check all possible dirs)
Domain Status: clientTransferProhibited https://www.icann.org/epp#clientTransferProhibitedCq
Domain Status: clientUpdateProhibited https://www.icann.org/epp#clientUpdateProhibited
Registry Registrant ID: Not Available From Registry'.
Registrant Name: Redacted For Privacy' found, with contents: The page could not be
Registrant Organization: Domain Protection Services, Inc. note host
Registrant Street: PO Box 1769 05 01:58:53 (GMT5.5) (5314 seconds)
Registrant City: Denver
Registrant State/Province: CO
Registrant Postal Code: 80201
Registrant Country: US
Registrant Phone: +1.7208009072

Registrant Fax: +1.7209758725d by the x-timer header. See: https://www.fastly.com/
Registrant Email: https://www.name.com/contact-domain-whois/redis.com 28542387 SNNN RT(1714849221
Registry Admin ID: Not Available From Registry
Admin Name: Redacted For Privacy' found, with contents: cache-yyz4552-YYZ, cache-yyz4552-YY
Admin Organization: Domain Protection Services, Inc. This could allow the user agent to
Admin Street: PO Box 1769 hion to the MIME type. See: https://www.netsparker.com/web-v
Admin City: Denver content-type-header/
Admin State/Province: CO to: https://redis.com/
Admin Postal Code: 80201 nbi_2621395 created without the httponly flag. See: https://
Admin Country: US Cookies
Admin Phone: +1.7208009072 cap_ses_883_2621395 created without the httponly flag. See:
Admin Fax: +1.7209758725 P/Cookies
Admin Email: https://www.name.com/contact-domain-whois/redis.com bable dirs)
Registry Tech ID: Not Available From Registry' found, with contents: RwcLZfmIVloAZGar
Tech Name: Redacted For Privacy
Tech Organization: Domain Protection Services, Inc. on'.
Tech Street: PO Box 1769 pantheon-serious-reason' found, with contents: The page could
Tech City: Denver error(s) and 14 item(s) reported on remote host
Tech State/Province: CO 2024-05-05 01:58:53 (GMT5.5) (5314 seconds)
Tech Postal Code: 80201
Tech Country: US d
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.orgthe x-timer header. See: https://www.fastly.com/
Name Server: ns-78.awsdns-09.comound, with contents: 13-28542378-28542387 SNNN RT(1
Name Server: ns-1966.awsdns-53.co.uk
Name Server: ns-800.awsdns-36.net' found, with contents: cache-yyz4552-YYZ, cache-yy
DNSSEC:unSignedInt-Type-Options header is not set. This could allow the user agent t
Registrar Abuse Contact Email: abuse@name.com. See: https://www.netsparker.com/web-
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<<<tponly Flag. See: https://
US/docs/Web/HTTP/Cookies
For more information on Whois status codes, please visit https://icann.org/epp;. See
a.org/en-US/docs/Web/HTTP/Cookies
```

```
For more information on Whois status codes, please visit https://icann.org/epp RT(1714849221034 800) q(0 0 0 -1
7170 0 0 024
+/- Uncommon header "x-served-by" found, with contents: cache-yyz4552-YYZ, cache-yyz4552-YYZ.
The data in the Name.com, Inc. WHOIS database is provided by Name.com, Inc. for information purposes, and to assist persons in obtaining information about or related to a domain name registration record. Name.com, Inc. does not guarantee its accuracy. Users accessing the Name.com, Inc. WHOIS service agree to use the data only for lawful purposes, and under no circumstances may this data be used to: a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than the registrar's own existing customers and b) enable high volume, automated, electronic 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 consider the following: the WHOIS service is not a replacement for standard EPP commands to the SRS service. WHOIS is not considered authoritative for registered domain objects. The WHOIS service may be scheduled for downtime during production or OTE maintenance periods. Where applicable, the presence of a [Non-Public Data] tag indicates that such data is not made publicly available due to applicable data privacy laws or requirements. Access to non-public data may be provided, upon request, where it can be reasonably confirmed that the requester holds a specific legitimate interest and a proper legal basis, for accessing the withheld data. Access to this data can be requested by submitting a request via the form found at https://www.name.com/layered-access-request. Name.com, Inc. reserves the right to modify these terms at any time. By submitting this query, you agree 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
# whatweb redis.com 0 error(s) and 14 item(s) reported on remote host
http://redis.com [302 Found] Cookies[incap_ses_883_2621395,visid_incap_2621395], Country[RESERVED][ZZ], HttpOnly[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
# wafw00f redis.com
+ /: Uncommon header 'x-served-by' found, with contents: cache-yyz4552-YYZ, c
+ /: The X-Content-Type-Options header is not set. This could allow the user
  to site in a different fashion to the MIME type. See: https://www.netsparker.c
  erabilities/missing-x-content-type-options
+ Root page / redirected to: https://redis.com/
+ /cHQrxs9R.INC: Cookie nlbi_2621395 created with the httponly flag. See:
  US/docs/Web/HTTP/Cookies
+ /cHQrxs9R.(); ; Capa ses_883_2621395 created without the httponly fl
  ag. See: https://www.netsparker.com/HTTP/Cookies
+ No CGI(Directories found) use '-C all' to find (check all possible dirs)
+ /: Uncommon header '/incapsula-session-cookie-hdr' found, with contents: RwcLZfmI
  LX8Wyaa3gqrYQ==
+ : Server banner changed from WAFW00F: v2.2.0 to 'Pantheon'.
+ /: The Web Application Firewall Fingerprinting Toolkit with contents: The pa
  tterns file contains 7977 requests: 0 error(s) and 14 item(s) reported on remote host
[*] 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:

```
[root@kali ~]# nmap -sV -A -T4 redis.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-05 02:11 +0530 (Sat, 05 May 2024)
Warning: 45.60.131.1 giving up on port because retransmission cap hit (6).
Nmap scan report for redis.com (45.60.131.1)
Host is up (0.075s latency).
Other addresses for redis.com (not scanned): 45.60.121.1 2a02:e980:127::1 2a02:e980:12f::1
Not shown: 746 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
21/tcp    open  ssl/ftp
|_tls-nextprotoneg:
|_http/1.1
|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, DNS: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
|_ssl-date: TLS randomness does not represent time
|fingerprint-strings:
|_GetRequest:
| HTTP/1.1 503 Service Unavailable
| Content-Type: text/html
| Cache-Control: no-cache, no-store
| Connection: close
| Content-Length: 687
```

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-detection" 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="/_Incapsula_Resource?CWUDNSAI=27&xinfo=2-14024673-0%200NNN%20RT%281714855501322%20685%29%20q%280%20-1%20-1%29%20r%280%20-1%295incident_id=0-67600006475677954&edet=9&cinfo=fffffff&rpinfo=0&mth=GET" frameborder=0 width="100%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-6760000647567954</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-detection" 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="/_Incapsula_Resource?CWUDNSAI=27&xinfo=3-17209138-0%200NNN%20RT%281714855502739%20505%29%20q%280%20-1%20-1%29%20r%280%20-1%295incident_id=0-81301720949063939&edet=9&cinfo=fffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="100%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-81301720949063939</iframe></body></html>
```

```

25/tcp  open  smtp?
|_smtp-commands: SMTP EHLO redis.com: failed to receive data: connection closed
| fingerprint-strings: cor(s) and 6 item(s) reported on remote host
| FourOhFourRequest, GenericLines, GetRequest, HTTPOptions, LDAPSearchReq, RTSPRequest:
|   452 syntax error (connecting)
| many errors
| Hello, Help, Kerberos, LPDString, SSLSessionReq, TLS SessionReq, 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, DNS: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: ror(s) and 6 items) reported on remote host
|  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, DNS: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
|cap-sess-cookies-hdr' found, with contents: fefLcvA0LCy0y327h7sKEVaQNmYAAAAAy2/S70hZW
| X-Info: 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=276xinfo=14-24435125-0%200NNN%20RT%281714855501537%20443%29%20q%280%20-1%20-1%29%20r
| %280%20-1%298incident_id=0-114090879971229966&edet=9&cinfo=fffffff&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-Info: 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=276xinfo=12-24348054-0%200NNN%20RT%281714855502669%20559%29%20q%280%20-1%20-1%29%20r
| %280%20-1%298incident_id=0-114512379471724812&edet=9&cinfo=fffffff&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?-(incap-sess-cookie-hdr) Found, with contents: FeLcVA0LCyOy327h7sKEVaQNmYAAAAAV2/S70hzw
| fingerprint-strings:
|_ DNSStatusRequestTCP: reached for host, giving up. Last error:
Scan 4jjom9fated: 0 error(s) and 6 item(s) reported on remote host
End incapdns      2024-05-05 02:12:59 (GMT5.5) (3634 seconds)
hostmaster incapsula
  boincapdnssted
    '\x94
  bgdfa8q6ge51ee59rilcc71nv83oe1hc
  \x1a
  incapdns
  =l1'
  3DXY
  yfiuh
DNSVersionBindReqTCP:
  version
  bind
80/tcp    open  ssl/http
| ssl-cert: Subject: commonName=impervava.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:impervava.com, DNS:www.redis.io
| Not valid before: 2024-04-22T21:11:57
| Not valid after:   2024-10-19T21:11:57
```

```
| HTTPOptions: domain?-(incap-sess-cookie-hdr) Found, with contents: FeLcVA0LCyOy327h7sKEVaQNmYAAAAAV2/S70hzw
|_ HTTP/1.1 503 Service Unavailable
| ERR Content-Type: text/html
| Content-Type: text/html; charset=UTF-8
| 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%29%20
%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 and use -c all to force check all possible dirs)
Content-Length: 691<open> cookie-hda' Found, with contents: FeFLCVA0LCyOy327h7sKEVaQNmYAAAAAy2/S70hZW
X-Iinfo: 4-18874066-0 0NNN RT(1714855503376 364) q(0 -1 -1 -1) r(0 -1)
[ERR] <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=278xinfo=4-18874066-0%20NNN%20RT%281714855503376%20364%29%20q%280%20-1%20-1%29%20r%
280%20-1%29&incident_id=0-90465239833510148&det=9&info=ffffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="10
0%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-904652398
3510148</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
34/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
```

```
38/tcp open ssl/kerberos-sec?-cookie-hdr' Found, with contents: FeFLCVA0LCyOy327h7sKEVaQNmYAAAAAy2/S70hZW
fingerprint-strings:
| GetRequest: limit (20) reached for host, giving up. Last error:
| Scan HTTP/1.1 503 Service Unavailable (m(s) reported on remote host
| End Content-Type: text/html 05 02:12:59 (GMT5.5) (3634 seconds)
| 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=278xinfo=10-14108147-0%20NNN%20RT%281714855503379%20339%29%20q%280%20-1%20-1%29%20r%
280%20-1%29&incident_id=0-68377013304164618&det=9&info=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:

```

| No: HTTP/1.1 503 Service Unavailable [to force check all possible dirs]
| . Content-Type: text/html
| . . . cookie-hdr' found, with contents: feFLCvA0LCyOy327h7sKEVaQNmYAAAAAy2/S70hZW
| 4bpsk Cache-Control: no-cache, no-store
| ERR Connection: close() reached for host, giving up. Last error:
| scalar Content-Length: 691
| End X-Info: 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-detection" 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="/_Incapsula_Resource?CWUDNSAI=5&xinfo=7-24060388-0%20NNN%20RT%281714855484131%2021%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29&incident_id=0-112948805217550599&edet=9&cinfo=fffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="100%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-112948805217550599</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-Info: 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-detection" 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="/_Incapsula_Resource?CWUDNSAI=5&xinfo=12-24345724-0%20NNN%20RT%281714855483478%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29&incident_id=0-112948805217550599&edet=9&cinfo=fffffff&rpinfo=0&mth=OPTIONS" frameborder=0 width="100%" height="100%" marginheight="0px" marginwidth="0px">Request unsuccessful. Incapsula incident ID: 0-112948805217550599</iframe></body></html>
```

```

SF:%281714855502354%20420%29%20q%280%20-1%20-1%20-1%29%20r%280%20-1%29&inc
SF:ident_id=0-101902106382565638&edet=9&cinfo=fffffff&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:\x2010-101902106382565638</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 Security 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:

```
# sqlmap -u redis.com and (use '-C all' to force check all possible dirs)
[!] Uncommon header 'X-ncap-sess-cookie-hdr' found, with contents: fefLcVA0LCy0y327h7sKEVaQNmYAAAAAY2/S70bZW
[!] b6SK87...H...
[!] FPR087...D] {1.7.9#stable}st, giving up. Last error:
[!] . [.] date [.] . [.] redis) and 6 item(s) reported on remote host
[!] T [.] [.] , [.] 2024-05-05 02:12:59 (GMT3.5) (3634 seconds)
[!] [v...] https://sqlmap.org
[*] hosts tested

[!] 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. Developers assume no liability
and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:14:46 /2024-05-05/

[22:14:47] [INFO] testing connection to the target URL
[22:14:47] [CRITICAL] WAF/IPS identified as 'Incapsula (Incapsula/Imperva)'
[22:14:47] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the resu
lts of the tests
you have not declared cookie(s), while server wants to set its own ('visid_incap_2621395=h3i5G+4NRLO ... OfVtWZLH
Lf;incap_ses_1249_2621395=tsYTJqDjFXA ... yX9B3zxcvw='). Do you want to use those [Y/n] Y
[22:14:51] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[22:14:51] [INFO] testing if the target URL content is stable
[22:14:52] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page compar
ison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, re
fer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(S)tring/(R)ege... C
[22:14:56] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.s
ite.com/index.php?id=1')
[22:14:56] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 2 times
[22:14:56] [WARNING] your sqlmap version is outdated

[*] ending @ 22:14:56 /2024-05-05/
```

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:

Edit Alert

Absence of Anti-CSRF Tokens	URL: http://redis.com								
Risk: Medium	Confidence: Low								
Parameter:	Attack:								
Evidence: <form id="searchForm" action="https://redis.io" method="get">	CWE ID: 352								
WASC ID: 9	Description: CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.								
Other Info: No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, __csrf, __csrfSecret, __csrf_magic, CSRF, __token, __csrftoken] was found in the following HTML form: [Form 1: "search-field"].									
Solution: Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. For example, use anti-CSRF packages such as the OWASP CSRFGuard.									
Reference: http://projects.webappsec.org/Cross-Site-Request-Forgery https://cve.mitre.org/data/definitions/352.html									
Alert Tags:									
<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>OWASP_2021_A01</td> <td>https://owasp.org/Top10/A01_2021-Broken_Access_Control/</td> </tr> <tr> <td>WSTG-v42-SESS-05</td> <td>https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management/05-Session_Exposure/</td> </tr> <tr> <td>OWASP_2017_A05</td> <td>https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html</td> </tr> </tbody> </table>		Key	Value	OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/	WSTG-v42-SESS-05	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management/05-Session_Exposure/	OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html
Key	Value								
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/								
WSTG-v42-SESS-05	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/06-Session_Management/05-Session_Exposure/								
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.html								

Other vulnerabilities were identified during the scan

- CSP: Wildcard Directive

Proof of concept:

Edit Alert

CSP: Wildcard Directive	http://redis.com						
URL:	Medium						
Risk:	High						
Parameter:	Content-Security-Policy						
Attack:							
Evidence:	frame-ancestors https://app.mutinyhq.com						
CWE ID:	693						
WASC ID:	15						
Description:	<p>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.</p>						
Other Info:	<p>The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined:</p> <pre>script-src, style-src, img-src, connect-src, frame-src, font-src, media-src, object-src, manifest-src, worker-src, form-action</pre>						
Solution:	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.						
Reference:	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://canuse.com/#search=content+security+policy						
Alert Tags:	<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>OWASP_2021_A05</td> <td>https://owasp.org/Top10/A05_2021-Security_Misconfiguration/</td> </tr> <tr> <td>OWASP_2017_A06</td> <td>https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html</td> </tr> </tbody> </table>	Key	Value	OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/	OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
Key	Value						
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/						
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html						

- CSP: script-src unsafe-inline

Proof of concept:

Edit Alert

CSP: script-src unsafe-inline	<input type="button" value="▼"/>						
URL: http://redis.com	<input type="button" value="▼"/>						
Risk: Medium	<input type="button" value="▼"/>						
Confidence: High	<input type="button" value="▼"/>						
Parameter: Content-Security-Policy	<input type="button" value="▼"/>						
Attack:	<input type="button" value="▼"/>						
Evidence: frame-ancestors https://app.mutinyhq.com	<input type="button" value="▼"/>						
CWE ID: 693	<input type="button" value="▼"/>						
WASC ID: 15	<input type="button" value="▼"/>						
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, etc.							
Other Info: script-src includes unsafe-inline.							
Solution: Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.							
Reference: http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://canuse.com/#search=content+security+policy							
Alert Tags:							
<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>OWASP_2021_A05</td> <td>https://owasp.org/Top10/A05_2021-Security_Misconfiguration/</td> </tr> <tr> <td>OWASP_2017_A06</td> <td>https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html</td> </tr> </tbody> </table>		Key	Value	OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/	OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
Key	Value						
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/						
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html						

CSP: style-src unsafe-inline

Proof of concept:

Edit Alert

CSP: style-src unsafe-inline	▼						
URL: http://redis.com	▼						
Risk: Medium	▼						
Confidence: High	▼						
Parameter: Content-Security-Policy	▼						
Attack:	▼						
Evidence: frame-ancestors https://app.mutinyhq.com	▼						
CWE ID: 693	▼						
WASC ID: 15	▼						
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.							
Other Info: style-src includes unsafe-inline.							
Solution: Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.							
Reference: http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://canuse.com/#search=content+security+policy							
Alert Tags:							
<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>OWASP_2021_A05</td> <td>https://owasp.org/Top10/A05_2021-Security_Misconfiguration/</td> </tr> <tr> <td>OWASP_2017_A06</td> <td>https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html</td> </tr> </tbody> </table>		Key	Value	OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/	OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html
Key	Value						
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/						
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html						

- HTTP to HTTPS Insecure Transition in Form Post

Proof of concept:

Edit Alert

HTTP to HTTPS Insecure Transition in Form Post

URL:	http://redis.com								
Risk:	Medium								
Confidence:	Medium								
Parameter:									
Attack:									
Evidence:	https://redis.io								
CWE ID:	319								
WASC ID:	15								
Description:	This check looks for insecure HTTP pages that host HTTPS forms. The issue is that an insecure HTTP page can easily be hijacked through MITM and the secure HTTPS form can be replaced or spoofed.								
Other Info:	The response to the following request over HTTP included an HTTPS form tag action attribute value: http://redis.comThe context was:								
Solution:	Use HTTPS for landing pages that host secure forms.								
Reference:									
Alert Tags:	<table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>OWASP_2021_A02</td> <td>https://owasp.org/Top10/A02_2021-Cryptographic_Failures/</td> </tr> <tr> <td>OWASP_2017_A06</td> <td>https://owasp.org/www-project-top-ten/2017/A6_2017-Se...</td> </tr> <tr> <td>WSTG-v42-CRYP-03</td> <td>https://owasp.org/www-project-web-security-testing-guide/...</td> </tr> </tbody> </table>	Key	Value	OWASP_2021_A02	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/	OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Se...	WSTG-v42-CRYP-03	https://owasp.org/www-project-web-security-testing-guide/...
Key	Value								
OWASP_2021_A02	https://owasp.org/Top10/A02_2021-Cryptographic_Failures/								
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Se...								
WSTG-v42-CRYP-03	https://owasp.org/www-project-web-security-testing-guide/...								

- Hidden File Found

Proof of concept:

Hidden File Found

URL: http://redis.com/.hg

Risk: Medium

Confidence: Low

Parameter:

Attack:

Evidence: HTTP/1.1 302 Found

CWE ID: 538

WASC ID: 13

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.

Other Info:

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

Reference:
<https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html>

Alert Tags:

Key	Value
OWASP_2021_A05	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
WSTG-v42-CONF-05	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/02-Configuration/05-Configuration-Review
OWASP_2017_A06	https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

- Cookie without SameSite Attribute

Proof of concept:

Edit Alert

Cookie without SameSite Attribute

URL:	http://redis.com								
Risk:	Low								
Confidence:	Medium								
Parameter:	visid_incap_2333592								
Attack:									
Evidence:	Set-Cookie: visid_incap_2333592								
CWE ID:	1275								
WASC ID:	13								
Description:	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.								
Other Info:									
Solution:	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.								
Reference:	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site								
Alert Tags:	<input style="margin-right: 10px;" type="button" value="+"/> <input type="button" value="-"/> <input type="button" value="Edit"/> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">Key</th> <th style="text-align: left;">Value</th> </tr> </thead> <tbody> <tr> <td>OWASP_2021_A01</td> <td>https://owasp.org/Top10/A01_2021-Broken_Access_Control/</td> </tr> <tr> <td>WSTG-v42-SESS-02</td> <td>https://owasp.org/www-project-web-security-testing-guide/v42/4-W...</td> </tr> <tr> <td>OWASP_2017_A05</td> <td>https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Acc...</td> </tr> </tbody> </table>	Key	Value	OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/	WSTG-v42-SESS-02	https://owasp.org/www-project-web-security-testing-guide/v42/4-W...	OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Acc...
Key	Value								
OWASP_2021_A01	https://owasp.org/Top10/A01_2021-Broken_Access_Control/								
WSTG-v42-SESS-02	https://owasp.org/www-project-web-security-testing-guide/v42/4-W...								
OWASP_2017_A05	https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Acc...								

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.