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

c. DNS enumeration
   - I. Dnsdumpster
   - II. Nikto

d. Public devices enumeration
   - I. Whatweb
   - II. whois

e. Find WAF (web application firewall) protection.
   - I. Wafwoof

f. Find open ports.
   - I. Nmap

g. Exploitation
   - I. sqlmap

vulnerability analysis phase

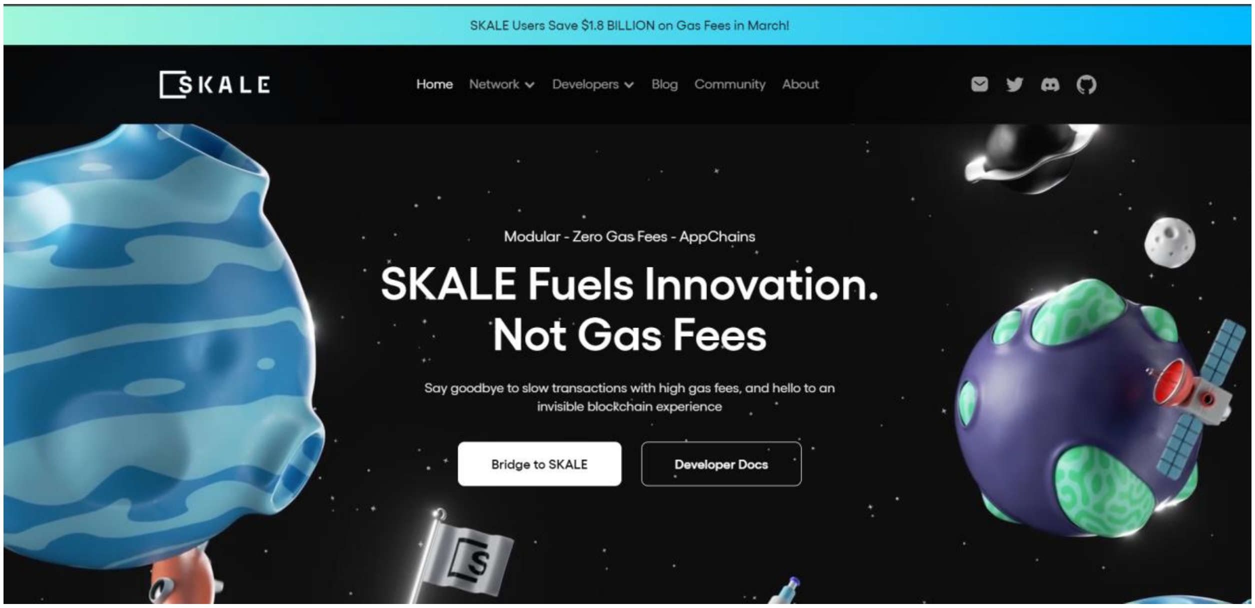
Target domain: https://skale.network.com

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:

The SKALE DAO oversees the management of the SKALE Network, which is done in an entirely transparent and decentralized manner. The SKALE Network is managed, supported, and operated by more than fifty distinct businesses, organizations, and DAOs. Thousands of engaged community members also contribute open-source code to the project, among other forms of assistance. A decentralized multisig permission from many distinct entities and contributors is necessary for any modifications to the core of a smart contract.



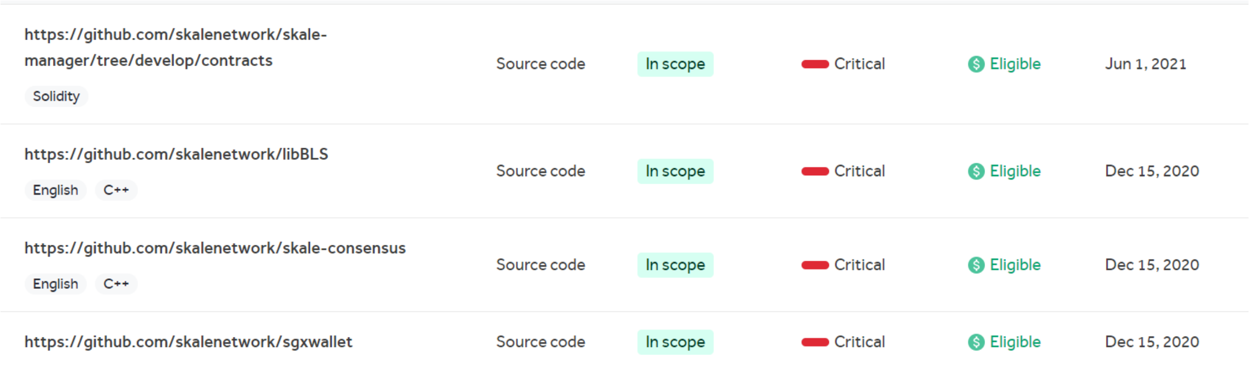
SKALE Users Save $1.8 BILLION on Gas Fees in March!

Modular - Zero Gas Fees - AppChains

SKALE Fuels Innovation. Not Gas Fees

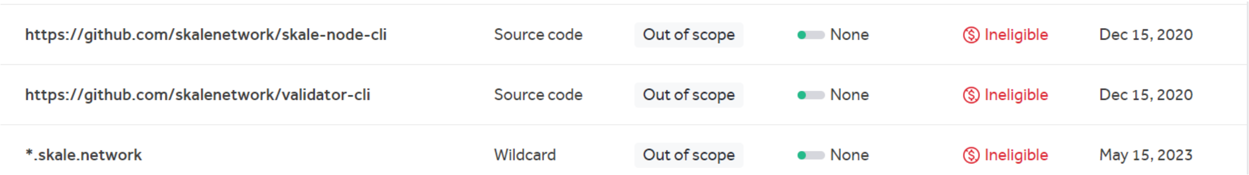
Say goodbye to slow transactions with high gas fees, and hello to an invisible blockchain experience

In Scope:



https://github.com/skalenetwork/skale-manager/tree/develop/contracts Solidity	Source code	In scope	Critical	Eligible	Jun 1, 2021
https://github.com/skalenetwork/libBLS English C++	Source code	In scope	Critical	Eligible	Dec 15, 2020
https://github.com/skalenetwork/skale-consensus English C++	Source code	In scope	Critical	Eligible	Dec 15, 2020
https://github.com/skalenetwork/sgxwallet	Source code	In scope	Critical	Eligible	Dec 15, 2020

Out of scope:



https://github.com/skalenetwork/skale-node-cli	Source code	Out of scope	None	Ineligible	Dec 15, 2020
https://github.com/skalenetwork/validator-cli	Source code	Out of scope	None	Ineligible	Dec 15, 2020
*.skale.network	Wildcard	Out of scope	None	Ineligible	May 15, 2023

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.

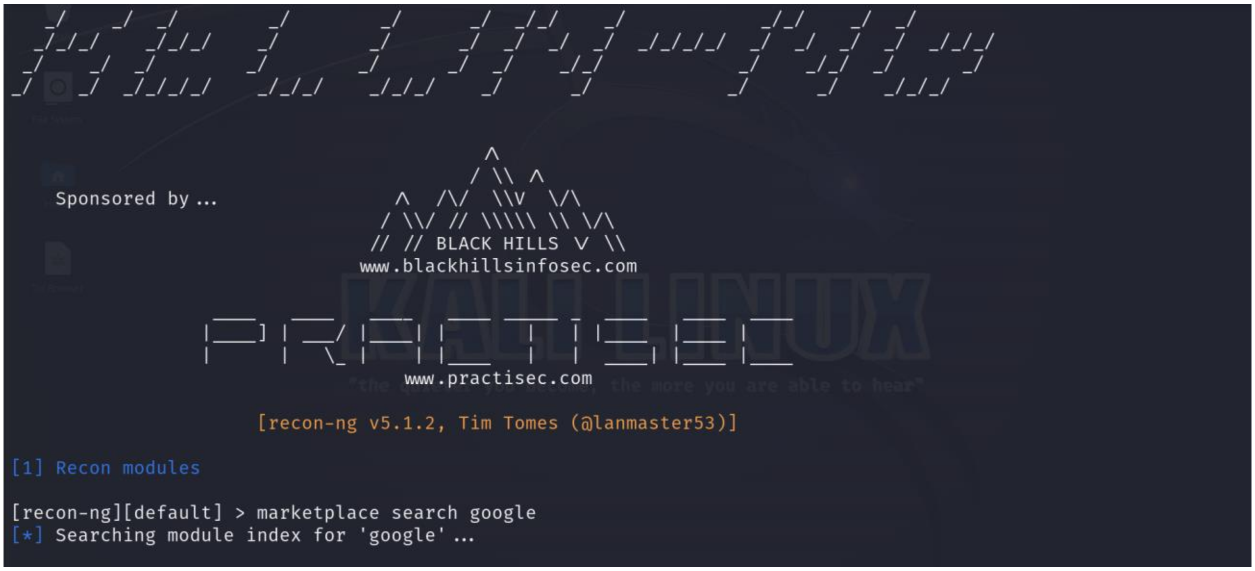
Domain: https://skale.network.com

Subdomain enumeration

- Recon-ng

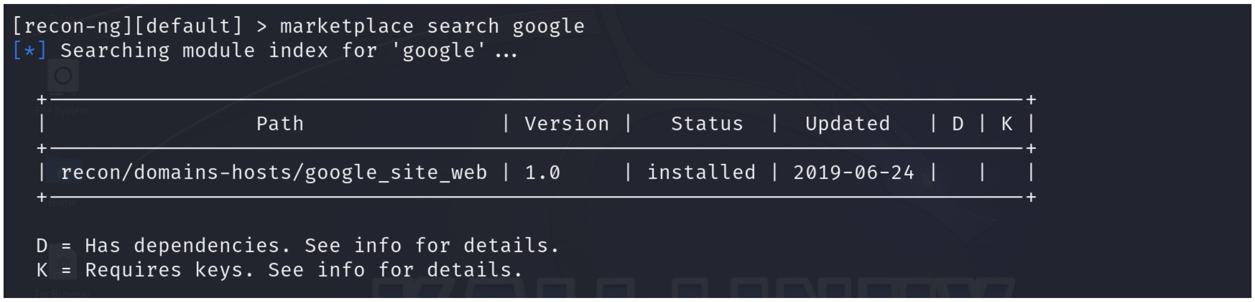
Recon-ng is an open-source reconnaissance tool with Python foundation that is used for penetration testing and security evaluations. It collects data from domains, IPs, emails, and social media platforms using a modular framework with different modules. The advantages of recon-ng are its flexibility 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:

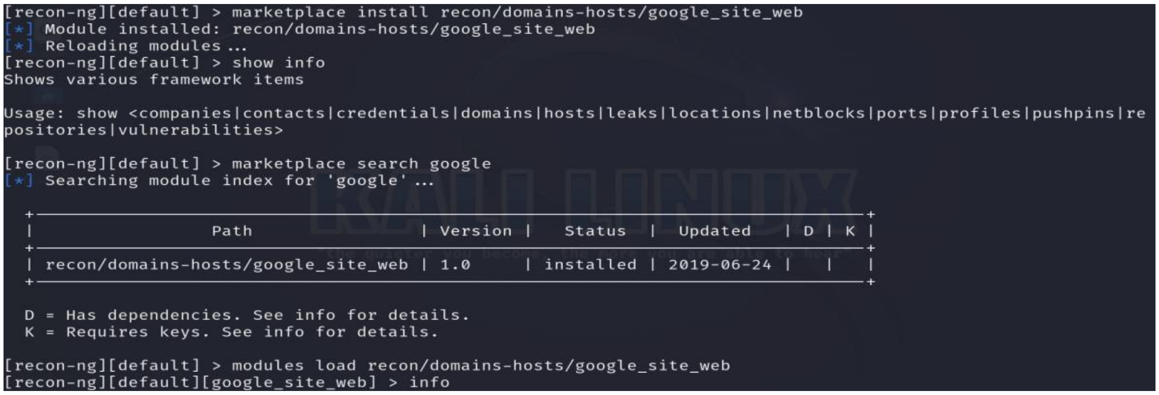


```
                                          ^
                                        / \\ ^
    Sponsored by ...               ^   /\/  \\V  \/\
                                  / \\/ // \\\\\ \\ \/\
                                 // // BLACK HILLS \/ \\
                                www.blackhillsinfosec.com

                                   www.practisec.com

                      [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

[1] Recon modules

[recon-ng][default] > marketplace search google
[*] Searching module index for 'google'...
```

Proof of concept:

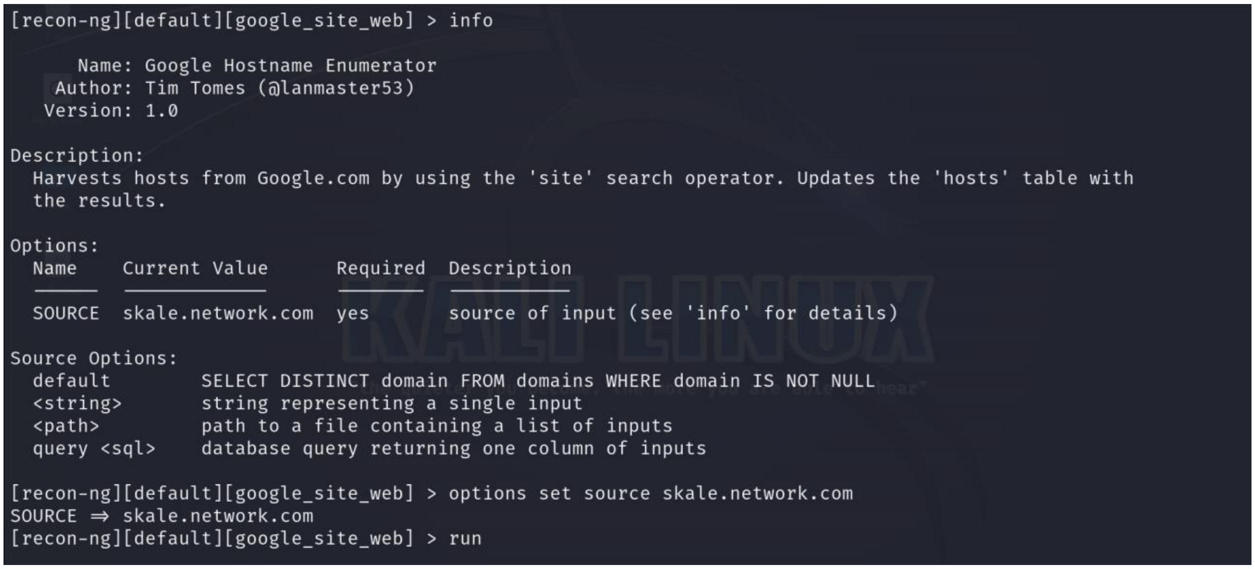


```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ...

  +--------------------------------------------------------------------------------+
  |                  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.
```

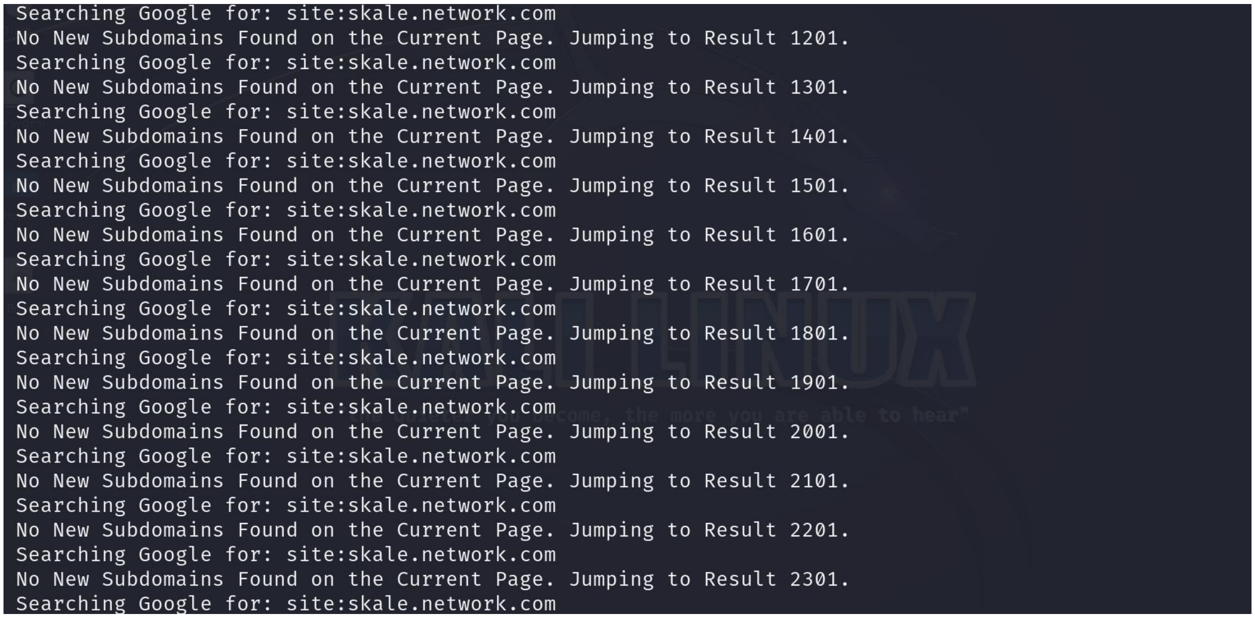


```
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > show info
Shows various framework items

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

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

Proof of concept:

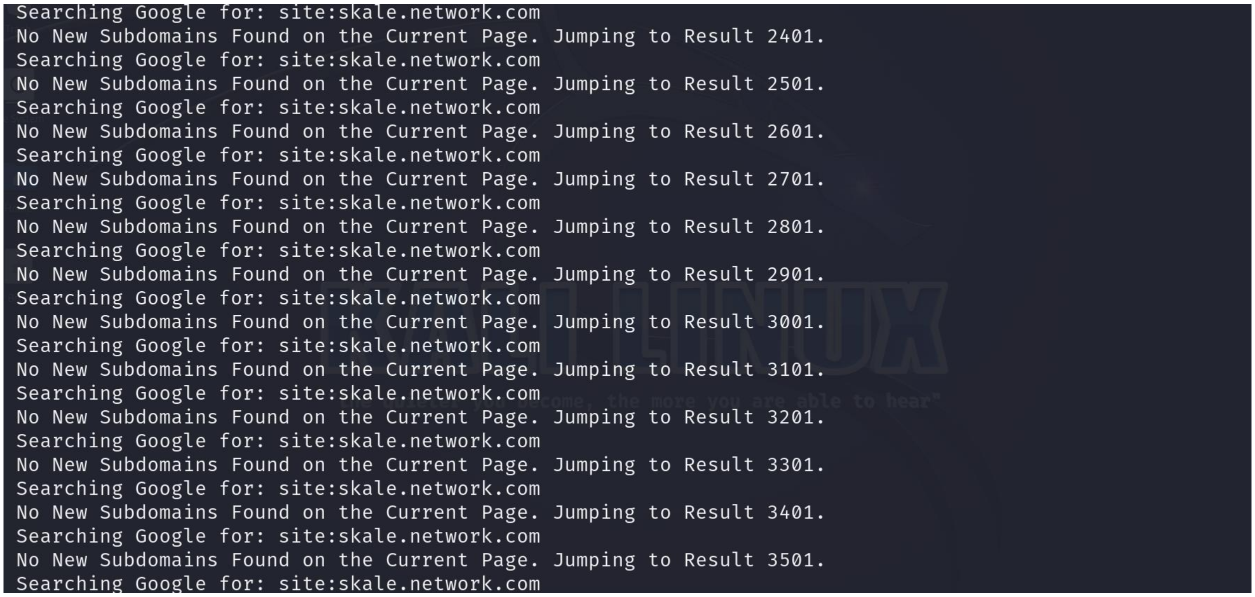


```
[recon-ng][default][google_site_web] > info

      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  skale.network.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 skale.network.com
SOURCE ⇒ skale.network.com
[recon-ng][default][google_site_web] > run
```

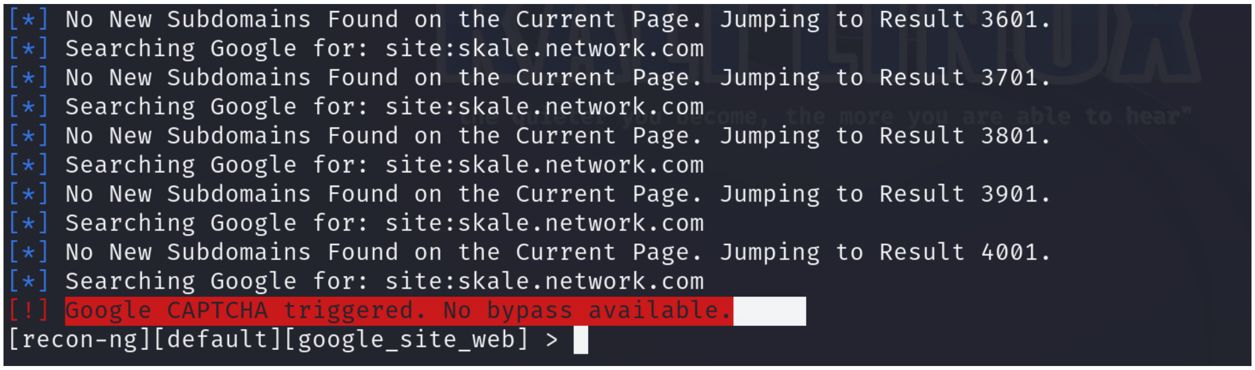


```
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1201.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1301.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1401.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1501.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1601.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1701.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1801.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 1901.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2001.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2101.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2201.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2301.
Searching Google for: site:skale.network.com
```

Proof of concept:



```
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2401.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2501.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2601.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2701.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2801.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 2901.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 3001.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 3101.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 3201.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 3301.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 3401.
Searching Google for: site:skale.network.com
No New Subdomains Found on the Current Page. Jumping to Result 3501.
Searching Google for: site:skale.network.com
```



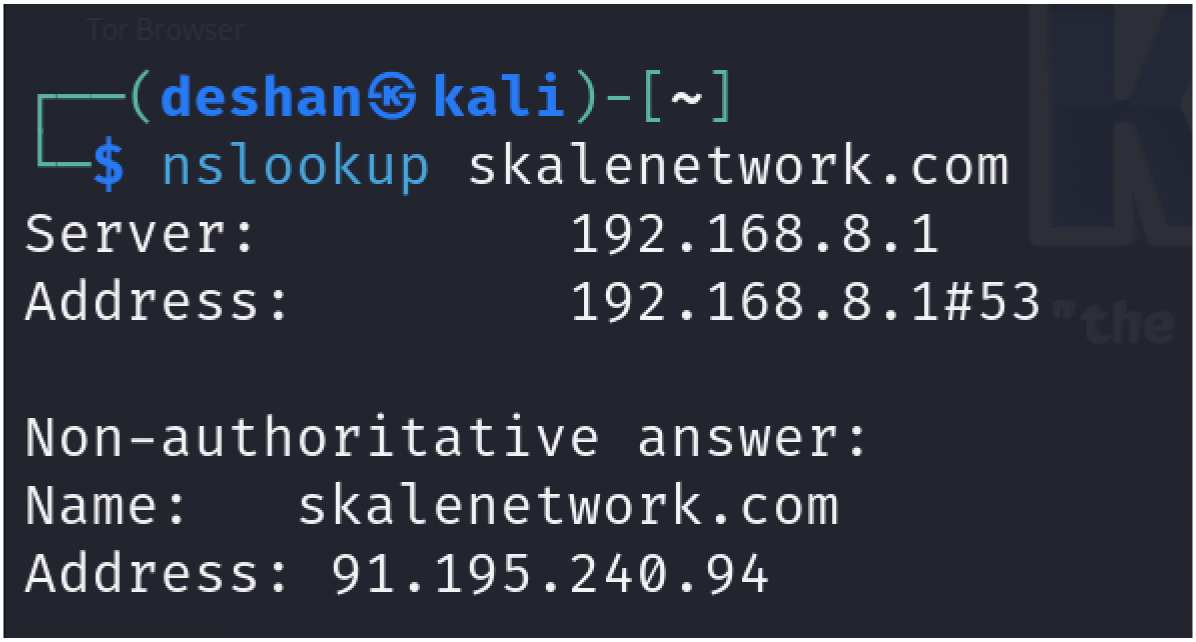
```
[*] No New Subdomains Found on the Current Page. Jumping to Result 3601.
[*] Searching Google for: site:skale.network.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3701.
[*] Searching Google for: site:skale.network.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3801.
[*] Searching Google for: site:skale.network.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 3901.
[*] Searching Google for: site:skale.network.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 4001.
[*] Searching Google for: site:skale.network.com
[!] Google CAPTCHA triggered. No bypass available.
[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:



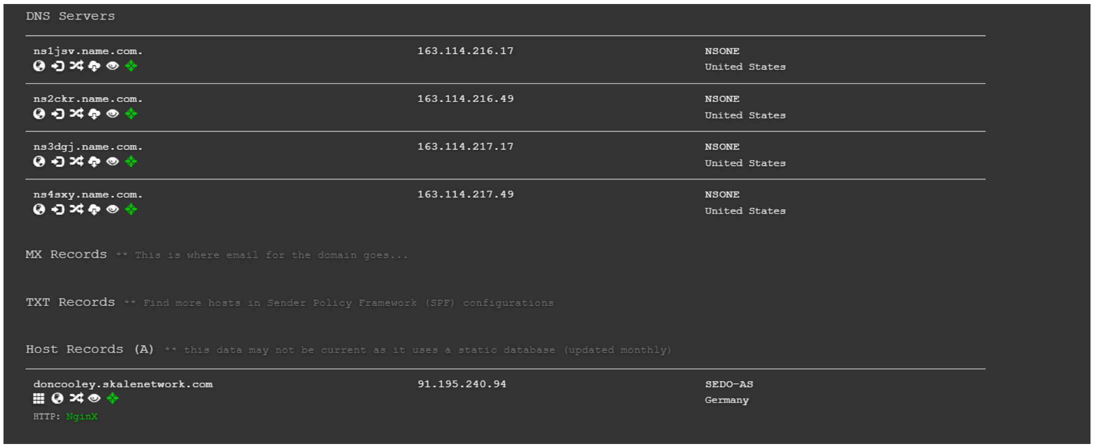
```
┌──(deshan㉿kali)-[~]
└─$ nslookup skalenetwork.com
Server:         192.168.8.1
Address:        192.168.8.1#53

Non-authoritative answer:
Name:   skalenetwork.com
Address: 91.195.240.94
```

DNS enumeration

- Dnsdumpster

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:

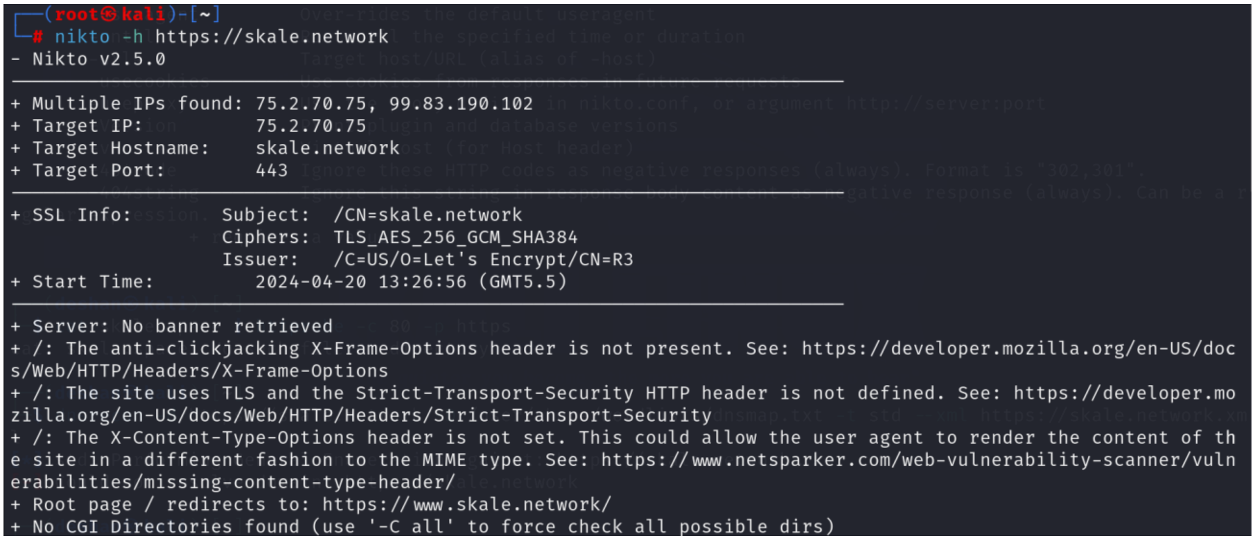


```
DNS Servers
 ns1jsv.name.com.                      163.114.216.17                  NSONE
                                                                       United States
 ns2ckr.name.com.                      163.114.216.49                  NSONE
                                                                       United States
 ns3dgj.name.com.                      163.114.217.17                  NSONE
                                                                       United States
 ns4sxy.name.com.                      163.114.217.49                  NSONE
                                                                       United States

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

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

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)
 doncooley.skalenetwork.com            91.195.240.94                   SEDO-AS
                                                                       Germany
 HTTP: NginX
```

- Nikto

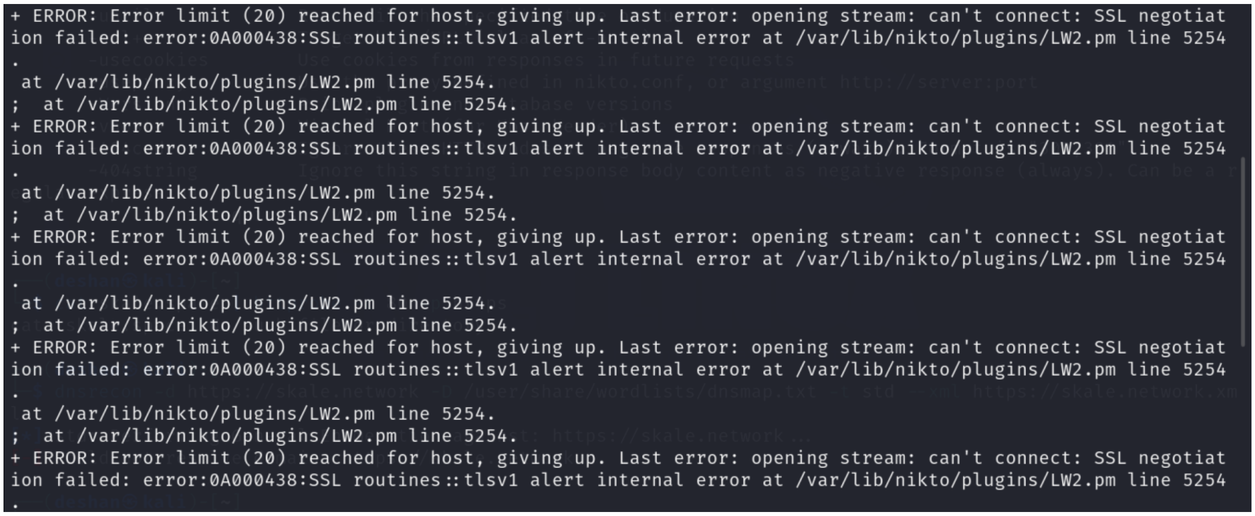
Nikto is an open-source web server scanner made to find possible security holes in applications and web servers. With its extensive scanning capabilities, it may identify problems including out-of-date software, unsafe configurations, weak scripts, and incorrect SSL/TLS settings. In addition to producing comprehensive results after scanning, Nikto may be customized and scripted, connects with automated workflows, and receives community assistance and frequent database upgrades. For security experts performing web security assessments, it's a useful tool that helps with vulnerability discovery and mitigation to improve overall security posture.

Proof of concept:

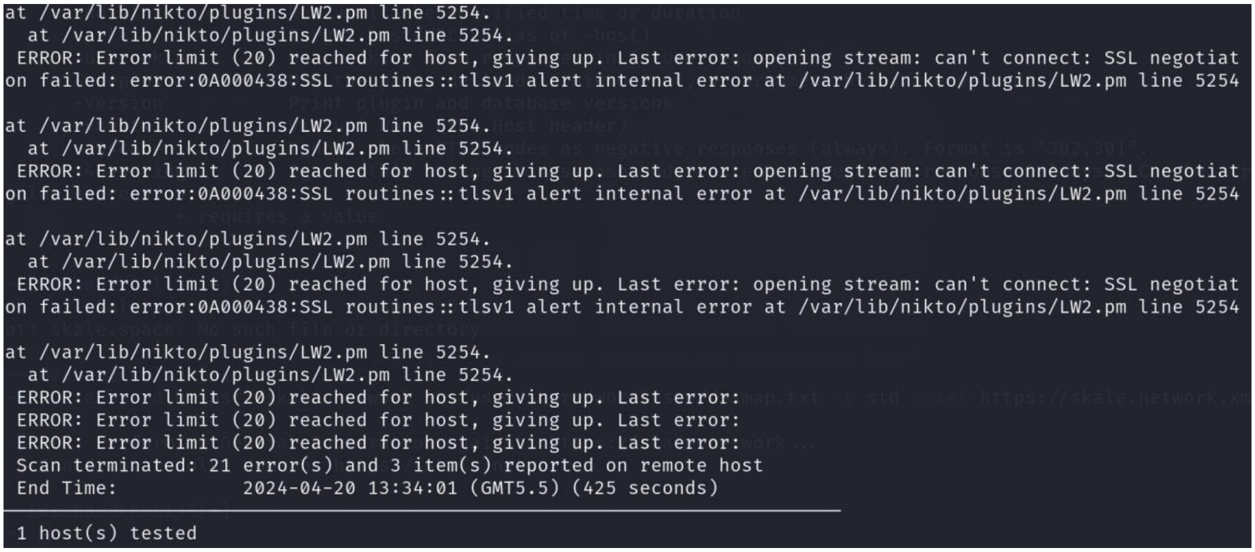


```
┌──(root㉿kali)-[~]
└─# nikto -h https://skale.network
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 75.2.70.75, 99.83.190.102
+ Target IP:          75.2.70.75
+ Target Hostname:    skale.network
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=skale.network
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2024-04-20 13:26:56 (GMT5.5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/doc
s/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mo
zilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of th
e site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vuln
erabilities/missing-content-type-header/
+ Root page / redirects to: https://www.skale.network/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Proof of concept:



```
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
ion failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254
.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
ion failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254
.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
ion failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254
.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
ion failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254
.
 at /var/lib/nikto/plugins/LW2.pm line 5254.
;  at /var/lib/nikto/plugins/LW2.pm line 5254.
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
ion failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254
.
```



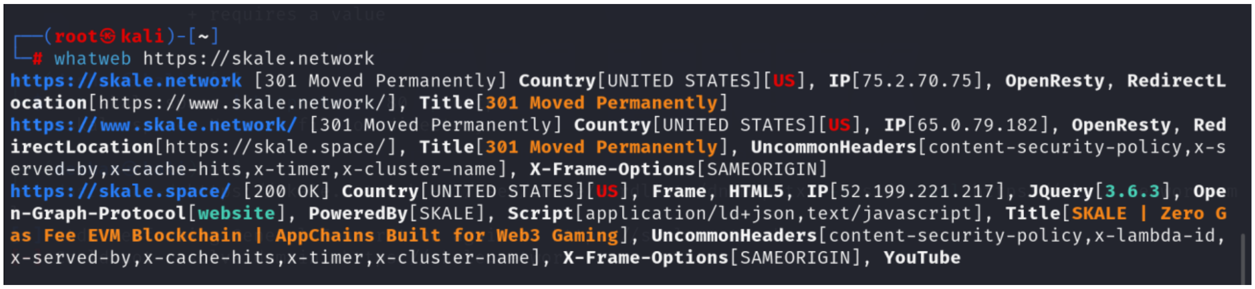
```
at /var/lib/nikto/plugins/LW2.pm line 5254.
  at /var/lib/nikto/plugins/LW2.pm line 5254.
 ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
on failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254

at /var/lib/nikto/plugins/LW2.pm line 5254.
  at /var/lib/nikto/plugins/LW2.pm line 5254.
 ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
on failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254

at /var/lib/nikto/plugins/LW2.pm line 5254.
  at /var/lib/nikto/plugins/LW2.pm line 5254.
 ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: can't connect: SSL negotiat
on failed: error:0A000438:SSL routines::tlsv1 alert internal error at /var/lib/nikto/plugins/LW2.pm line 5254

at /var/lib/nikto/plugins/LW2.pm line 5254.
  at /var/lib/nikto/plugins/LW2.pm line 5254.
 ERROR: Error limit (20) reached for host, giving up. Last error:
 ERROR: Error limit (20) reached for host, giving up. Last error:
 ERROR: Error limit (20) reached for host, giving up. Last error:
 Scan terminated: 21 error(s) and 3 item(s) reported on remote host
 End Time:           2024-04-20 13:34:01 (GMT5.5) (425 seconds)
---------------------------------------------------------------------------
 1 host(s) tested
```

Public devices enumeration

- 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:

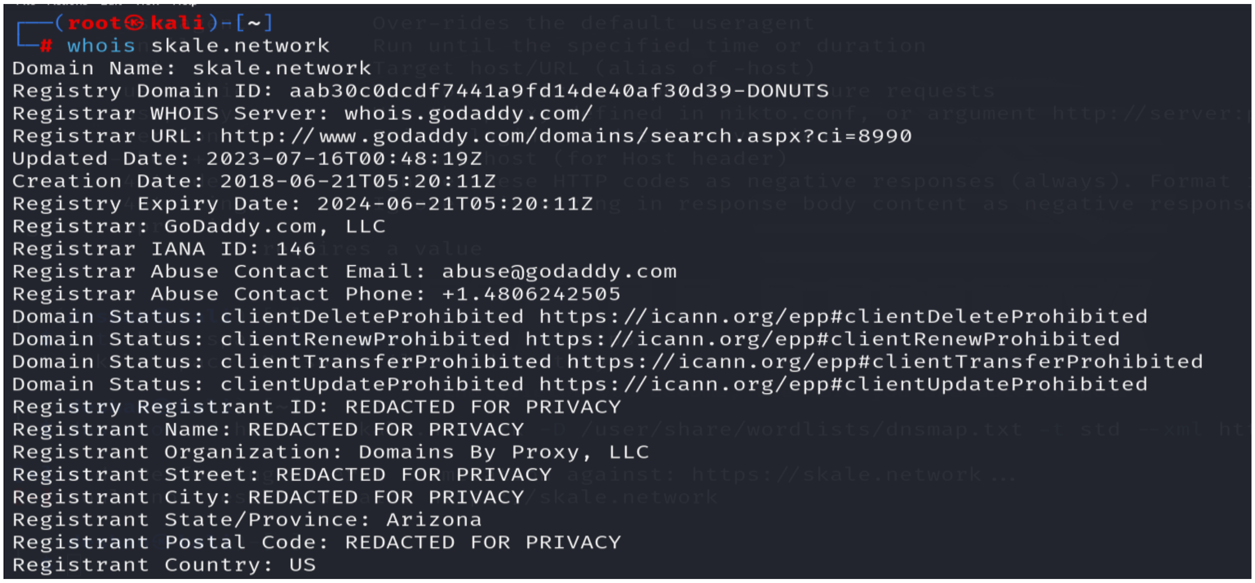


```
┌──(root㉿kali)-[~]
└─# whatweb https://skale.network
https://skale.network [301 Moved Permanently] Country[UNITED STATES][US], IP[75.2.70.75], OpenResty, RedirectL
ocation[https://www.skale.network/], Title[301 Moved Permanently]
https://www.skale.network/ [301 Moved Permanently] Country[UNITED STATES][US], IP[65.0.79.182], OpenResty, Red
irectLocation[https://skale.space/], Title[301 Moved Permanently], UncommonHeaders[content-security-policy,x-s
erved-by,x-cache-hits,x-timer,x-cluster-name], X-Frame-Options[SAMEORIGIN]
https://skale.space/ [200 OK] Country[UNITED STATES][US], Frame, HTML5, IP[52.199.221.217], JQuery[3.6.3], Ope
n-Graph-Protocol[website], PoweredBy[SKALE], Script[application/ld+json,text/javascript], Title[SKALE | Zero G
as Fee EVM Blockchain | AppChains Built for Web3 Gaming], UncommonHeaders[content-security-policy,x-lambda-id,
x-served-by,x-cache-hits,x-timer,x-cluster-name], X-Frame-Options[SAMEORIGIN], YouTube
```

- Whois

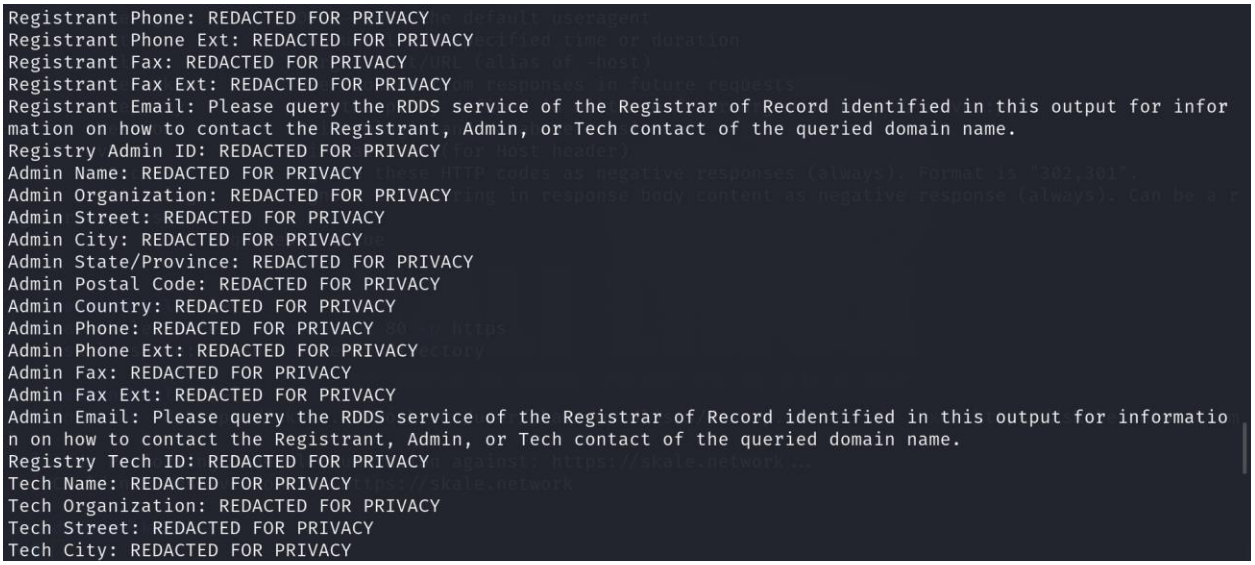
A key networking tool and protocol, whois is used to query databases and obtain data on IP addresses, domain names, and autonomous system numbers (ASNs). It offers information about domain registration, owner contact details, DNS information, IP address allocation, and ASN ownership. Whois is frequently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



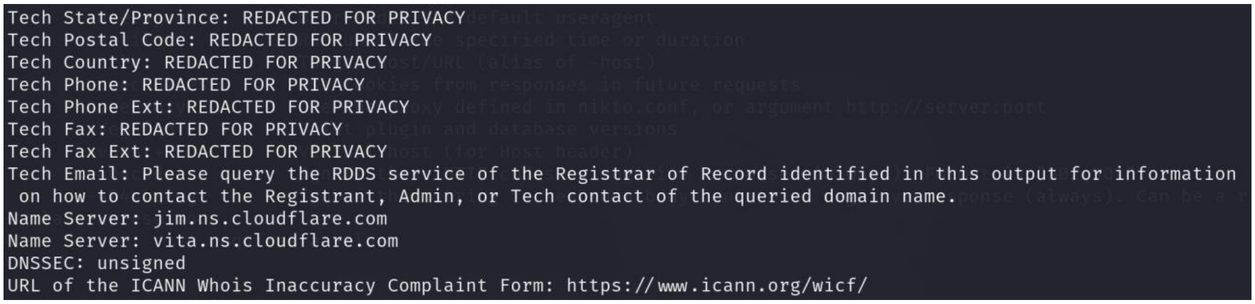
```
┌──(root㉿kali)-[~]
└─# whois skale.network
Domain Name: skale.network
Registry Domain ID: aab30c0dcdf7441a9fd14de40af30d39-DONUTS
Registrar WHOIS Server: whois.godaddy.com/
Registrar URL: http://www.godaddy.com/domains/search.aspx?ci=8990
Updated Date: 2023-07-16T00:48:19Z
Creation Date: 2018-06-21T05:20:11Z
Registry Expiry Date: 2024-06-21T05:20:11Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Domains By Proxy, LLC
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Arizona
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: US
```

Proof of concept:

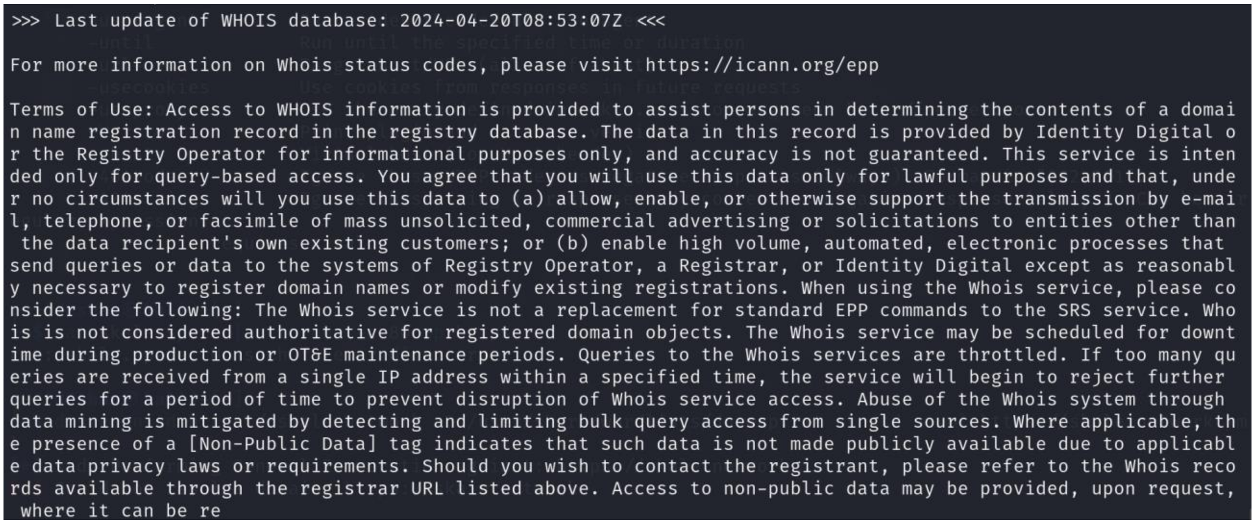


```
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for infor
mation on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for informatio
n on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
```

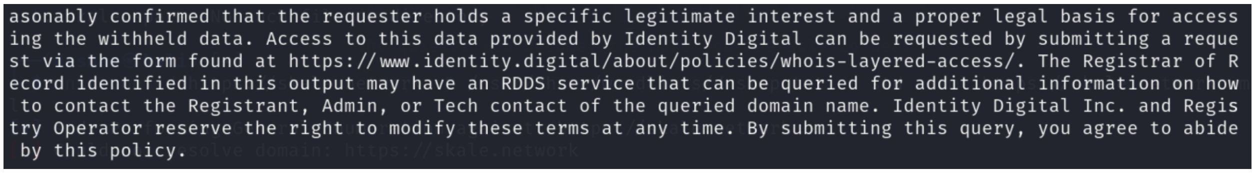
Proof of concept:



```
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please query the RDDS service of the Registrar of Record identified in this output for information
 on how to contact the Registrant, Admin, or Tech contact of the queried domain name.
Name Server: jim.ns.cloudflare.com
Name Server: vita.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```



```
>>> Last update of WHOIS database: 2024-04-20T08:53:07Z <<<

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

Terms of Use: Access to WHOIS information is provided to assist persons in determining the contents of a domai
n name registration record in the registry database. The data in this record is provided by Identity Digital o
r the Registry Operator for informational purposes only, and accuracy is not guaranteed. This service is inten
ded only for query-based access. You agree that you will use this data only for lawful purposes and that, unde
r no circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mai
l, telephone, or facsimile of mass unsolicited, commercial advertising or solicitations to entities other than
 the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that
send queries or data to the systems of Registry Operator, a Registrar, or Identity Digital except as reasonabl
y necessary to register domain names or modify existing registrations. When using the 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. Queries to the Whois services are throttled. If too many qu
eries are received from a single IP address within a specified time, the service will begin to reject further
queries for a period of time to prevent disruption of Whois service access. Abuse of the Whois system through
data mining is mitigated by detecting and limiting bulk query access from single sources. Where applicable, th
e presence of a [Non-Public Data] tag indicates that such data is not made publicly available due to applicabl
e data privacy laws or requirements. Should you wish to contact the registrant, please refer to the Whois reco
rds available through the registrar URL listed above. Access to non-public data may be provided, upon request,
 where it can be re
```



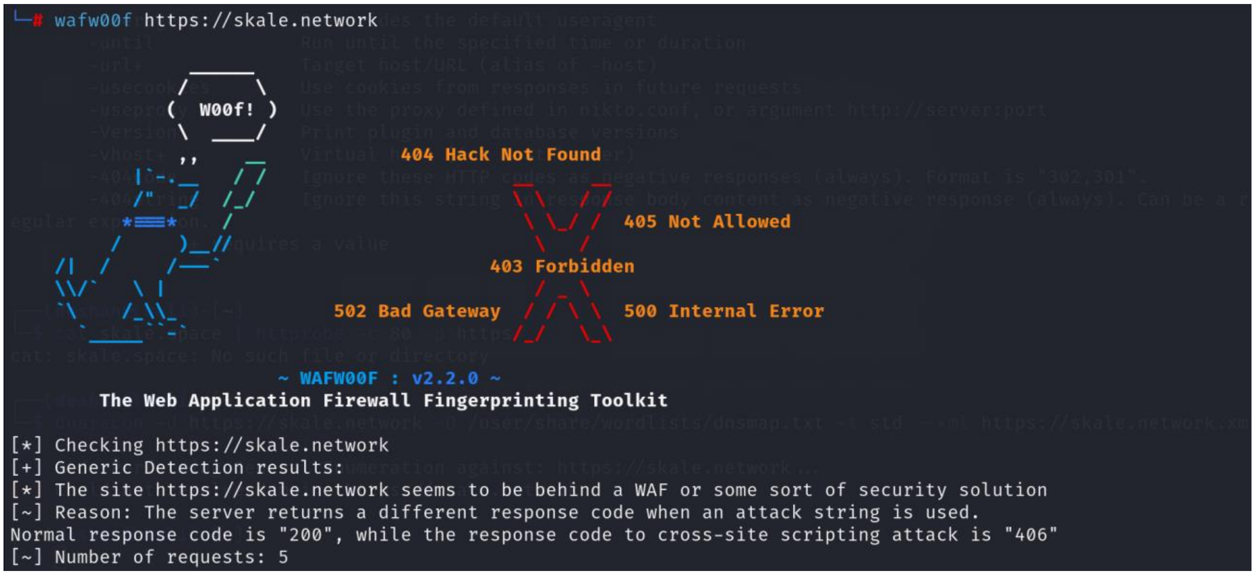
```
asonably confirmed that the requester holds a specific legitimate interest and a proper legal basis for access
ing the withheld data. Access to this data provided by Identity Digital can be requested by submitting a reque
st via the form found at https://www.identity.digital/about/policies/whois-layered-access/. The Registrar of R
ecord identified in this output may have an RDDS service that can be queried for additional information on how
 to contact the Registrant, Admin, or Tech contact of the queried domain name. Identity Digital Inc. and Regis
try Operator reserve the right to modify these terms at any time. By submitting this query, you agree to abide
 by this policy.
```

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:



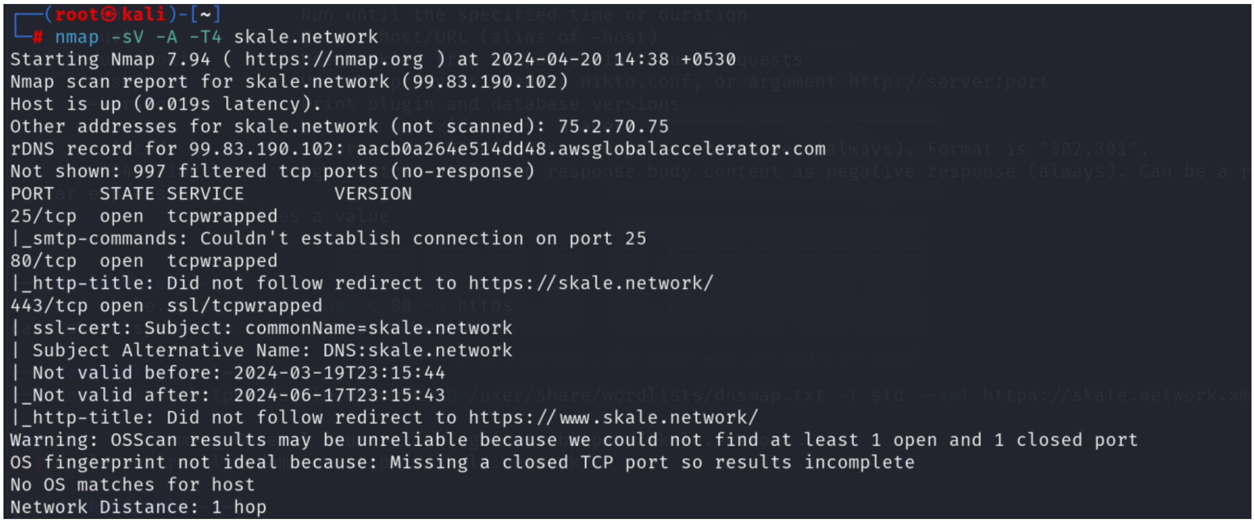
```
└─# wafw00f https://skale.network

                  ( W00f! )

                                    404 Hack Not Found

                                                    405 Not Allowed

                                        403 Forbidden

                            502 Bad Gateway         500 Internal Error

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

[*] Checking https://skale.network
[+] Generic Detection results:
[*] The site https://skale.network seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "406"
[~] Number of requests: 5
```

Find open ports.

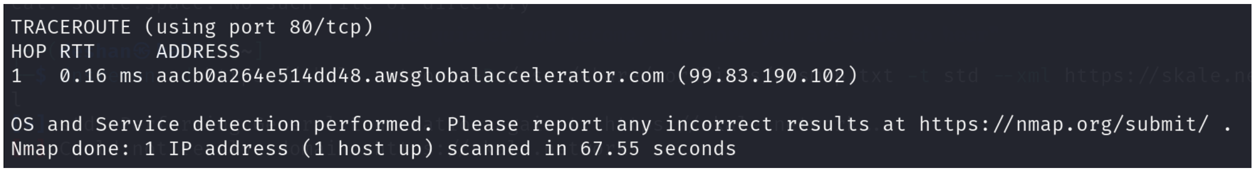
- Nmap

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 skale.network
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-20 14:38 +0530
Nmap scan report for skale.network (99.83.190.102)
Host is up (0.019s latency).
Other addresses for skale.network (not scanned): 75.2.70.75
rDNS record for 99.83.190.102: aacb0a264e514dd48.awsglobalaccelerator.com
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE        VERSION
25/tcp  open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp  open  tcpwrapped
|_http-title: Did not follow redirect to https://skale.network/
443/tcp open  ssl/tcpwrapped
| ssl-cert: Subject: commonName=skale.network
| Subject Alternative Name: DNS:skale.network
| Not valid before: 2024-03-19T23:15:44
|_Not valid after:  2024-06-17T23:15:43
|_http-title: Did not follow redirect to https://www.skale.network/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop
```



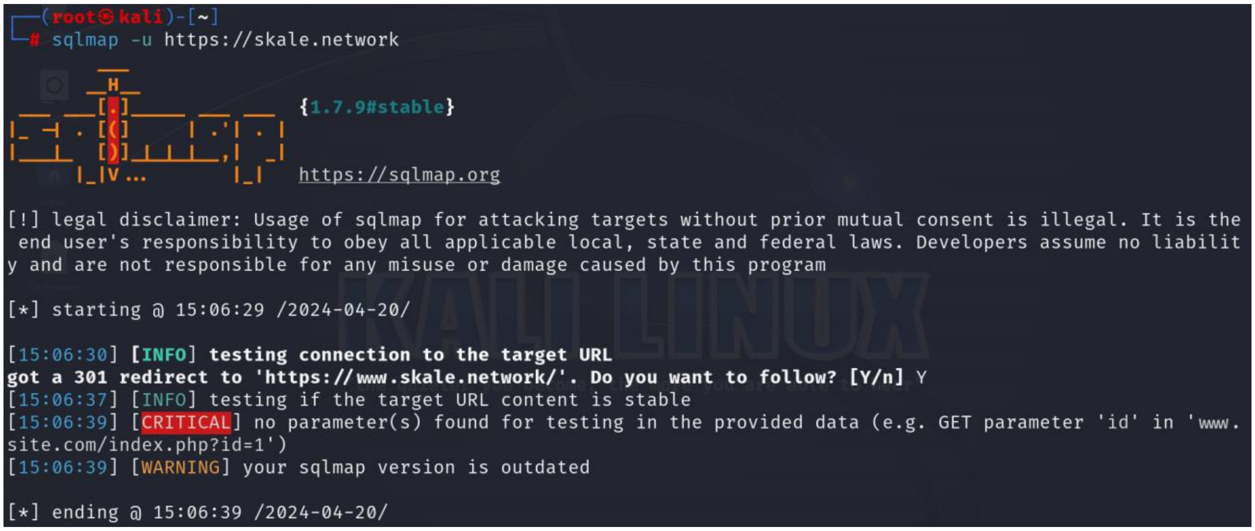
```
TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.16 ms aacb0a264e514dd48.awsglobalaccelerator.com (99.83.190.102)

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 67.55 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:



```
┌──(root㉿kali)-[~]
└─# sqlmap -u https://skale.network
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.7.9#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
 end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liabilit
y and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:06:29 /2024-04-20/

[15:06:30] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.skale.network/'. Do you want to follow? [Y/n] Y
[15:06:37] [INFO] testing if the target URL content is stable
[15:06:39] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.
site.com/index.php?id=1')
[15:06:39] [WARNING] your sqlmap version is outdated

[*] ending @ 15:06:39 /2024-04-20/
```

Vulnerability analysis phase

I used tool like netsparker to process and catch bugs and vulnerabilities are based on OWASP top 10.

Targeted Domain: - https://skale.network.com

- Netsparker

An automated web application security scanner known for its precision and extensive vulnerability finding capabilities is called Netsparker. It simplifies the procedure for examining online applications and finds many security flaws, such as SQL injection, XSS, and misconfigurations. With its ability to provide comprehensive reports for compliance audits and vulnerability monitoring, Netsparker seamlessly interacts with development workflows. Because of its intuitive interface, sophisticated features like support for continuous monitoring and authentication, and free support and upgrades, it's a great resource for security experts and companies looking to effectively strengthen their web application security posture.

Vulnerability title

HTTP Strict Transport Security (HSTS) Policy Not Enabled

Vulnerability description

The HTTP Strict Transport Security (HSTS) policy is not enabled, according to Netsparker.In addition to being delivered via HTTPS, the target website does not implement HSTS policies. Over the use of HTTP Strict Transport Security (HSTS), a web server can establish rules mandating that compliant user agents—like a web browser—interact with it exclusively over secure (HTTPS) connections. "Strict-Transport-Security" is an HTTP response header field that the server uses to transmit the HSTS Policy to the user agent. The HSTS Policy establishes a time frame for the user agent to exclusively employ secure methods of server access.

Impact assessment

The impact assessment of not having HSTS enabled includes vulnerabilities to SSL stripping, man-in-the-middle attacks, and data tampering during transit, posing risks to user data protection, trust, and compliance.

Affected components

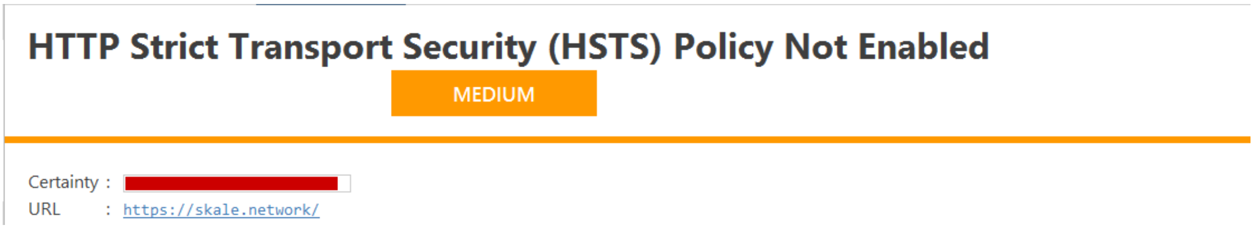
When HTTP Strict Transport Security (HSTS) is not there, there are security vulnerabilities associated with different parts of a web application and its infrastructure. The web server configuration, network traffic, user sessions, data integrity while in transit, adherence to compliance standards, and user trust and experience are among the components that are impacted.

How to mitigate?

1. Enable the Strict-Transport-Security header in your web server's HTTP responses.
2. Set appropriate directives such as max-age, includeSubDomains, and preload to enforce HTTPS connections and secure subdomains.
3. Ensure your website uses HTTPS with a valid SSL/TLS certificate and implement server-side redirects to HTTPS.

4. Thoroughly test and validate HTTPS enforcement across all pages and subdomains after enabling HSTS.
5. Consider submitting your domain to the HSTS preload list for wider browser support.
6. Regularly monitor and update your website's security configurations and HSTS policy to stay protected against evolving threats.

Proof of concept:



HTTP Strict Transport Security (HSTS) Policy Not Enabled

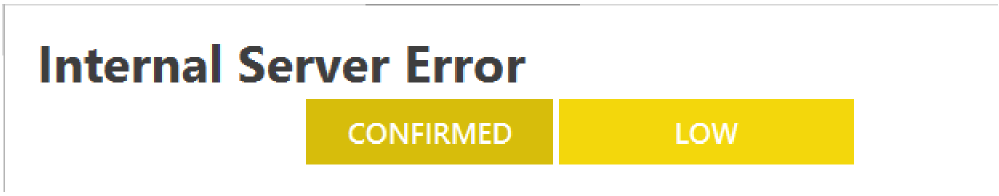
MEDIUM

Certainty :

URL : https://skale.network/

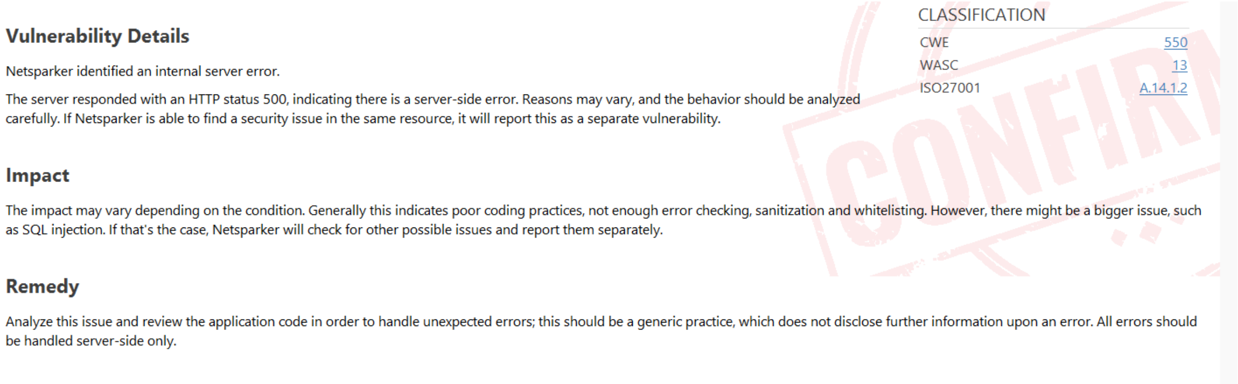
Other vulnerabilities were identified during the scan

- Internal Server Error (Confirmed)



Internal Server Error

CONFIRMED LOW



Vulnerability Details

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

CLASSIFICATION	
CWE	550
WASC	13
ISO27001	A.14.1.2

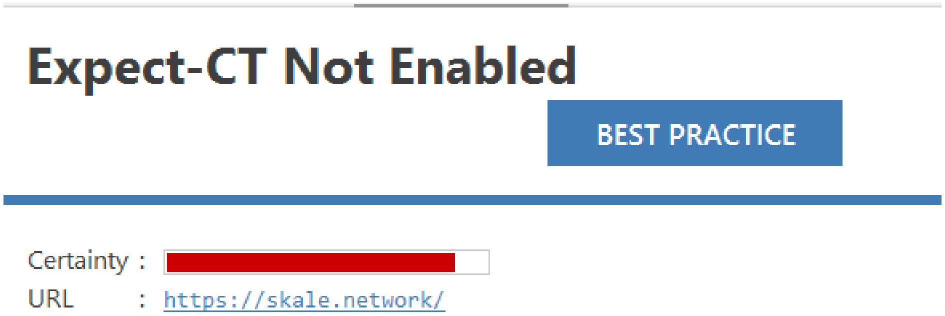
Impact

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting. However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Remedy

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error. All errors should be handled server-side only.

- Expect-CT Not Enabled

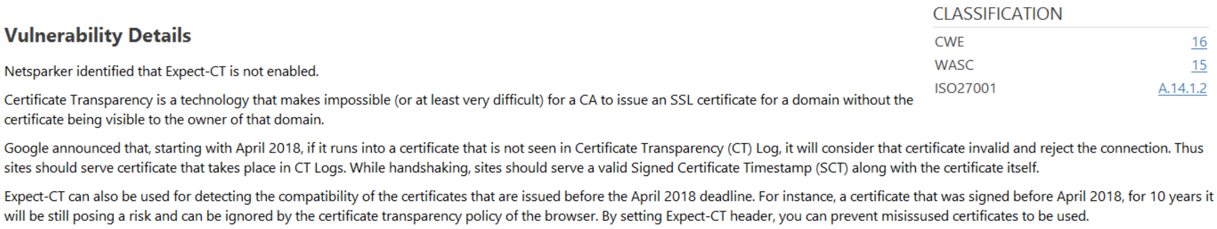


Expect-CT Not Enabled

BEST PRACTICE

Certainty :

URL : https://skale.network/



Vulnerability Details

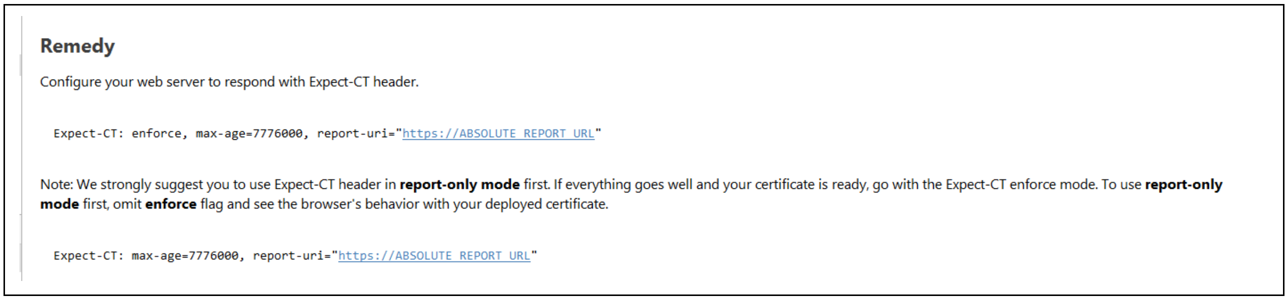
Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

CLASSIFICATION	
CWE	16
WASC	15
ISO27001	A.14.1.2

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissused certificates to be used.



Remedy

Configure your web server to respond with Expect-CT header.

```
Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

```
Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"
```

Conclusion

Emphasized the decentralized management of the SKALE Network and the engagement of multiple entities and contributors. Addressed security concerns based on OWASP top 10 vulnerabilities including broken access control, cryptographic failures, injection flaws, insecure design, misconfigurations, and more.Your assessment provides a holistic view of the security posture of the SKALE Network, highlighting vulnerabilities and suggesting actionable mitigation steps to improve overall security and reduce risks.