Sri Lanka Institute of Information Technology

IE2062-Web Security

IT Number	Name
IT22581402	C.D.Aluthge

Information gathering and reconnaissance phase

1. Subdomain enumeration
    i. Recon-ng

    b. Getting alive subdomains
        i. dnsdumpster

    c. DNS (Domain Name System) enumeration
        i. Dnsrecon
        ii. Nikto

    d. Public devices enumeration
        i. Censys
        ii. Whois

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

    f. Find open ports.
        i. Nmap

    g. Exploitation
        i. Sqlmap

vulnerability analysis phase

1. Target domain: http://smtp2go.com

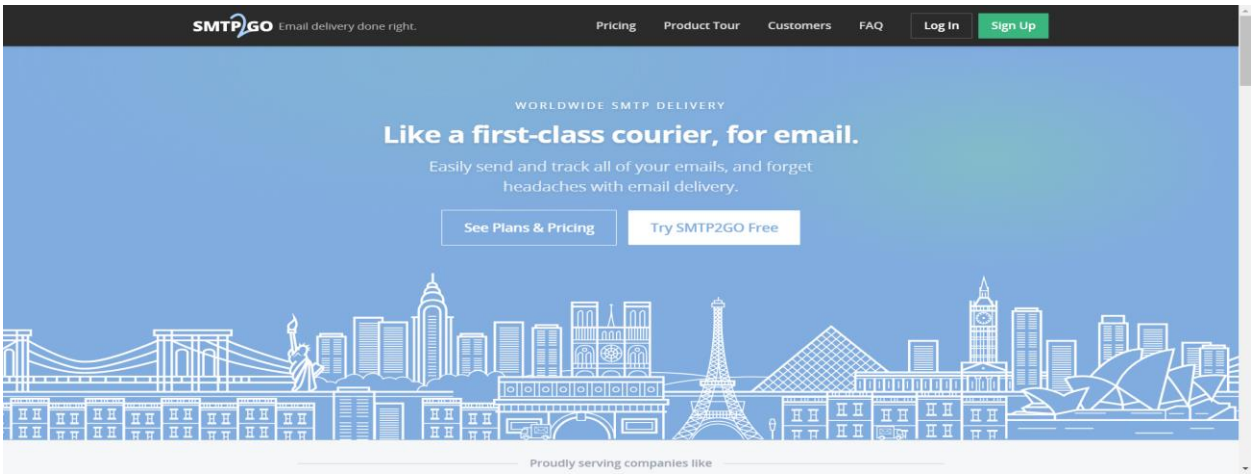
a. Cloud Metadata Potentially Exposed
b. Content Security Policy (CSP) Header Not Set (Medium)
c. HTTP to HTTPS Insecure Transition in Form Post (Medium) d
d. Missing Anti-clickjacking Header (Medium)
e. Absence of Anti-CSRF Tokens (Medium)
f. Hidden File Found (Medium)

Conclusion

Scope:

SMTP2GO is an email delivery service provider that specializes in ensuring that your emails are delivered reliably and securely. They offer features such as email authentication, real-time analytics, and dedicated

IP addresses to help improve email deliverability rates. SMTP2GO is commonly used by businesses and organizations that rely on email communication for marketing, transactional emails, and general correspondence.



In Scope:

Asset name	Type	Coverage	Max. severity	Bounty	Last update
api.smtp2go.com Most of the endpoints are handled by Flask on Python3 with Postgres as a main database. Newer endpoints use Go on Gin framework. Redis is mostly used for cache and ratelimitting. Instructions and documentations can be found here: https://apidoc.smtp2go.com/documentation/ English apache Flask Go PostgresSQL Python Redis	Domain	In scope	Critical	Eligible	Mar 15, 2022
app.smtp2go.com Flask based app running on Python 2.7, some pages are VueJS but most are scripted with custom JQuery. Create a free account in order to gain login access. English JavaScript PostgresSQL Python Redis	Domain	In scope	Critical	Eligible	Mar 15, 2022
smtp2go.com Standard Wordpress site hosted with WPEngine, scripting is all custom JQuery based. English MySQL PHP Wordpress	Domain	In scope	Critical	Eligible	Mar 15, 2022

Out Of Scope

support.smtp2go.com	Domain	Out of scope	None	Ineligible	Mar 15, 2022

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 is 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://smtp2go.com

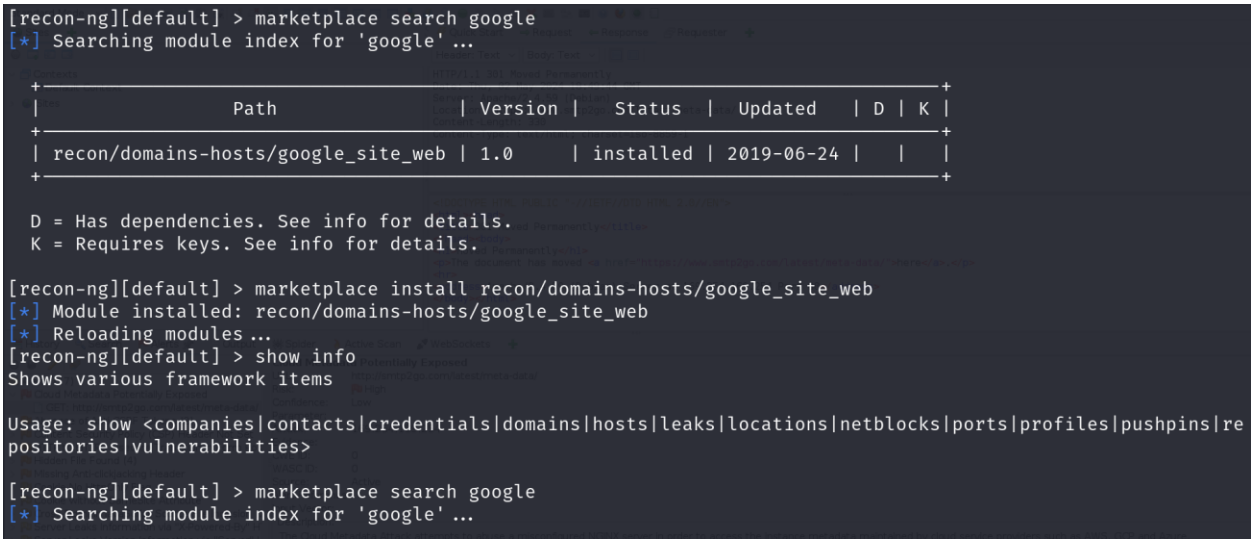
Subdomain enumeration

- Recon-ng

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

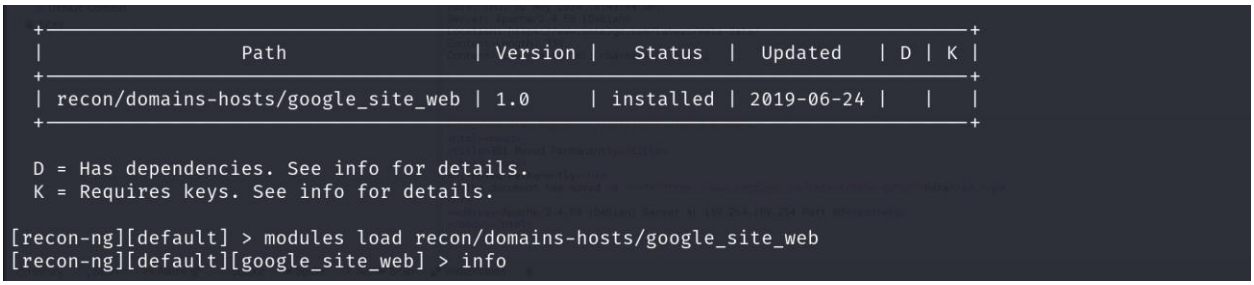
Proof of concept:

To get google website give this command.

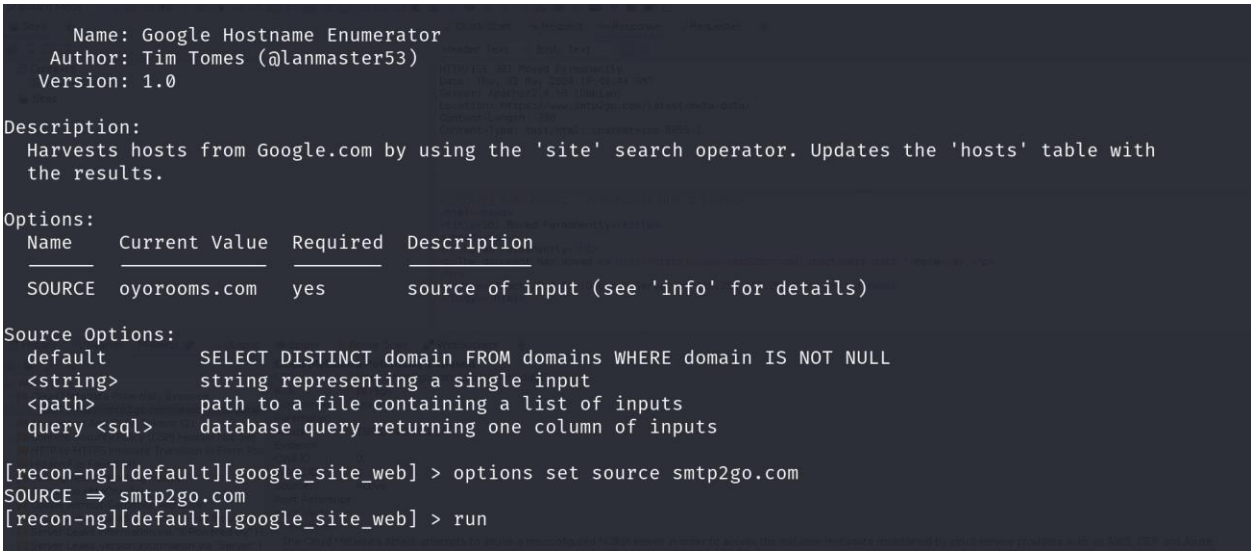


Proof of concept:

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



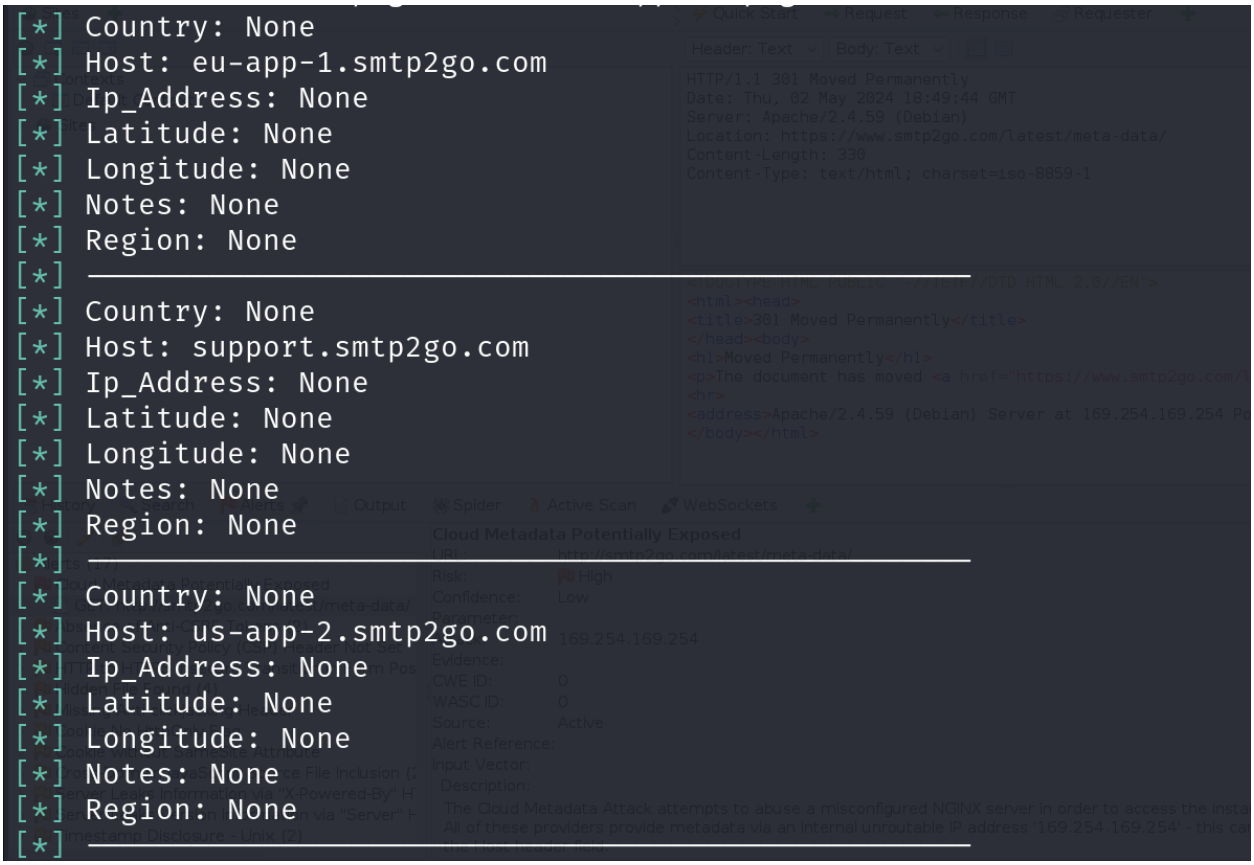
```
  +-------------------------------------------------------------------------------+
  |                 Path                 | Version |   Status  |  Updated   | D | K |
  +-------------------------------------------------------------------------------+
  | recon/domains-hosts/google_site_web | 1.0     | 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
```



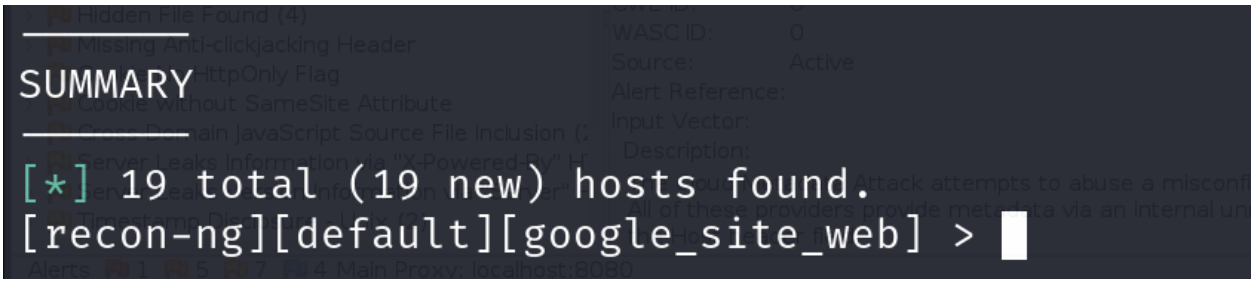
```
       Name: Google Hostname Enumerator
     Author: Tim Tomes (@lanmaster53)
    Version: 1.0

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  oyorooms.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 smtp2go.com
SOURCE => smtp2go.com
[recon-ng][default][google_site_web] > run
```

Proof of concept:

Proof of concept:



Proof of concept:

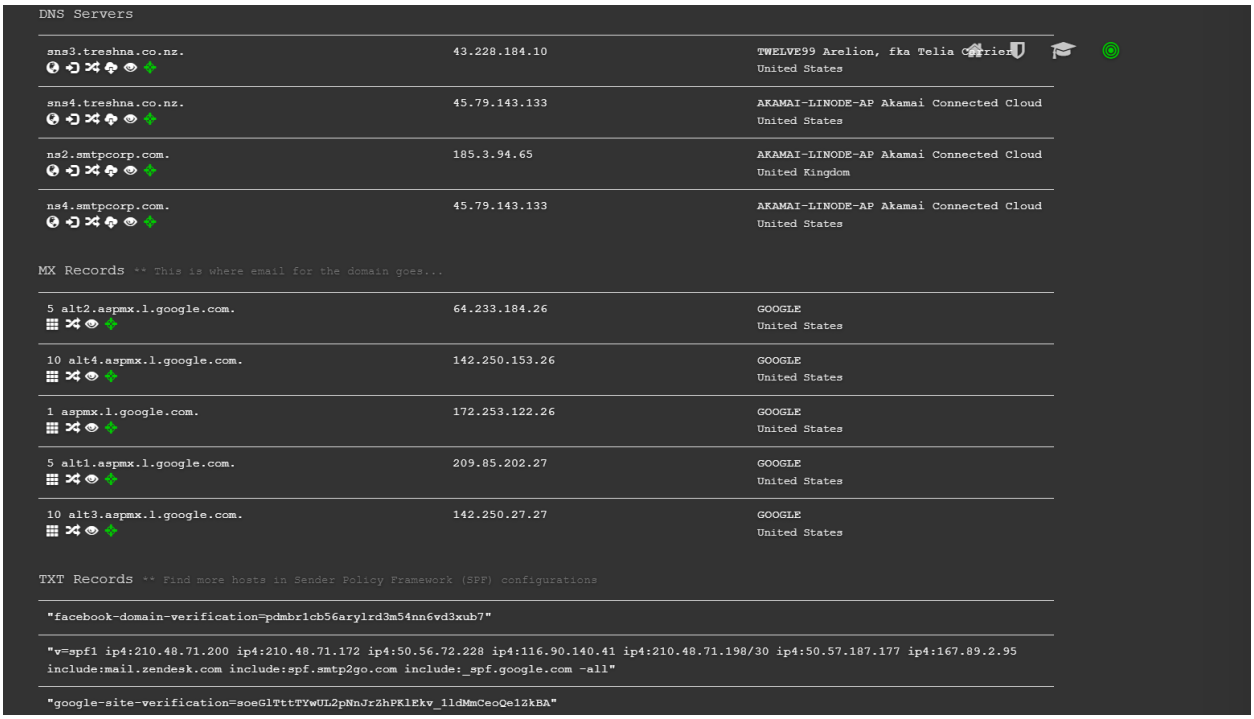


Getting alive subdomains

- 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

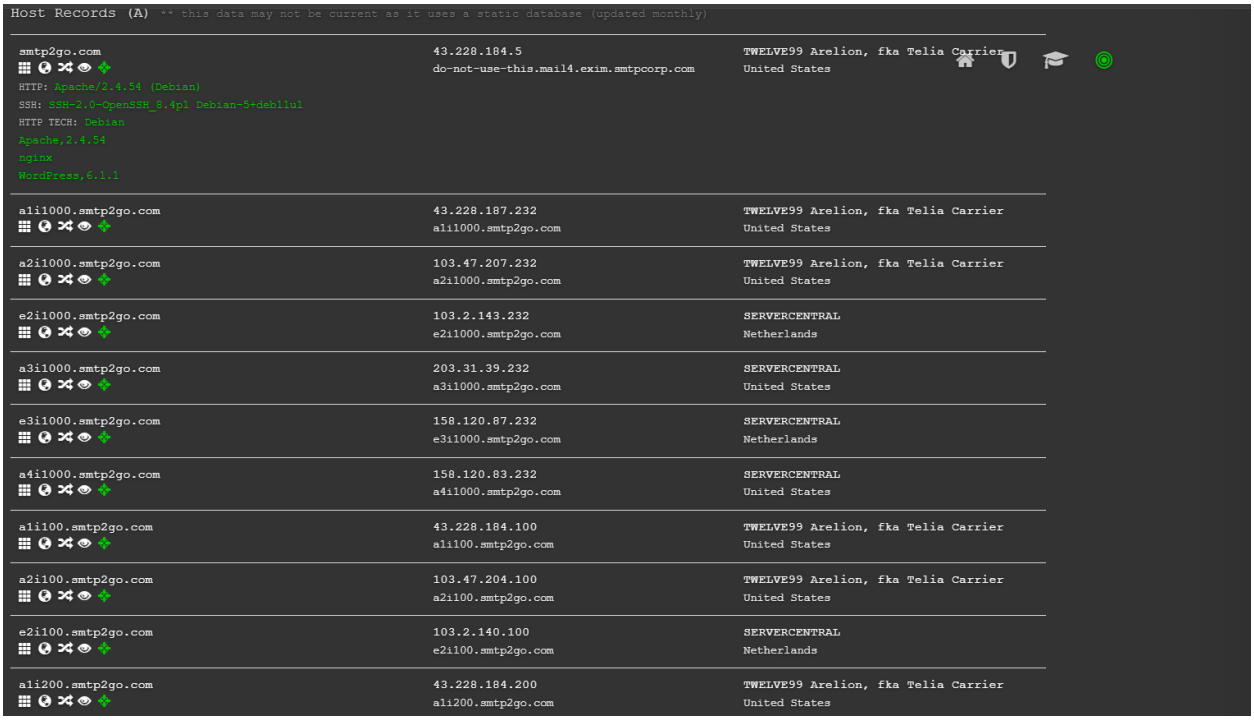
sns3.treshna.co.nz.	43.228.184.10	TWELVE99 Arelion, fka Telia Carrier United States
sns4.treshna.co.nz.	45.79.143.133	AKAMAI-LINODE-AP Akamai Connected Cloud United States
ns2.smtpcorp.com.	185.3.94.65	AKAMAI-LINODE-AP Akamai Connected Cloud United Kingdom
ns4.smtpcorp.com.	45.79.143.133	AKAMAI-LINODE-AP Akamai Connected Cloud United States

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

5 alt2.aspmx.l.google.com.	64.233.184.26	GOOGLE United States
10 alt4.aspmx.l.google.com.	142.250.153.26	GOOGLE United States
1 aspmx.l.google.com.	172.253.122.26	GOOGLE United States
5 alt1.aspmx.l.google.com.	209.85.202.27	GOOGLE United States
10 alt3.aspmx.l.google.com.	142.250.27.27	GOOGLE United States

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

"facebook-domain-verification=pdmbr1cb56arylrd3m54nn6vd3xub7"
"v=spf1 ip4:210.48.71.200 ip4:210.48.71.172 ip4:50.56.72.228 ip4:116.90.140.41 ip4:210.48.71.198/30 ip4:50.57.187.177 ip4:167.89.2.95 include:mail.zendesk.com include:spf.smtp2go.com include:_spf.google.com -all"
"google-site-verification=soeGlTttTYwUL2pNnJrZhPKlEkv_11dMmCeoQe1ZkBA"



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

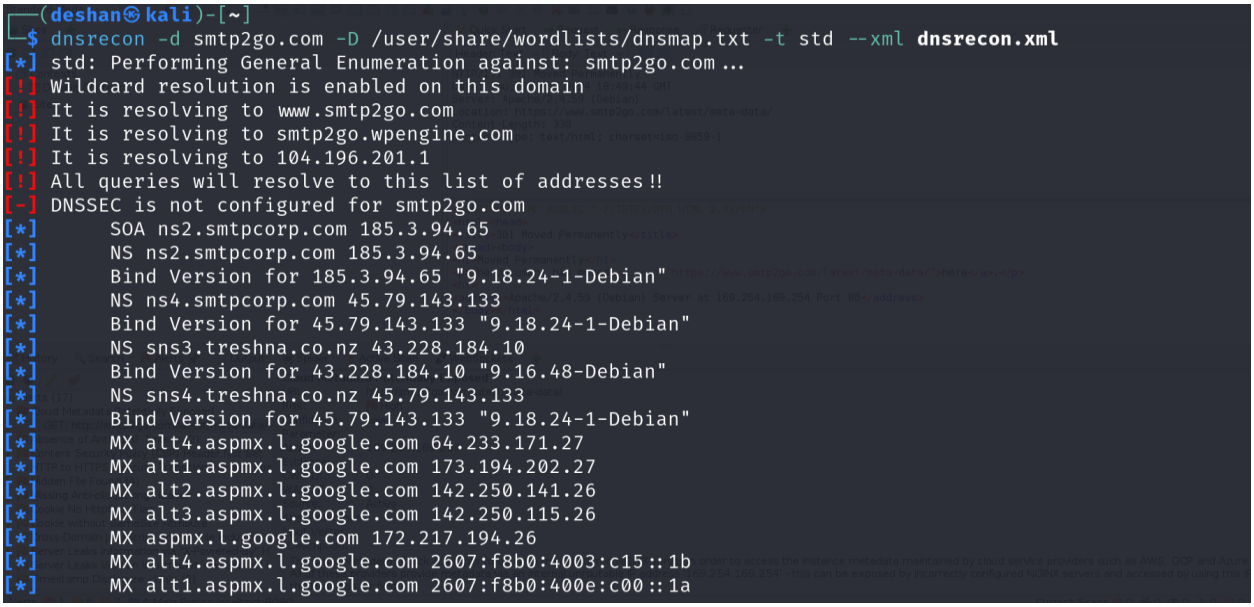
smtp2go.com HTTP: Apache/2.4.54 (Debian) SSH: SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 HTTP TECH: Debian Apache,2.4.54 nginx WordPress,6.1.1	43.228.184.5 do-not-use-this.mail4.exim.smtpcorp.com	TWELVE99 Arelion, fka Telia Carrier United States
a1i1000.smtp2go.com	43.228.187.232 a1i1000.smtp2go.com	TWELVE99 Arelion, fka Telia Carrier United States
a2i1000.smtp2go.com	103.47.207.232 a2i1000.smtp2go.com	TWELVE99 Arelion, fka Telia Carrier United States
e2i1000.smtp2go.com	103.2.143.232 e2i1000.smtp2go.com	SERVERCENTRAL Netherlands
a3i1000.smtp2go.com	203.31.39.232 a3i1000.smtp2go.com	SERVERCENTRAL United States
e3i1000.smtp2go.com	158.120.87.232 e3i1000.smtp2go.com	SERVERCENTRAL Netherlands
a4i1000.smtp2go.com	158.120.83.232 a4i1000.smtp2go.com	SERVERCENTRAL United States
a1i100.smtp2go.com	43.228.184.100 a1i100.smtp2go.com	TWELVE99 Arelion, fka Telia Carrier United States
a2i100.smtp2go.com	103.47.204.100 a2i100.smtp2go.com	TWELVE99 Arelion, fka Telia Carrier United States
e2i100.smtp2go.com	103.2.140.100 e2i100.smtp2go.com	SERVERCENTRAL Netherlands
a1i200.smtp2go.com	43.228.184.200 a1i200.smtp2go.com	TWELVE99 Arelion, fka Telia Carrier United States

DNS enumeration

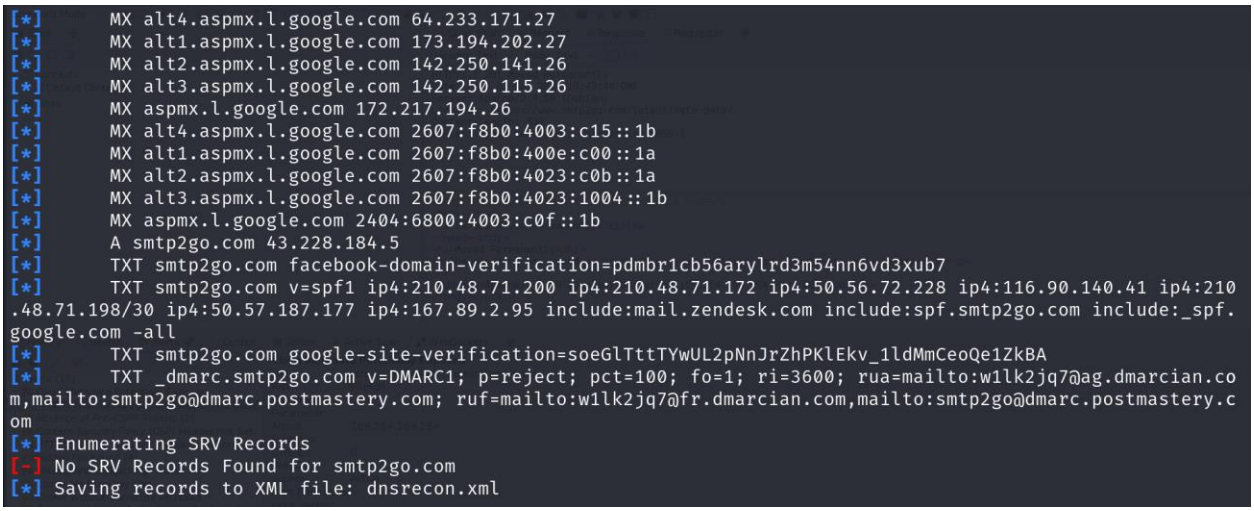
- Dnsrecon

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

Proof of concept:



Proof of concept:



- 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:

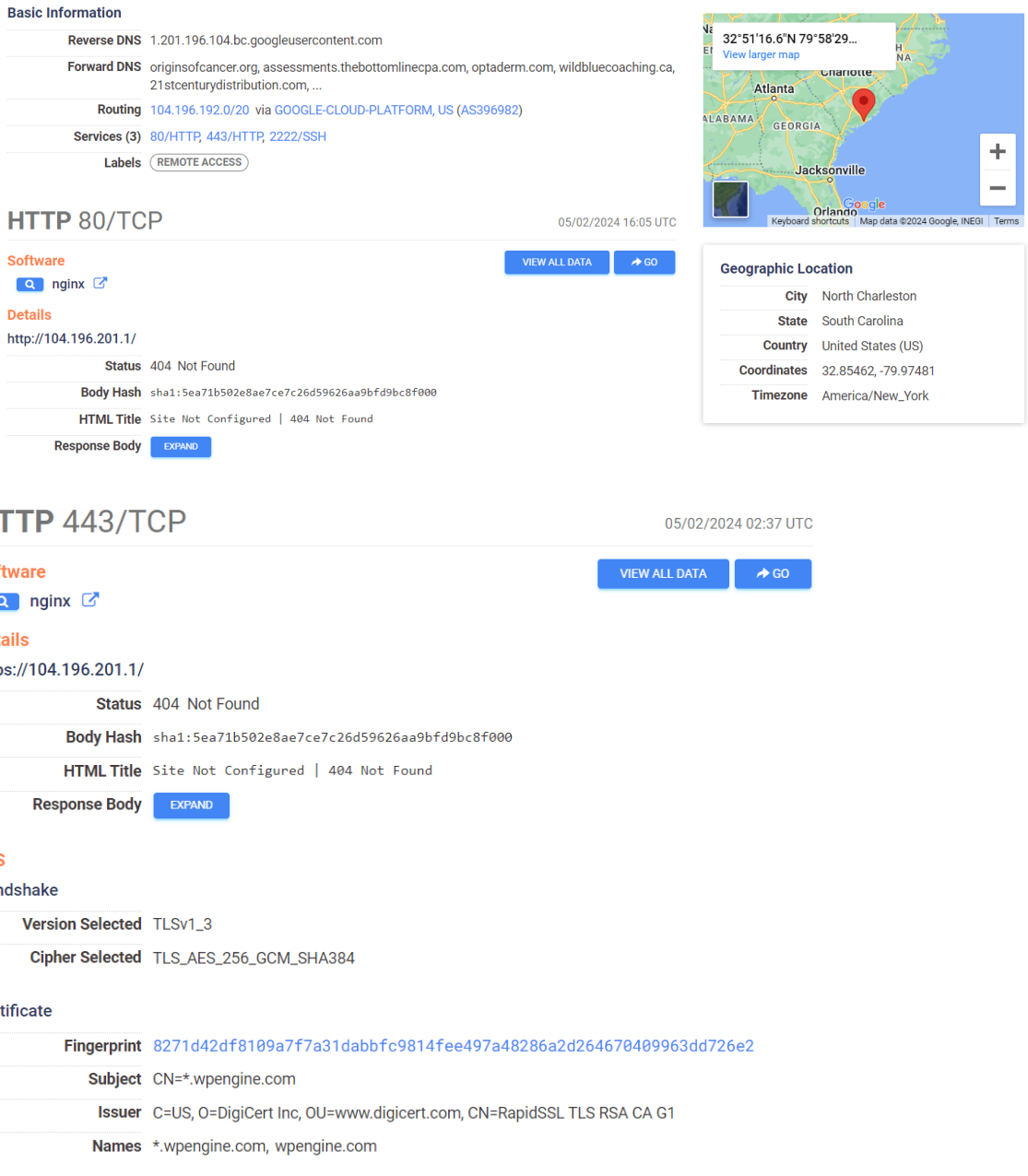
```
┌──(root㉿kali)-[~]
└─# nikto -h http://smtp2go.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          43.228.184.5
+ Target Hostname:    smtp2go.com
+ Target Port:        80
+ Start Time:         2024-05-03 02:17:12 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.59 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://www.smtp2go.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7963 requests: 0 error(s) and 2 item(s) reported on remote host
+ End Time:           2024-05-03 03:01:13 (GMT5.5) (2641 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Public devices enumeration

- Censys

Censys is a potent internet scanning tool that scans and monitors devices, networks, and services online all the time. It performs thorough scans, keeps track of SSL/TLS certificates, keeps an eye on attack surfaces, finds vulnerabilities, and offers threat information. Large volumes of data may be searched and analyzed, processes can be automated with the help of the API, and Censys can be integrated into security workflows. In the connected digital world of today, Censys is useful for asset discovery, vulnerability management, compliance monitoring, and proactive risk reduction.

Proof of concept:



Proof of concept:

- 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 smtp2go.com
   Domain Name: SMTP2GO.COM
   Registry Domain ID: 491952227_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.godaddy.com
   Registrar URL: http://www.godaddy.com
   Updated Date: 2022-09-04T05:23:42Z
   Creation Date: 2006-06-20T10:35:02Z
   Registry Expiry Date: 2025-06-20T10:35:02Z
   Registrar: GoDaddy.com, LLC
   Registrar IANA ID: 146
   Registrar Abuse Contact Email: abuse@godaddy.com
   Registrar Abuse Contact Phone: 480-624-2505
   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
   Name Server: NS2.SMTPCORP.COM
   Name Server: SNS1.TRESHNA.CO.NZ
   Name Server: SNS2.TRESHNA.CO.NZ
   Name Server: SNS3.TRESHNA.CO.NZ
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-05-02T20:48:44Z <<<
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: SMTP2GO.COM
Registry Domain ID: 491952227_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2022-04-17T20:19:57Z
Creation Date: 2006-06-20T05:35:02Z
Registrar Registration Expiration Date: 2025-06-20T05:35:02Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
```

Proof of concept:

```
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=SMTP2
GO.COM
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=SMTP2GO.CO
M
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
```

```
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=SMTP2GO.COM
Name Server: SNS1.TRESHNA.CO.NZ
Name Server: SNS2.TRESHNA.CO.NZ
Name Server: SNS3.TRESHNA.CO.NZ
Name Server: NS2.SMTPCORP.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-05-02T20:49:01Z <<<
```

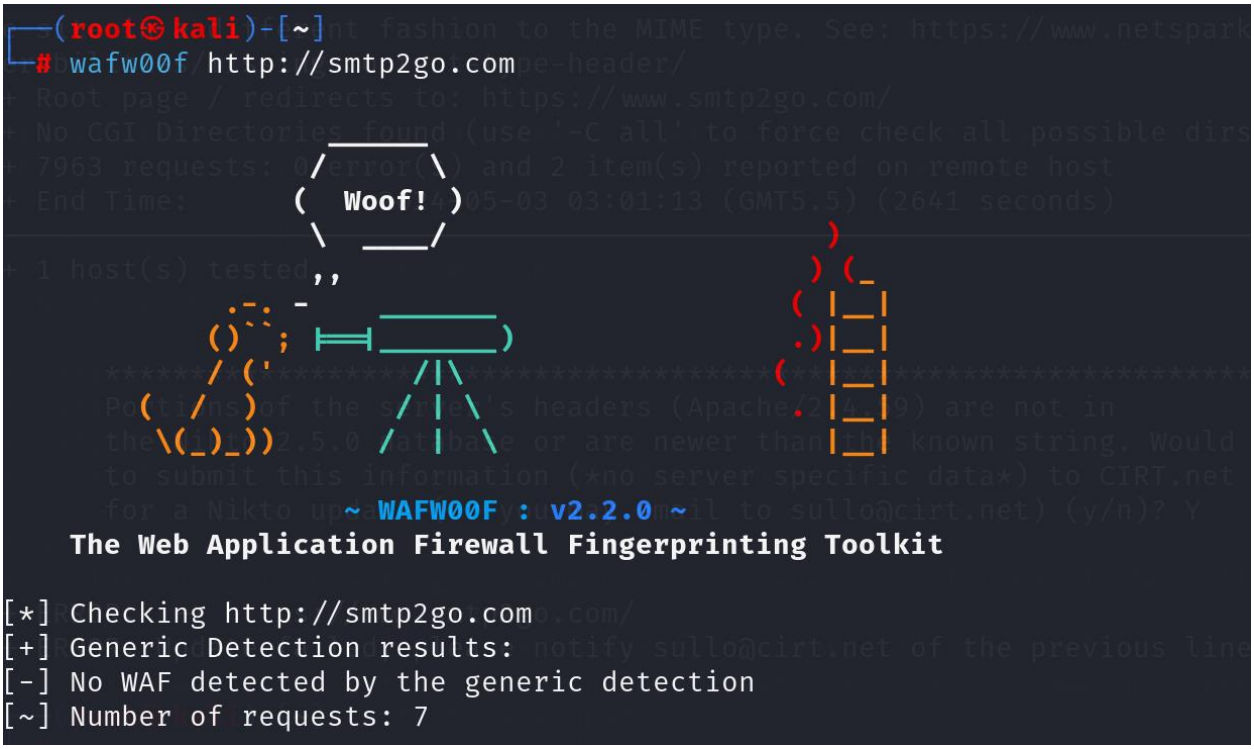
Find WAF (web application firewall) protection.

- 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:



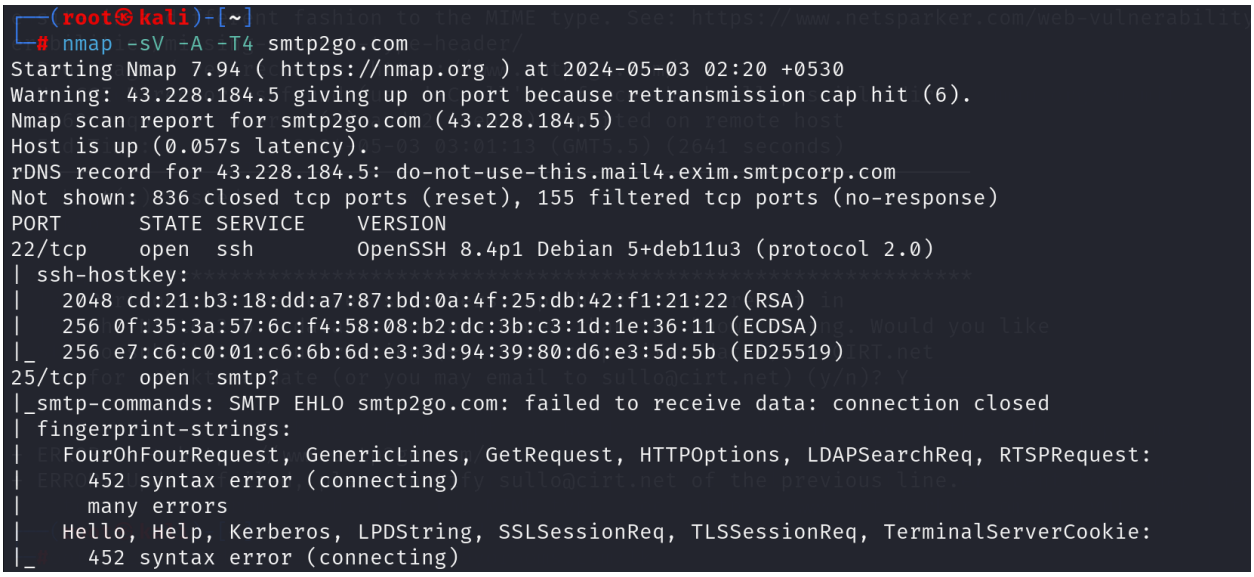
Find open ports.

- Nmap

Nmap, sometimes known as "Network Mapper," is a potent open-source network scanning program used for vulnerability analysis, security audits, and network discovery. It is particularly good at operating system detection, host discovery, port scanning, and service version detection. Because it supports custom scripting and automation, Nmap's scripting engine (NSE) is adaptable to a wide range of security

activities and integration requirements. Because of its dependability, adaptability, and large feature set, network administrators, security experts, and penetration testers frequently use it for network reconnaissance, security audits, and network monitoring.

Proof of concept:



Proof of concept:

```
80/tcp   open  http      Apache httpd 2.4.59
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Did not follow redirect to https://www.smtp2go.com/
443/tcp  open  ssl/http  Apache httpd 2.4.59
|_http-server-header: Apache/2.4.59 (Debian)
|_http-title: Did not follow redirect to https://www.smtp2go.com/
| ssl-cert: Subject: commonName=*.smtp2go.com
| Subject Alternative Name: DNS:*.smtp2go.com, DNS:smtp2go.com
| Not valid before: 2023-05-18T00:00:00
|_Not valid after:  2024-06-17T23:59:59
|_ssl-date: TLS randomness does not represent time
465/tcp  open  ssl/smtp  Exim smtpd 4.96.1-S2G
| smtp-commands: mail.smtp2go.com Hello smtp2go.com [175.157.23.242], SIZE 52428800, 8BITMIME, DSN, PIPELINING
, PIPECONNECT, AUTH CRAM-MD5 PLAIN LOGIN, CHUNKING, PRDR, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.smtp2go.com
| Subject Alternative Name: DNS:*.smtp2go.com, DNS:smtp2go.com
| Not valid before: 2023-05-18T00:00:00
|_Not valid after:  2024-06-17T23:59:59
```

```
587/tcp  open  smtp      Exim smtpd 4.96.1-S2G
| ssl-cert: Subject: commonName=*.smtp2go.com
| Subject Alternative Name: DNS:*.smtp2go.com, DNS:smtp2go.com
| Not valid before: 2023-05-18T00:00:00
|_Not valid after:  2024-06-17T23:59:59
| smtp-commands: mail.smtp2go.com Hello smtp2go.com [175.157.23.242], SIZE 52428800, 8BITMIME, DSN, PIPELINING
, PIPECONNECT, AUTH CRAM-MD5 PLAIN LOGIN, CHUNKING, STARTTLS, PRDR, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|_ssl-date: TLS randomness does not represent time
2525/tcp  open  smtp      Exim smtpd 4.96.1-S2G
| ssl-cert: Subject: commonName=*.smtp2go.com
| Subject Alternative Name: DNS:*.smtp2go.com, DNS:smtp2go.com
| Not valid before: 2023-05-18T00:00:00
|_Not valid after:  2024-06-17T23:59:59
| smtp-commands: mail.smtp2go.com Hello smtp2go.com [175.157.23.242], SIZE 52428800, 8BITMIME, DSN, PIPELINING
, PIPECONNECT, AUTH CRAM-MD5 PLAIN LOGIN, CHUNKING, STARTTLS, PRDR, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
|_ssl-date: TLS randomness does not represent time
5666/tcp  open  tcpwrapped
```

Proof of concept:

```
10025/tcp open  unknown
| fingerprint-strings:
|   NULL:
|     521-See https://www.smtp2go.com/setupguide/salesforce/ for new SMTP
|_    settings
2 services unrecognized despite returning data. If you know the service/version, please submit the following f
ingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.94%I=7%D=5/3%Time=6633FD3D%P=x86_64-pc-linux-gnu%r(Hello
SF:,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x20s
SF:yntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,34,"452\x20syntax
SF:\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")%r(Get
SF:Request,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20m
SF:any\x20errors\r\n")%r(HTTPOptions,34,"452\x20syntax\x20error\x20\(conne
SF:cting\)\r\n421\x20too\x20many\x20errors\r\n")%r(RTSPRequest,34,"452\x20
SF:syntax\x20error\x20\(connecting\)\r\n421\x20too\x20many\x20errors\r\n")
SF:%r(SSLSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(T
SF:erminalServerCookie,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%
SF:r(TLSSessionReq,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Ke
SF:rberos,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(FourOhFourR
SF:equest,34,"452\x20syntax\x20error\x20\(connecting\)\r\n421\x20too\x20ma
SF:ny\x20errors\r\n")%r(LPDString,1F,"452\x20syntax\x20error\x20\(connecti
SF:ng\)\r\n")%r(LDAPSearchReq,34,"452\x20syntax\x20error\x20\(connecting\)
SF:\r\n421\x20too\x20many\x20errors\r\n");
```

```
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port10025-TCP:V=7.94%I=7%D=5/3%Time=6633FD30%P=x86_64-pc-linux-gnu%r(NU
SF:LL,53,"521-See\x20https://www\.smtp2go\.com/setupguide/salesforce/\x20f
SF:or\x20new\x20SMTP\r\n521\x20settings\r\n");
Device type: VoIP phone|webcam|specialized|firewall
Running (JUST GUESSING): Grandstream embedded (89%), Garmin embedded (85%), 2N embedded (85%), FireBrick embed
ded (85%)
OS CPE: cpe:/h:grandstream:gxp1105 cpe:/h:garmin:virb_elite cpe:/h:2n:helios cpe:/h:firebrick:fb2700
Aggressive OS guesses: Grandstream GXP1105 VoIP phone (89%), Garmin Virb Elite action camera (85%), 2N Helios
IP VoIP doorbell (85%), FireBrick FB2700 firewall (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: smtp2go.com, mail.smtp2go.com; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.31 ms do-not-use-this.mail4.exim.smtpcorp.com (43.228.184.5)

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 315.92 seconds
```

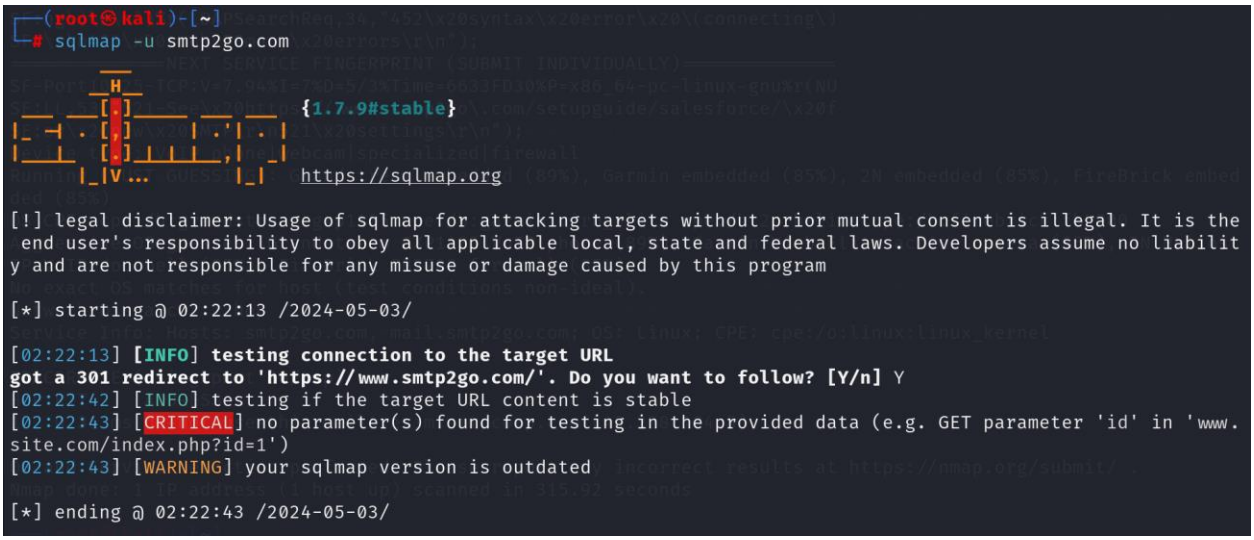
Exploitation

- Sqlmap

Web applications with SQL injection vulnerabilities can be automatically found and exploited with SQLMap, an open-source penetration testing tool. It employs a

number of detecting methods, supports a number of database management systems, and provides customization choices. Security experts and penetration testers find SQLMap useful as it automates testing, enumeration, data extraction, and reporting procedures during security assessments. It should, therefore, be utilized sensibly, morally, and with the appropriate authorization to test programs and systems.

Proof of concept:



Vulnerability analysis phase

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

Targeted Domain: - http://smtp2go.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

- Cloud Metadata Potentially Exposed

Vulnerability description

When sensitive information found in cloud service metadata is unintentionally made public, it's referred to as "cloud metadata potentially exposed." Cloud metadata usually consists of access

credentials, configuration information, and other pertinent facts about cloud resources. This metadata may be vulnerable to unauthorized access, data breaches, and other malicious acts, which could provide serious security problems.

Impact assessment

The impact assessment for potentially exposed cloud metadata involves evaluating the sensitivity and scope of the data, assessing associated risks including compliance and legal implications, understanding business impacts such as financial losses and reputational damage, prioritizing remediation actions like access controls and encryption, and updating incident response plans for effective mitigation and recovery strategies. A thorough assessment helps organizations understand and address risks to enhance overall security in cloud environments.

Affected components

In an impact assessment for potentially exposed cloud metadata, identifying affected components is crucial. This includes cloud services, configuration settings, access credentials, sensitive data stores, networking infrastructure, IAM components, logging/monitoring configurations, and third-party integrations. Understanding how each of these components is impacted helps prioritize remediation efforts and strengthen overall security in the cloud environment.

How to mitigate?

Putting strong security measures in place is necessary to reduce dangers associated with potentially exposed cloud metadata.

1. Access Controls: For critical resources, employ multi-factor authentication (MFA) and enforce least privilege access.

2. Encryption: Securely handle encryption keys and encrypt data both in transit and at rest.

3. Secure Configurations: Segment networks efficiently and adhere to cloud provider security best practices.

4. Monitoring and Logging: To detect threats in real time, enable auditing, monitoring, and integration with SIEM systems.

5. Regular Audits: Perform regular compliance checks, security audits, and vulnerability assessments.

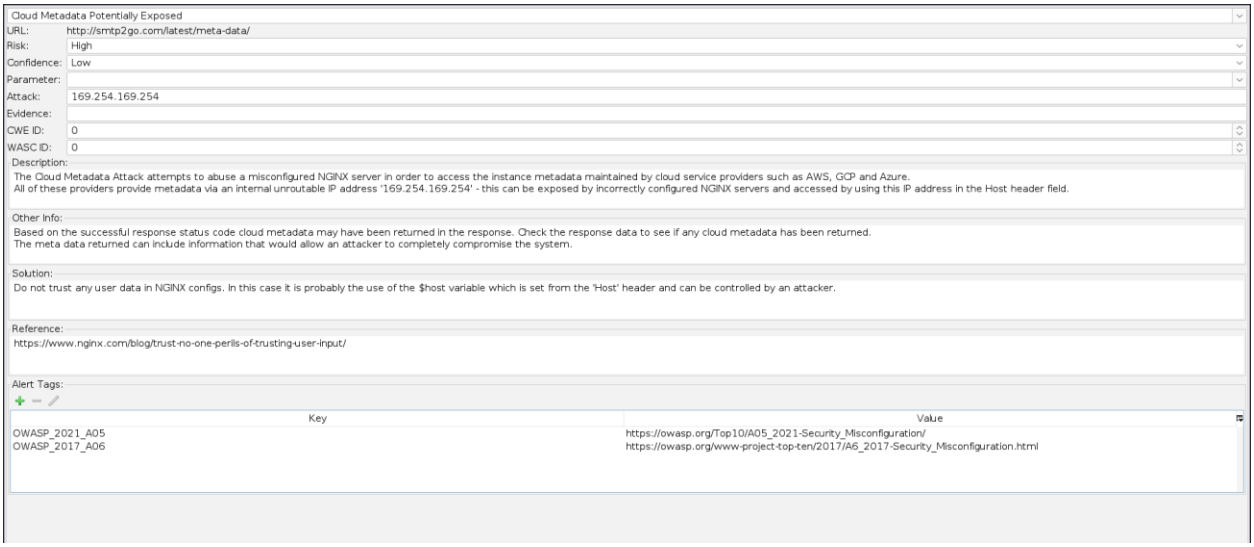
6. Security Awareness: Inform stakeholders and staff members about recommended practices and potential threats to cloud security.

7. Incident Response: Create and evaluate a plan specifically for handling occurrences involving cloud security.

8. Third-party Security: Check for security compliance with and keep an eye on cloud service providers and third-party vendors.

Organizations can improve overall cloud security resilience and lessen the effect of potential exposure of cloud metadata by combining these strategies.

Proof of concept:



Other vulnerabilities were identified during the scan

- Content Security Policy (CSP) Header Not Set (Medium)

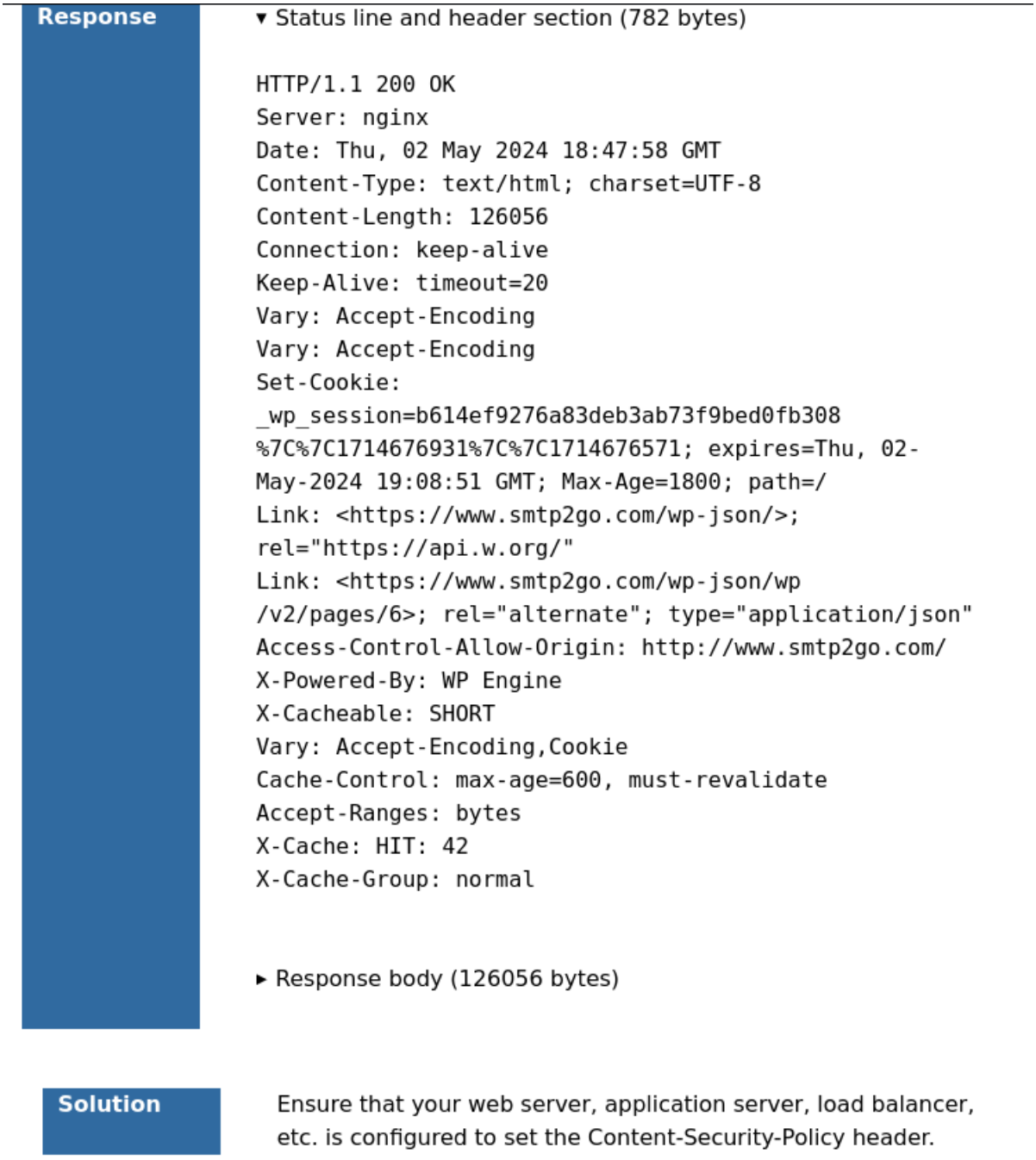
Proof of concept:

▾ GET http://smtp2go.com

Alert tags	▪ OWASP_2021_A05 ▪ OWASP_2017_A06
Alert description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including 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.

Request	▾ Request line and header section (222 bytes)
	
	`GET http://smtp2go.com HTTP/1.1`
	`host: smtp2go.com`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)`
	`AppleWebKit/537.36 (KHTML, like Gecko)`
	`Chrome/116.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`
	
	▾ Request body (0 bytes)

Proof of concept:



- HTTP to HTTPS Insecure Transition in Form Post (Medium)

Proof of concept:

▾ GET http://smtp2go.com

Alert tags	▪ OWASP_2021_A02 ▪ OWASP_2017_A06 ▪ WSTG-v42-CRYP-03
Alert 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://smtp2go.comThe context was: <form action="https://www.smtp2go.com"> <label class="label-signup" for="fullname">Username</label> <input type="text" name="fullname" autofocus placeholder="Your Name"> <label class="label-signup" for="password">Password</label> <input type="password" name="password" placeholder="Enter Password"> <input type="submit" value="Log In →"> </form>

Proof of concept:

Request

▾ Request line and header section (222 bytes)

```
GET http://smtp2go.com HTTP/1.1
host: smtp2go.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▾ Request body (0 bytes)

Response

▾ Status line and header section (782 bytes)

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 02 May 2024 18:47:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 126056
Connection: keep-alive
Keep-Alive: timeout=20
Vary: Accept-Encoding
Vary: Accept-Encoding
Set-Cookie:
_wp_session=b614ef9276a83deb3ab73f9bed0fb308
%7C%7C1714676931%7C%7C1714676571; expires=Thu, 02-
May-2024 19:08:51 GMT; Max-Age=1800; path=/
Link: <https://www.smtp2go.com/wp-json/>;
rel="https://api.w.org/"
Link: <https://www.smtp2go.com/wp-json/wp
/v2/pages/6>; rel="alternate";
type="application/json"
Access-Control-Allow-Origin: http://www.smtp2go.com/
X-Powered-By: WP Engine
X-Cacheable: SHORT
Vary: Accept-Encoding,Cookie
Cache-Control: max-age=600, must-revalidate
Accept-Ranges: bytes
X-Cache: HIT: 42
X-Cache-Group: normal
```

▸ Response body (126056 bytes)

Proof of concept:

Evidence	https://www.smtp2go.com
Solution	Use HTTPS for landing pages that host secure forms.

- Missing Anti-clickjacking Header (Medium)

Proof of concept:

▾ GET http://smtp2go.com

Alert tags	▪ OWASP_2021_A05 ▪ WSTG-v42-CLNT-09 ▪ OWASP_2017_A06
Alert description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
Request	▾ Request line and header section (222 bytes) GET http://smtp2go.com HTTP/1.1 host: smtp2go.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache ▾ Request body (0 bytes)

Proof of concept:

Response	▾ Status line and header section (782 bytes) HTTP/1.1 200 OK Server: nginx Date: Thu, 02 May 2024 18:47:58 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 126056 Connection: keep-alive Keep-Alive: timeout=20 Vary: Accept-Encoding Vary: Accept-Encoding Set-Cookie: _wp_session=b614ef9276a83deb3ab73f9bed0fb308 %7C%7C1714676931%7C%7C1714676571; expires=Thu, 02- May-2024 19:08:51 GMT; Max-Age=1800; path=/ Link: <https://www.smtp2go.com/wp-json/>; rel="https://api.w.org/" Link: <https://www.smtp2go.com/wp-json/wp /v2/pages/6>; rel="alternate"; type="application/json" Access-Control-Allow-Origin: http://www.smtp2go.com/ X-Powered-By: WP Engine X-Cacheable: SHORT Vary: Accept-Encoding,Cookie Cache-Control: max-age=600, must-revalidate Accept-Ranges: bytes X-Cache: HIT: 42 X-Cache-Group: normal ▸ Response body (126056 bytes)
Parameter	x-frame-options
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.

- Absence of Anti-CSRF Tokens (Medium)

Proof of concept:

Alert tags	▪ OWASP_2021_A01 ▪ WSTG-v42-SESS-05 ▪ OWASP_2017_A05
Alert description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site.

Proof of concept:

	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, _csrf_token] was found in the following HTML form: [Form 1: "affiliate" "captcha_response" "countryCode" "countryName" "g-recaptcha-response" "hiddenRecaptchaSignup" "input-email" "input-name" "input-phone" "plan-id" "plan-type" "radio-annual" "radio-monthly" "signup" "signup-password" "signup-step-1" "signup-step-sms" "signup-submit" "signup-submit-sms" "verification-number-1" "verification-number-2" "verification-number-3" "verification-number-4" "verification-number-5"].

Request	▾ Request line and header section (222 bytes)
	
	`GET http://smtp2go.com HTTP/1.1`
	`host: smtp2go.com`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`

Proof of concept:

Response

▾ Status line and header section (782 bytes)

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 02 May 2024 18:47:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 126056
Connection: keep-alive
Keep-Alive: timeout=20
Vary: Accept-Encoding
Vary: Accept-Encoding
Set-Cookie:
_wp_session=b614ef9276a83deb3ab73f9bed0fb308
%7C%7C1714676931%7C%7C1714676571; expires=Thu, 02-
May-2024 19:08:51 GMT; Max-Age=1800; path=/
Link: <https://www.smtp2go.com/wp-json/>;
rel="https://api.w.org/"
Link: <https://www.smtp2go.com/wp-json/wp
/v2/pages/6>; rel="alternate"; type="application/json"
Access-Control-Allow-Origin: http://www.smtp2go.com/
X-Powered-By: WP Engine
X-Cacheable: SHORT
Vary: Accept-Encoding,Cookie
Cache-Control: max-age=600, must-revalidate
Accept-Ranges: bytes
X-Cache: HIT: 42
X-Cache-Group: normal
```

▸ Response body (126056 bytes)

Evidence

```
<form id="signup-form" action="#" method="post" data-
form-step="signup-step-1" autocomplete="false">
```

Proof of concept:

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.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

- Hidden File Found (Medium)

Proof of concept:

Alert tags	▪ OWASP_2021_A05 ▪ WSTG-v42-CONF-05 ▪ OWASP_2017_A06
Alert 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.

Request	▾ Request line and header section (226 bytes)
	
	`GET http://smtp2go.com/.hg HTTP/1.1`
	`host: smtp2go.com`
	`user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36`
	`pragma: no-cache`
	`cache-control: no-cache`
	
	▾ Request body (0 bytes)

Proof of concept:

Response

▾ Status line and header section (208 bytes)

```
HTTP/1.1 301 Moved Permanently
Date: Thu, 02 May 2024 18:50:03 GMT
Server: Apache/2.4.59 (Debian)
Location: https://www.smtp2go.com/.hg
Content-Length: 312
Content-Type: text/html; charset=iso-8859-1
```

▾ Response body (312 bytes)

```
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a
href="https://www.smtp2go.com/.hg">here</a>.</p>
<hr>
<address>Apache/2.4.59 (Debian) Server at
smtp2go.com Port 80</address>
</body></html>
```

Evidence

```
HTTP/1.1 301 Moved Permanently
```

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.

Conclusion

The report on web security vulnerabilities for http://smtp2go.com presents a thorough assessment covering various phases such as information gathering, reconnaissance, exploitation, and vulnerability analysis. It begins with subdomain enumeration using tools like Recon-ng, DNSDumpster, and Dnsrecon to collect data and identify potential weaknesses. DNS enumeration and public devices enumeration further uncover vulnerabilities and possible attack points. The report also identifies the presence of a Web Application Firewall (WAF) using Wafwoof and conducts port scanning with Nmap for a comprehensive security assessment. Exploitation tools like SQLMap are employed to identify and exploit SQL injection vulnerabilities, emphasizing the importance of secure coding practices. The vulnerability analysis phase outlines OWASP top 10 vulnerabilities, including Broken Access Control, Cryptographic Failures, and Injection, among others, and recommends mitigation strategies such as access controls, encryption, and regular audits. Additional vulnerabilities like Cloud Metadata Exposure and Missing Security Headers are also highlighted, underscoring the need for robust security measures and continuous monitoring to ensure a secure web environment.