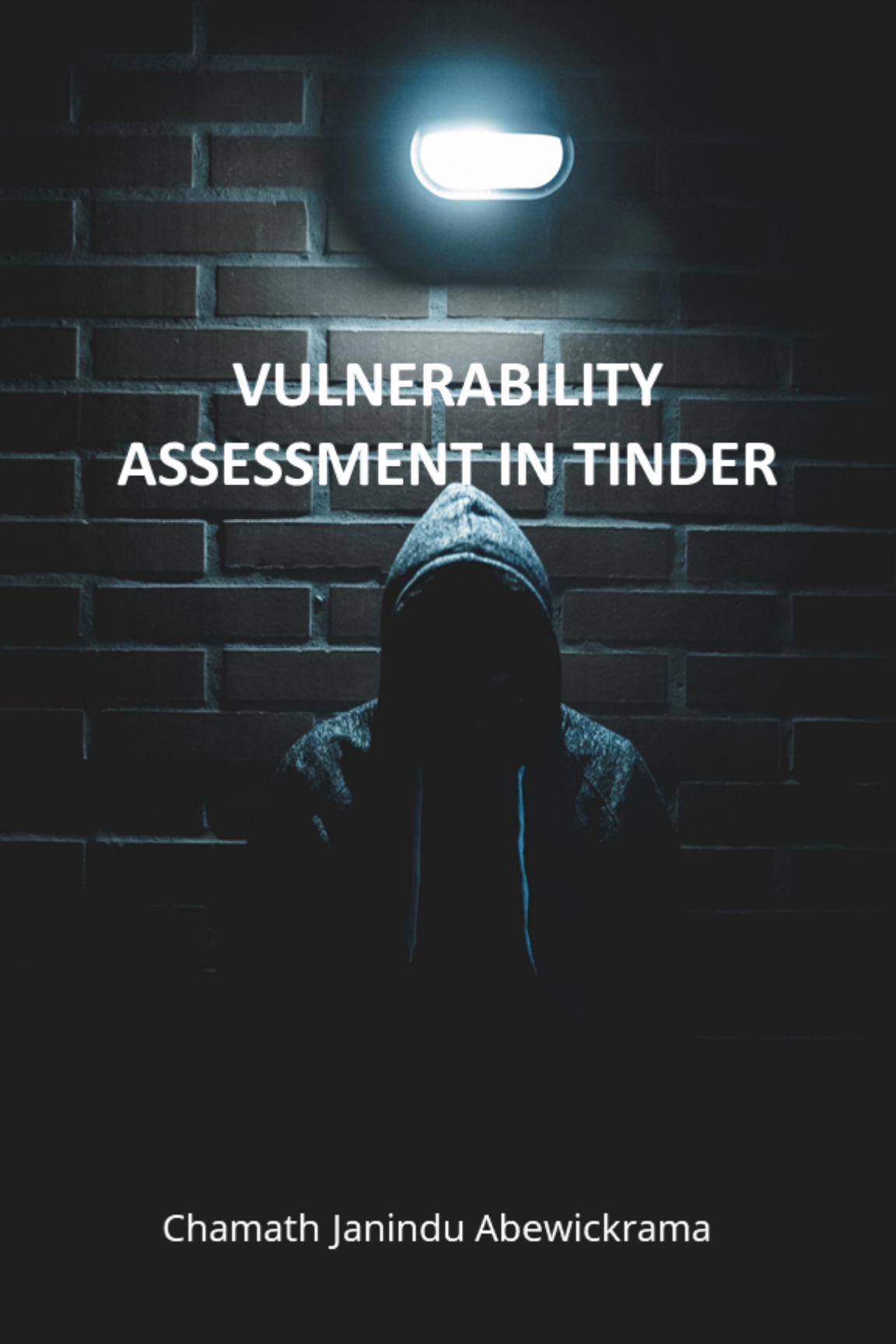


Chamath Janindu Abewickrama

VULNERABILITY ASSESSMENT IN TINDER

Chamath Janindu Abewickrama, Menaka Moonamaldeniya and Chathuri Udagedara

This book is for sale at
http://leanpub.com/vulnerabilityassessmentintinder

This version was published on 2021-11-05

Contents

Purpose

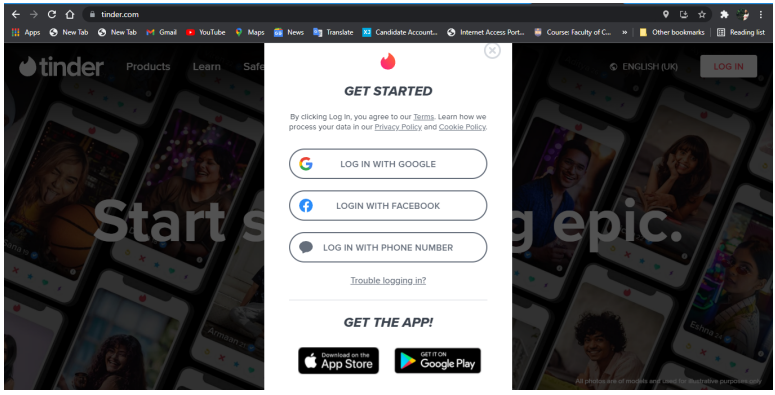
This web audit is mainly based on web vulnerabilities and how we can prevent. We use some tools for scan vulnerabilities and target domain. Sublist3r, Anubis subdomain enumerator, recon-ng tool, netsparker, nikto, nmap and burp-suite these are the tools to scan web application. I use automatic and manual scan complete this.

Introduction

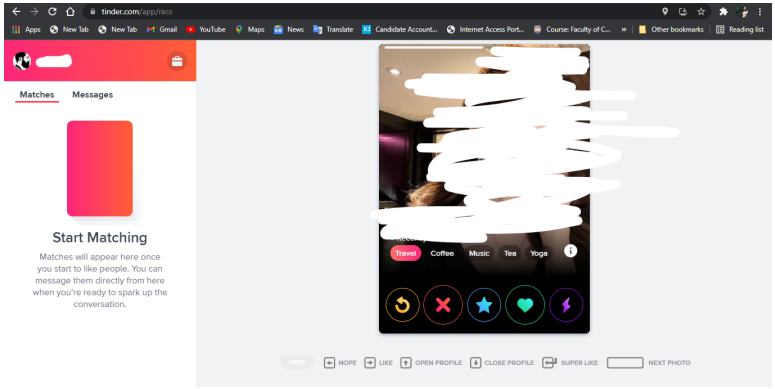
Website vulnerability assessments reveal all of the flaws and security concerns that hackers may take advantage of.To help you understand how your website may be
attacked, online audits cover all elements of a web application, such as the infrastructure, extensions, themes, server settings, SSL connection, and so on.
At that moment, we may use this audit to identify defects and security flaws. We may then move on to web penetration. At this point, security experts can mitigate the risks posed by these flaws. The goal of website security audits is to identify and fix vulnerabilities in your website's design before they are discovered by hostile hackers.

Scope

Tinder is an American geosocial networking and online dating application that allows
users to anonymously swipe to like or dislike other users' posted profiles, which generally comprise their photo, a short bio, and a list of their personal interests. Once two users have "matched", they can exchange messages.Tinder launched in 2012 we can use this lot of languages.
As cyber security student I went hackerone website to learn about bug bounty hunting. At this time I saw "www tinder.com "domain in hackerone. So , I selected this web site do my first bug bunty report.



Login page


tinder.com/app/recs
Matches
Messages
Start Matching
Matches will appear here once you start to like people. You can message them directly from here when you're ready to spark up the conversation.
Travel
Coffee
Music
Tea
Yoga
NOPE
LIKE
OPEN PROFILE
CLOSE PROFILE
SUPER LIKE
NEXT PHOTO

After Login

OWASP Top 10 Security Risks and Vulnerabilities

1. A01:2021-Broken Access Control
Broken authentication attacks attempt to gain control of one or more accounts by granting the attacker the same privileges as the victim. Authentication is "broken" when attackers can assume user identities via compromising passwords, keys or session tokens, user account information, and other data.

2. A02:2021-Cryptographic Failures
Cryptographic failure is like failure about cryptographic algorithm. These days many cryptographic algorithms use to encrypt sensitive data.
For example, of sensitive data -passwords, credit card numbers, health recodes, business secrets etc.

3. A03:2021-Injection
Attacker use malicious code inject to the website using java script, xml, sql, programing language. After injecting this code attacker can gain access web database and web site privileges.

4. A04:2021-Insecure Design
This is new added vulnerability in owasp top 10. This means web site design has very low security. Simply this is developer mistake. Example – using unwanted APIs and functions. If developer use these APIs web site goes to risk.

5. A05:2021-Security Misconfiguration
This vulnerability like, security misconfiguration occurs when a server or web application fails to enforce all of the security rules or implements them properly.

6. A06:2021-Vulnerable and Outdated Components

It likes, software, web application, operating systems, data base management systems, APIs and all of runtime environments are out of date and do not use security patches. It was vulnerable. This is simple example of Vulnerable and Outdated Components

7. A07:2021-Identification and Authentication Failures
To defend against authentication-related threats, it's essential to confirm the user's identity, authenticate them, and manage their sessions. Authentication weaknesses may exist if the application:

8. A08:2021-Software and Data Integrity Failures
Software and Data Integrity Failures mean "Integrity breaches are not protected by code and infrastructure."
For example – some applications allow auto-updating features, that time attacker sends malicious plugins, extensions to those applications, and the attacker can use this auto-updating feature to steal sensitive data. Previously applications are trusted by the system. It was the main thing the system cannot detect attackers.

9. A09:2021-Security Logging and Monitoring Failures
Lack of recoding proper historical information about events that happened in side an application.
The application does not log auditable events, such as logins, failed logins, and high-value transaction.
The application is unable to detect escalate, or alert for active attacks in real time or, at least in near real time.
Penetration testing and vulnerability scans do not trigger alert.

10. A10:2021-Server-Side Request Forgery
Server-Side Request Forgery allows an attacker to include the server-side application to make http request to an arbitrary domain of the attacker's choosing
Unauthorized activities or access to data inside the company may frequently arise from a successful SSRF attack, either in the vulnerable application itself or on other back-end systems with which the program can interact. The SSRF vulnerability may enable an attacker to execute arbitrary commands in certain circumstances.

Severity Levels

Critical The exploitation of the vulnerability will very certainly result in server or infrastructure device root-level penetration.

Exploitation is straightforward

High The flaw is tough to exploit, but if it is, it may lead to higher privileges. Data loss or downtime may occur because of the exploit.

Medium Vulnerabilities that require the attacker to use social engineering techniques to influence specific victims.Vulnerabilities that cause a denial of service are tough to set up.Exploits that need the attacker's presence on the victim's local network.Vulnerabilities to which only a limited amount of access may be gained via exploitation.Vulnerabilities that require the usage of user privileges in order to be exploited.

Low Low-level vulnerabilities usually have minimal effect on an organization's operations. Exploiting such flaws typically requires local or physical system access.

In Scope Domains

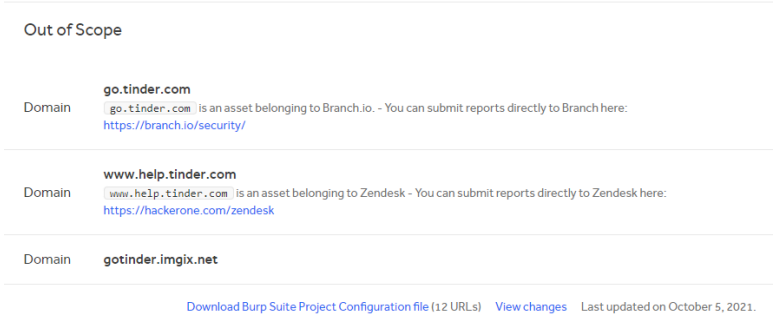
Scopes

In Scope

Domain	*.tinder.com	Critical	Eligible
Domain	*.gotinder.com	Critical	Eligible
Domain	*.tinderops.net	Critical	Eligible
Android: Play Store	com.tinder	Critical	Eligible
iOS: App Store	547702041	Critical	Eligible

In Scope Domains

Out of Scope Domains



Out of Scope

Domain	**go.tinder.com** `go.tinder.com` is an asset belonging to Branch.io. - You can submit reports directly to Branch here: https://branch.io/security/
Domain	**www.help.tinder.com** `www.help.tinder.com` is an asset belonging to Zendesk - You can submit reports directly to Zendesk here: https://hackerone.com/zendesk
Domain	**gotinder.imgix.net**

Download Burp Suite Project Configuration file (12 URLs) View changes Last updated on October 5, 2021.

Out of Scope Domains

Out of Scope

- Denial of service
- Social engineering
- Spamming
- Tap-jacking
- Tab-nabbing
- SPF/DKIM/DMARC related issues, including missing SPF records on subdomains
- Scenarios that require unlikely user interaction and/or outdated OS or software version
- Self-XSS
- Login/Logout CSR

Information Gathering

• Information gathering is part of penetration testing it helps to find more information about target. We use some tools to gather the information like zap, burp suite, netsparker and etc.
• The information-gathering step is used to identify potential system vulnerabilities, followed by the exploitation phase, in which the vulnerabilities are tried to be exploited in order to get access to the system.
• There are two types of information gathering.

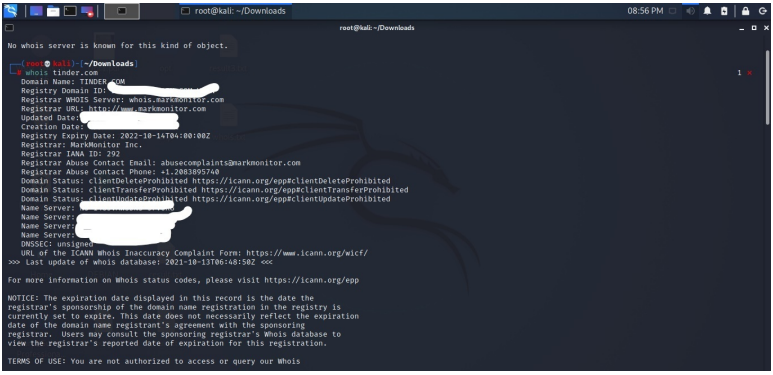
i. Collecting network data
Such as public, private and associated domain names, network hosts, public and private IP blocks, routing tables, TCP and UDP running services, SSL certificates, open ports and more
ii. Collecting system-related information
This includes user enumeration, system groups, OS hostnames, OS system type (probably by fingerprinting), system banners (as seen in the banner grabbing blog post), etc.
• We can gather the information using active and passive scan. **Active scan** is uses known attacks against the chosen targets to try to identify possible vulnerabilities.
Passive scanning is a vulnerability detection technique that depends on data gathered from network data collected from a target machine without requiring direct interaction. **We use passive scan for this web audit**.

Automated testing

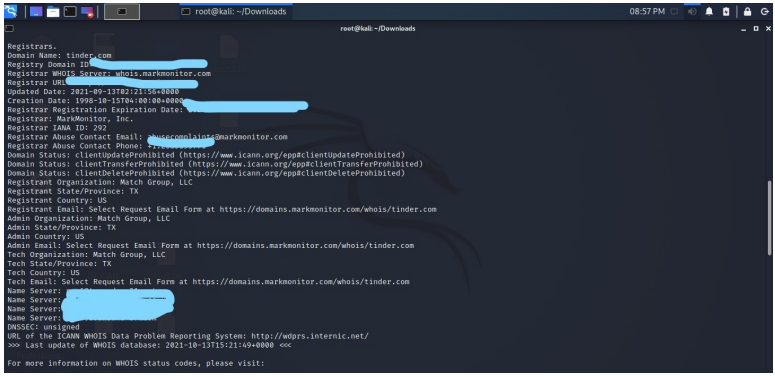
Passive scan

1. Target validation

I use **whois** commands to find details about www.tinder.com. We can find out this target domain is valid or not using this.



Target validation



Target validation

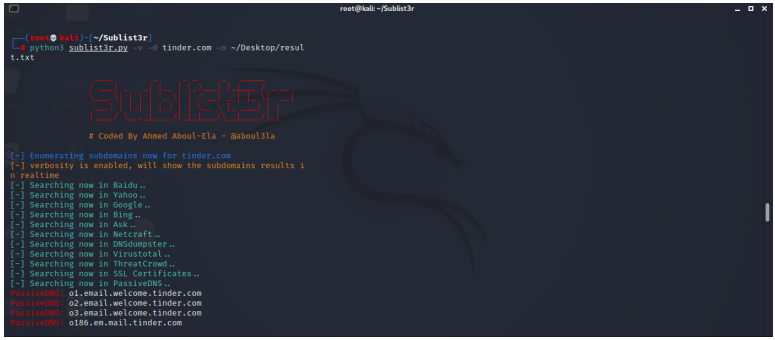
2. Find subdomains

Identifying subdomains is a part of information gathering. We can use some tools to
identify the subdomains.

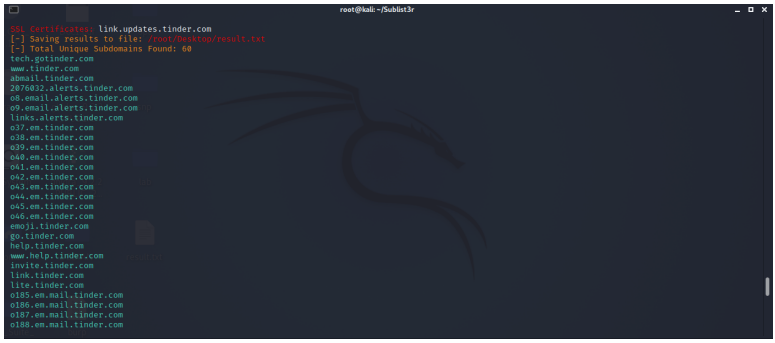
1. Sublist3r
2. Anubis Subdomain Enumerator
3. Recon –ng Tools
4. Amass
5. Crt.sh tool

Sublist3r

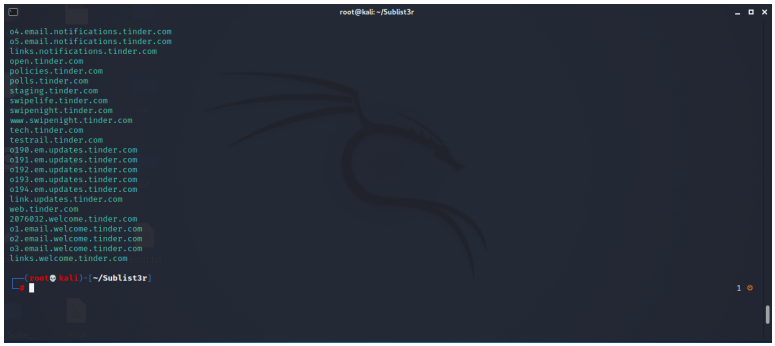
• Sublist3r is a python tool designed to scan subdomains of websites. It helps penetration testers to collect subdomains in targeted domain.
• Sublist3r use google, yahoo, bing, baidu and ask search engines to find subdomains.
• We can install our kali machine using this command.
"git clone **https://github.com/about3la/sublist3r.git**"
After installing sublist3r, type this command to scan target domain.
"**Python3 sublist3r.py -v -d tinder.com -o ~/Desktop/result**"



Sublist3r



Sublist3r

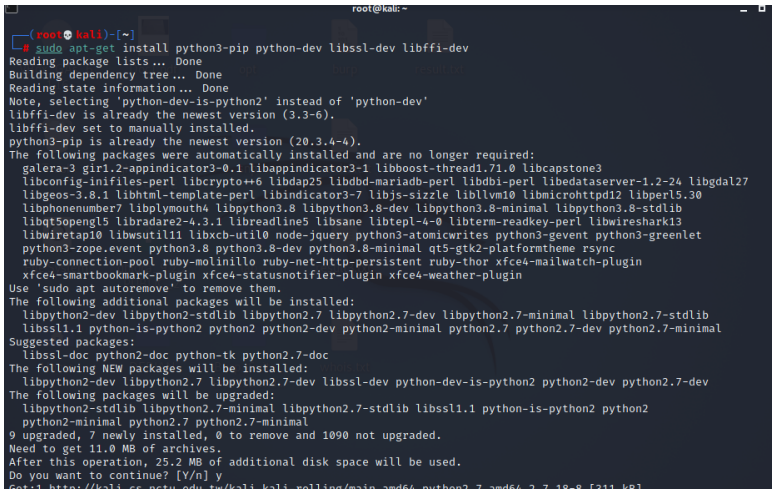


Sublist3r

Anubis Subdomain Enumerator

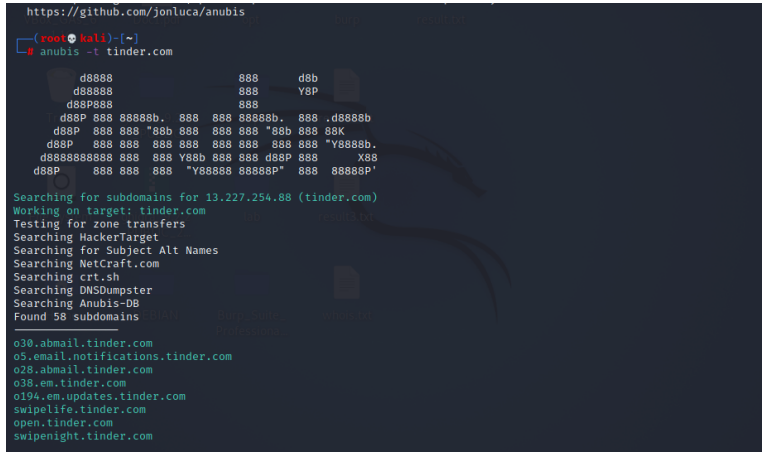
• Anubis is a subdomain scanning tool and it collates data from a diffrent of sources,including HackerTarget, DNSDumpster, x509 certs, VirusTotal, Google, Pkey, and NetCraft.
• Then we can get this tool to our kali machine using these commands.

sudo apt-get install python3-pip python-dev libssl-dev libffi-dev
pip3 install anubis-netsec

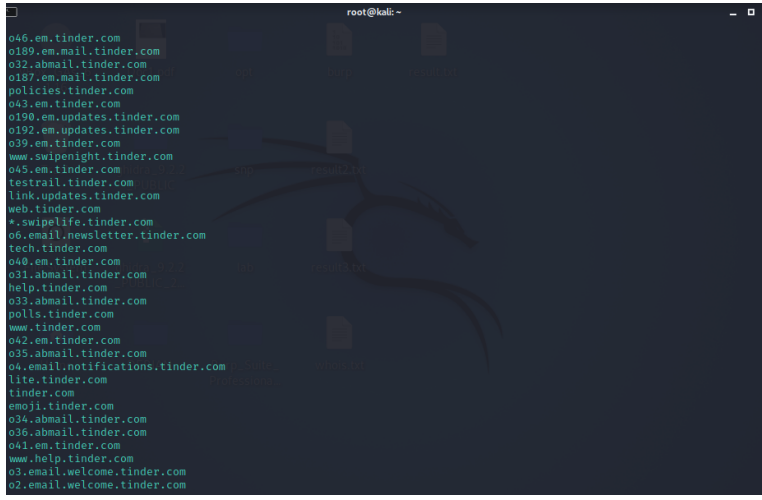


Anubis Subdomain Enumerator

and use this command to scan our target.
anubis -t tinder.com



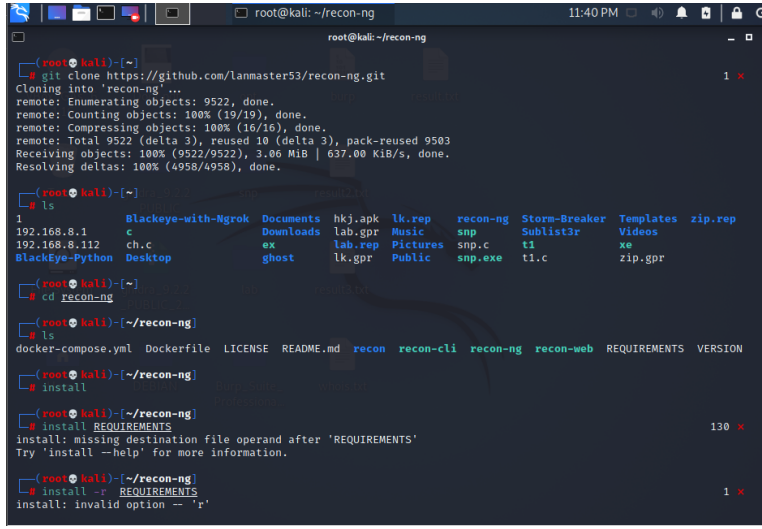
Anubis Subdomain Enumerator



Anubis Subdomain Enumerator

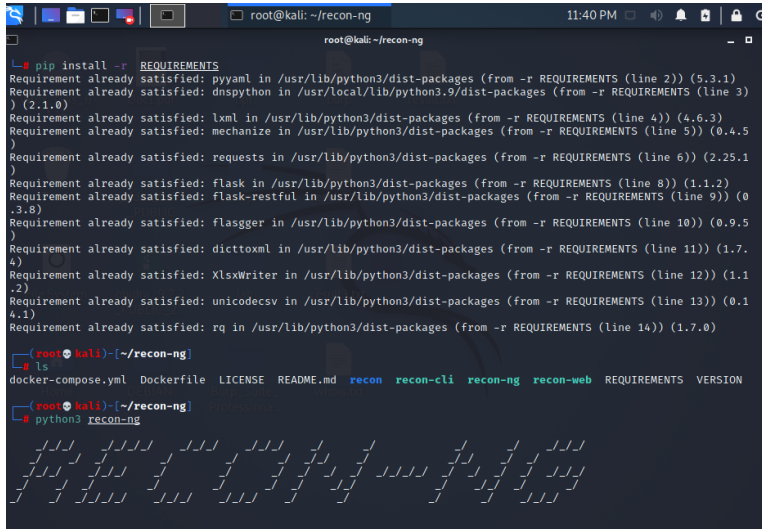
Recon –ng Tools

- This tool is python base tool and open source. [6]
- First we need to install this tool in our kali machine.
- Command- "**git clone https://github.com/lanmaster53/recon-ng.git**"

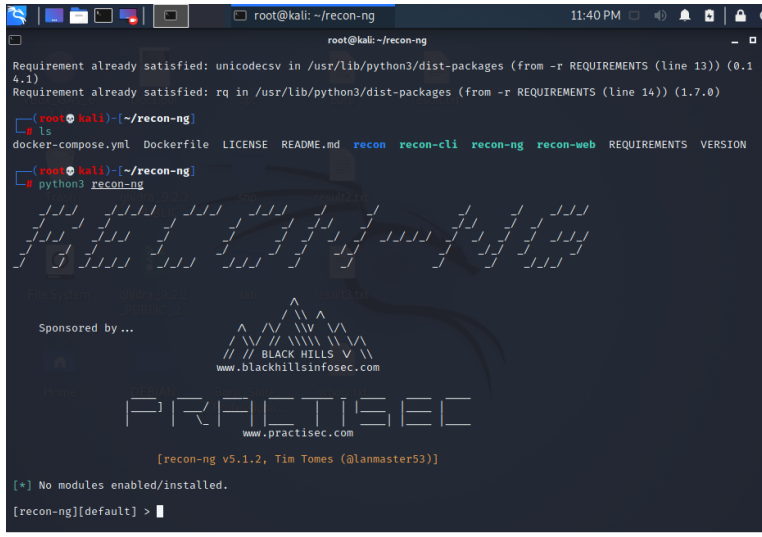


Recon –ng Tools

- After installing we need to install requirements file.
- **Pip install -r REQUIRMENT**

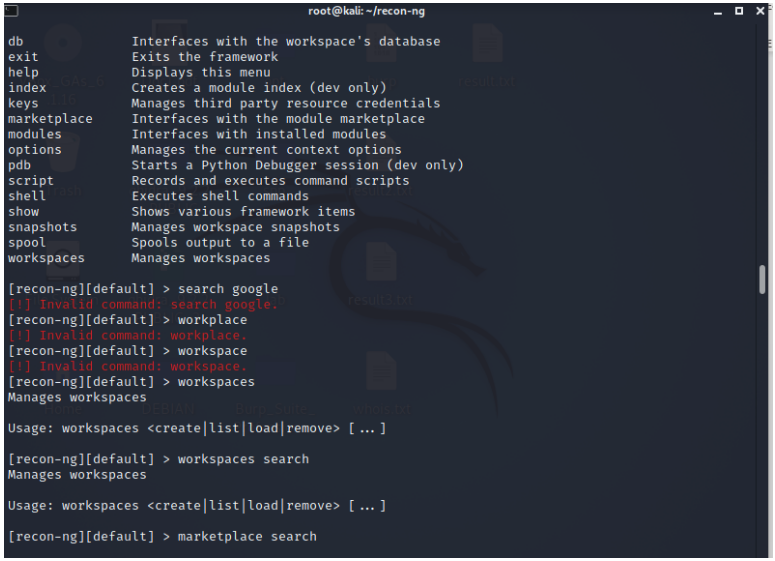


Recon –ng Tools



Recon –ng Tools

- Then open options using **–h** command.



Recon –ng Tools

• Using marketplace command to find google_site_web.

Marketplace search google

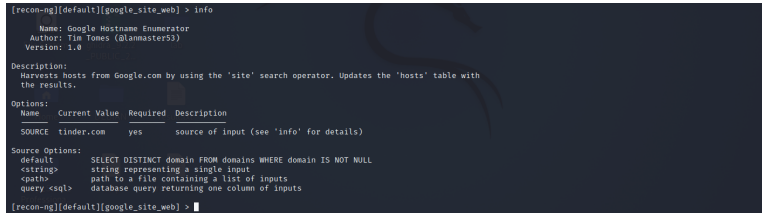
• After find this, insatall module using this.

Marketplace install recon/domains-hosts/google_site_web (this is parth of installation)

• **“modules load (path)” **command to load moudel. use **modules load recon/domainshosts/google_site_web** command load this.

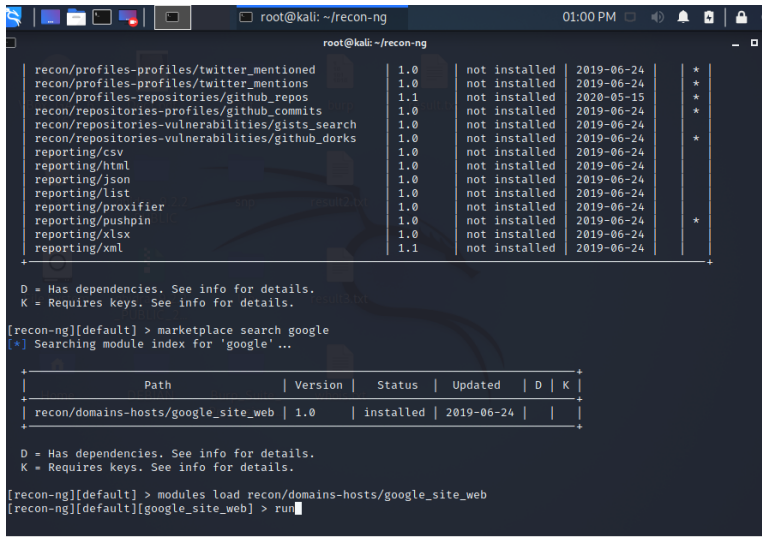
• Next type **“info” **

• Now set our domain as a SOURCE “**options set SOURCE tinder.com**”

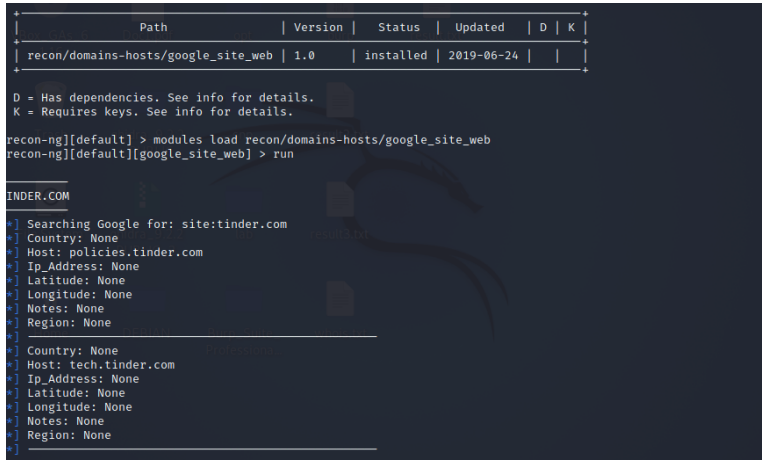


Recon –ng Tools

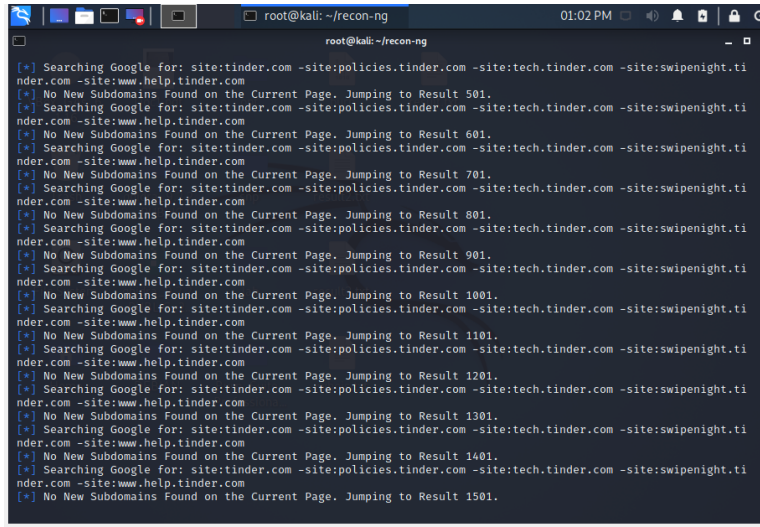
- After use run command to run this process.



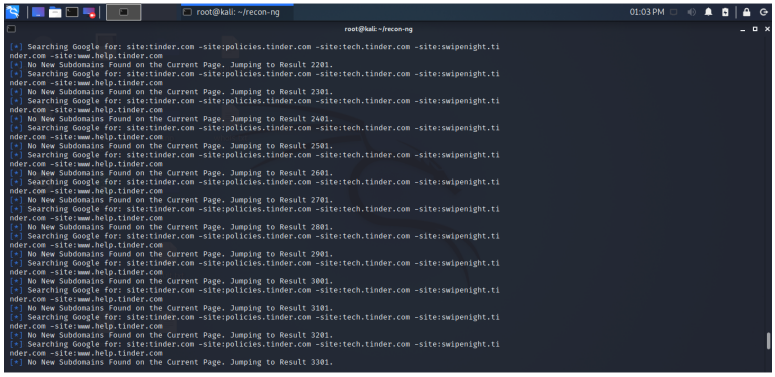
Recon –ng Tools



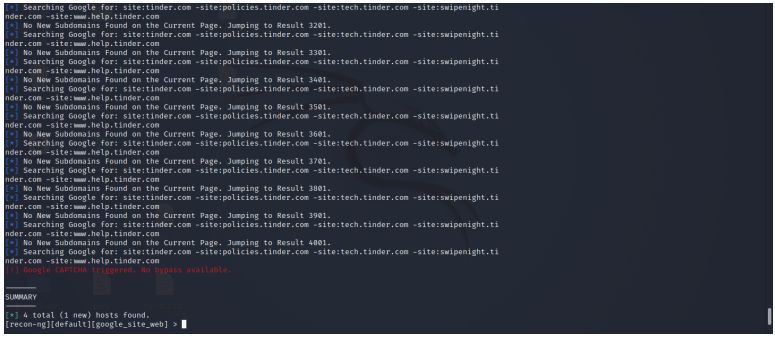
Recon –ng Tools



Recon –ng Tools



Recon –ng Tools

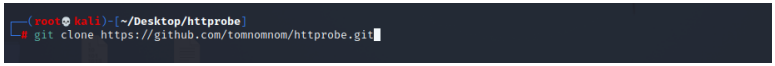


Recon –ng Tools

Before select subdomains we need to verify these subdomains are alive subdomains. Then we select tool find alive subdomain. Tool name is **httprobe**

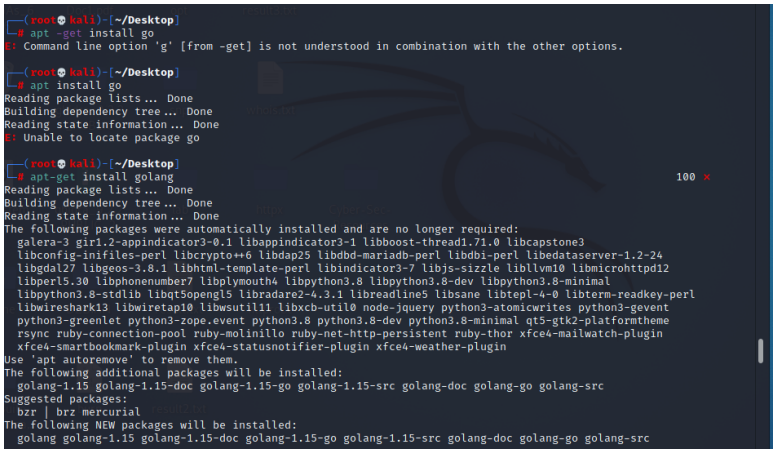
httprobe

- This tool design using go language.
- First we need to clone this tool in github.
- git clone **https://github.com/tomnomnom/httprobe.gi**



httprobe

after we need to get go language.



Go

then go inside the httprobe directory and use **“go build main.go” **this command to compile the tool.

```
┌──(root💀kali)-[~/Desktop/httprobe]
└─# go build main.go

┌──(root💀kali)-[~/Desktop/httprobe]
└─# ls
Dockerfile  LICENSE  main  main.go  README.md  script

┌──(root💀kali)-[~/Desktop/httprobe]
└─# ./main

^C

┌──(root💀kali)-[~/Desktop/httprobe]
└─# ./main -h
Usage of ./main:
  -c int
        set the concurrency level (split equally between HTTPS and HTTP requests) (default 20)
  -method string
        HTTP method to use (default "GET")
  -p value
        add additional probe (proto:port)
  -prefer-https
        only try plain HTTP if HTTPS fails
  -s    skip the default probes (http:80 and https:443)
  -t int
        timeout (milliseconds) (default 10000)

┌──(root💀kali)-[~/Desktop/httprobe]
└─# echo path
path

┌──(root💀kali)-[~/Desktop/httprobe]
└─# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games
```

Go

then change the path httprobe tool and change name main.go to httprobe. That was usefull to run this tool anywhere.

```
┌──(root💀kali)-[~/Desktop/httprobe]
└─# echo path
path

┌──(root💀kali)-[~/Desktop/httprobe]
└─# echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/local/games:/usr/games

┌──(root💀kali)-[~/Desktop/httprobe]
└─# mv main /bin

┌──(root💀kali)-[~/Desktop/httprobe]
└─# ls
Dockerfile  LICENSE  main.go  README.md  script

┌──(root💀kali)-[~/Desktop/httprobe]
└─# mv main /bin/
mv: cannot stat 'main': No such file or directory
```

Go

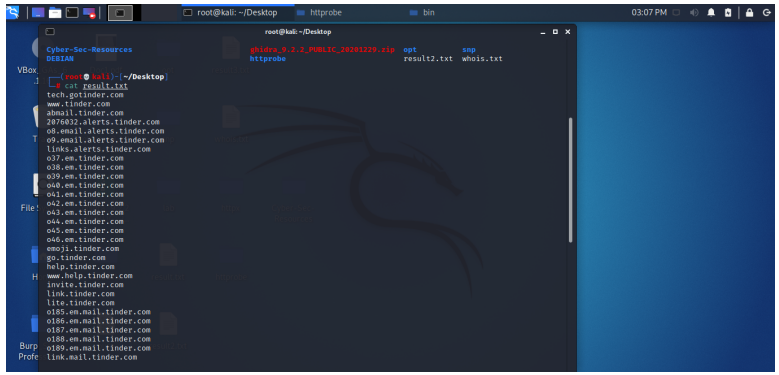
```
root@kali: /usr/bin

┌──(root💀kali)-[/usr/bin]
└─# mv main httprobe
```

Go

then run httprobe tool.

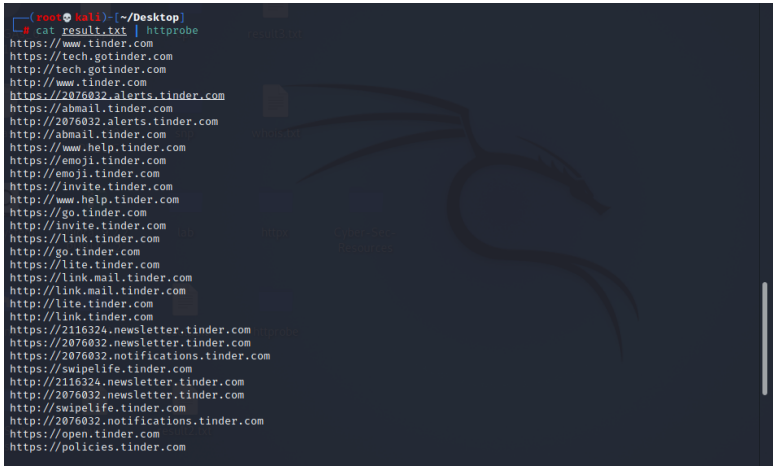
httprobe

after, open the output folder of saving subdomains' previous scans and use cat command to display this output in terminal.

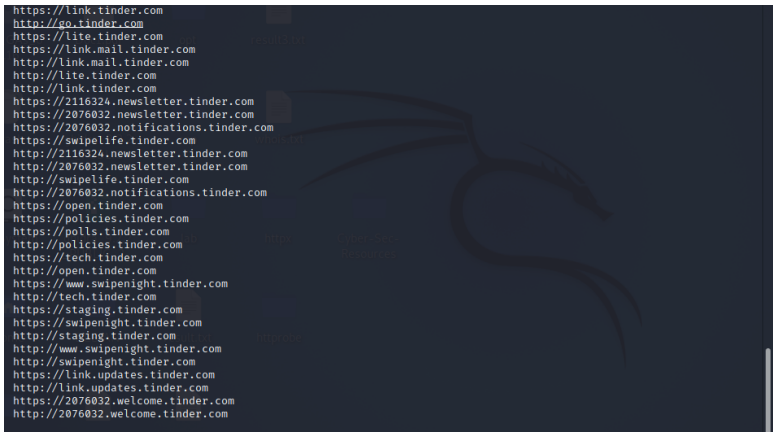


httprobe

These are the alive subdomain in www.tinder.com



Alive Subdomains



Alive Subdomains

I have selected few subdomains to complete this web audit.

https://emoji.tinder.com
https://swipelife.tinder.com
https://policies.tinder.com/
https://staging.tinder.com
https://tech.gotinder.com

http://www.tinder.com

Vulnerability scanning

• When it comes to systems and software, vulnerability scanning is the process of detecting security vulnerabilities and defects in the systems and software that runs on them.
• We can use some tools to identify the vulnerabilities. Vulnerability scanner is s program that detects and generates an inventory of all systems linked to a network. It is used to detect and prevent cyber-attacks. Additionally, for each device that it detects, it makes an effort to determine which operating system is currently running and which software is installed on it, in addition to other characteristics such as open ports and user accounts.

These are the tools of scan vulnerabilities.
1. Netsparker
2. Nessus
3. OpenVAS
4. Nikto
5. Nmap
6. OpernSCAP
7. OWASP ZAP
8. Burp suite
9. W3af
10. Metasploit framework

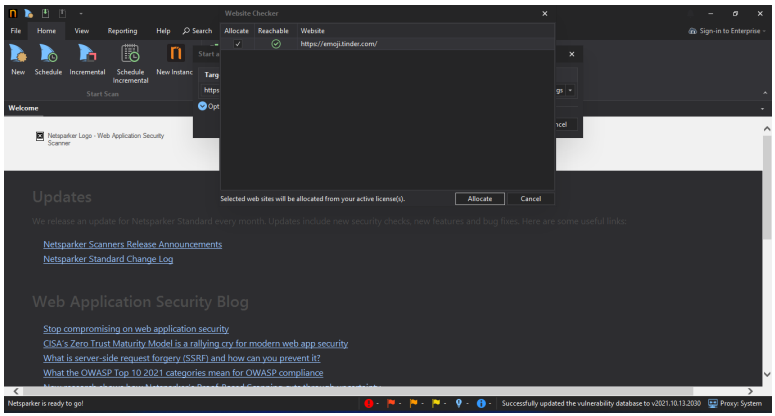
Netsparker

• Netsparker is fully automated web application vulnerability scanner. Netsparker can scan any kind of web application, independent of platform or programming language. It allows you to scan and detect security vulnerabilities in websites, web applications, and web services.

How to work,
• Open Netsparker.
• Then go the home tab and click New.

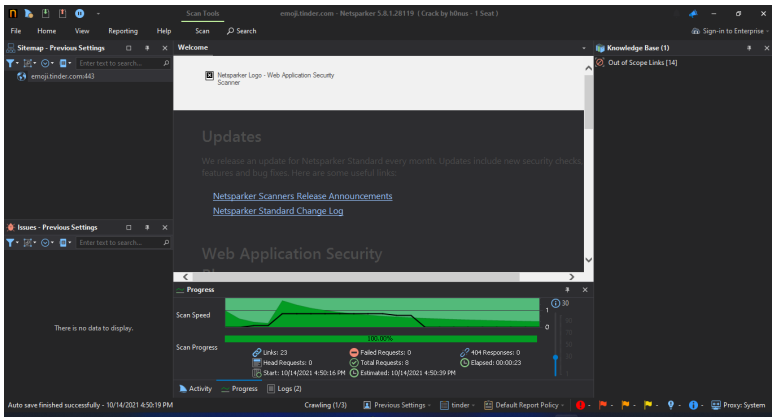
- Paste your target domain url.
- Then we can start our scan.

Subdomain -https://emoji.tinder.com



Scanning

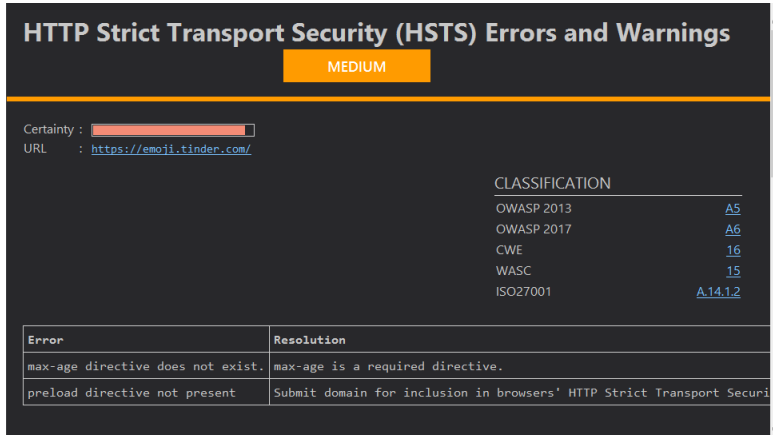
This is screenshot is scanning tinder.com web url using netsparker.



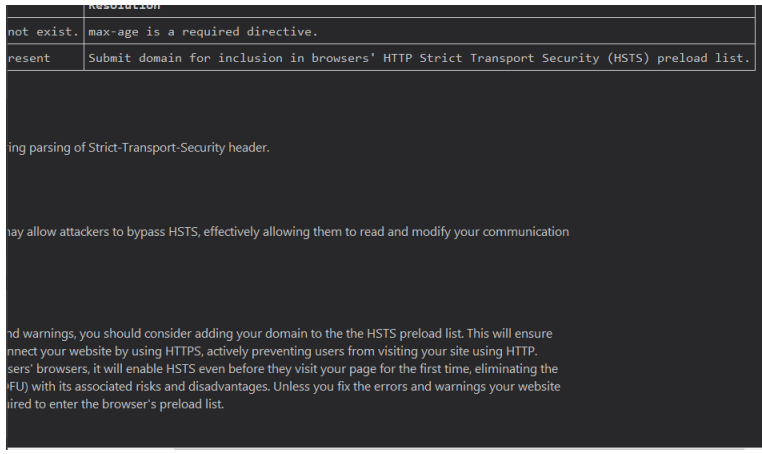
Scanning https://emoji.tinder.com

This subdomain has medium type vulnerability

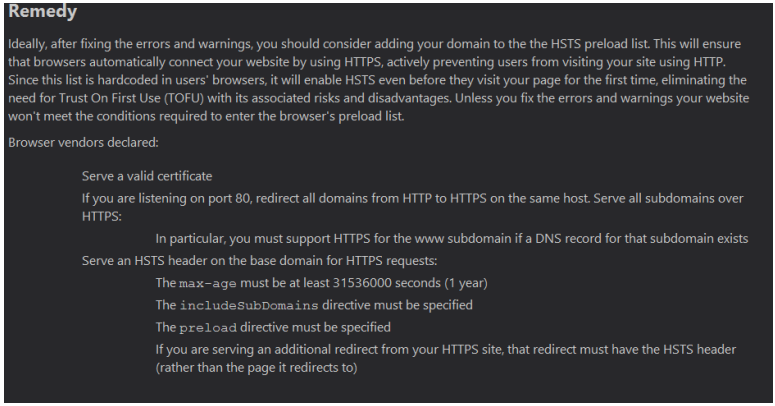
HSTS error.
Max-age directive does not exits.
Perload directive not present



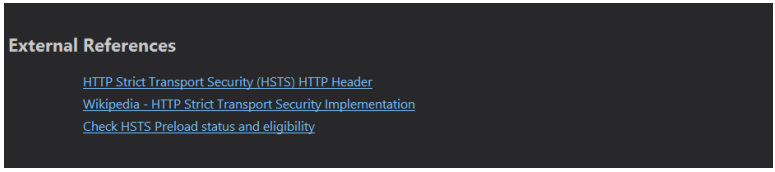
result



result

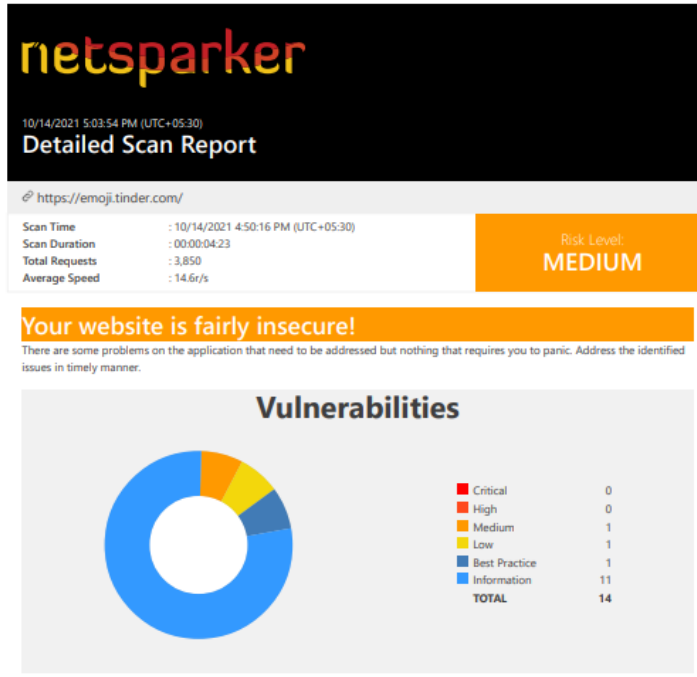


result



result

This is summery of scan report.


netsparker
10/14/2021 5:03:54 PM (UTC+05:30)
Detailed Scan Report
https://emoji.tinder.com/
Scan Time : 10/14/2021 4:50:16 PM (UTC+05:30)
Scan Duration : 00:00:04:23
Total Requests : 3,850
Average Speed : 14.6r/s
Risk Level:
MEDIUM
Your website is fairly insecure!
There are some problems on the application that need to be addressed but nothing that requires you to panic. Address the identified issues in timely manner.
Vulnerabilities
Critical 0
High 0
Medium 1
Low 1
Best Practice 1
Information 11
TOTAL 14

report

Vulnerability	Suggested Action
HTTP Strict Transport Security (HSTS) Errors and Warnings	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Insecure Frame (External)	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Expect-CT Not Enabled	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
An Unsafe Content Security Policy (CSP) Directive in Use	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
CDN Detected (Netlify)	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Cross-site Referrer Leakage through Referrer-Policy	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
data: Used in a Content Security Policy (CSP) Directive	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
default-src Used in Content Security Policy (CSP)	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Email Address Disclosure	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Generic Email Address Disclosure	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Missing object-src in CSP Declaration	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Robots.txt Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

report

Compliance Summary

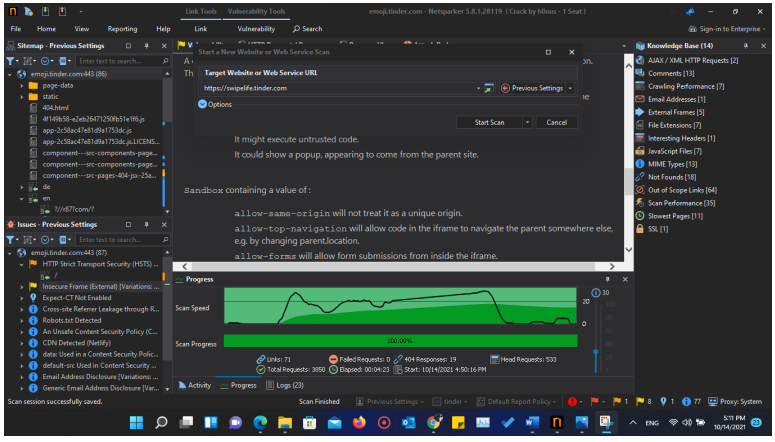
Compliance	Vulnerabilities
OWASP 2013	2
OWASP 2017	3
ISO27001	14

PCI compliance data is generated based on the classifications and it has no validity. PCI DSS scans must be performed by an approved scanning vendor.

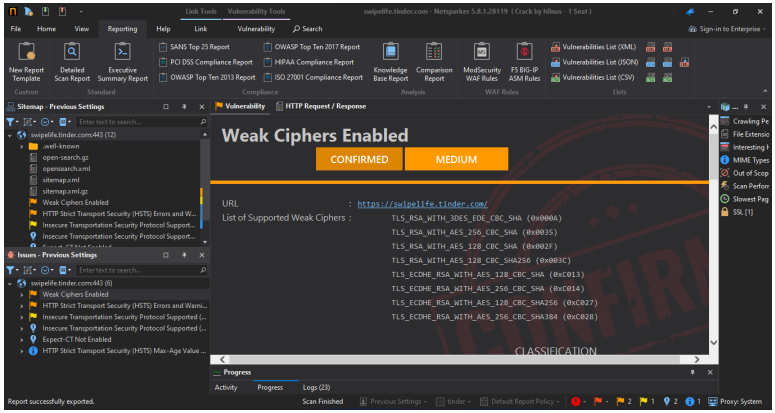
This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com

report

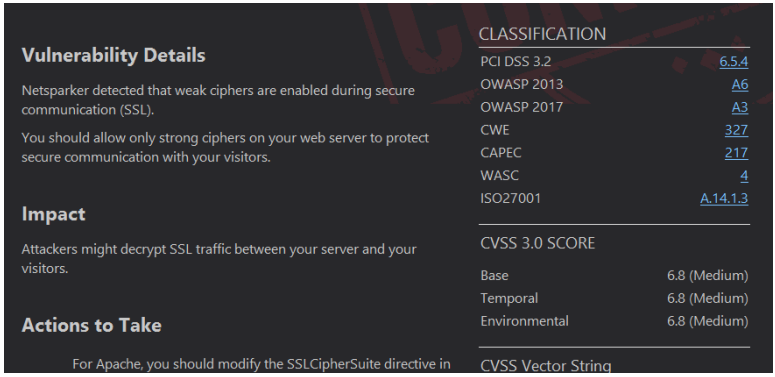
Subdomain -https://swipelife.tinder.com



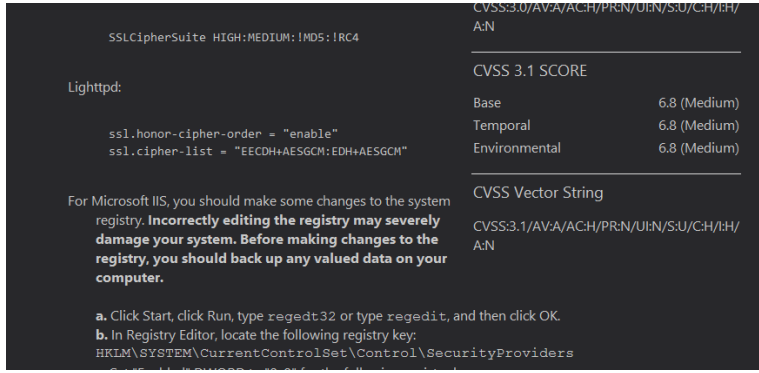
Scaning



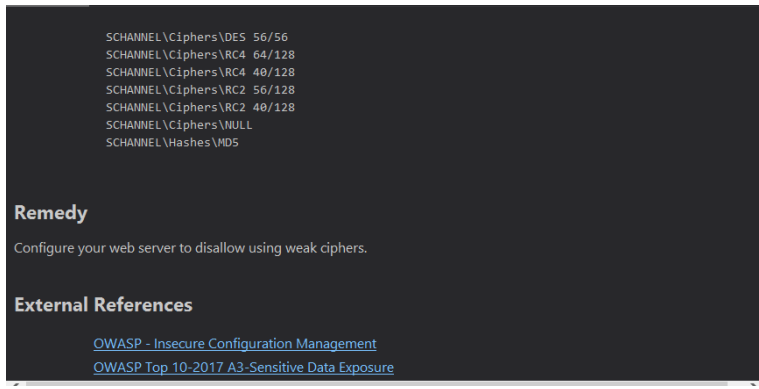
Scaning



Result



Result



Result


netsparker
10/14/2021 5:13:47 PM (UTC+05:30)
Detailed Scan Report
https://swipelife.tinder.com/
Scan Time : 10/14/2021 5:11:54 PM (UTC+05:30)
Scan Duration : 00:00:00:55
Total Requests : 693
Average Speed : 12.5r/s
Risk Level:
MEDIUM
Your website is fairly insecure!
There are some problems on the application that need to be addressed but nothing that requires you to panic. Address the identified issues in timely manner.
Vulnerabilities
Critical 0
High 0
Medium 2
Low 1
Best Practice 2
Information 1
TOTAL 6

Report

Vulnerability	Suggested Action
HTTP Strict Transport Security (HSTS) Errors and Warnings	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Weak Ciphers Enabled	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Insecure Transportation Security Protocol Supported (TLS 1.0)	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Expect-CT Not Enabled	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Insecure Transportation Security Protocol Supported (TLS 1.1)	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

Report

Compliance Summary

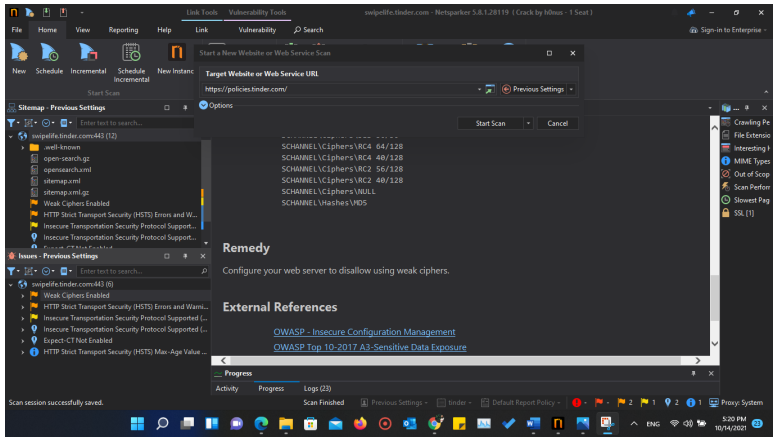
Compliance	Vulnerabilities
PCI DSS v3.2	3
OWASP 2013	4
OWASP 2017	4
HIPAA	2
ISO27001	6

PCI compliance data is generated based on the classifications and it has no validity. PCI DSS scans must be performed by an approved scanning vendor.

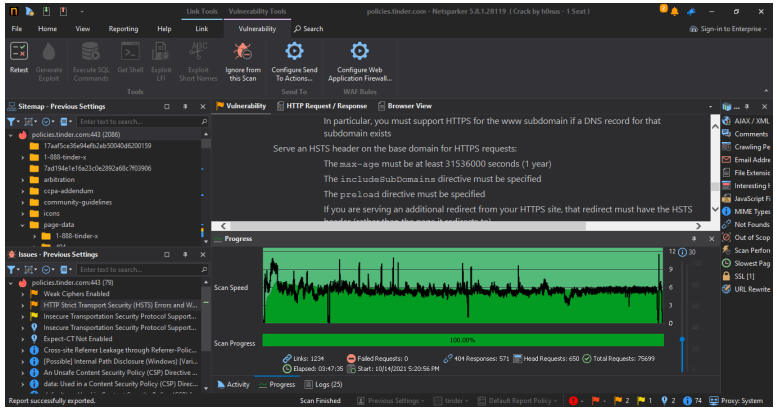
This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com

Report

Subdomain-https://policies.tinder.com/

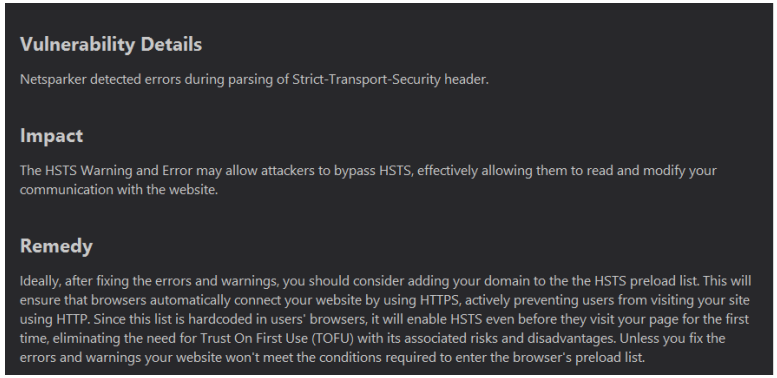


Scaning

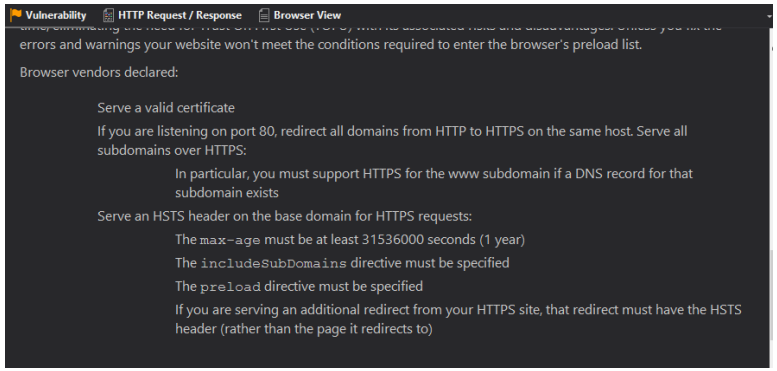


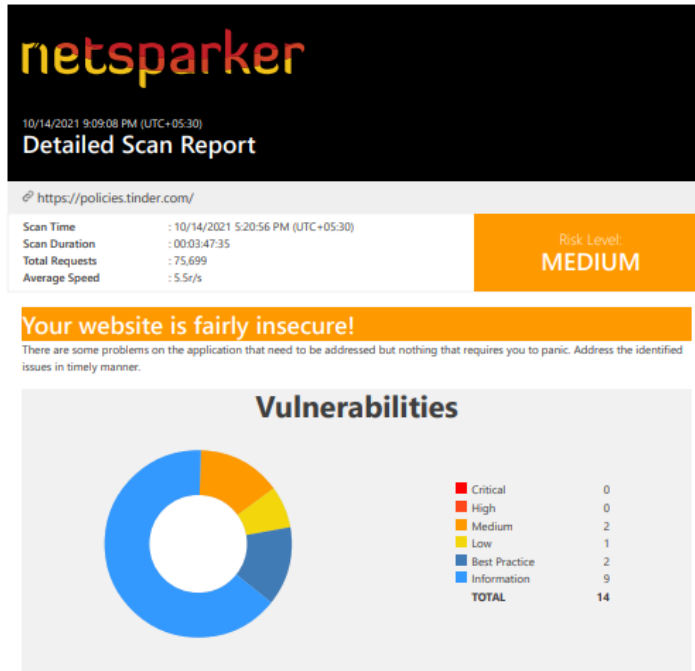
Scaning

Scanning


Vulnerability Details
Netsparker detected errors during parsing of Strict-Transport-Security header.
Impact
The HSTS Warning and Error may allow attackers to bypass HSTS, effectively allowing them to read and modify your communication with the website.
Remedy
Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list.

Result


Vulnerability
HTTP Request / Response
Browser View
errors and warnings your website won't meet the conditions required to enter the browser's preload list.
Browser vendors declared:
Serve a valid certificate
If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
Serve an HSTS header on the base domain for HTTPS requests:
The max-age must be at least 31536000 seconds (1 year)
The includeSubDomains directive must be specified
The preload directive must be specified
If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)


netsparker
10/14/2021 9:09:08 PM (UTC+05:30)
Detailed Scan Report
https://policies.tinder.com/
Scan Time : 10/14/2021 5:20:56 PM (UTC+05:30)
Scan Duration : 00:03:47:35
Total Requests : 75,699
Average Speed : 5.5r/s
Risk Level:
MEDIUM
Your website is fairly insecure!
There are some problems on the application that need to be addressed but nothing that requires you to panic. Address the identified issues in timely manner.
Vulnerabilities
Critical 0
High 0
Medium 2
Low 1
Best Practice 2
Information 9
TOTAL 14

Vulnerability	Suggested Action
HTTP Strict Transport Security (HSTS) Errors and Warnings	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Weak Ciphers Enabled	**Fix soon:** You should fix them soon. Once you've done this, you may want to rescan to check they're gone.
Insecure Transportation Security Protocol Supported (TLS 1.0)	**Consider fixing:** These vulnerabilities aren't very bad but they might help an attacker. You should think about fixing them.
Expect-CT Not Enabled	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Insecure Transportation Security Protocol Supported (TLS 1.1)	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
[Possible] Internal Path Disclosure (Windows)	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
An Unsafe Content Security Policy (CSP) Directive in Use	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Cross-site Referrer Leakage through Referrer-Policy	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
data: Used in a Content Security Policy (CSP) Directive	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
default-src Used in Content Security Policy (CSP)	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Email Address Disclosure	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Generic Email Address Disclosure	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Missing object-src in CSP Declaration	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

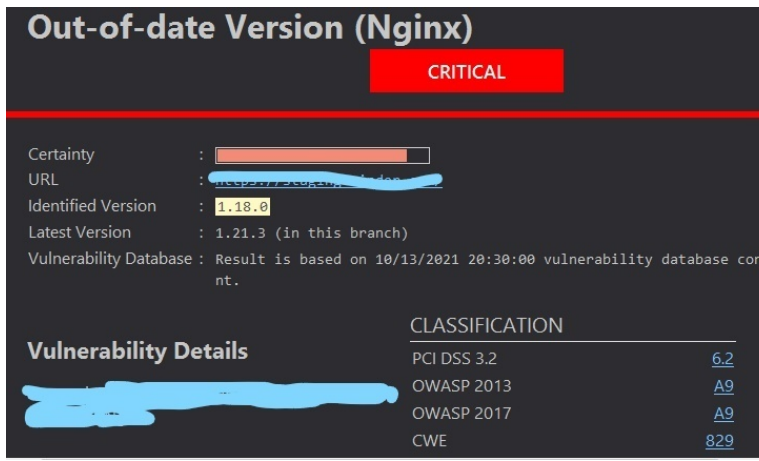
Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	3
OWASP 2013	5
OWASP 2017	5
HIPAA	3
ISO27001	14

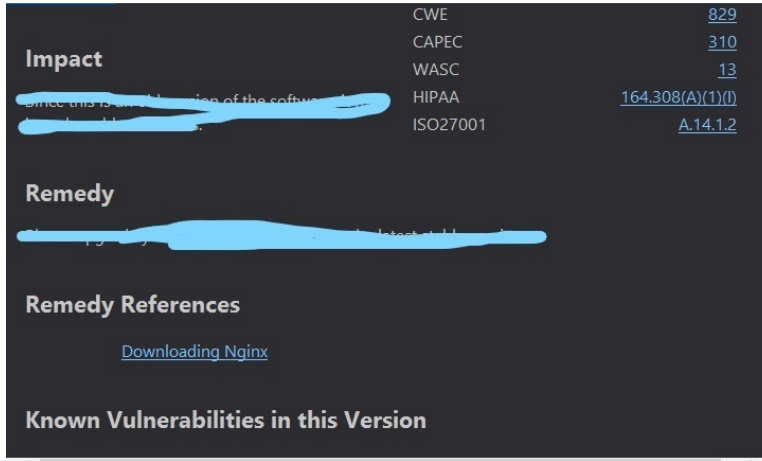
PCI compliance data is generated based on the classifications and it has no validity. PCI DSS scans must be performed by an approved scanning vendor.

This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com

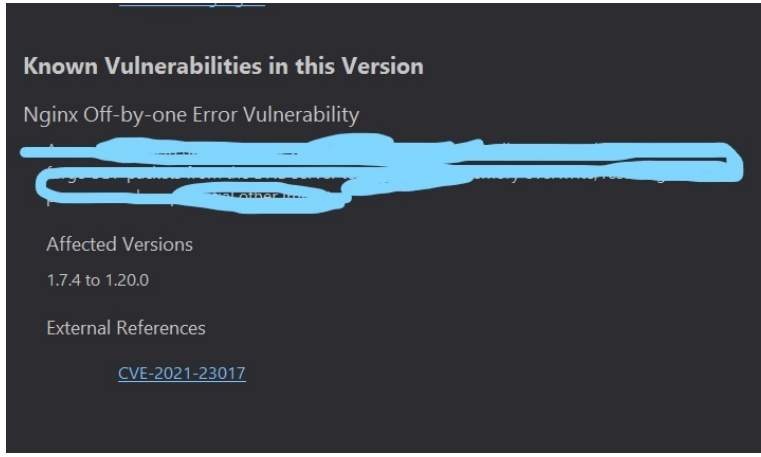
Subdomain- https://staging.tinder.com



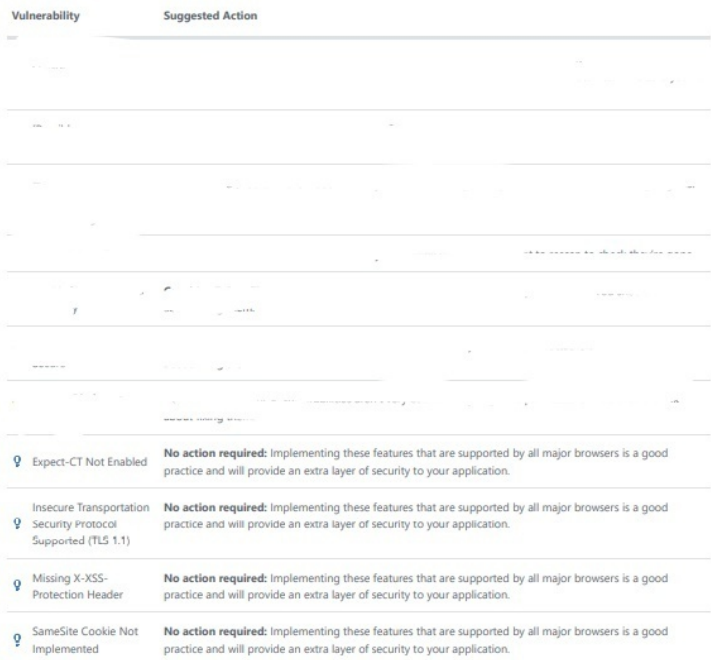
Scaning



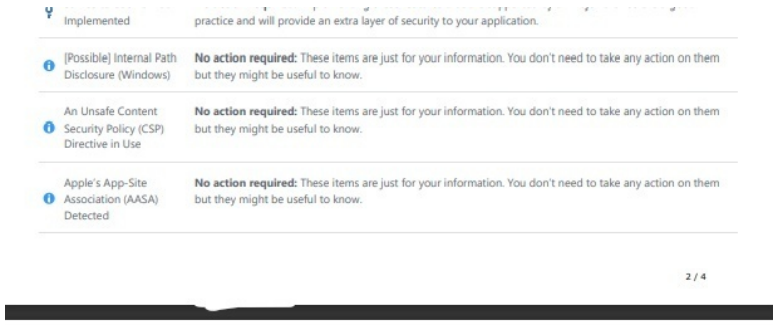
Scaning



Scaning

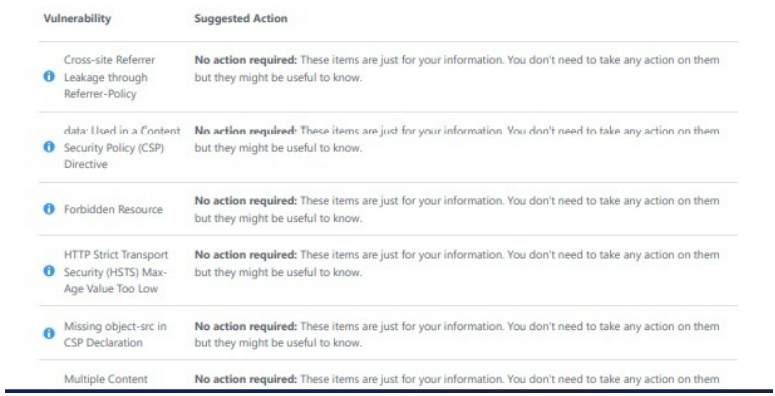


Vulnerability	Suggested Action
Expect-CT Not Enabled	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Insecure Transportation Security Protocol Supported (TLS 1.1)	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Missing X-XSS-Protection Header	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
SameSite Cookie Not Implemented	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.



Implemented	practice and will provide an extra layer of security to your application.
[Possible] Internal Path Disclosure (Windows)	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
An Unsafe Content Security Policy (CSP) Directive in Use	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Apple's App-Site Association (AASA) Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

2 / 4



Vulnerability	Suggested Action
Cross-site Referrer Leakage through Referrer-Policy	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
data: Used in a Content Security Policy (CSP) Directive	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Forbidden Resource	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Missing object-src in CSP Declaration	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Multiple Content	**No action required:** These items are just for your information. You don't need to take any action on them

Vulnerability	Suggested Action
Cross-site Referrer Leakage through Referrer-Policy	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
data: Used in a Content Security Policy (CSP) Directive	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Forbidden Resource	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Missing object-src in CSP Declaration	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Multiple Content Security Policy (CSP) Implementation Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Nginx Web Server Identified	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Robots.txt Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Sitemap Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

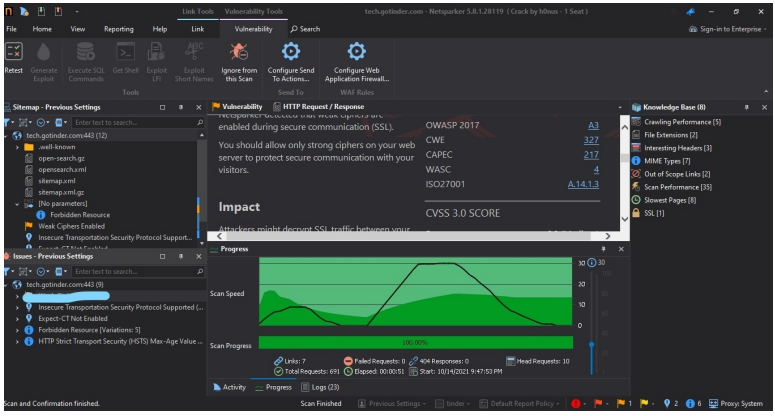
Compliance Summary

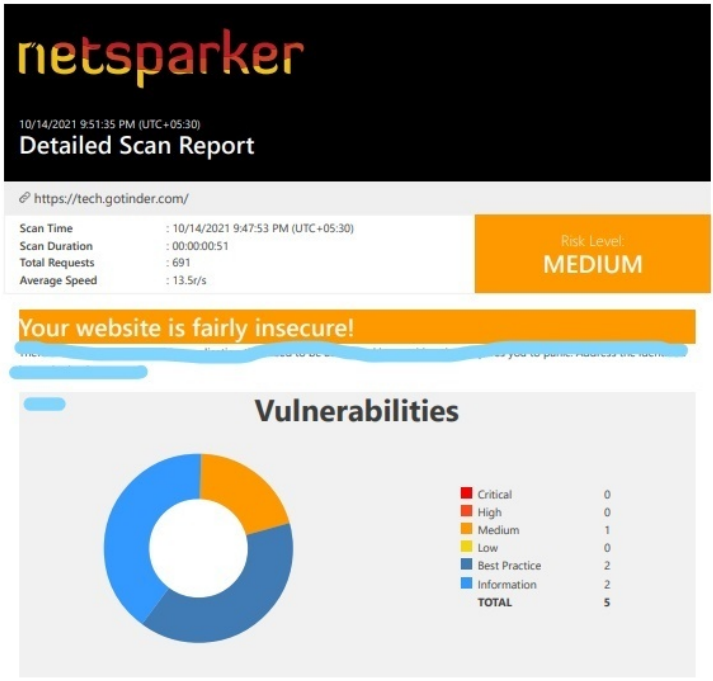
Compliance	Vulnerabilities
PCI DSS v3.2	4
OWASP 2013	9
OWASP 2017	9
HIPAA	5
ISO27001	22

PCI compliance data is generated based on the classifications and it has no validity. PCI DSS scans must be performed by an approved scanning vendor.

This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com

Subdomain-https://tech.gotinder.com

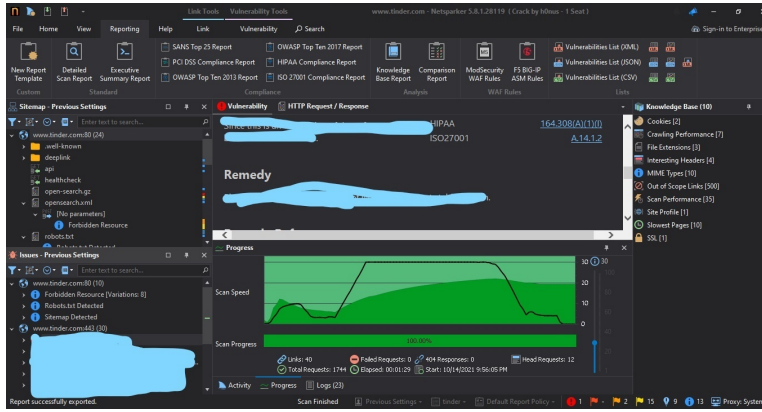


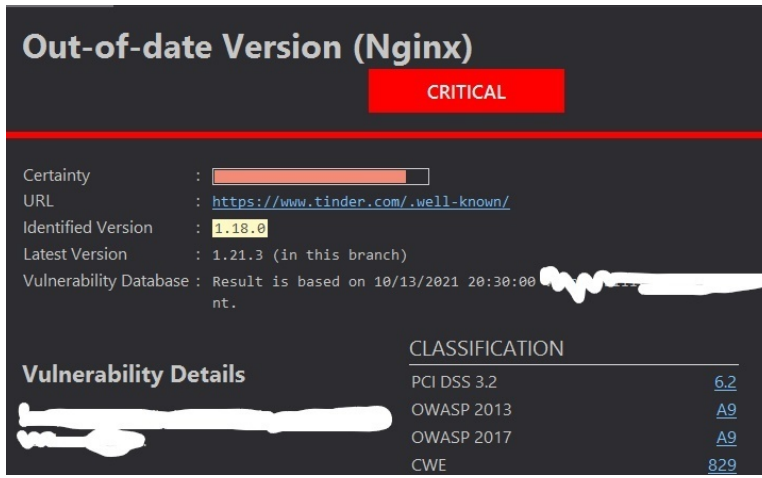

netsparker
10/14/2021 9:51:35 PM (UTC+05:30)
Detailed Scan Report
https://tech.gotinder.com/
Scan Time : 10/14/2021 9:47:53 PM (UTC+05:30)
Scan Duration : 00:00:00:51
Total Requests : 691
Average Speed : 13.5r/s
Risk Level:
MEDIUM
Your website is fairly insecure!
Vulnerabilities
Critical 0
High 0
Medium 1
Low 0
Best Practice 2
Information 2
TOTAL 5

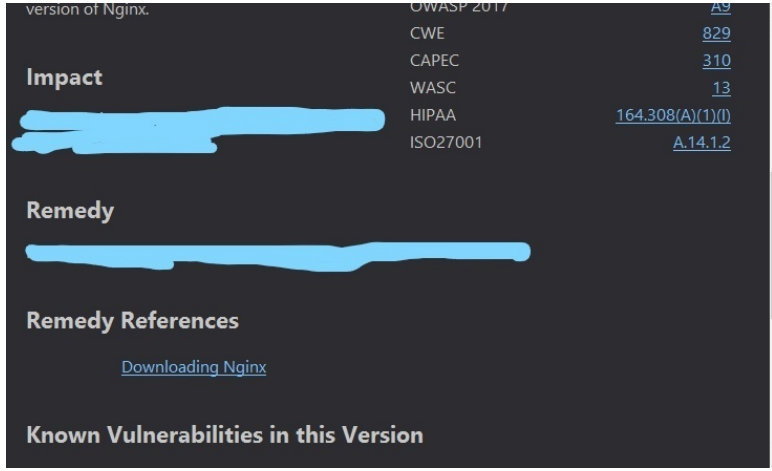
Vulnerability	Suggested Action
Expect-CT Not Enabled	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Insecure Transportation Security Protocol Supported (TLS 1.1)	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Forbidden Resource	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

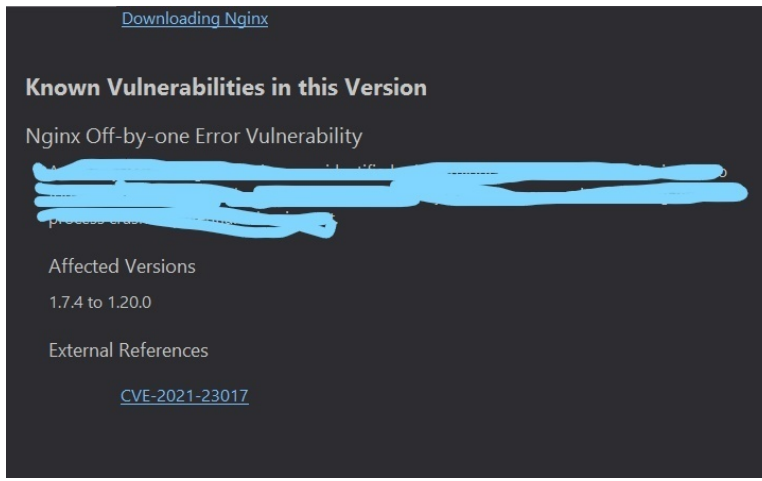
Vulnerability	Suggested Action
Expect-CT Not Enabled	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Insecure Transportation Security Protocol Supported (TLS 1.1)	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Forbidden Resource	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

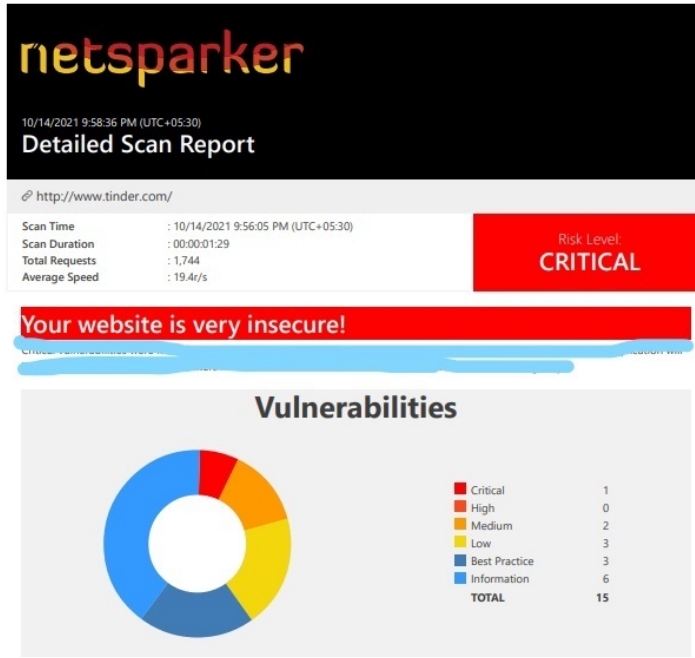
Subdomain-http://www.tinder.com

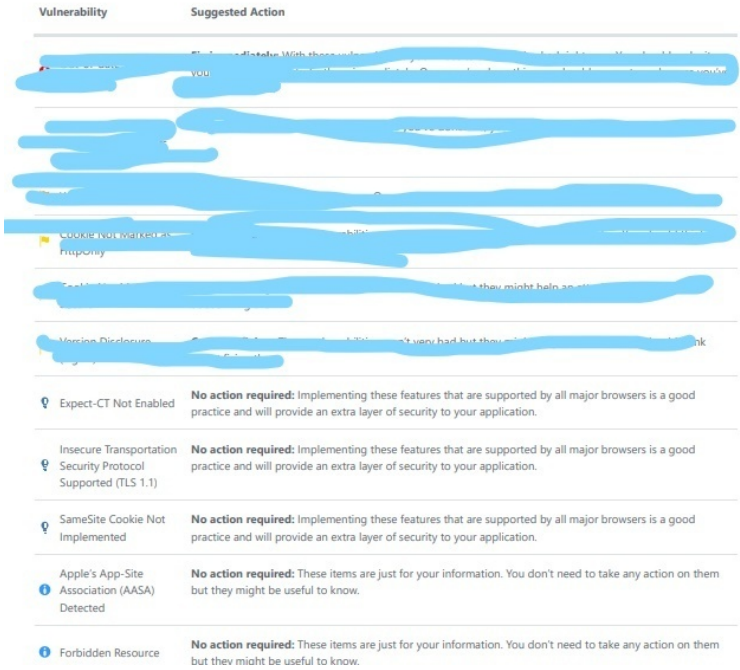

Remedy
Progress
Scan Speed
Scan Progress


Out-of-date Version (Nginx)
CRITICAL
Certainty :
URL : https://www.tinder.com/.well-known/
Identified Version : 1.18.0
Latest Version : 1.21.3 (in this branch)
Vulnerability Database : Result is based on 10/13/2021 20:30:00
Vulnerability Details
CLASSIFICATION
PCI DSS 3.2 6.2
OWASP 2013 A9
OWASP 2017 A9
CWE 829


version of Nginx.
OWASP 2017 A9
CWE 829
CAPEC 310
WASC 13
HIPAA 164.308(A)(1)(I)
ISO27001 A.14.1.2
Impact
Remedy
Remedy References
Downloading Nginx
Known Vulnerabilities in this Version


Downloading Nginx
Known Vulnerabilities in this Version
Nginx Off-by-one Error Vulnerability
Affected Versions
1.7.4 to 1.20.0
External References
CVE-2021-23017


netsparker
10/14/2021 9:58:36 PM (UTC+05:30)
Detailed Scan Report
http://www.tinder.com/
Scan Time : 10/14/2021 9:56:05 PM (UTC+05:30)
Scan Duration : 00:00:01:29
Total Requests : 1,744
Average Speed : 19.4r/s
Risk Level:
CRITICAL
Your website is very insecure!
Vulnerabilities
Critical 1
High 0
Medium 2
Low 3
Best Practice 3
Information 6
TOTAL 15

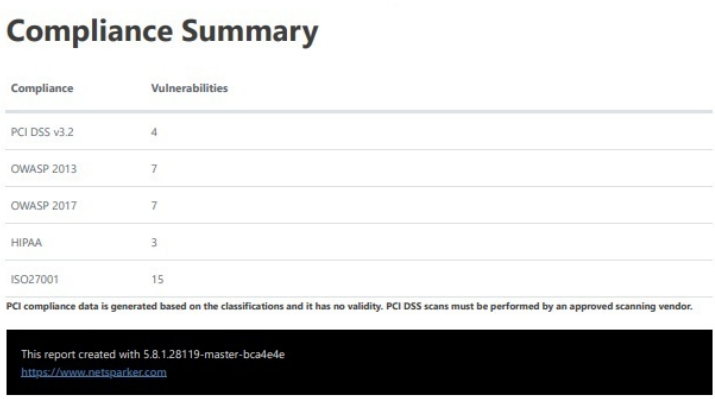


Vulnerability	Suggested Action
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
Expect-CT Not Enabled	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Insecure Transportation Security Protocol Supported (TLS 1.1)	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
SameSite Cookie Not Implemented	**No action required:** Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
Apple's App-Site Association (AASA) Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Forbidden Resource	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

Forbidden Resource	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Nginx Web Server Identified	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.
Robots.txt Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.

2 / 4

Vulnerability	Suggested Action
Sitemap Detected	**No action required:** These items are just for your information. You don't need to take any action on them but they might be useful to know.



Compliance Summary

Compliance	Vulnerabilities
PCI DSS v3.2	4
OWASP 2013	7
OWASP 2017	7
HIPAA	3
ISO27001	15

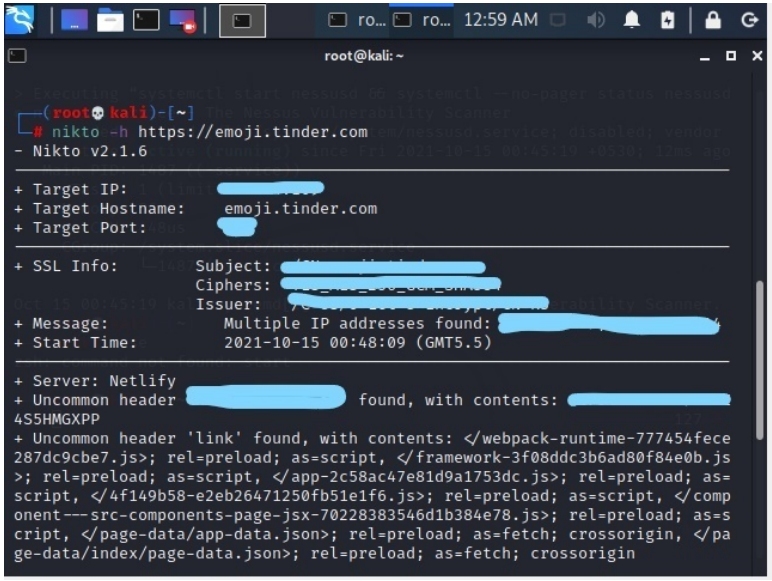
PCI compliance data is generated based on the classifications and it has no validity. PCI DSS scans must be performed by an approved scanning vendor.

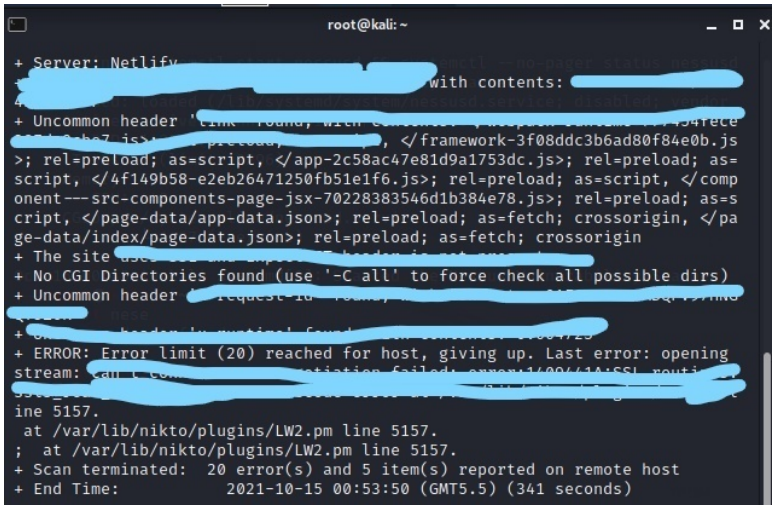
This report created with 5.8.1.28119-master-bca4e4e
https://www.netsparker.com

Nikto

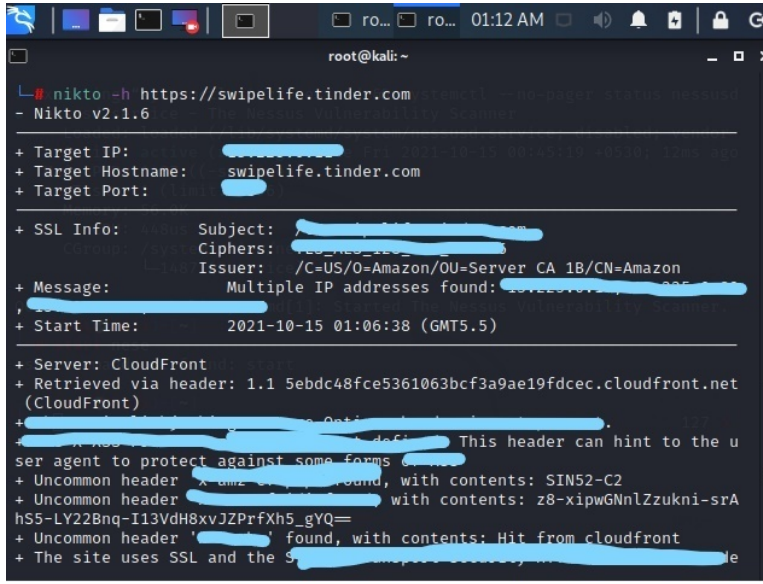
• Nikto is open source web vulnerability scanner.
• This service may be used to check for known security vulnerabilities and
misconfigurations on a website, virtual host, or web server.

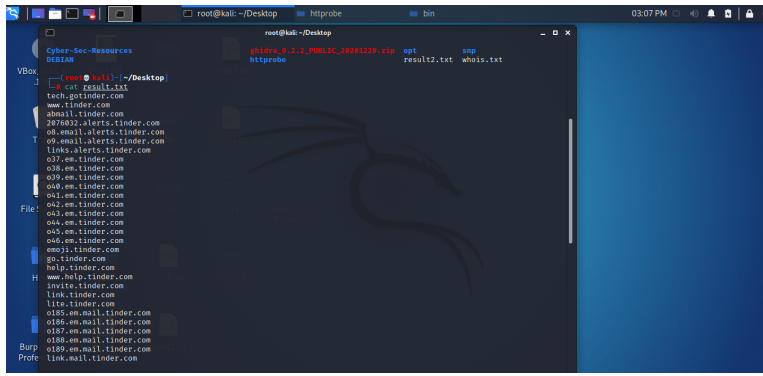
Subdomain- https://emoji.tinder.com



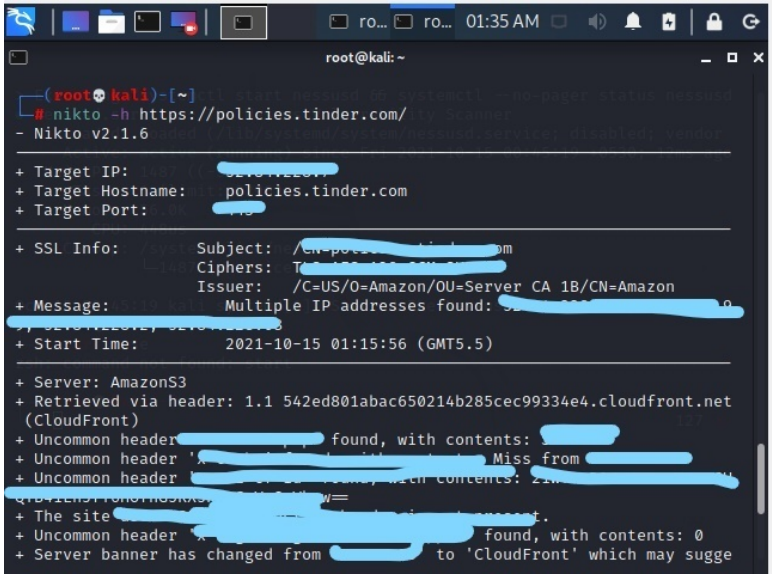


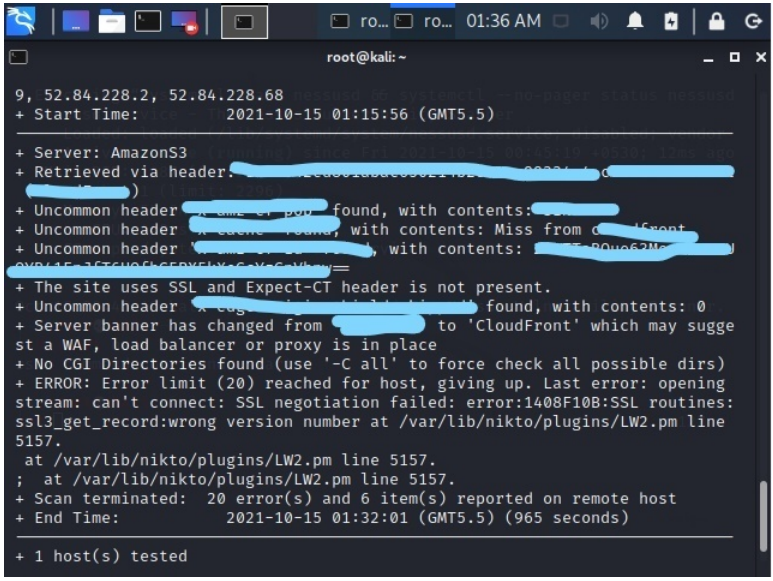
Subdomain- https://swipelife.tinder.com



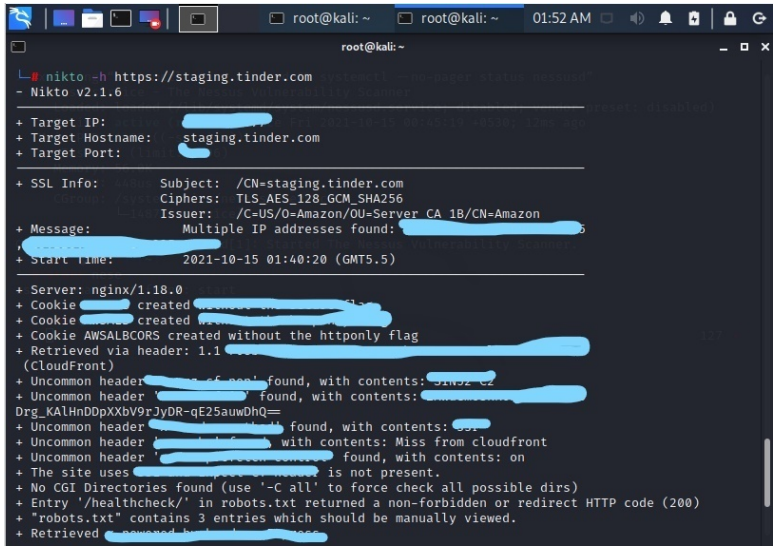


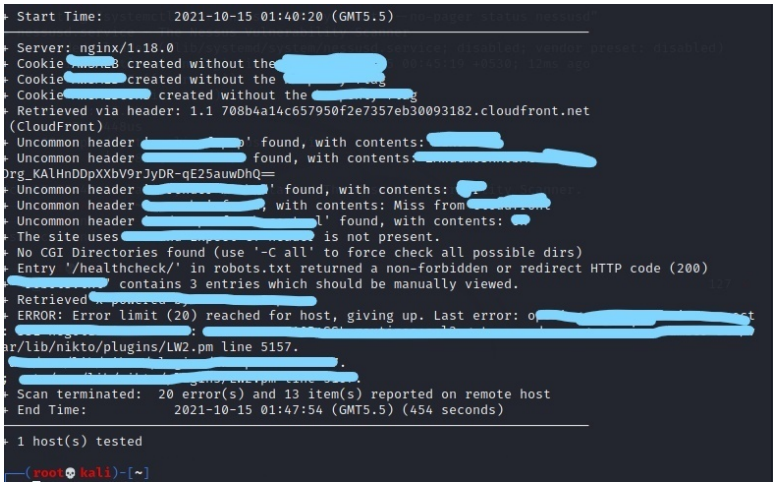
Subdomain- https:// policies.tinder.com/





Subdomain- https://staging.tinder.com





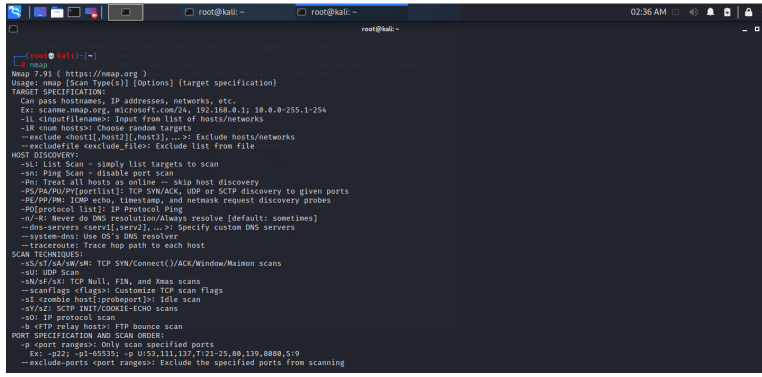
Find target has open ports using nmap tool

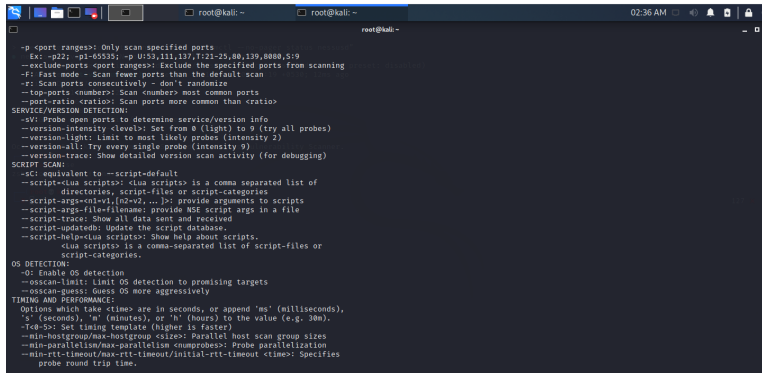
Nmap tool

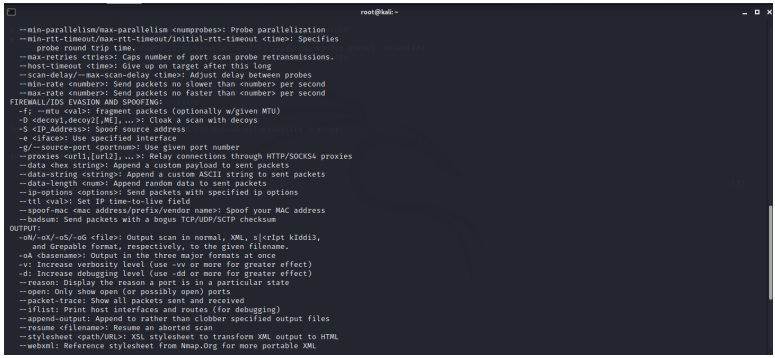
Nmap is open source network scanner. It use for network detection and security auditing. Nmap was created to scan big networks

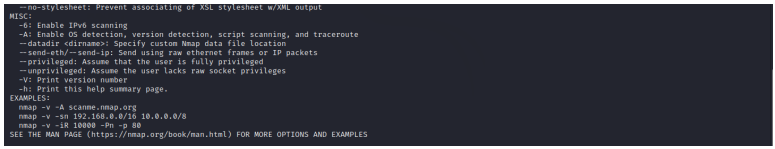
quickly, although it also works well on single hosts. It'salso helpful for controlling service upgrade timetables, according to several system and networkmanagers. Nmap is compatible with all major computer operating systems, and official binary packages for Linux, Windows, and Mac OS X are available.

We can open nmap tool using "nmap" command.



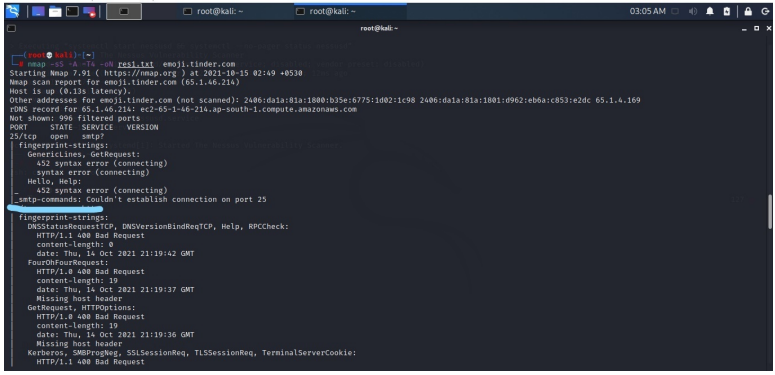


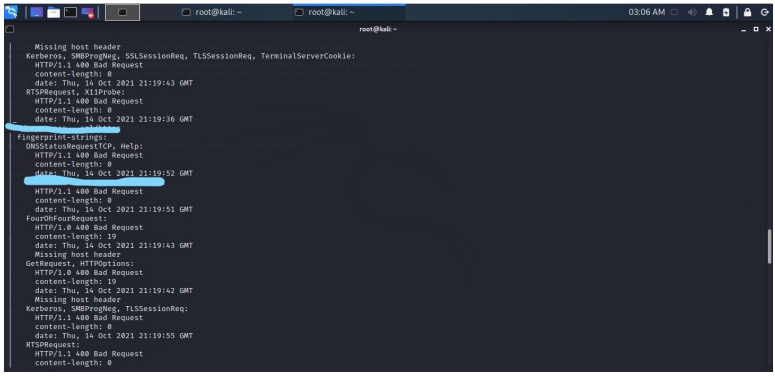


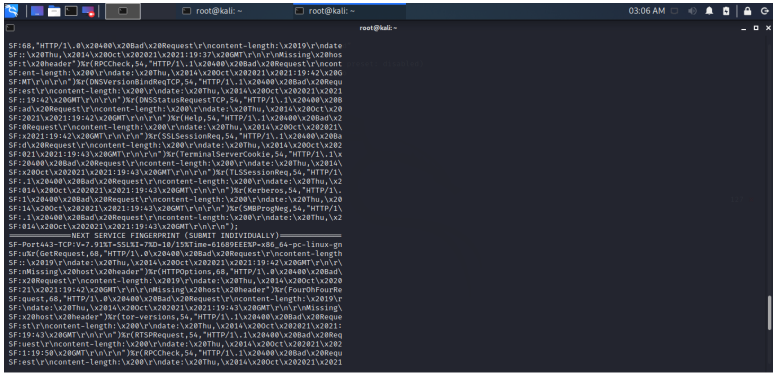


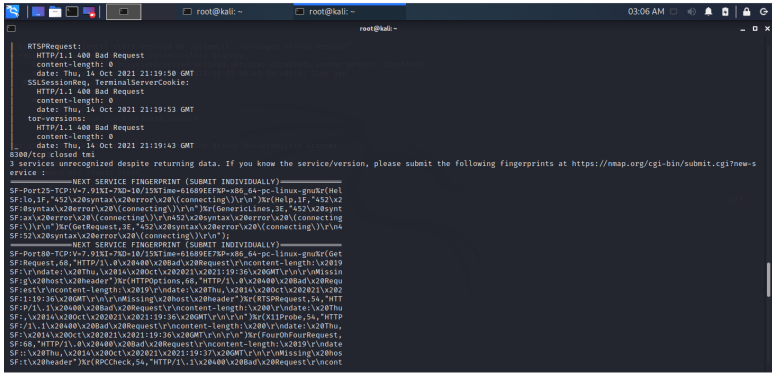
Then find target subdomain open ports and details about subdomains.

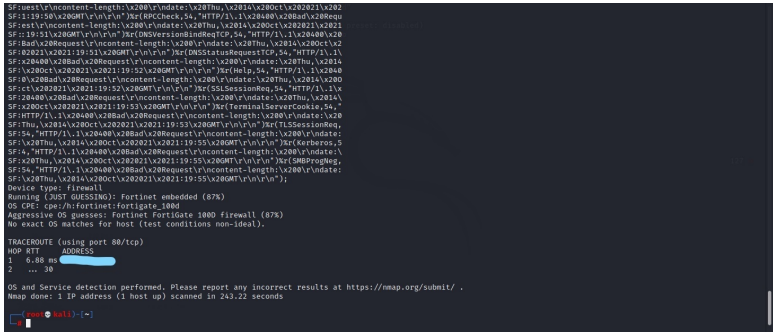
Subdomain- https://emoji.tinder.com

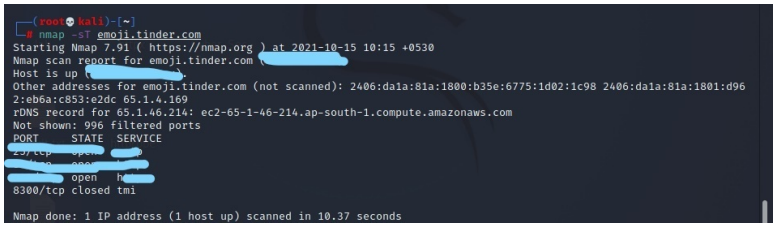



root@kali: ~
root@kali: ~
03:06 AM
root@kali: ~
Missing host header
Kerberos, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:43 GMT
RTSPRequest, X11Probe:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:36 GMT
fingerprint-strings:
DNSStatusRequestTCP, Help:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:52 GMT
DNSVersionBindReqTCP:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:51 GMT
FourOhFourRequest:
HTTP/1.0 400 Bad Request
content-length: 19
date: Thu, 14 Oct 2021 21:19:43 GMT
Missing host header
GetRequest, HTTPOptions:
HTTP/1.0 400 Bad Request
content-length: 19
date: Thu, 14 Oct 2021 21:19:42 GMT
Missing host header
Kerberos, SMBProgNeg, TLSSessionReq:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:55 GMT
RTSPRequest:
HTTP/1.1 400 Bad Request
content-length: 0

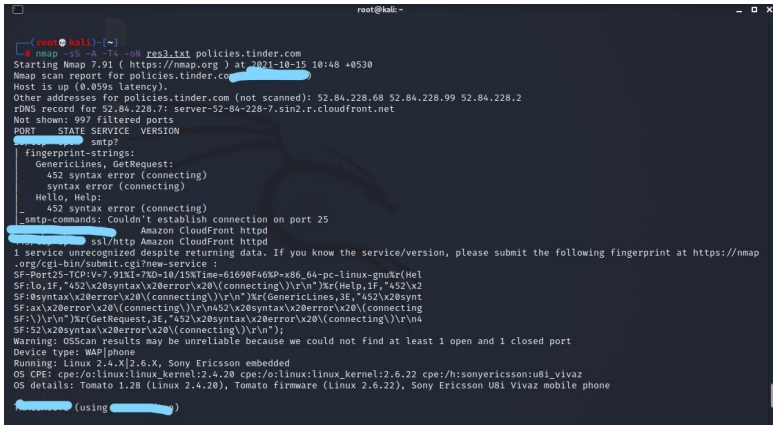

root@kali: ~
root@kali: ~
03:06 AM
root@kali: ~
SF:68,"HTTP/1\.0\x20400\x20Bad\x20Request\r\ncontent-length:\x2019\r\ndate
SF:r\x20Thu,\x2014\x20Oct\x202021\x2021:19:37\x20GMT\r\n\r\nMissing\x20hos
SF:t\x20header"%r(RPCCheck,54,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncont
SF:ent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x2021:19:42\x20G
SF:MT\r\n\r\n")%r(DNSVersionBindReqTCP,54,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x2021
SF::19:42\x20GMT\r\n\r\n")%r(DNSStatusRequestTCP,54,"HTTP/1\.1\x20400\x20B
SF:ad\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x20
SF:2021\x2021:19:42\x20GMT\r\n\r\n")%r(Help,54,"HTTP/1\.1\x20400\x20Bad\x2
SF:0Request\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x202021\
SF:x2021:19:42\x20GMT\r\n\r\n")%r(SSLSessionReq,54,"HTTP/1\.1\x20400\x20Ba
SF:d\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x202
SF:021\x2021:19:43\x20GMT\r\n\r\n")%r(TerminalServerCookie,54,"HTTP/1\.1\x
SF:20400\x20Bad\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\
SF:x20Oct\x202021\x2021:19:43\x20GMT\r\n\r\n")%r(TLSSessionReq,54,"HTTP/1\
SF:.1\x20400\x20Bad\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2
SF:014\x20Oct\x202021\x2021:19:43\x20GMT\r\n\r\n")%r(Kerberos,54,"HTTP/1\.
SF:1\x20400\x20Bad\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu,\x20
SF:14\x20Oct\x202021\x2021:19:43\x20GMT\r\n\r\n")%r(SMBProgNeg,54,"HTTP/1\
SF:.1\x20400\x20Bad\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2
SF:014\x20Oct\x202021\x2021:19:43\x20GMT\r\n\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port443-TCP:V=7.91%T=SSL%I=7%D=10/15%Time=61689EEE%P=x86_64-pc-linux-gn
SF:uRequest,68,"HTTP/1\.0\x20400\x20Bad\x20Request\r\ncontent-length
SF::\x2019\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x2021:19:42\x20GMT\r\n\r\
SF:nMissing\x20host\x20header"%r(HTTPOptions,68,"HTTP/1\.0\x20400\x20Bad\
SF:x20Request\r\ncontent-length:\x2019\r\ndate:\x20Thu,\x2014\x20Oct\x2020
SF:21\x2021:19:42\x20GMT\r\n\r\nMissing\x20host\x20header"%r(FourOhFourRe
SF:quest,68,"HTTP/1\.0\x20400\x20Bad\x20Request\r\ncontent-length:\x2019\r
SF:\ndate:\x20Thu,\x2014\x20Oct\x202021\x2021:19:43\x20GMT\r\n\r\nMissing\
SF:x20host\x20header"%r(tor-versions,54,"HTTP/1\.1\x20400\x20Bad\x20Reque
SF:st\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x2021:
SF:19:43\x20GMT\r\n\r\n")%r(RTSPRequest,54,"HTTP/1\.1\x20400\x20Bad\x20Req
SF:uest\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x202
SF:1:19:50\x20GMT\r\n\r\n")%r(RPCCheck,54,"HTTP/1\.1\x20400\x20Bad\x20Requ
SF:est\r\ncontent-length:\x200\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x2021

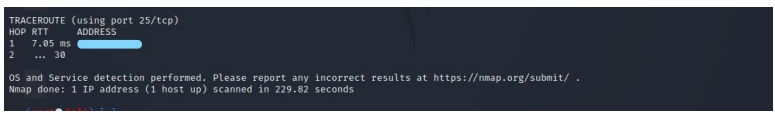

root@kali: ~
root@kali: ~
03:06 AM
root@kali: ~
RTSPRequest:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:50 GMT
SSLSessionReq, TerminalServerCookie:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:53 GMT
tor-versions:
HTTP/1.1 400 Bad Request
content-length: 0
date: Thu, 14 Oct 2021 21:19:43 GMT
8300/tcp closed tmi
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-s
ervice :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port25-TCP:V=7.91%I=7%D=10/15%Time=61689EEF%P=x86_64-pc-linux-gnu%r(Hel
SF:lo,1F,"452\x20syntax\x20error\x20(connecting)\r\n")%r(Help,1F,"452\x2
SF:0syntax\x20error\x20(connecting)\r\n")%r(GenericLines,3E,"452\x20synt
SF:ax\x20error\x20(connecting)\r\n452\x20syntax\x20error\x20(connecting
SF:)\r\n")%r(GetRequest,3E,"452\x20syntax\x20error\x20(connecting)\r\n4
SF:52\x20syntax\x20error\x20(connecting)\r\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.91%I=7%D=10/15%Time=61689EE7%P=x86_64-pc-linux-gnu%r(Get
SF:Request,68,"HTTP/1\.0\x20400\x20Bad\x20Request\r\ncontent-length:\x2019
SF:\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x2021:19:36\x20GMT\r\n\r\nMissin
SF:g\x20host\x20header"%r(HTTPOptions,68,"HTTP/1\.0\x20400\x20Bad\x20Requ
SF:est\r\ncontent-length:\x2019\r\ndate:\x20Thu,\x2014\x20Oct\x202021\x202
SF:1:19:36\x20GMT\r\n\r\nMissing\x20host\x20header"%r(RTSPRequest,54,"HTT
SF:P/1\.1\x20400\x20Bad\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu
SF:,\x2014\x20Oct\x202021\x2021:19:36\x20GMT\r\n\r\n")%r(X11Probe,54,"HTTP
SF:/1\.1\x20400\x20Bad\x20Request\r\ncontent-length:\x200\r\ndate:\x20Thu,
SF:\x2014\x20Oct\x202021\x2021:19:36\x20GMT\r\n\r\n")%r(FourOhFourRequest,
SF:68,"HTTP/1\.0\x20400\x20Bad\x20Request\r\ncontent-length:\x2019\r\ndate
SF::\x20Thu,\x2014\x20Oct\x202021\x2021:19:37\x20GMT\r\n\r\nMissing\x20hos
SF:t\x20header"%r(RPCCheck,54,"HTTP/1\.1\x20400\x20Bad\x20Request\r\ncont



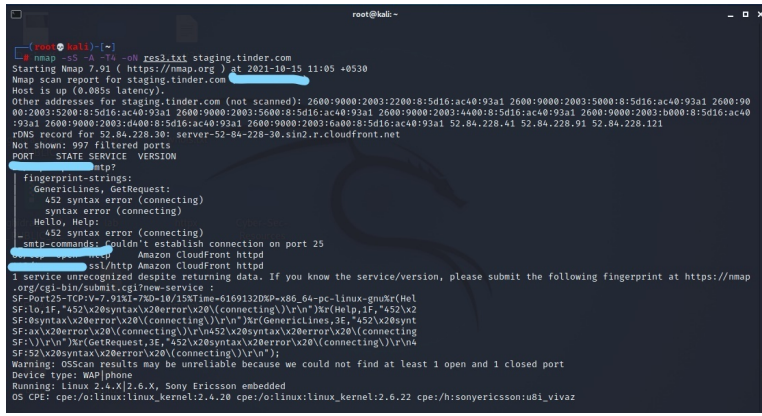


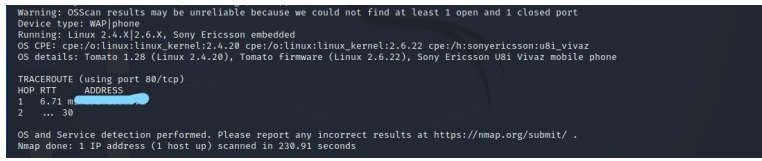
Subdomain-https://policies.tinder.com/



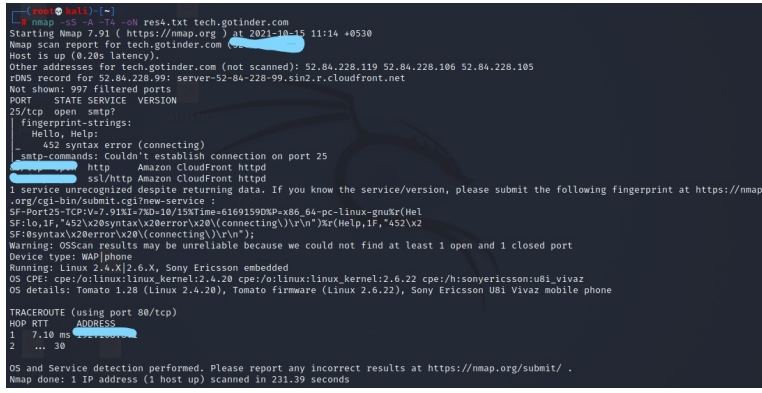


Subdomain-https://staging.tinder.com

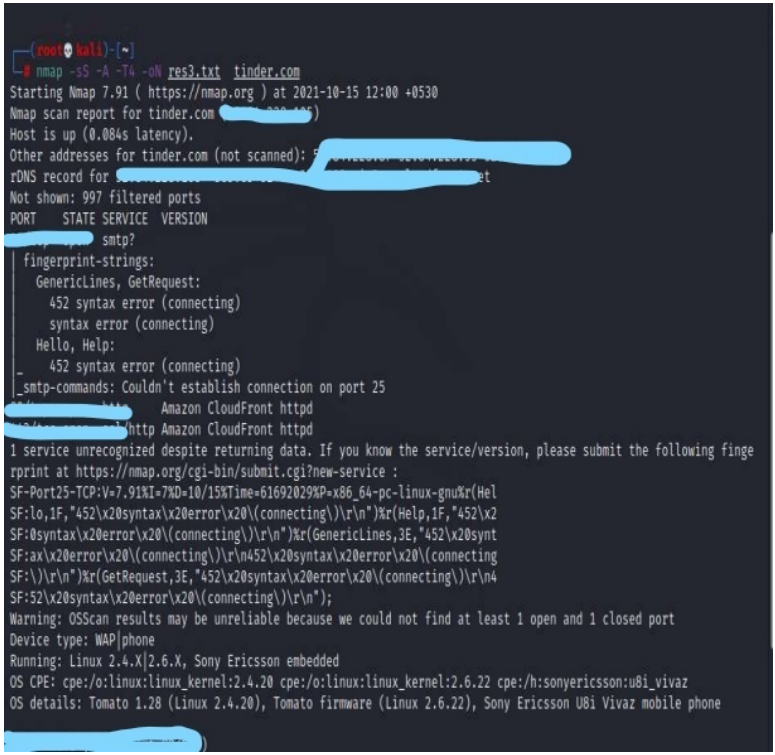




Subdomain- https://tech.gotinder.com



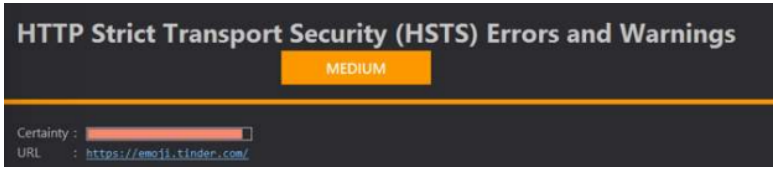
Subdomain - http://www.tinder.com


(root kali)-[~]
nmap -sS -A -T4 -oN res3.txt tinder.com
Starting Nmap 7.91 (https://nmap.org) at 2021-10-15 12:00 +0530
Nmap scan report for tinder.com
Host is up (0.084s latency).
Other addresses for tinder.com (not scanned):
rDNS record for
Not shown: 997 filtered ports
PORT STATE SERVICE VERSION
smtp?
| fingerprint-strings:
| GenericLines, GetRequest:
| 452 syntax error (connecting)
| syntax error (connecting)
| Hello, Help:
|_ 452 syntax error (connecting)
|_smtp-commands: Couldn't establish connection on port 25
Amazon CloudFront httpd
http Amazon CloudFront httpd
1 service unrecognized despite returning data. If you know the service/version, please submit the following finge
rprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.91%I=7%D=10/15%Time=61692029%P=x86_64-pc-linux-gnu%r(Hel
SF:lo,1F,"452\x20syntax\x20error\x20\(connecting\)\r\n")%r(Help,1F,"452\x2
SF:0syntax\x20error\x20\(connecting\)\r\n")%r(GenericLines,3E,"452\x20synt
SF:ax\x20error\x20\(connecting\)\r\n452\x20syntax\x20error\x20\(connecting
SF:\)\r\n")%r(GetRequest,3E,"452\x20syntax\x20error\x20\(connecting\)\r\n4
SF:52\x20syntax\x20error\x20\(connecting\)\r\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP phone
Running: Linux 2.4.X 2.6.X, Sony Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.20 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

Analyze vulnerabilities

Analyzing vulnerabilities is a study focused on security-related problems that have a
moderate to severe effect on the product or system's security.
I use nikto and netsparker to complete my scan process. Then I can found some
vulnerabilities in these sub domains.

Subdomain- - https://emoji.tinder.com



HSTS

• Hsts is a security header.it s means when we type domain http protocol that security header converts it to https protocol. This security header helps to protect against man-inthe middle attack, protocol downgrade attacks and cookie hijacking.
Implementation

• The server sends the HSTS Policy to the user agent through the "**Strict-TransportSecurity**" HTTP response header field.

• The HSTS Policy specifies a time period during which the user agent should only
communicate with the server via secure means.

• Then HSTS enabled web sites drop the http requests and this request redirected as a
https.

How to fix vulnerabilities

• we need to add this domain to the hsts preload list. this will ensure that browser
automatically connect website by using https.

1. The max-age must be at least 31536000 seconds (1year)
2. The includeSubdomains directive must be specified
3. The preload directive must be specified

Subdomain -https://swipelife.tinder.com

Weak Ciphers

• weak ciphers is an encryption/decryption technique that utilizes a key that isn't long enough. The stronger the encryption, the bigger the key size. Weak ciphers are
encryption/decryption methods with key sizes smaller than 128 bits.

Impact

• attackers might decrypt ssl traffic between server and web site visitors.

How to fix vulnerabilities

• Use strong ciphers.

Subdomain- https://staging.tinder.com

NGINX

• NGINX is an open source web server that also includes a reverse proxy, caching, load balancing, video streaming, and other features. It started out as a web server with the aim of delivering the best possible speed and stability. In addition to being an HTTP server, NGINX may also function as an email proxy server (IMAP, POP3, and SMTP), as well as a reverse proxy and load balancer for HTTP, TCP, and UDP servers.

Impact

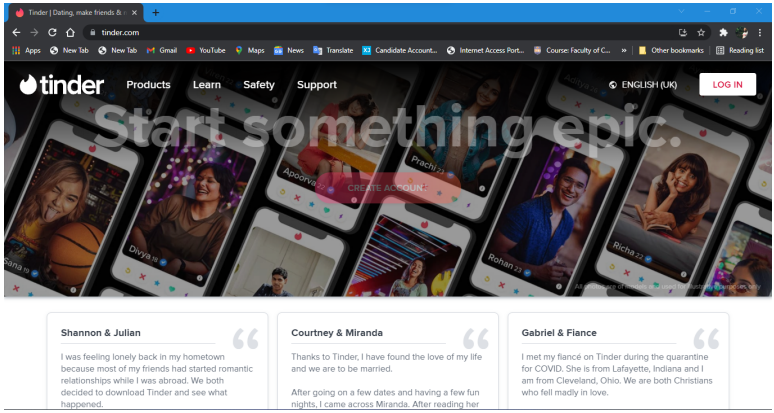
• Netspark identifies the this service is out-of-date. This is critical vulnerability in this subdomain.

How to fix

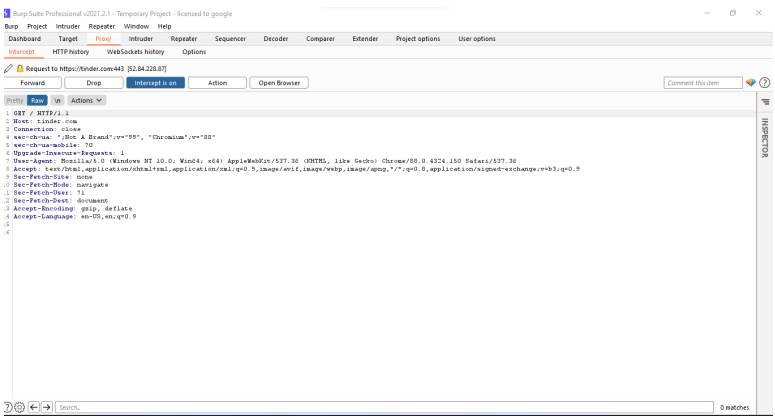
• Upgrade the software.

Manual testing

I use this Subdomain-“ https://swipelife.tinder.com “ complete the manual testing.



- Then, I try to intercept this web page using burp-suite.

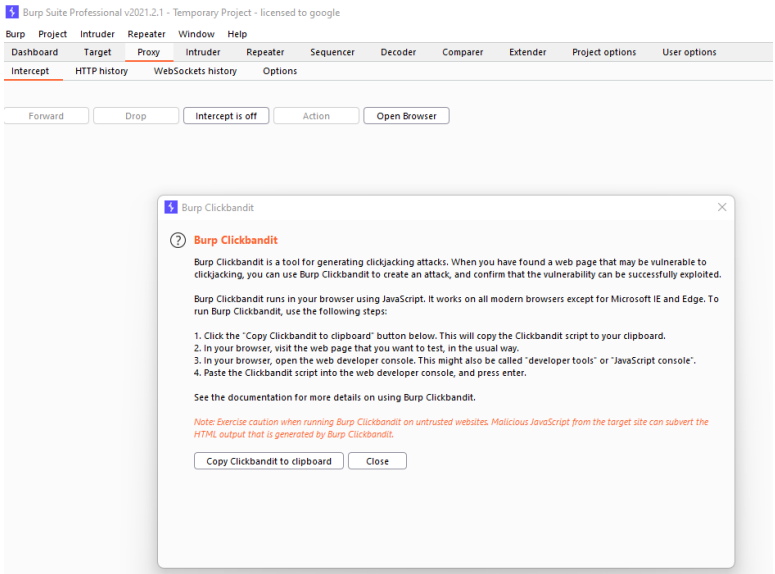


After I try do click jacking attack. Using burp suite tool

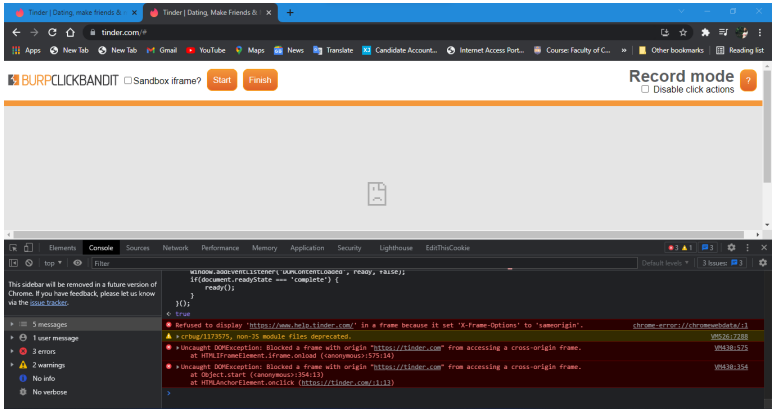
Clickjacking

• A clickjacking attack is when a user is tricked into clicking a website element that is hidden or disguised as another element. Users may inadvertently download malware, browse dangerous web sites, give passwords or sensitive information, send money, or make online purchases as a result of this.

• First we need to go burp option and click the clickbandit option . after copy
clickbandit to clipboard .



• After copying clickbandit. Go to the target web application and press f12 and go to the console and submit it.
• Now we can see this result. This website is secure site for click jacking.


Tinder | Dating, make friends &
Tinder | Dating, Make Friends &
tinder.com/#
Apps
New Tab
New Tab
Gmail
YouTube
Maps
News
Translate
Candidate Account...
Internet Access Port...
Course: Faculty of C...
Other bookmarks
Reading list
BURPCLICKBANDIT
Sandbox iframe?
Start
Finish
Record mode
Disable click actions
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
EditThisCookie
Filter
Default levels
3 Issues:
This sidebar will be removed in a future version of Chrome. If you have feedback, please let us know via the issue tracker.
5 messages
1 user message
3 errors
2 warnings
No info
No verbose
window.addEventListener('DOMContentLoaded', ready, false);
if(document.readyState === 'complete') {
ready();
}
})();
true
Refused to display 'https://www.helo.tinder.com/' in a frame because it set 'X-Frame-Options' to 'sameorigin'.
chrome-error://chromewebdata/:1
crbug/1173575, non-JS module files deprecated.
VM526:7288
Uncaught DOMException: Blocked a frame with origin "https://tinder.com" from accessing a cross-origin frame.
at HTMLIFrameElement.iframe.onload (<anonymous>:575:14)
VM430:575
Uncaught DOMException: Blocked a frame with origin "https://tinder.com" from accessing a cross-origin frame.
at Object.start (<anonymous>:354:13)
at HTMLAnchorElement.onclick (https://tinder.com/:1:13)
VM430:354

Conclusion

This web audit for https://tinder.com. Then I can find subdomains in https://tinder.com using some tools. After I scan all of subdomains, what subdomains are alive subdomain. Finding alive subdomains, I selected few subdomains to find vulnerabilities. After I've checked each subdomain for security flaws, and I analyzed each subdomain. Then try to exploit some vulnerabilities and finally, I explain how to avoid these vulnerabilities. (this part in vulnerability analyzing part).