

VULNERABILITY ASSESSMENT IN TINDER

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



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2021 Chamath Janindu Abewickrama, Menaka
Moonamaldeniya and Chathuri Udagedara

Contents

Purpose	1
Introduction	2
Scope	3
OWASP Top 10 Security Risks and Vulnerabilities	5
Severity Levels	7
In Scope Domains	8
Out of Scope Domains	9
Information Gathering	10
Automated testing	11
Analyze vulnerabilities	66
Manual testing	69
Conclusion	72

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.

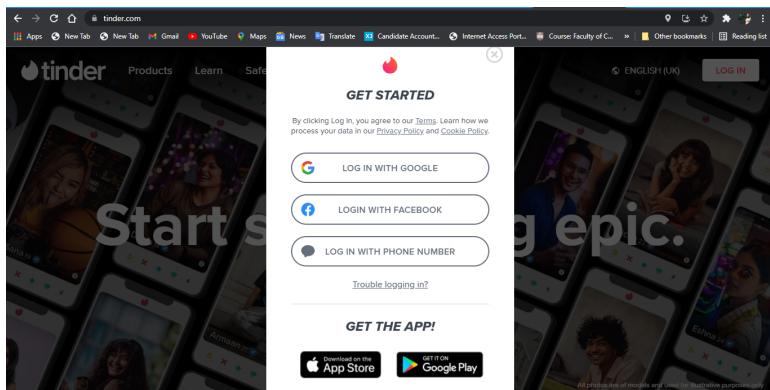
At that moment, we may use this audit to identify defects and security flaws. We may then move on to web penetration. At this point, security experts can mitigate the risks posed by these flaws. The goal of website security audits is to identify and fix vulnerabilities in your website's design before they are discovered by hostile hackers.

Scope

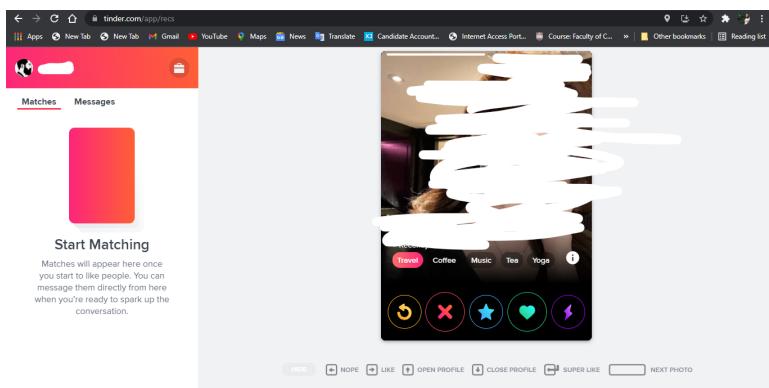
Tinder is an American geosocial networking and online dating application that allows

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 bunt report.



Login page



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 records, business secrets etc.

3. A03:2021-Injection

Attacker use malicious code inject to the website using java script, xml, sql, programming 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 recording 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.imgur.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
- Spaming
- 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.

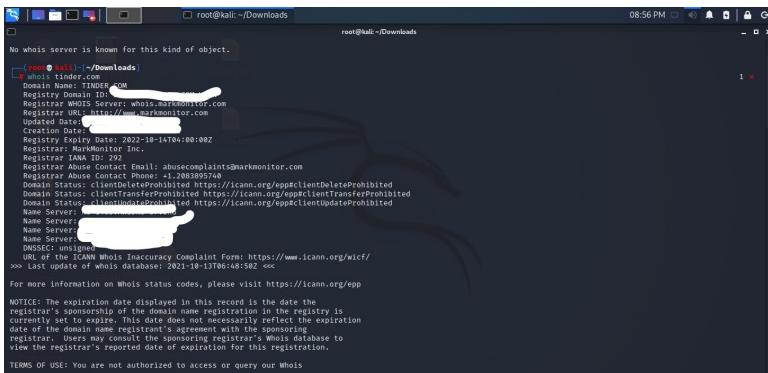
Passive scanning is a vulnerability detection technique that depends on data gathered from network data collected from a target machine without requiring direct interaction. **We use passive scan for this web audit.**

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.



A terminal window titled 'root@kali: ~/Downloads' showing the output of a 'whois' command for the domain 'TINDER.COM'. The output includes the following information:

```
root@kali:~/Downloads
08:56 PM
root@kali:~/Downloads

No whois server is known for this kind of object.

[whois.kali: ~] ->/Downloads
Domain Name: TINDER.COM
Registry Domain ID:
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: https://www.markmonitor.com
Updated Date:
Creation Date:
Registry Expiry Date: 2022-10-14T00:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID:
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1208389746
Domain Status: clientDeleteProhibited https://icann.org/epp/clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp/clientUpdateProhibited
Name Server:
Name Server:
Name Server:
DNSSEC Unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>> Last update of whois database: 2021-08-17T06:48:59Z <<

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

NOTICE: The expiration date displayed in this record is the date the
responsible registrar reported the domain to be registered. This date is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. The registrant is responsible for maintaining the contact information
in the WHOIS database to view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
```

Target validation

```

root@kali:~/Downloads
root@kali:~/Downloads

Registrars:
Domain Name: tinder.com
Registry Domain ID: 1371521164#0000
Registrar: WHOIS Server: whois.markmonitor.com
Registrar URL: https://whois.markmonitor.com/
Updated Date: 2021-09-13T02:21:16+0000
Creation Date: 2019-01-15T00:00:00+0000
Registrar Registration Expiration Date: [REDACTED]
Registrar: MarkMonitor, Inc.
Reg. ID: 1371521164#0000
Registrar Abuse Contact Email: [REDACTED]@markmonitor.com
Registrar Abuse Contact Phone: +1(800)555-1234
Domain Status: clientUpdateProhibited ([https://www.icann.org/epp#clientUpdateProhibited])
Domain Status: clientTransferProhibited ([https://www.icann.org/epp#clientTransferProhibited])
Domain Status: clientDeleteProhibited ([https://www.icann.org/epp#clientDeleteProhibited])
Registrar: Match Group, LLC
Registrar State/Province: TX
Registrant Country: US
Registrant: [REDACTED]
Registrant Email: [REDACTED]@markmonitor.com
Admin Organization: Match Group, LLC
Admin State/Province: TX
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/tinder.com
Tech Organization: Match Group, LLC
Tech State/Province: TX
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/tinder.com
Name Server: [REDACTED]
Name Server: [REDACTED]
Name Server: [REDACTED]
Name Server: [REDACTED]
DNSSEC: unsigned
URL: http://www.iana.org/WHOIS Data Problem Reporting System: http://wopr3.internic.net/
>>> Last update of WHOIS database: 2021-10-13T152116+0000 <<
For more information on WHOIS status codes, please visit:

```

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”



```
(root㉿kali:)[~/Sublist3r]
└─# python3 sublist3r.py -v -d tinder.com > ~/Desktop/result.txt

# Coded By Ahmed Aboul-Ela - Baboulla

[+] Enumerating subdomains now for tinder.com
[+] Verbosity is enabled, will show the subdomains results in real time
[+] Searching now in Baidu...
[+] Searching now in Yahoo...
[+] Searching now in Google...
[+] Searching now in Bing...
[+] Searching now in Yandex...
[+] Searching now in Netcraft...
[+] Searching now in DNSdumpster...
[+] Searching now in VirusShare...
[+] Searching now in Threatcrowd...
[+] Searching now in SSL Certificates...
[+] Searching now in PassiveDNS...
PassiveDNS: 01_email.welcome.tinder.com
PassiveDNS: 02_email.welcome.tinder.com
PassiveDNS: 03_email.welcome.tinder.com
PassiveDNS: 040_email.mail.tinder.com
```

Sublist3r



```
ssl_certificates: link_updates.tinder.com
[+] Saving results to file: /root/Desktop/result.txt
[+] Total Unique Subdomains Found: 60
tinder.com
www.tinder.com
abmail.tinder.com
287003.tinder.com
040_email.alerts.tinder.com
09_email.alerts.tinder.com
links.alerts.tinder.com
03_email.alerts.tinder.com
030_email.tinder.com
039_email.tinder.com
040_email.tinder.com
041_email.tinder.com
042_email.tinder.com
043_email.tinder.com
044_email.tinder.com
045_email.tinder.com
046_email.tinder.com
047_email.tinder.com
go.tinder.com
help.tinder.com
www.help.tinder.com
link.tinder.com
links.tinder.com
like.tinder.com
032_email.tinder.com
0186_email.mail.tinder.com
0187_email.mail.tinder.com
0188_email.mail.tinder.com
```

Sublist3r



```
ok_email.notifications.tinder.com
05_email.notifications.tinder.com
links.notifications.tinder.com
open.tinder.com
polis.notifications.tinder.com
polis.tinder.com
staging.tinder.com
swipeleft.tinder.com
swipenight.tinder.com
www.swipenight.tinder.com
tech.tinder.com
tech.notifications.tinder.com
0190_email.updates.tinder.com
0191_email.updates.tinder.com
0192_email.updates.tinder.com
0193_email.updates.tinder.com
0194_email.updates.tinder.com
link.updates.tinder.com
mail.updates.tinder.com
2076032.welcome.tinder.com
01_email.welcome.tinder.com
02_email.welcome.tinder.com
03_email.welcome.tinder.com
links.welcome.tinder.com
```

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

```

root@kali:~#
# sudo apt-get install python3-pip python-dev libssl-dev libffi-dev
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Note, selecting 'python-dev-is-python2' instead of 'python-dev'
libffi-dev is already the newest version (3.3-6).
libffi-dev set to manually installed.
python3-pip is already the newest version (20.3.4-4).
The following packages were automatically installed and are no longer required:
  galera-3 gir1.2-appindicator3-0.1 libappindicator3-1 libboost-thread1.71.0 libcapstone3
  libconfig-inifiles-perl libcryptopp-6 libldap25 libdd-mariadb-perl libdbi-perl libdataserver-1.2-24 libgdal27
  libgeo-3.8.1 libhtml-template-perl libindicator3-7 libjs-sizzle liblvm10 libmicrohttpd12 libperl5.30
  libphonenumber7 libplymouth4 libpython3.8 libpython3.8-dev libpython3.8-minimal libpythont3.8-stdlib
  libqt5opengl5 libtesseract4.0.1 libxml2 libxslt1.1 libyaml0 node-jquery python3-atomicwrites python3-greenlet
  python3-zope.event python3.8-dev python3.8-minimal qt5-gtk2-platformtheme rsync
  ruby-connection-pool ruby-molinillo ruby-net-https-persistent ruby-thor xfce4-mailwatch-plugin
  xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libpython2-dev libpython2.7-stdlib libpython2.7 libpython2.7-dev libpython2.7-minimal libpython2.7-stdlib
  libssl1.1.1 python-is-python2 python2 python2-dev python2-minimal python2.7 python2.7-dev python2.7-minimal
Suggested packages:
  libssl-dev python2-doc python-tk python2.7-doc
The Following NEW packages will be installed:
  libpython2-dev libpython2.7 libpython2.7-dev libssl-dev python-dev-is-python2 python2-dev python2.7-dev
The following packages will be upgraded:
  libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib libssl1.1 python-is-python2 python2
  python2-minimal python2.7 python2.7-minimal
9 upgraded, 7 newly installed, 0 to remove and 1090 not upgraded.
Need to get 11.0 MB of archives.
After this operation, 25.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get: http://kali.cc.kali.org/kali kali-rolling/main amd64 python2.7-upgrade 2.7.18-2 [11.0 kB]

```

Anubis Subdomain Enumerator

and use this command to scan our target.

anubis -t tinder.com

```
https://github.com/jonluca/anubis
└─[root@kali: ~]─[anubis -t tinder.com
d8888          888      d8b
d88888         888      Y8B
d88P888        888
d88P 888 888888b. 888 888 888888b. 888 .d8888b
d88P 888 888 "88b 888 888 888 "88b 888 88K
d88P 888 888 888 888 888 888 888 888 "Y8888b.
d8888888888 888 888 Y88b 888 888 d88P 888   X88
d88P 888 888 888 "Y88888 888888P" 888 88888P

Searching for subdomains for 13.227.254.88 (tinder.com)
Working on target: tinder.com
Testing for zone transfers
Searching HackerTarget
Searching for Subject Alt Names
Searching NetCraft.com
Searching crt.sh
Searching DNSdumpster
Searching Anubis-DB
Found 58 subdomains
o30.abmail.tinder.com
o5.email.notifications.tinder.com
o28.abmail.tinder.com
o38.em.tinder.com
o194.em.updates.tinder.com
swipeLife.tinder.com
open.tinder.com
swipeNight.tinder.com
```

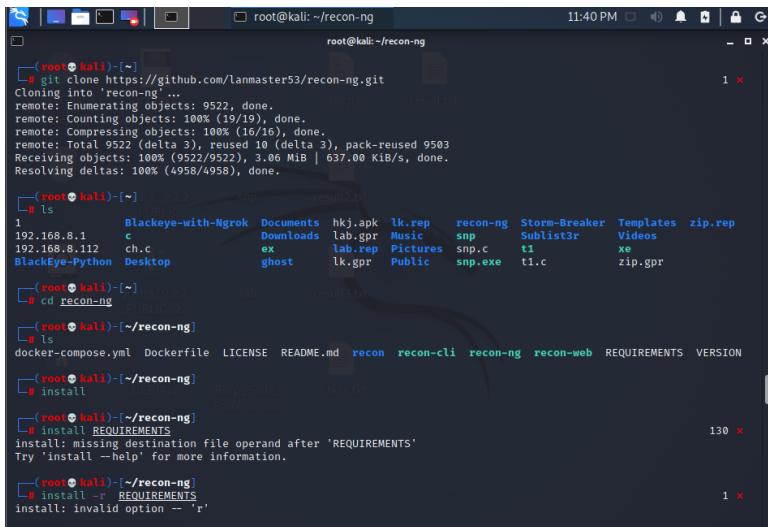
Anubis Subdomain Enumerator

```
root@kali: ~
o46.em.tinder.com
o189.em.mail.tinder.com
o32.abmail.tinder.com
o187.em.mail.tinder.com
policies.tinder.com
o43.em.tinder.com
o190.em.updates.tinder.com
o192.em.updates.tinder.com
o39.em.tinder.com
www.swipeNight.tinder.com
o45.em.tinder.com
testrail.tinder.com
link.updates.tinder.com
web.tinder.com
*.swipeLife.tinder.com
o6.email.newsletter.tinder.com
elite.tinder.com
o40.em.tinder.com
o21.abmail.tinder.com
help.tinder.com
o33.abmail.tinder.com
golls.tinder.com
www.tinder.com
o42.em.tinder.com
o35.abmail.tinder.com
o4_email.notifications.tinder.com
elite.tinder.com
emoji.tinder.com
o34.abmail.tinder.com
o36.abmail.tinder.com
o41.em.tinder.com
www.help.tinder.com
o3_email.welcome.tinder.com
o2_email.welcome.tinder.com
```

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”



The screenshot shows a terminal window titled "root@kali: ~/recon-ng". The session starts with cloning the Recon-NG repository from GitHub. It then lists the contents of the directory, which includes several sub-directories and files. The user runs "docker-compose up" to start the Docker containers. Finally, they attempt to install requirements using "pip install -r REQUIREMENTS", but receive an error message indicating that the command is invalid.

```
root@kali:~/recon-ng
root@kali:~/recon-ng
# git clone https://github.com/LanMaster53/recon-ng.git
Cloning into 'recon-ng' ...
remote: Counting objects: 9592, done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 9522 (delta 3), reused 10 (delta 3), pack-reused 9503
Receiving objects: 100% (9522/9522), 3.06 MiB | 637.00 KiB/s, done.
Resolving deltas: 100% (4958/4958), done.

root@kali:~/
# ls
1         Blackeye-with-Ngrok  Documents  hkj.apk  lk.rep  recon-ng  Storm-Breaker  Templates  zip.rep
192.168.8.1   c               Downloads  lab.gpr  Music    sns       Sublist3r  Videos
192.168.8.112 ch.c           ex        lab.rep  Pictures  sns.c     t1          xe
BlackEye-Python Desktop      ghost     lk.gor   Public    sns.exe   t1.c      zip.gpr

root@kali:~/
# cd recon-ng
root@kali:~/recon-ng
# ls
docker-compose.yml  Dockerfile  LICENSE  README.md  recon  recon-cli  recon-nginx  recon-web  REQUIREMENTS  VERSION

root@kali:~/recon-ng
# install
root@kali:~/recon-ng
# install REQUIREMENTS
root@kali:~/recon-ng
# install -r REQUIREMENTS
install: missing destination file operand after 'REQUIREMENTS'
Try 'install --help' for more information.

root@kali:~/recon-ng
# install -r REQUIREMENTS
root@kali:~/recon-ng
```

Recon –ng Tools

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

```

root@kali:~/recon-ng
11:40 PM
root@kali:~/recon-ng
└─# pip install -r REQUIREMENTS
Requirement already satisfied: pyyaml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 2)) (5.3.1)
Requirement already satisfied: dnspython in /usr/local/lib/python3.9/dist-packages (from -r REQUIREMENTS (line 3)) (2.1.0)
Requirement already satisfied: lxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 4)) (4.6.3)
Requirement already satisfied: mechanize in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 5)) (0.4.5)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 6)) (2.25.1)
Requirement already satisfied: flask in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 8)) (1.1.2)
Requirement already satisfied: flask-restful in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 9)) (0.3.8)
Requirement already satisfied: flasgger in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 10)) (0.9.5)
Requirement already satisfied: dicttoxml in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 11)) (1.7.4)
Requirement already satisfied: XlsxWriter in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 12)) (1.1.2)
Requirement already satisfied: unicodedcsv in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 13)) (0.1.4.1)
Requirement already satisfied: rq in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 14)) (1.7.0)

└─# ls
docker-compose.yml Dockerfile LICENSE README.md recon recon-cli recon-ng recon-web REQUIREMENTS VERSION

└─# python3 recon-ng

```

Recon –ng Tools

```

root@kali:~/recon-ng
11:40 PM
root@kali:~/recon-ng
Requirement already satisfied: unicodedcsv in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 13)) (0.1.4.1)
Requirement already satisfied: rq in /usr/lib/python3/dist-packages (from -r REQUIREMENTS (line 14)) (1.7.0)

└─# ls
docker-compose.yml Dockerfile LICENSE README.md recon recon-cli recon-ng recon-web REQUIREMENTS VERSION

└─# python3 recon-ng

```

The terminal shows the execution of the Recon-NG tool, which then opens a web browser displaying a landing page for the Black Hills InfoSec PractiseCom challenge. The page includes a logo for Black Hills InfoSec, a banner for the challenge, and navigation links for Home, DENIED, and RECON.

Recon –ng Tools

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

```
root@kali:~/recon-ng
db           Interfaces with the workspace's database
exit         Exits the framework
help         Displays this menu
index        Creates a module index (dev only)
keys         Manages third party resource credentials
marketplace  Interfaces with the module marketplace
modules      Interfaces with installed modules
options      Manages the current context options
pdb          Starts a Python Debugger session (dev only)
script       Records and executes command scripts
shell        Executes shell commands
show         Shows various framework items
snapshots    Manages workspace snapshots
spool        Spools output to a file
workspaces   Manages workspaces

[recon-ng][default] > search google
[!] Invalid command: search google.
[recon-ng][default] > workplace
[!] Invalid command: workplace.
[recon-ng][default] > workspace
[!] Invalid command: workspace.
[recon-ng][default] > workspaces
Manages workspaces
Usage: workspaces <create|list|load|remove> [ ... ]
[recon-ng][default] > workspaces search
Manages workspaces
Usage: workspaces <create|list|load|remove> [ ... ]
[recon-ng][default] > marketplace search
```

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 part 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][default][google_site_web] > info
  Name: Google Hostname Enumerator
  Author: Tim Tomes (@lannmaster53)
  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: tinder.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] >
```

Recon -ng Tools

- After use run command to run this process.

```
root@kali:~/recon-ng
root@kali:~/recon-ng
+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/domains-hosts/google_site_web | 1.0 | installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

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

+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/domains-hosts/google_site_web | 1.0 | installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

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

Recon -ng Tools

```

+-----+-----+-----+-----+-----+
| 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] > run

INDER.COM
[+] Searching Google for: site:tinder.com
Country: None
Host: policies.tinder.com
Ip_Address: None
Latitude: None
Longitude: None
Notes: None
Region: None
[+] Country: None
[+] Host: tech.tinder.com
[+] Ip_Address: None
[+] Latitude: None
[+] Longitude: None
[+] Notes: None
[+] Region: None

```

Recon -ng Tools

```

root@kali: ~/recon-ng
root@kali:~/recon-ng
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 501.
[*] Searching Google for: sitetinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 601.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 701.
[*] Searching Google for: sitetinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 801.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 901.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1001.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1101.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1201.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1301.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1401.
[*] Searching Google for: site:tinder.com -site:policies.tinder.com -site:tech.tinder.com -site:swipenight.ti
nder.com -site:www.help.tinder.com
[*] No New Subdomains Found on the Current Page. Jumping to Result 1501.

```

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**

httpprobe

- This tool design using go language.
 - First we need to clone this tool in github.
 - git clone <https://github.com/tomnomnom/httpprobe.git>

```
(root㉿kali)-[~/Desktop/httpprobe]
└─# git clone https://github.com/tomnomnom/httpprobe.git
```

httpprobe

after we need to get go language.

```
(root㉿kali)-[~/Desktop]
└─# apt -get install go
E: Command line option 'g' [from -get] is not understood in combination with the other options.

[root@kali ~]# apt install go
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package go

[root@kali ~]# apt-get install golang
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  galera-3 gir1.2-appindicator3-0.1 libappindicator3-1 libboost-thread1.71.0 libcapstone3
  libconfig-inifiles-perl libcrypto++6 libddap25 libdbd-mariadb-perl libdbi-perl libedataserver-1.2-24
  libgdal27 libgeos-3.8.1 libhtml-template-perl libindicator3-7 libjs-sizzle liblomm10 libmicrohttpd12
  libperl5.30 libphonenumber7 libplymouth4 libpython3.8-dev libpython3.8-minimal
  libpython3.8-stdlib libqt5opengl5 libradares2-4.3.1 libreadline5 libsane libtepl-4-0 libterm-readkey-perl
  libwireshark13 libwiretap10 libwsutil11 libxml2-node-jquery python3-atomiconwrites python3-gevent
  python3-greenlet python3-zope.event python3.8 python3.8-dev python3.8-minimal qt5-gtk2-platformtheme
  rsync ruby-connection-pool ruby-net-httppersistent ruby-thor xfce4-mailwatch-plugin
  xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  golang-1.15 golang-1.15-doc golang-1.15-go golang-1.15-src golang-doc golang-src
Suggested packages:
  bzr | brz mercurial
The following NEW packages will be installed:
  golang golang-1.15 golang-1.15-doc golang-1.15-go golang-1.15-src golang-doc golang-go golang-src
```

Go

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

```

└─(root㉿kali)-[~/Desktop/httpprobe] └── build.sh
  └─# go build main.go

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

└─(root㉿kali)-[~/Desktop/httpprobe]
  └─# ./main
  └─# curl -v https://www.google.com
  └─# ^C

└─(root㉿kali)-[~/Desktop/httpprobe]
  └─# ./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
  -prefer-https
  -s           add additional probe (proto:port)
  -s prefer-https
  -s skip the default probes (http:80 and https:443)
  -t int      timeout (milliseconds) (default 10000)

└─(root㉿kali)-[~/Desktop/httpprobe]
  └─# echo path
path

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

```

Go

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

```

  timeout (milliseconds) (default 10000)
└─(root㉿kali)-[~/Desktop/httpprobe] └── httpprobe
  └─# echo path
path

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

└─(root㉿kali)-[~/Desktop/httpprobe] └── httpprobe
  └─# mv main /bin
  └─# ls
Dockerfile LICENSE main.go README.md script

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

```

Go

```

└─(root㉿kali)-[~] └── root@kali:/usr/bin
  └─# mv main httpprobe

```

Go

then run httpprobe tool.

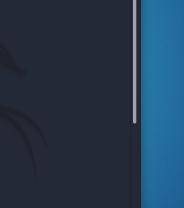


```
root@kali:~/Desktop# httpprobe --h
Usage of httpprobe:
  -c int          set the concurrency level (split equally between HTTPS and HTTP requests) (default 20)
  -method string  HTTP method to use (default "GET")
  -p value        add additional probe (proto:port)
  -prefer-https   only try plain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

root@kali:~/Desktop#
```

httpprobe

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



```
VBox: root@kali:~/Desktop# httpprobe
root@kali:~/Desktop# ghidra_9.1.2_PUBLIC_202001229.zip opt smp result2.txt whois.txt
root@kali:~/Desktop# cat result2.txt
t3s.gotinder.com
t3s.m.tinder.com
abmail.tinder.com
2976832.alerts.tinder.com
307.alerts.tinder.com
307.em.alerts.tinder.com
308.em.tinder.com
309.em.tinder.com
os1.em.tinder.com
os1.m.tinder.com
os3.em.tinder.com
os4.em.tinder.com
os5.em.tinder.com
os6.em.tinder.com
os601.tinder.com
os602.tinder.com
help.tinder.com
www.help.tinder.com
link.tinder.com
link.tinder.com
0185.en.mail.tinder.com
0186.en.mail.tinder.com
0188.en.mail.tinder.com
0189.en.mail.tinder.com
Profe.link.mail.tinder.com
```

httpprobe

These are the alive subdomain in www.tinder.com

```
[root@sat1 ~]# ./Desktop
└─* cat result.txt | httpprobe
https://www.tinder.com
https://tech.gotinder.com
https://tech.gotinder.com
http://www.tinder.com
https://2076032.alerts.tinder.com
https://abmail.tinder.com
http://2076032.alerts.tinder.com
https://abmail.tinder.com
https://www.help.tinder.com
https://emoji.tinder.com
https://invite.tinder.com
http://www.help.tinder.com
https://invite.tinder.com
https://link.tinder.com
http://go.tinder.com
https://lite.tinder.com
https://link.mail.tinder.com
http://link.mail.tinder.com
http://lite.tinder.com
http://link.tinder.com
https://2116324.newsletter.tinder.com
https://2076032.newsletter.tinder.com
https://2076032.notifications.tinder.com
https://swipelife.tinder.com
http://2116324.newsletter.tinder.com
http://2076032.newsletter.tinder.com
http://swipelife.tinder.com
http://2076032.notifications.tinder.com
https://open.tinder.com
https://policies.tinder.com
```

Alive Subdomains

```
https://link.tinder.com
http://go.tinder.com
https://lite.tinder.com
https://link.mail.tinder.com
http://link.mail.tinder.com
http://lite.tinder.com
http://link.tinder.com
https://2116324.newsletter.tinder.com
https://2076032.newsletter.tinder.com
https://2076032.notifications.tinder.com
https://swipelife.tinder.com
http://2116324.newsletter.tinder.com
http://swipelife.tinder.com
http://2076032.notifications.tinder.com
https://open.tinder.com
https://policies.tinder.com
https://polls.tinder.com
http://policies.tinder.com
https://tech.tinder.com
http://open.tinder.com
https://www.swipenight.tinder.com
http://tech.tinder.com
https://staging.tinder.com
https://swipenight.tinder.com
http://staging.tinder.com
https://swipenight.tinder.com
http://swipenight.tinder.com
https://link.updates.tinder.com
http://link.updates.tinder.com
https://2076032.welcome.tinder.com
https://2076032.welcome.tinder.com
```

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 a 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. OpenSCAP
7. OWASP ZAP
8. Burp suite
9. W3af
10. Metasploit framework

Netsparker

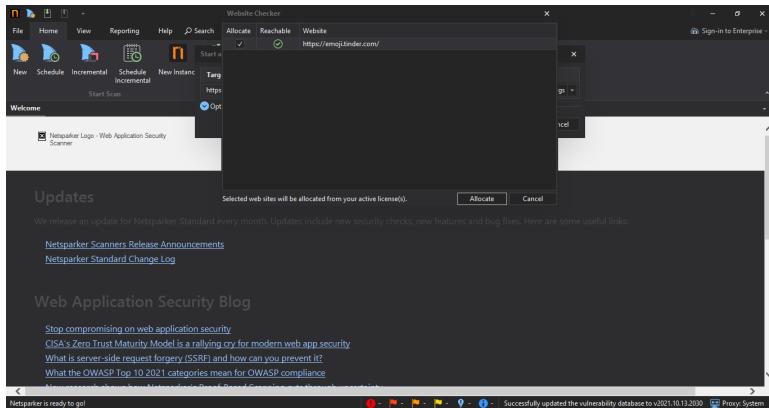
- Netsparker is fully automated web application vulnerability scanner. Netsparker can scan any kind of web application, independent of platform or programming language. It allows you to scan and detect security vulnerabilities in websites, web applications, and web services.

How to work,

- Open Netsparker.
- Then go the home tab and click New.

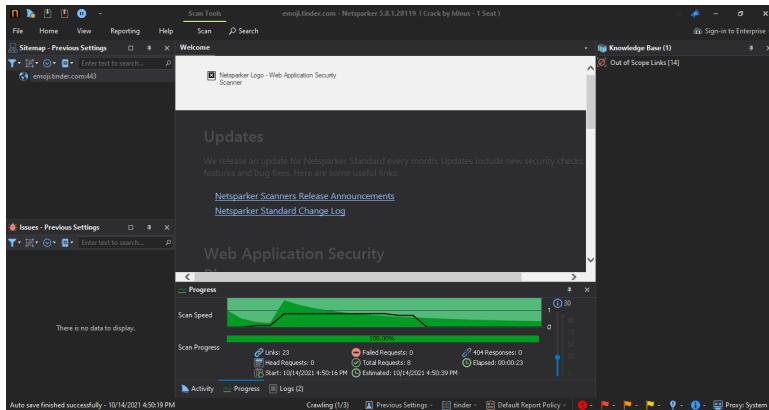
- Paste your target domain url.
- Then we can start our scan.

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

HTTP Strict Transport Security (HSTS) Errors and Warnings

MEDIUM

Certainty : [REDACTED]

URL : <https://emoji.tinder.com/>

CLASSIFICATION	
OWASP 2013	A5
OWASP 2017	A6
CWE	16
WASC	15
ISO27001	A.14.1.2

Error	Resolution
max-age directive does not exist.	max-age is a required directive.
preload directive not present	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

result

Resolution	
not exist.	max-age is a required directive.
resent	Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list.

ing parsing of Strict-Transport-Security header.

ay allow attackers to bypass HSTS, effectively allowing them to read and modify your communication

nd warnings, you should consider adding your domain to the the HSTS preload list. This will ensure
nnect your website by using HTTPS, actively preventing users from visiting your site using HTTP.
ers' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the
FU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website
ured to enter the browser's preload list.

result

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.

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)

result**External References**

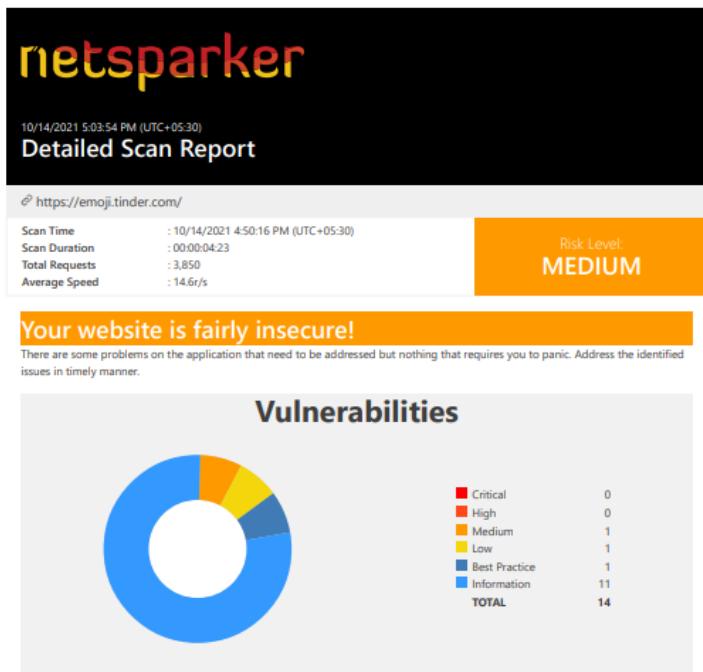
[HTTP Strict Transport Security \(HSTS\) HTTP Header](#)

[Wikipedia - HTTP Strict Transport Security Implementation](#)

[Check HSTS Preload status and eligibility](#)

result

This is summery of scan report.



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

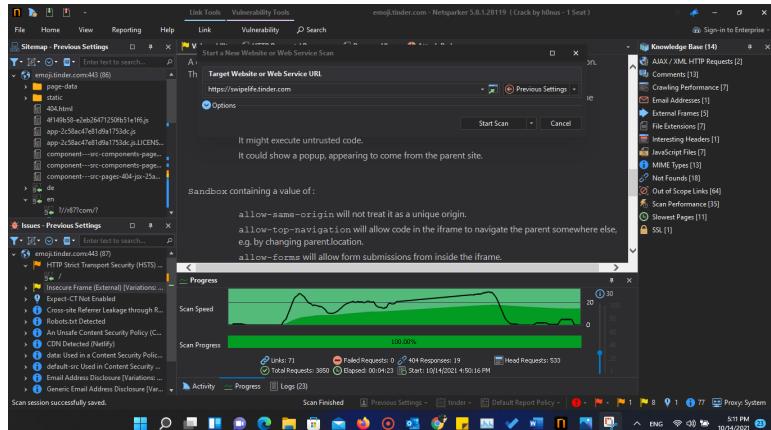
Compliance	Vulnerabilities
OWASP 2013	2
OWASP 2017	3
ISO27001	14

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.

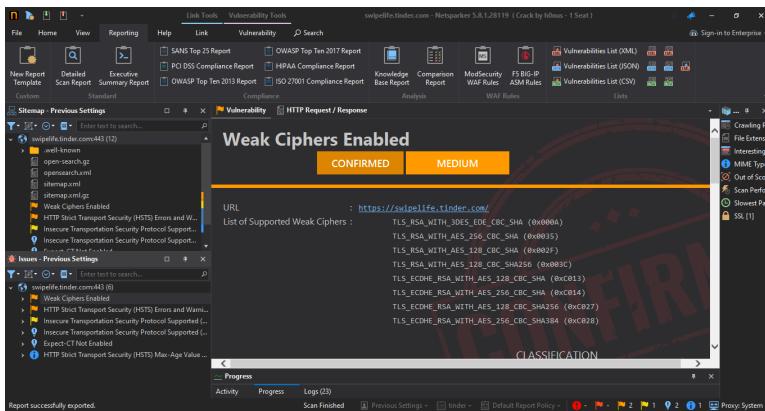
This report created with 5.8.1.28119-master-bca4e4e
<https://www.netsparker.com>

report

Subdomain -<https://swipelife.tinder.com>



Scanning



Scanning

Vulnerability Details

Nessparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

Attackers might decrypt SSL traffic between your server and your visitors.

Actions to Take

For Apache, you should modify the SSLCipherSuite directive in

CLASSIFICATION	
PCI DSS 3.2	<u>6.5.4</u>
OWASP 2013	<u>A6</u>
OWASP 2017	<u>A3</u>
CWE	<u>327</u>
CAPEC	<u>217</u>
WASC	<u>4</u>
ISO27001	<u>A14.1.3</u>

CVSS 3.0 SCORE	
Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

Result

SSLCipherSuite HIGH: MEDIUM: !MD5: !RC4

Lighttpd:

```
ssl.honor-cipher-order = "enable"
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

For Microsoft IIS, you should make some changes to the system registry. **Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.**

a. Click Start, click Run, type `regedit32` or type `regedit`, and then click OK.
b. In Registry Editor, locate the following registry key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\control\SecurityProviders\SCHANNEL\Hashes\MD5`

CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS 3.1 SCORE

Base	6.8 (Medium)
Temporal	6.8 (Medium)
Environmental	6.8 (Medium)

CVSS Vector String

CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Result

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

Remedy

Configure your web server to disallow using weak ciphers.

External References

[OWASP - Insecure Configuration Management](#)
[OWASP Top 10-2017 A3-Sensitive Data Exposure](#)

Result

The screenshot shows a detailed scan report from netsparker. At the top, it displays the URL <https://swipelife.tinder.com/>, the scan time (10/14/2021 5:13:47 PM (UTC+05:30)), and the duration (00:00:05). The total requests were 693, and the average speed was 12.5r/s. The risk level is categorized as MEDIUM. A prominent orange banner at the bottom states "Your website is fairly insecure!" followed by a note: "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." Below this, a section titled "Vulnerabilities" features a donut chart illustrating the distribution of findings across six categories: Critical (0), High (0), Medium (2), Low (1), Best Practice (2), and Information (1). The total number of vulnerabilities is 6.

Vulnerability Type	Count
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.



Report

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

The screenshot shows the NetSparker interface with a scan session for <https://policies.tinder.com>. The main pane displays a list of findings, including:

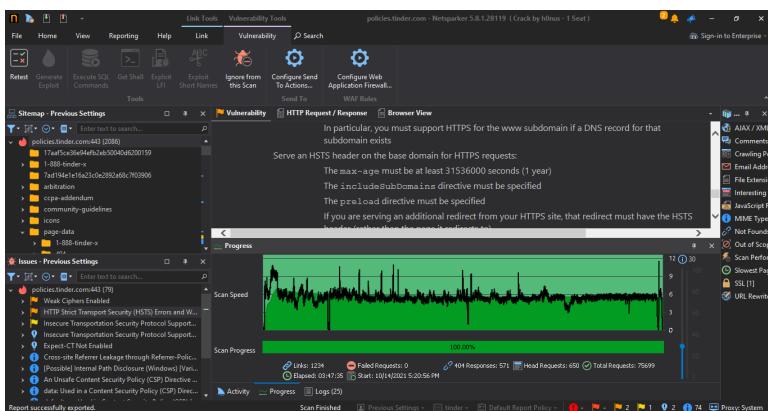
- Weak Ciphers Enabled
- HTTP Strict Transport Security (HSTS) Errors and Warnings
- Insecure Transportation Security Protocol Supported
- Insecure Transportation Security Protocol Supported
- Expect CT Not Enabled
- HTTP Strict Transport Security (HSTS) Max-Age Value

The sidebar on the right contains links to external resources:

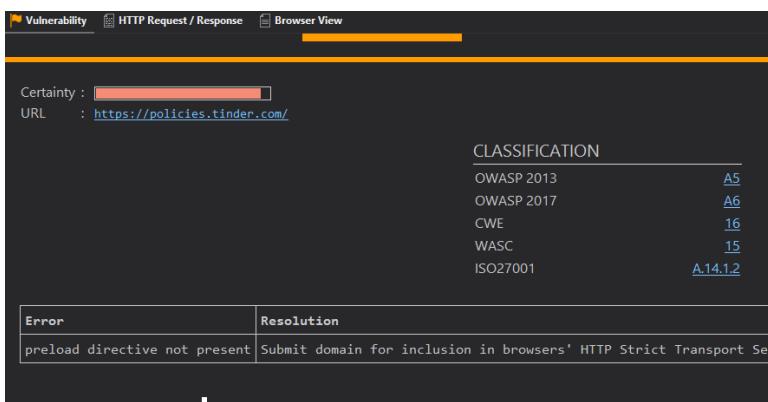
- OWASP - Insecure Configuration Management
- OWASP Top 10-2017 A3-Sensitive Data Exposure

The bottom status bar shows the scan finished at 5:20 PM on 10/14/2021.

Scanning



Scanning



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 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.

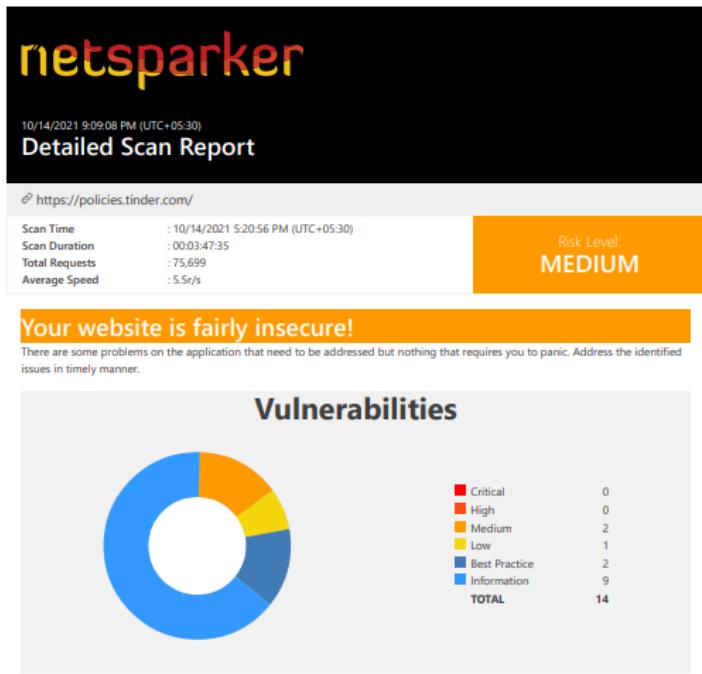
Result

Vulnerability HTTP Request / Response Browser View

Since commanding the need for Trust On First Use (TOFU), there is associated risk and disadvantage. Unless you fix the 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)



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>

Out-of-date Version (Nginx)

CRITICAL

Certainty : 

URL : <https://staging.tinder.com>

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 database content.

Vulnerability Details



CLASSIFICATION	
PCI DSS 3.2	6.2
OWASP 2013	A9
OWASP 2017	A9
CWE	829

Scanning

Impact

CWE 829
CAPEC 310
WASC 13
HIPAA 164.308(A)(1)(I)
ISO27001 A.14.1.2

Remedy

Remedy References

[Downloading Nginx](#)

Known Vulnerabilities in this Version

Scanning

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](#)

Scanning

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.



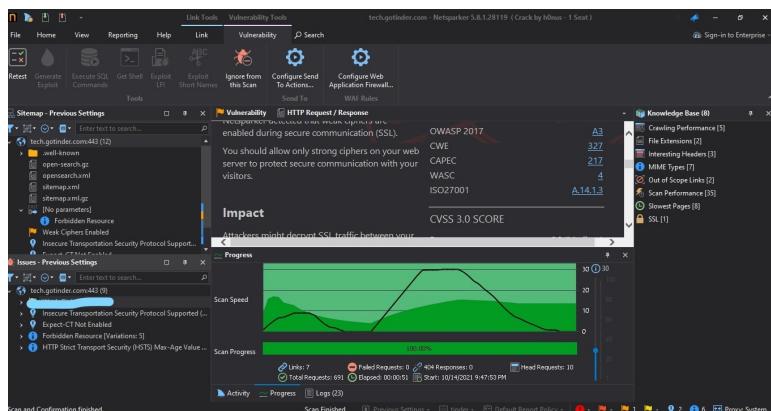
Compliance Summary

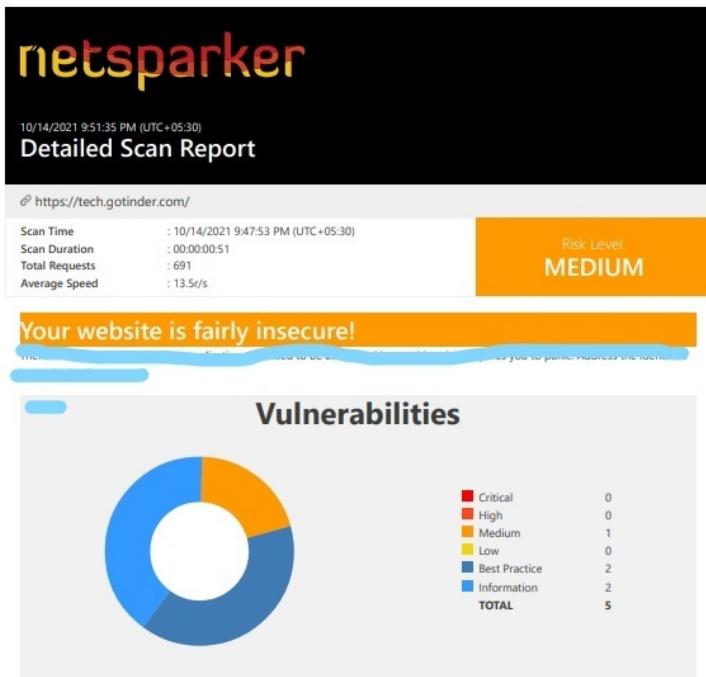
Compliance	Vulnerabilities
PCI DSS v3.2	4
OWASP 2013	9
OWASP 2017	9
HIPAA	5
ISO27001	22

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.



Subdomain-<https://tech.gotinder.com>

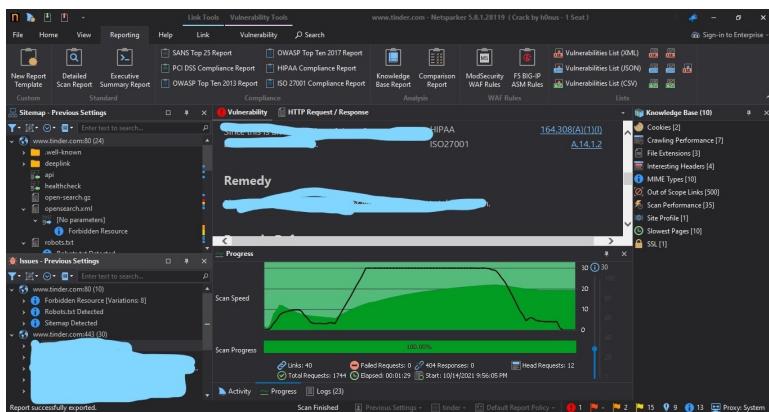




Vulnerability	Suggested Action
⌚ Expect-CT Not Enabled	No action required: Implementing these features that are supported by all major browsers is a good practice and will provide an extra layer of security to your application.
⌚ Insecure Transportation Security Protocol Supported (TLS 1.1)	No action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



Out-of-date Version (Nginx)

CRITICAL

Certainty	:	<div style="width: 100px; height: 10px; background-color: #f08080;"></div>
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
[REDACTED]

Remedy
[REDACTED]

Remedy References

[Downloading Nginx](#)

Known Vulnerabilities in this Version

[Downloading Nginx](#)

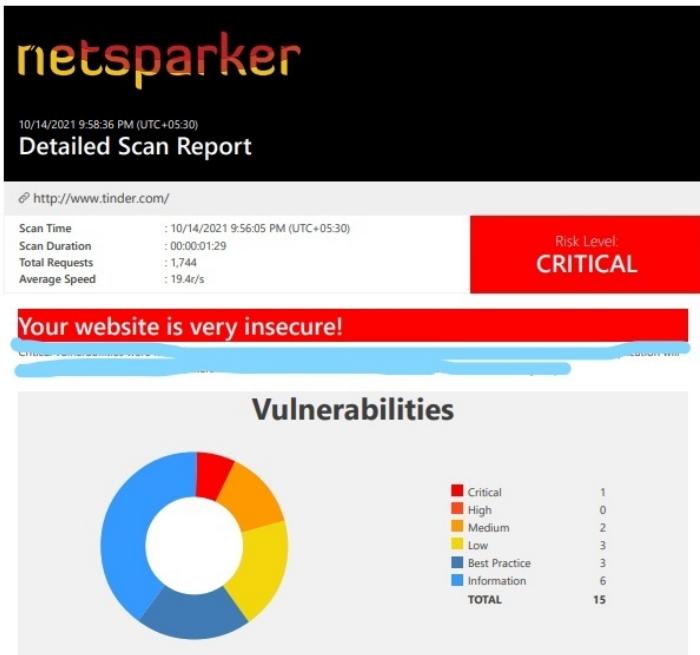
Known Vulnerabilities in this Version

Nginx Off-by-one Error Vulnerability
[REDACTED]
process crash [REDACTED]

Affected Versions
1.7.4 to 1.20.0

External References

[CVE-2021-23017](#)



Vulnerability	Suggested Action
HTTP Response Headers - Content-Security-Policy	HTTP Response Headers - Content-Security-Policy
HTTP Response Headers - X-Content-Type-Options	HTTP Response Headers - X-Content-Type-Options
HTTP Response Headers - X-XSS-Protection	HTTP Response Headers - X-XSS-Protection
Cookie Value Marked as Secure but not HttpOnly	Cookie Value Marked as Secure but not HttpOnly
Version Disclosure	Version Disclosure
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>

```
root@kali:~
```

```
+ Executing "systemctl start nessusd; systemctl --no-pager status nessusd"
[~] The Nessus Vulnerability Scanner
# nikto -h https://emoji.tinder.com | less; nessusd.service; disabled; vendor
- Nikto v2.1.6
[+] Target IP: [REDACTED]
[+] Target Hostname: emoji.tinder.com
[+] Target Port: 443

+ SSL Info: Subject: [REDACTED]
  Ciphers: [REDACTED]
  Issuer: /C=US/ST=California/L=San_Bruno/CN=nikto.vulnerability.Scanner
+ Message: Multiple IP addresses found: [REDACTED]
+ Start Time: 2021-10-15 00:48:09 (GMT5.5)

+ Server: Netlify
+ Uncommon header [REDACTED] found, with contents: [REDACTED]
4S5HMGXPP
+ Uncommon header 'link' found, with contents: </webpack-runtime-777454fce
287dc9cbe7.js>; rel=preload; as=script, </framework-3f08ddc3b6ad80f84e0b.js
>; rel=preload; as=script, </app-2c58ac47e81d9a1753dc.js>; rel=preload; as=
script, </4f149b58-e2eb26471250fb5le1f6.js>; rel=preload; as=script, </comp
onent--src-components-page-jsx-70228383546d1b384e78.js>; rel=preload; as=s
cript, </page-data/app-data.json>; rel=preload; as=fetch; crossorigin, </pa
ge-data/index/page-data.json>; rel=preload; as=fetch; crossorigin
[REDACTED]
```

```
root@kali:~
```

```
+ Server: Netlify
[REDACTED] with contents: [REDACTED]
[REDACTED]
+ Uncommon header 'time' found, with contents: [REDACTED]
</framework-3f08ddc3b6ad80f84e0b.js>; rel=preload; as=script, </app-2c58ac47e81d9a1753dc.js>; rel=preload; as=
script, </4f149b58-e2eb26471250fb5le1f6.js>; rel=preload; as=script, </comp
onent--src-components-page-jsx-70228383546d1b384e78.js>; rel=preload; as=s
cript, </page-data/app-data.json>; rel=preload; as=fetch; crossorigin, </pa
ge-data/index/page-data.json>; rel=preload; as=fetch; crossorigin
+ The site [REDACTED] is down
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'request_id' found, with contents: [REDACTED]
[REDACTED]
+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host
+ End Time: 2021-10-15 00:53:50 (GMT5.5) (341 seconds)
```

Subdomain- <https://swipelife.tinder.com>

```
root@kali:~# nikto -h https://swipelife.tinder.com stemcti --no-pager status nessusd
- Nikto v2.1.6
  The Nessus Vulnerability Scanner

+ Target IP: [REDACTED] FRI 2021-10-15 00:45:19 +0530; 12ms ago
+ Target Hostname: swipelife.tinder.com
+ Target Port: [REDACTED]

+ SSL Info: 443S Subject: [REDACTED]
  CGroup: /system/Certificates
  Ciphers: [REDACTED]
  Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message: Multiple IP addresses found: [REDACTED]
+ Start Time: 2021-10-15 01:06:38 (GMT5.5)

+ Server: CloudFront
+ Retrieved via header: 1.1 5ebdc48fce5361063bcf3a9ae19fdcec.cloudfront.net
(CloudFront)
+ [REDACTED] This header can hint to the user agent to protect against some forms of [REDACTED].
+ Uncommon header x-amz-crc32 found, with contents: SIN52-C2
+ Uncommon header [REDACTED] with contents: z8-xipwGNlZzukni-srA
h55-LY2Bnq-I13VdH8xvJZPrfxh5_gYQ==
+ Uncommon header [REDACTED] found, with contents: Hit from cloudfront
+ The site uses SSL and the S [REDACTED]
```

```
root@kali:~/Desktop$ httpprobe
[REDACTED] http://tinder.com
[REDACTED] http://www.tinder.com
[REDACTED] http://2076832.alerts.tinder.com
[REDACTED] http://01.email.alerts.tinder.com
[REDACTED] http://links.alerts.tinder.com
[REDACTED] http://038.em.tinder.com
[REDACTED] http://039.em.tinder.com
[REDACTED] http://040.em.tinder.com
[REDACTED] http://041.em.tinder.com
[REDACTED] http://042.em.tinder.com
[REDACTED] http://043.em.tinder.com
[REDACTED] http://044.em.tinder.com
[REDACTED] http://emoj1.tinder.com
[REDACTED] http://go.tinder.com
[REDACTED] http://www.help.tinder.com
[REDACTED] http://invite.tinder.com
[REDACTED] http://www.invite.tinder.com
[REDACTED] http://lite.tinder.com
[REDACTED] http://0186.en.mail.tinder.com
[REDACTED] http://0187.en.mail.tinder.com
[REDACTED] http://0188.en.mail.tinder.com
[REDACTED] http://link.mail.tinder.com
```

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

```
[root@kali:~] + start_nessus systemctl --no-pager status nessusd
[+] nikto -h https://policies.tinder.com/ -t
- Nikto v2.1.6 loaded (/usr/share/nikto/nikto)
+ Target IP: [REDACTED]
+ Target Hostname: policies.tinder.com
+ Target Port: [REDACTED]

+ SSL Info: Subject: /CN=policies.tinder.com
  Ciphers: T... Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message: Multiple IP addresses found: [REDACTED]
+, SERVERSELECT, SERVERSELECT
+ Start Time: 2021-10-15 01:15:56 (GMT5.5)

+ Server: AmazonS3
+ Retrieved via header: 1.1 542ed801abac650214b285cec99334e4.cloudfront.net
(CloudFront)
+ Uncommon header [REDACTED] found, with contents: [REDACTED]
+ Uncommon header [REDACTED] found, with contents: Miss from [REDACTED]
+ Uncommon header [REDACTED] found, with contents: 21...
[REDACTED]
+ The site [REDACTED] uses SSL and Expect-CT header is not present.
+ Uncommon header [REDACTED] found, with contents: 0
+ Server banner has changed from [REDACTED] to 'CloudFront' which may sugge
[REDACTED]
```

```
[root@kali:~] + Start Time: 2021-10-15 01:15:56 (GMT5.5)
- Nikto v2.1.6 loaded (/usr/share/nikto/nikto)
+ Target IP: [REDACTED]
+ Target Hostname: [REDACTED]
+ Target Port: [REDACTED]

+ SSL Info: Subject: /CN=policies.tinder.com
  Ciphers: T... Issuer: /C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
+ Message: Multiple IP addresses found: [REDACTED]
+, SERVERSELECT, SERVERSELECT
+ Start Time: 2021-10-15 01:15:56 (GMT5.5)

+ Server: AmazonS3 (running) since Fri 2021-10-15 00:45:19 +0530; 12ms ago
+ Retrieved via header: [REDACTED] (CloudFront)
+ Uncommon header [REDACTED] found, with contents: [REDACTED]
+ Uncommon header [REDACTED] found, with contents: Miss from [REDACTED]
+ Uncommon header [REDACTED] found, with contents: [REDACTED]
[REDACTED]
+ The site uses SSL and Expect-CT header is not present.
+ Uncommon header [REDACTED] found, with contents: 0
+ Server banner has changed from [REDACTED] to 'CloudFront' which may sugge
st a WAF, load balancer or proxy is in place
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ ERROR: Error limit (20) reached for host, giving up. Last error: opening
stream: can't connect: SSL negotiation failed: error:1408F10B:SSL routines:
ssl3_get_record:wrong version number at /var/lib/nikto/plugins/LW2.pm line
5157.
at /var/lib/nikto/plugins/LW2.pm line 5157.
; at /var/lib/nikto/plugins/LW2.pm line 5157.
+ Scan terminated: 20 error(s) and 6 item(s) reported on remote host
+ End Time: 2021-10-15 01:32:01 (GMT5.5) (965 seconds)

+ 1 host(s) tested
```

Subdomain- <https://staging.tinder.com>

```

└─# nikto -h https://staging.tinder.com
[+] Nikto v2.1.6 - The Nmap Vulnerability Scanner (http://nmap.org/nikto.html)
[+] Target IP: [REDACTED]
[+] Target Hostname: staging.tinder.com
[+] Target Port: 443
[+] SSL Info: Subject: /CN=staging.tinder.com
[+] Ciphers: TLS_AES_128_GCM_SHA256
[+] Issuer: /=US/O=Amazon/OU=Server CA 1B/CN=Amazon
[+] Message: Multiple IP addresses found: [REDACTED]
[+] Start Time: 2021-10-15 01:40:20 (GMT5.5)

[+] Server: nginx/1.18.0
[+] Cookie [REDACTED] created without the 'Secure' flag
[+] Cookie [REDACTED] created without the 'SameSite' flag
[+] Cookie AWSALBCORS created without the 'httponly' flag
[+] Retrieved via header: 1.1 [REDACTED] (CloudFront)
[+] Uncommon header 'Content-Type' found, with contents: [REDACTED]
[+] Uncommon header 'Content-Length' found, with contents: [REDACTED]
Drg_KAL1nDpXXb9rJyDR-qE25auwDhQ=
[+] Uncommon header 'Content-Encoding' found, with contents: [REDACTED]
[+] Uncommon header 'Content-Language' found, with contents: Miss from CloudFront
[+] Uncommon header 'Content-MD5' found, with contents: on
[+] The site uses 'Content-Security-Policy' is not present.
[+] No CGI Directories Found (use '-C all' to force check all possible dirs)
[+] Entry '/healthcheck/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
[+] "robots.txt" contains 3 entries which should be manually viewed.
[+] Retrieved [REDACTED] bytes in 0.00s

```

```

[+] Start Time: 2021-10-15 01:40:20 (GMT5.5) - no pager status nessed
[+] Server: nginx/1.18.0
[+] Cookie [REDACTED] created without the 'Secure' flag
[+] Cookie [REDACTED] created without the 'SameSite' flag
[+] Cookie [REDACTED] created without the 'httponly' flag
[+] Retrieved via header: 1.1 70884a14c657950f2e7357eb30093182.cloudfront.net (CloudFront)
[+] Uncommon header 'Content-Type' found, with contents: [REDACTED]
[+] Uncommon header 'Content-Length' found, with contents: [REDACTED]
Drg_KAL1nDpXXb9rJyDR-qE25auwDhQ=
[+] Uncommon header 'Content-Encoding' found, with contents: [REDACTED]
[+] Uncommon header 'Content-Language' found, with contents: Miss from CloudFront
[+] Uncommon header 'Content-MD5' found, with contents: on
[+] The site uses 'Content-Security-Policy' is not present.
[+] No CGI Directories found (use '-C all' to force check all possible dirs)
[+] Entry '/healthcheck/' in robots.txt returned a non-forbidden or redirect HTTP code (200)
[+] "robots.txt" contains 3 entries which should be manually viewed.
[+] Retrieved [REDACTED] bytes in 0.00s
[+] ERROR: Error limit (20) reached for host, giving up. Last error: open [REDACTED] ar/lib/nikto/plugins/LW2.pm line 5157.
[+] Scan terminated: 20 error(s) and 13 item(s) reported on remote host
[+] End Time: 2021-10-15 01:47:54 (GMT5.5) (454 seconds)

[+] 1 host(s) tested
[+] (root💀 kali㉿[~])

```

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's also helpful for controlling service upgrade timetables, according to several system and network managers. 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.

```

Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] [target specification]
Targets:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanne-nmap.org, microsec.com[24,192.168.0.1-10.0.0-255.1-254
      -iL file.txt: Read targets from list of hosts/networks
      -iR num hosts: Choose random targets
      -iN filelist: Read targets from list > Exclude Hosts/networks
      -ecludefile <excl-file>: Exclude list from file
      -eclude <excl-file>: Exclude list from file

      -sT: Ping Scan - Simply list targets to scan
      -sN: Ping Scan - Disable port scan
      -sP: Treat all hosts as online, skip host discovery
      -sA: All protocols - Perform full OS detection, discovery to given ports
      -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
      -PO[rotocol]: IP Protocol Ping
      -n: No DNS resolution - Always resolve [default: sometimes]
      -dNST-servers <serv1[,serv2,...>: Specify custom DNS servers
      -sS/-sU/-sM: Use OS's DNS resolver
      -T<0-5>: Trace hop path to each host

      SCAN TECHNIQUES:
      -sS/S/T/A/W/M: TCP SYN/Connect//ACK/Window/Maimon scans
      -sU: UDP scan
      -sN/s/x: TCP Null, FIN, and Xmas scans
      -sF: FIN scan
      -sT/z: TCP Idle scan
      -sI: zombie host/probeport: idle scan
      -sV/sZ: SCTP INIT/COOKIE-ECHO scans
      -sO: OS detection
      -b <FTP relay host>: FTP bounce scan

      PORT SPECIFICATION AND SCAN ORDER:
      -p <port ranges>: Only scan specified ports
          Ex: -p23: Only scan port 23
              -p 1-65535: Scan all ports from 1 to 65535
              -p 80,8080,5:9: Scan ports 80, 8080, and 5-9
      ---exclude-ports <port ranges>: Exclude the specified ports from scanning

      SERVICE/VERSION DETECTION:
      -sV: Service detection
      -O: OS detection
      -A: All options to determine service/version info
      -version-intensity <level>: Set from 0 (light) to 9 (try all probes)
      -version-all: Try every probe (intensity 9)
      -version-trace: Show detailed version scan activity (for debugging)

      SCRIPTS:
      -sc <script>: Run a single script
      -sc <script>,-script <script>: Run multiple scripts
      -script<=lua scripts>,-c <scripts>: Is a comma separated list of
          scripts to run. -script or -script <script> can be used
      -script-args=<opt>|-v1,|-m2|v3,...>: provide arguments to scripts
      -script-args-file<file>: name: provide NSE script args in a file
      -script-help: Show help about scripts
      -script-updated: Update the script database.
      -script-help[<script>]: Show help about script.

      OS DETECTION:
      -O: Enable OS detection
      -osscan-limit: Limit OS detection to promising targets
      -osscan-guess: Guess OS more aggressively

      TIMING AND PERFORMANCE:
      Options which take <time> are in seconds, or append 'ms' (milliseconds),
      's' (seconds), or 'ms' (milliseconds) to the value (e.g. 300s).
      -t<0-5>: Set timing template (higher is faster)
      -min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
      -min-parallelism/max-parallelism <count>: Probe parallelization
      -min-rtt-timeout/max-rtt-timeout/minidle-rtt-timeout <time>: Specifies
          probe round trip time.
  
```

```

Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] [target specification]
Targets:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanne-nmap.org, microsec.com[24,192.168.0.1-10.0.0-255.1-254
      -iL file.txt: Read targets from list of hosts/networks
      -iR num hosts: Choose random targets
      -iN filelist: Read targets from list > Exclude Hosts/networks
      -ecludefile <excl-file>: Exclude list from file
      -eclude <excl-file>: Exclude list from file

      -sT: Ping Scan - Simply list targets to scan
      -sN: Ping Scan - Disable port scan
      -sP: Treat all hosts as online, skip host discovery
      -sA: All protocols - Perform full OS detection, discovery to given ports
      -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
      -PO[rotocol]: IP Protocol Ping
      -n: No DNS resolution - Always resolve [default: sometimes]
      -dNST-servers <serv1[,serv2,...>: Specify custom DNS servers
      -sS/-sU/-sM: Use OS's DNS resolver
      -T<0-5>: Trace hop path to each host

      SCAN TECHNIQUES:
      -sS/S/T/A/W/M: TCP SYN/Connect//ACK/Window/Maimon scans
      -sU: UDP scan
      -sN/s/x: TCP Null, FIN, and Xmas scans
      -sF: FIN scan
      -sT/z: TCP Idle scan
      -sI: zombie host/probeport: idle scan
      -sV/sZ: SCTP INIT/COOKIE-ECHO scans
      -sO: OS detection
      -b <FTP relay host>: FTP bounce scan

      PORT SPECIFICATION AND SCAN ORDER:
      -p <port ranges>: Only scan specified ports
          Ex: -p23: Only scan port 23
              -p 1-65535: Scan all ports from 1 to 65535
              -p 80,8080,5:9: Scan ports 80, 8080, and 5-9
      ---exclude-ports <port ranges>: Exclude the specified ports from scanning

      SERVICE/VERSION DETECTION:
      -sV: Service detection
      -O: OS detection
      -A: All options to determine service/version info
      -version-intensity <level>: Set from 0 (light) to 9 (try all probes)
      -version-all: Try every probe (intensity 9)
      -version-trace: Show detailed version scan activity (for debugging)

      SCRIPTS:
      -sc <script>: Run a single script
      -sc <script>,-script <script>: Run multiple scripts
      -script<=lua scripts>,-c <scripts>: Is a comma separated list of scripts to run. -script or -script <script> can be used
      -script-args=<opt>|-v1,|-m2|v3,...>: provide arguments to scripts
      -script-args-file<file>: name: provide NSE script args in a file
      -script-help[<script>]: Show help about script.

      OS DETECTION:
      -O: Enable OS detection
      -osscan-limit: Limit OS detection to promising targets
      -osscan-guess: Guess OS more aggressively

      TIMING AND PERFORMANCE:
      Options which take <time> are in seconds, or append 'ms' (milliseconds),
      's' (seconds), or 'ms' (milliseconds) to the value (e.g. 300s).
      -t<0-5>: Set timing template (higher is faster)
      -min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
      -min-parallelism/max-parallelism <count>: Probe parallelization
      -min-rtt-timeout/max-rtt-timeout/minidle-rtt-timeout <time>: Specifies
          probe round trip time.
  
```

```
--min-parallelism=nx--parallelism=n: numprobes= Prone parallelization
--min-rtt-timeout=nx--rtt-timeout=n: initial-rtt-timeout ctime=: Specifies
    probe round trip time
--max-scan-delay=n: Set number of port scan probe retransmissions.
--host-timeout=ctime=: Give up on target after this long
--scan-delay=<max>--scan-delay=<time>: Adjust delay between probes
--max-retries=n: Set number of times to retry a probe per second
--max-rate=n: Set rate in bytes per second
--max-rate-number=n: Send packets no faster than <numbers> per second
FIREWALL/IDS EVASION AND SPOOFING:
--decoy1,decoy2,...>: Scan ports (optionally w/given MTU)
--decoy1,decoy2,...>: Cloak a scan with decoys
--c IP Address: Spoof source address
--r IP Address: Identify spoofed source
--g--source-port=<portnum>: Use given port number
proxies <list>[<list>]: Set up connections through HTTP/2/OKX4 proxies
--data-string=<string>: Append a custom ASCII string to sent packets
--data-strings=<string>: Append multiple custom strings to sent packets
--data-tuples=<tuple>: Set up port tuples to send packets
--no-options options=: Send packets with specified options
--ttl <n>: Set IP time-to-live field
--spoof-mac <mac>: Set MAC address to spoofed name. Spoof your MAC address
--bssum: Send packets with a bogus TCP/UDP/GTP checksum
OUTPUT:
--out <x>/<y>/<z>/<file>: Output scan in normal, XML, JSON, Kiddi3,
    and Greppable format, respectively, to the given filename.
--oA <basename>: Output in the three major formats at once
--v: Verbose output (use -vv or more for greater effect)
--d: Increase debugging level (use -dd or more for greater effect)
--reason: Display the reason a port is in a particular state
--opendir: Open a file for writing and save results there
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--output-dir <dir>: Set output directory for user specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path>/URL>: XSL stylesheet to transform XML output to HTML
--webfont: Reference stylesheet from Nmap-Org for more portable XML
```



```
MISC:
--enable-IPv6-scanning
--script-fingerprint-detection: Version detection, script scanning, and traceroute
--datadir <dir>: Specify custom Nmap Data file location
--send-eth/<-send-ip>: Send using raw ethernet frames or IP packets
--privileged: Assume the user is fully privileged
--no-privileged: Assume the user lacks raw socket privileges
--print version number
--print-help: Print this help summary page.
EXAMPLES:
nmap -v -A scanne.nmap.org
nmap -v -A -p 21,22,23,25,80,100,1000-10000,10.0.0.8
nmap -v -T 10000 -m 90
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Then find target subdomain open ports and details about sub-domains.

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

```
[root@kali ~]# ./msap -S -A -T -o res1.tlmp emoji.tinder.com
Starting Msap 7.91 ( https://msap.org ) at 2021-10-15 02:49 +0530
[...]
Host is up (0.13s latency).
Other addresses for emoji.tinder.com (not scanned): 2a00:600:b30::6775:1d00:21c9 2a06:dala:81:1801:d962:eb6a:c853:e2dc 65.1.4.169
Not shown: 998 filtered ports
PORT      STATE SERVICE VERSION
25/tcp    open  smtp   vsftpd  3.0.3
[...]
Fingerprint-strings:
  General:
    -> syntax error (request)
    -> syntax error (connecting)
    -> syntax error (connecting)
    -> syntax error (connecting)
    -> syntax error (connecting)
  _smtp-commands: Couldn't establish connection on port 25

Fingerprint-strings:
  General:
    -> [REDACTED]_version=Unknown[REDACTED]_TCP, Help, RPCCheck:
    -> HTTP/1.1 400 Bad Request
    -> content-length: 0
    -> Date: Thu, 14 Oct 2021 21:19:42 GMT
  FourOhFourRequest:
    -> HTTP/1.0 400 Bad Request
    -> content-length: 19
    -> date: Thu, 14 Oct 2021 21:19:37 GMT
    -> MISSING host header
    -> GETOptions:
    -> HTTP/1.0 400 Bad Request
    -> content-length: 19
    -> date: Thu, 14 Oct 2021 21:19:36 GMT
    -> MISSING host header
    -> KEYExchangeReq, SSLSessionReq, TLSSessionReq, TerminalServerCookie:
    -> HTTP/1.1 400 Bad Request
```

Automated testing

62

```
[root@kali:~]# nmap -sT emoji.tinder.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 10:15 +0530
Nmap scan report for emoji.tinder.com (REDACTED)
Host is up (0.000s latency).
Other addresses for emoji.tinder.com (not scanned): 2406:da1a:1800:b35e:6775:1d02:1c98 2406:da1a:81a:1801:d96
2:eb6ac8b53:e2dc 65.1.4.189
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
8300/tcp  closed   tmi

Nmap done: 1 IP address (1 host up) scanned in 10.37 seconds
```

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

```
TRACEROUTE (using port 25/tcp)
HOP RTT      ADDRESS
1  7.05 ms  [REDACTED]
2  ... 30

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 229.82 seconds
```

Subdomain-<https://staging.tinder.com>

```
[root@kali ~]# nmap -sS -A -T4 -nH res2.txt staging.tinder.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 11:05 +0530
Nmap scan report for staging.tinder.com [REDACTED]
Host is up (pingable) with no interfaces up.
No open ports found.
Device type: Web server
Running: Linux 2.6.X|2.6.16, Some Ericsson embedded
OS CPE: cpe:/o:linux:linux_kernel:2.4.24 cpe:/o:linux:linux_kernel:2.6.22 cpe:/h:sonyericsson:u81_vivaz
[REDACTED]
```

```
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:w8i_vivaz
OS details: Tomato 1.28 (Linux 2.4.20), Tomato firmware (Linux 2.6.22), Sony Ericsson Ubi Vivaz mobile phone

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 6.71 ms [REDACTED]
2 ... 30

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 230.91 seconds
```

Subdomain- https://tech.gotinder.com

```
[root@kali ~]# nmap -sS -A -T4 -oN res-4.txt tech.gotinder.com
Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-15 11:14 +0530
Nmap scan report for gotinder.com (...)
Host is up (0.28s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
25/tcp    open  smtp
25/tcp    open  smtp
fingerprint_string:
Hello [Help]:
|_ 452 syntax error (connecting)
|_smb-commands: Couldn't establish connection on port 25
|_http: Amazon CloudFront httpd
|_https: Amazon CloudFront httpd
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP-V7.73D-10\15KMPX*x86_64_pc-linux-gnu\${Hel
\$!F01,1F,"452\>x20\r\nyntax x20rerror x20\<(connecting)\r\n"\r\n"\%${Help},1F,"452\x2
WFN\${Help},1F,"452\>x20rerror x20\<(connecting)\r\n"\r\n"
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP/mobile
Running: Linux 2.4.X|2.6.X, Sony Ericsson embedded
OS cpe: cpe:/o:linux:linux_kernel_2.6.20-24_cpe:/o:linux:linux_kernel:2.6.22 cpe:/o:sonyericsson:u81_vivaz
OS details: Tomato 2.1.20 (Linux 2.6.20), Tomato firmware (Linux 2.6.22), Sony Ericsson U8i Vivaz mobile phone

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  7.10 ms  74.120.24.1
2  ... 30

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 231.39 seconds
```

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 [REDACTED]
Host is up (0.084s latency).
Other addresses for tinder.com (not scanned): [REDACTED]
rDNS record for [REDACTED]
Not shown: 997 filtered ports
PORT      STATE SERVICE VERSION
PORT      STATE SERVICE VERSION
[REDACTED] 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
[REDACTED] http Amazon CloudFront httpd
[REDACTED] 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%T=61692029P=x86_64-pc-linux-gnu%R(He
SF:Lo,1F,"452\x20syntax\x20error\x20(connecting)\r\n")%R(Hello,1F,"452\x20
SF:0syntax\x20error\x20(connecting)\r\n")%R(GenericLines,3E,"452\x20synt
SF:a\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
[REDACTED]
```

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>

The screenshot shows a tool interface with the title "HTTP Strict Transport Security (HSTS) Errors and Warnings". Below the title, there is a yellow button labeled "MEDIUM". Underneath the button, there is a section labeled "Certainty" with a progress bar, followed by the URL "URL : https://emoji.tinder.com/".

HSTS

- Hsts is a security header. It means when we type domain http protocol that security header converts it to https protocol. This security header helps to protect against man-in-the-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 Enabled

CONFIRMED MEDIUM

URL : <https://swipelife.tinder.com/>

List of Supported Weak Ciphers :

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000A)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

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

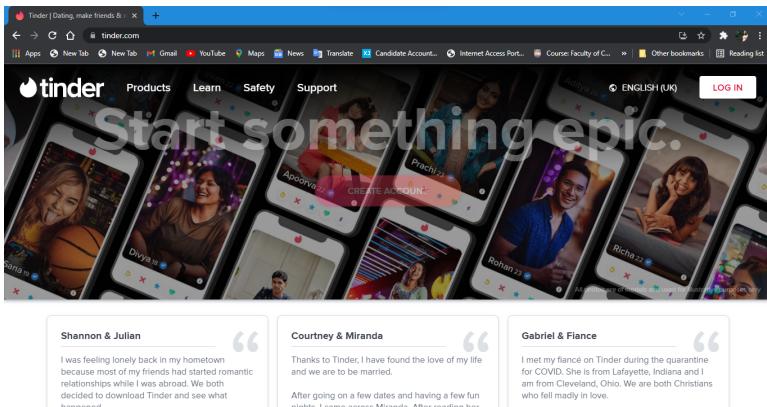
- Netspark identifies the this service is out-of-date. This is critical vulnerability in this subdomain.

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.

A screenshot of the Burp Suite Professional interface. The top navigation bar includes "Burp", "Project", "Intruder", "Repeater", "Window", and "Help". The "Intercept" tab is selected. Below the tabs, there is a "Request" section with the URL "https://tinder.com:443 [32.54.220.87]". The "Actions" dropdown is set to "Intercept is on". The main pane displays a list of network requests. The first request is highlighted with the following details:

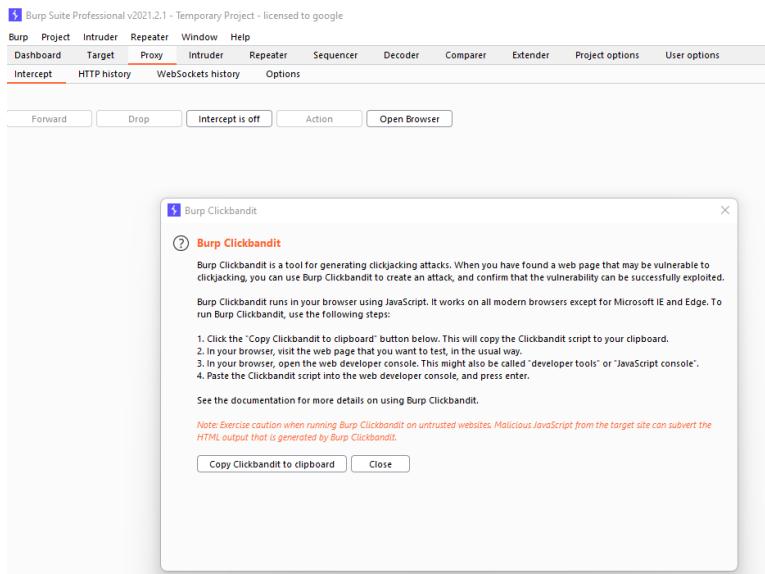
HTTP / 1.1
Host: tinder.com
Connection: close
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.4292.150 Safari/537.36
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Accept-Charset: utf-8,*,utf-8
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.5

The right side of the interface shows a "Dumper" panel and a status bar at the bottom indicating "0 matches".

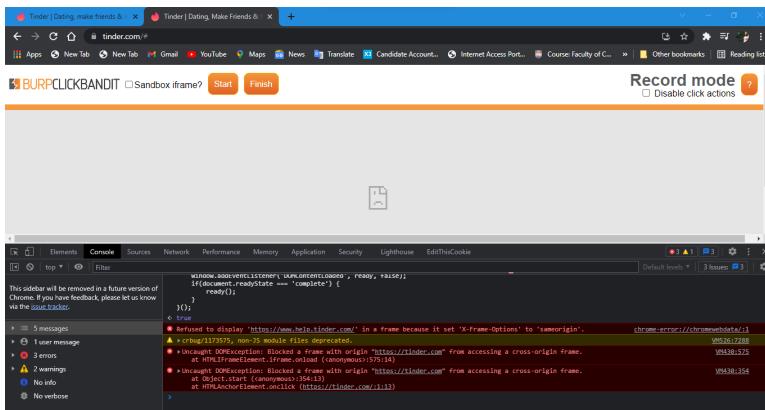
After I try do click jacking attack. Using burp suite tool

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.



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).