Sri Lanka Institute of Information Technology

WEB SECURITY

(IE2062)

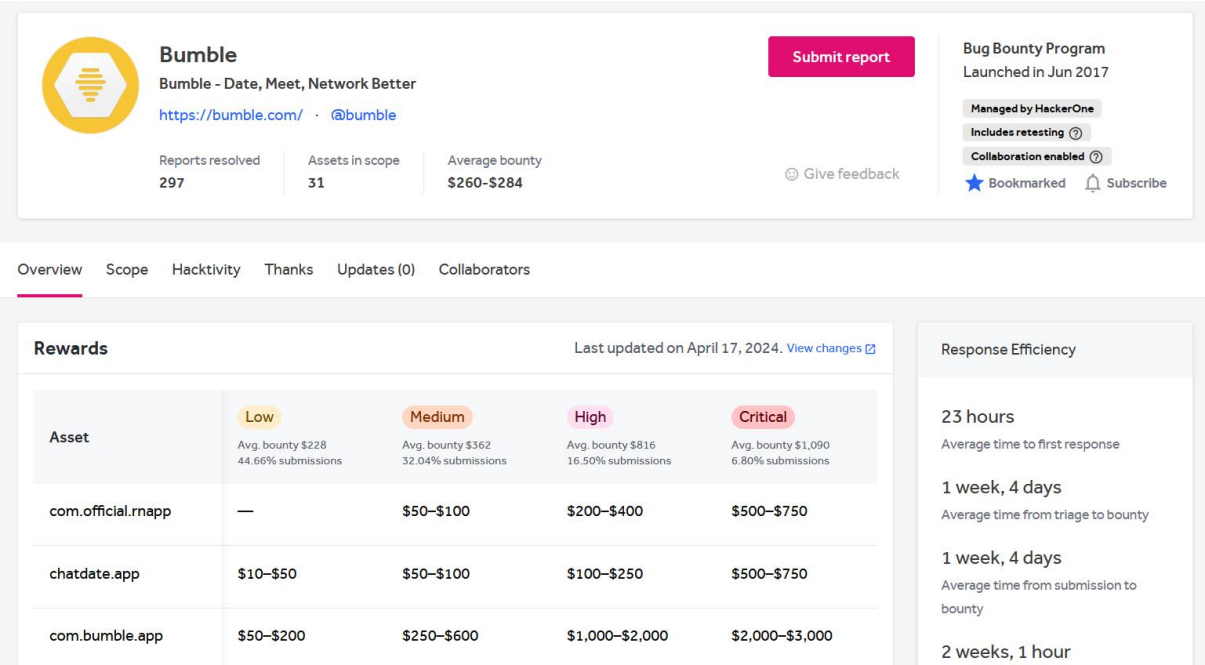
BUG BOUNTY

REPORT 6

Thilakarathna S.T.D- IT22578914

B.Sc. (Hons) in Information Technology Specializing in cyber security

Overview of the website



Bumble
Bumble - Date, Meet, Network Better
https://bumble.com/ · @bumble

Reports resolved 297 | Assets in scope 31 | Average bounty $260-$284

Submit report
Give feedback

Bug Bounty Program
Launched in Jun 2017
Managed by HackerOne
Includes retesting
Collaboration enabled
Bookmarked Subscribe

Overview Scope Hacktivity Thanks Updates (0) Collaborators

Rewards — Last updated on April 17, 2024. View changes

Asset	Low Avg. bounty $228 44.66% submissions	Medium Avg. bounty $362 32.04% submissions	High Avg. bounty $816 16.50% submissions	Critical Avg. bounty $1,090 6.80% submissions
com.official.rnapp	—	$50–$100	$200–$400	$500–$750
chatdate.app	$10–$50	$50–$100	$100–$250	$500–$750
com.bumble.app	$50–$200	$250–$600	$1,000–$2,000	$2,000–$3,000

Response Efficiency
23 hours — Average time to first response
1 week, 4 days — Average time from triage to bounty
1 week, 4 days — Average time from submission to bounty
2 weeks, 1 hour

By giving women authority over the dating and networking process, Bumble.com is a social networking site that is leading the way in standardizing these practices. Bumble gives users the freedom to create deep connections at their own pace by adopting a unique "women make the first move" philosophy. Apart from romantic partnerships, Bumble provides platforms for business and friendship networking, meeting a variety of social requirements. The website creates a friendly atmosphere where users feel emboldened to express themselves honestly because of its emphasis on safety, respect, and diversity. Bumble enhances user experience and builds real connections with its cutting-edge features, which include video calls and profile verification. Setting the standard for a more equal and powerful online social experience, Bumble is a trailblazer in the digital dating space.

Scope

- **InScope**

com.badoo.mobile https://play.google.com/store/apps/details?id=com.badoo.mobile	Android: Play Store	In scope	Critical	Eligible	Feb 12, 2021	6 (2%)
351331194 https://apps.apple.com/gb/app/badoo-dating-ch friends/id351331194	iOS: App Store	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
corp.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
m.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
meu1.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
mus1.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
bma.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
translate.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
ccardsus1.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
bma.bumble.com	Domain	In scope	Critical	Eligible	Jan 15, 2021	1 (0%)
com.flashgap.fruits	iOS: App Store	In scope	Critical	Eligible	Apr 5, 2022	0 (0%)
com.flashgap.fruitz	Android: Play Store	In scope	Critical	Eligible	Apr 5, 2022	2 (1%)
6444040977	iOS: App Store	In scope	Critical	Eligible	Mar 27, 2023	0 (0%)
com.bumblebff.app	Android: Play Store	In scope	Critical	Eligible	Mar 27, 2023	0 (0%)
com.hotornot.app	Android: Play Store	In scope	Critical	Eligible	Oct 5, 2022	0 (0%)
com.badoo.hotornot	iOS: App Store	In scope	Critical	Eligible	Oct 5, 2022	0 (0%)
ccardseu1.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
us1.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
com.bumble.app https://play.google.com/store/apps/details?id=com.bumble.app	Android: Play Store	In scope	Critical	Eligible	Feb 3, 2021	6 (2%)
930441707 https://apps.apple.com/us/app/bumble-dating-meet-people/id930441707	iOS: App Store	In scope	Critical	Eligible	Feb 3, 2021	2 (1%)
com.badoo.twa https://play.google.com/store/apps/details?id=com.badoo.twa	Android: Play Store	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)

403684733 https://apps.apple.com/gb/app/badoo-premium/id403684733	iOS: App Store	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
eu1.badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	2 (1%)
badoocdn.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	1 (0%)
hotornot.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	0 (0%)
chatdate.app	Domain	In scope	Critical	Eligible	Feb 12, 2021	5 (2%)
getofficial.co	Domain	In scope	Critical	Eligible	Mar 12, 2024	0 (0%)
www.bumble.com	Domain	In scope	Critical	Eligible	Jan 15, 2021	25 (8%)
1604650263	iOS: App Store	In scope	Critical	Eligible	Mar 12, 2024	0 (0%)
com.official.rnapp	Android: Play Store	In scope	Critical	Eligible	Mar 12, 2024	14 (5%)
badoo.com	Domain	In scope	Critical	Eligible	Feb 12, 2021	16 (5%)

- **OutScope**

blog.bumble.com	Domain	Out of scope	None	Ineligible	Jan 15, 2021	0 (0%)
shop.bumble.com	Domain	Out of scope	None	Ineligible	Jan 15, 2021	0 (0%)
honey.bumble.com	Domain	Out of scope	None	Ineligible	Jan 15, 2021	0 (0%)
thebeehive.bumble.com	Domain	Out of scope	None	Ineligible	Jan 15, 2021	0 (0%)
com.studio.projects.zodia	Android: Play Store	Out of scope	None	Ineligible	Mar 12, 2024	0 (0%)
zodia.studio	Domain	Out of scope	None	Ineligible	Mar 12, 2024	0 (0%)
1660741163	iOS: App Store	Out of scope	None	Ineligible	Mar 12, 2024	0 (0%)
com.sgiggle.Mango	Android: Play Store	Out of scope	None	Ineligible	Mar 12, 2024	0 (0%)
heyfiesta.com	Domain	Out of scope	None	Ineligible	Mar 12, 2024	0 (0%)
com.sgiggle.Mango	iOS: App Store	Out of scope	None	Ineligible	Mar 12, 2024	0 (0%)

Information Gathering

Security researchers and ethical hackers must first gather data through bug bounty programs in order to identify vulnerabilities in a target system or application. This step's objective is to learn as much as you can about the target, including its technologies, architecture, known vulnerabilities, and potential weak points. Open-source intelligence gathering (OSINT), network scanning, fingerprinting, and asset enumeration are typically required to give a complete view of the target's attack surface.

Since it enables ethical hackers to identify potential points of entry and focus their search for system security flaws, efficient information gathering is the cornerstone of a successful bug hunting operation.

Subdomains for Hunting

The process of listing sub-domains for one or more domains is called sub-domain enumeration. This is a critical stage in the reconnaissance process. Finding vulnerabilities is made more likely by sub-domain enumeration, which can identify several domains and sub-domains that are part of a security assessment.

Seen through cryptic, abandoned sub-domains, programs may have dangerous bugs.

The same weaknesses are frequently found throughout numerous domains and applications within a single organization.

- **Assetfinder**

A program called Assetfinder is mainly meant for penetration testers and cybersecurity experts to detect and count domains and subdomains connected to a certain target domain.Its primary purpose is to list subdomains, but that is not all that important. Each subdomain that is found may be an application, a component of an organization's infrastructure, or even unrecognized online assets that are open to intrusions.

```
┌──(root㉿kali)-[/home/tharusha]
└─# assetfinder --subs-only bumble.com
eu1.bumble.com
ambassador.ccs-000005.bumble.com
bma.bumble.com
bumble.com
bmaam.bumble.com
sce-coll-0062.sciengcam.honey-cards.bumble.com
sce-coll-0062.scieng.honey-cbibizrds.bumble.com
stheraclesrefrheraclesnt.futurefheracleslihеracles.bumble.com
fr1.bumble.com
shop.bumble.com
mybigaddondomain.bumble.com
users.pcachep.bumble.com
team.bumble.com
0.do-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.debian-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.ars-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.util-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
am1.bumble.com
cdn.bumble.com
0.tool-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.perf-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.dashboard-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.erp-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.pgweb-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.images-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.hosting-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.eu-east-2-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.member-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
0.sys-polishlove1relyingparty-okta-stable.europe.autoconfig.php.assets.bumble.com
bma-gew3.bumble.com
bmaeu.bumble.com
bmafr.bumble.com
bmaus.bumble.com
gss1.bumble.com
gss3.bumble.com
gss6.bumble.com
gss8.bumble.com
ns1.bumble.com
ns2.bumble.com
ns3.bumble.com
ns4.bumble.com
ns5.bumble.com
ns6.bumble.com
s.bumble.com
seu1.bumble.com
shot.bumble.com
studio.bumble.com
dev.studio.bumble.com
us1.bumble.com
```

```
vpn-shot.bumble.com
vpn-shot.bumble.com
vpn-shot.bumble.com
shot.bumble.com
shot.bumble.com
mshot.bumble.com
mshot.bumble.com
bumble.com
bumble.com
toau10tix.bumble.com
toau10tix.bumble.com
blog.bumble.com
www.thebeehive.bumble.com
ub-lp.bumble.com
www.blog.bumble.com
www.studio.bumble.com
consent.bumble.com
r5y2gy824h6rdjjax3en.blog.bumble.com
design.bumble.com
design-bumble.bumble.com
design-badoo.bumble.com
support.bumble.com
thebeehive.bumble.com
www.dev.studio.bumble.com
ir.bumble.com
ambassador.bumble.com
ambassador.bumble.com
*.amb.bumble.com
amb.bumble.com
eblgnwwk7jawlzh6bzg4.thebeehive.bumble.com
france-love-guide.bumble.com
city-guides.bumble.com
d2zh3kxlwenffrxx7pjc.lesgrandesfemmes.bumble.com
www.lesgrandesfemmes.bumble.com
ololo.shop.bumble.com
autoconfig.shop.bumble.com
casting-bachelor.shop.bumble.com
ambassador.bumble.com
amb.bumble.com
```

SSL/TLS

Assurance

Common name

Organisation

State

Country

Organisational unit

Subject Alternative Name

Validity period From Jul 1

Matches hostname

Server

Public key algorithm

Protocol version

Public key length

Certificate check

- **Amass**

A tool has been developed by the OWASP Amass Project to assist information security professionals in external asset discovery and network mapping of attack surfaces.

```
┌──(root㉿kali)-[/home/tharusha]
└─# amass enum -passive -d bumble.com
bumble.com (FQDN) --> ns_record --> ns5.bumble.com (FQDN)
bumble.com (FQDN) --> ns_record --> ns7.bumble.com (FQDN)
bumble.com (FQDN) --> ns_record --> ns2.bumble.com (FQDN)
bumble.com (FQDN) --> ns_record --> ns4.bumble.com (FQDN)
bumble.com (FQDN) --> ns_record --> ns1.bumble.com (FQDN)
bumble.com (FQDN) --> ns_record --> ns6.bumble.com (FQDN)
bumble.com (FQDN) --> ns_record --> ns3.bumble.com (FQDN)
bumble.com (FQDN) --> ns_record --> ns8.bumble.com (FQDN)
bumble.com (FQDN) --> mx_record --> mailin1eu.monopost.com (FQDN)
bumble.com (FQDN) --> mx_record --> mailin1us.monopost.com (FQDN)
enterpriseregistration.windows.net (FQDN) --> cname_record --> na.privatelink.msidentity.com (FQDN)
mqaus.bumble.com (FQDN) --> cname_record --> sus1.bumble.com (FQDN)
team.bumble.com (FQDN) --> mx_record --> aspmx2.googlemail.com (FQDN)
team.bumble.com (FQDN) --> mx_record --> alt1.aspmx.l.google.com (FQDN)
team.bumble.com (FQDN) --> mx_record --> aspmx.l.google.com (FQDN)
team.bumble.com (FQDN) --> mx_record --> aspmx3.googlemail.com (FQDN)
team.bumble.com (FQDN) --> mx_record --> alt2.aspmx.l.google.com (FQDN)
eblgnwwk7jawlzh6bzg4.thebeehive.bumble.com (FQDN) --> cname_record --> verify.squarespace.com (FQDN)
toau10tix.bumble.com (FQDN) --> cname_record --> sprout.monopost.com (FQDN)
thebeehive.bumble.com (FQDN) --> cname_record --> ext-cust.squarespace.com (FQDN)
static-eu.bumble.com (FQDN) --> cname_record --> eu1.bumble.com (FQDN)
eu1.bumble.com (FQDN) --> a_record --> 31.222.67.113 (IPAddress)
gss2.bumble.com (FQDN) --> cname_record --> gss3.bumble.com (FQDN)
mqaeu.bumble.com (FQDN) --> cname_record --> seu1.bumble.com (FQDN)
www.studio.bumble.com (FQDN) --> cname_record --> ghs.googlehosted.com (FQDN)
mshot.bumble.com (FQDN) --> cname_record --> sprout.monopost.com (FQDN)
short-s.bumble.com (FQDN) --> cname_record --> s.bumble.com (FQDN)
design.bumble.com (FQDN) --> cname_record --> fatal-flyingfish-amaranth.custom.supernova-docs.io (FQDN)
inc-bma.bumble.com (FQDN) --> a_record --> 31.222.75.198 (IPAddress)
www.blog.bumble.com (FQDN) --> cname_record --> blog.bumble.com (FQDN)
mqa.bumble.com (FQDN) --> cname_record --> s.bumble.com (FQDN)
ub-lp.bumble.com (FQDN) --> cname_record --> f3f700b15d214e82bbbad843ebf09d60.unbouncepages.com (FQDN)
design-bumble.bumble.com (FQDN) --> cname_record --> hostile-jellyfish-tomato.custom.supernova-docs.io (FQDN)
alt2.aspmx.l.google.com (FQDN) --> a_record --> 64.233.184.27 (IPAddress)
alt2.aspmx.l.google.com (FQDN) --> aaaa_record --> 2607:f8b0:400e:c00::1b (IPAddress)
sprout.monopost.com (FQDN) --> a_record --> 31.222.68.67 (IPAddress)
ghs.googlehosted.com (FQDN) --> a_record --> 142.250.180.243 (IPAddress)
ghs.googlehosted.com (FQDN) --> aaaa_record --> 2607:f8b0:4006:809::2013 (IPAddress)
dev.studio.bumble.com (FQDN) --> a_record --> 216.239.38.21 (IPAddress)
dev.studio.bumble.com (FQDN) --> a_record --> 216.239.32.21 (IPAddress)
dev.studio.bumble.com (FQDN) --> a_record --> 216.239.34.21 (IPAddress)
64.233.160.0/19 (Netblock) --> contains --> 64.233.184.27 (IPAddress)
31.222.64.0/21 (Netblock) --> contains --> 31.222.67.113 (IPAddress)
31.222.64.0/21 (Netblock) --> contains --> 31.222.68.67 (IPAddress)
31.222.75.0/24 (Netblock) --> contains --> 31.222.75.198 (IPAddress)
15169 (ASN) --> managed_by --> GOOGLE - Google LLC (RIROrganization)
15169 (ASN) --> announces --> 64.233.160.0/19 (Netblock)
12678 (ASN) --> managed_by --> BADOO-U (RIROrganization)
```

```
inc-bmaus.bumble.com (FQDN) ⟶ a_record ⟶ 31.222.75.198 (IPAddress)
13.35.16.0/21 (Netblock) ⟶ contains ⟶ 13.35.18.94 (IPAddress)
13.35.16.0/21 (Netblock) ⟶ contains ⟶ 13.35.18.28 (IPAddress)
104.16.0.0/14 (Netblock) ⟶ contains ⟶ 104.16.51.111 (IPAddress)
104.16.0.0/14 (Netblock) ⟶ contains ⟶ 104.16.53.111 (IPAddress)
173.194.202.0/24 (Netblock) ⟶ contains ⟶ 173.194.202.26 (IPAddress)
2607:f8b0::/32 (Netblock) ⟶ contains ⟶ 2607:f8b0:4023:c0b::1a (IPAddress)
31.222.64.0/21 (Netblock) ⟶ contains ⟶ 31.222.69.253 (IPAddress)
31.222.72.0/23 (Netblock) ⟶ contains ⟶ 31.222.72.5 (IPAddress)
2a00:aea0:200::/40 (Netblock) ⟶ contains ⟶ 2a00:aea0:211::5 (IPAddress)
16509 (ASN) ⟶ managed_by ⟶ AMAZON-02 - Amazon.com, Inc. (RIROrganization)
16509 (ASN) ⟶ announces ⟶ 13.35.16.0/21 (Netblock)
15169 (ASN) ⟶ announces ⟶ 2607:f8b0::/32 (Netblock)
13335 (ASN) ⟶ managed_by ⟶ CLOUDFLARENET - Cloudflare, Inc. (RIROrganization)
13335 (ASN) ⟶ announces ⟶ 104.16.0.0/14 (Netblock)
13.35.16.0/21 (Netblock) ⟶ contains ⟶ 13.35.18.71 (IPAddress)
13.35.16.0/21 (Netblock) ⟶ contains ⟶ 13.35.18.6 (IPAddress)
142.250.141.0/24 (Netblock) ⟶ contains ⟶ 142.250.141.27 (IPAddress)
2404:6800:4008::/48 (Netblock) ⟶ contains ⟶ 2404:6800:4008:c13::1b (IPAddress)
15169 (ASN) ⟶ announces ⟶ 142.250.141.0/24 (Netblock)
15169 (ASN) ⟶ announces ⟶ 2404:6800:4008::/48 (Netblock)
www.tm.f.prd.aadg.akadns.net (FQDN) ⟶ cname_record ⟶ www.a.f.prd.aadg.akadns.net (FQDN)
www.a.f.prd.aadg.akadns.net (FQDN) ⟶ cname_record ⟶ sin.a.f.prd.aadg.akadns.net (FQDN)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ a_record ⟶ 20.190.163.0 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ a_record ⟶ 20.190.163.128 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ a_record ⟶ 40.126.35.132 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ a_record ⟶ 40.126.35.131 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ a_record ⟶ 20.190.163.23 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ aaaa_record ⟶ 2603:1047:1:188::8 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ aaaa_record ⟶ 2603:1046:2000:190::6 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ aaaa_record ⟶ 2603:1047:1:188::7 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ aaaa_record ⟶ 2603:1046:2000:190::7 (IPAddress)
sin.a.f.prd.aadg.akadns.net (FQDN) ⟶ aaaa_record ⟶ 2603:1046:2000:198::4 (IPAddress)
20.184.0.0/13 (Netblock) ⟶ contains ⟶ 20.190.163.0 (IPAddress)
20.184.0.0/13 (Netblock) ⟶ contains ⟶ 20.190.163.128 (IPAddress)
20.184.0.0/13 (Netblock) ⟶ contains ⟶ 20.190.163.23 (IPAddress)
8075 (ASN) ⟶ managed_by ⟶ MICROSOFT-CORP-MSN-AS-BLOCK - Microsoft Corporation (RIROrganization)
8075 (ASN) ⟶ announces ⟶ 20.184.0.0/13 (Netblock)
8075 (ASN) ⟶ announces ⟶ 40.126.0.0/18 (Netblock)
40.126.0.0/18 (Netblock) ⟶ contains ⟶ 40.126.35.132 (IPAddress)
40.126.0.0/18 (Netblock) ⟶ contains ⟶ 40.126.35.131 (IPAddress)
2603:1000::/25 (Netblock) ⟶ contains ⟶ 2603:1047:1:188::8 (IPAddress)
2603:1000::/25 (Netblock) ⟶ contains ⟶ 2603:1046:2000:190::6 (IPAddress)
2603:1000::/25 (Netblock) ⟶ contains ⟶ 2603:1046:2000:198::4 (IPAddress)
2603:1000::/25 (Netblock) ⟶ contains ⟶ 2603:1046:2000:190::7 (IPAddress)
2603:1000::/25 (Netblock) ⟶ contains ⟶ 2603:1047:1:188::7 (IPAddress)
8075 (ASN) ⟶ announces ⟶ 2603:1000::/25 (Netblock)
^C
The enumeration has finished
```

- **Dnsdumpster**

Block addresses, emails, domain names, and other kinds of DNS-related data can be gathered using an online passive scanning tool called DNSdumpster.

Result of bumble.com

dns recon & research, find & lookup dns records

bumble.com | Search

DNS Servers

ns1.bumble.com.	31.222.73.253	BADOO-U United States
ns5.bumble.com.	31.222.67.253	BADOO-U Czechia
ns4.bumble.com.	159.253.177.253	BADOO-U Czechia
ns2.bumble.com.	31.222.75.253	BADOO-U United States
ns7.bumble.com.	31.222.78.39	BADOO-U United States
ns3.bumble.com.	31.222.77.253	BADOO-U United States
ns8.bumble.com.	31.222.70.39	BADOO-U Cyprus
ns6.bumble.com.	31.222.69.253	BADOO-U Czechia

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

5 mailin1us.monopost.com.	31.222.73.202	BADOO-U United States
5 mailin1eu.monopost.com.	159.253.176.122	BADOO-U Czechia

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

"google-site-verification=Jhg7q3xSAR-558RAxnV2cXQTiJXyl5nNmRYdvhkGOyI"

"google-site-verification=cAE3aRSPaGrxU7N-rJw5O4APM62yLqvb8TLTX8hJNrk"

"mailru-verification: c4d2d72602d6f569"

"google-site-verification=ohC5seycw-H7ZPPq3csVsqydCN5taaDzUfvXpp0A1ss"

"facebook-domain-verification=zkrfxt6s5z5jeli68o4wkxw3f16g4k"

"google-site-verification=lNZiO6KN_WztgPDCPcQgUz5RimSqj01COtpBOnBS9WA"

"v=spf1 include:mail.zendesk.com ip4:31.222.64.0/20 ip4:159.253.176.0/21 -all"

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

am1.bumble.com HTTP: nginx HTTP TECH: nginx	31.222.70.21	BADOO-U Cyprus
ns1.bumble.com	31.222.73.253 ns1.magic-lab.com	BADOO-U United States
gss1.bumble.com	159.253.176.5 gss1.monopost.com	BADOO-U Czechia
us1.bumble.com HTTP: nginx HTTP TECH: nginx	31.222.75.113	BADOO-U United States
eu1.bumble.com HTTP: nginx HTTP TECH: nginx	31.222.67.113	BADOO-U Czechia
seu1.bumble.com HTTP: nginx HTTP TECH: nginx	159.253.176.102 seu1.bumble.com	BADOO-U Czechia

- **DNSrecon**

For DNS enumeration and reconnaissance, an open-source tool named DNSRecon is utilized. The purpose of gathering information is to assist with penetration testing and security evaluations by providing details on DNS servers, domains, subdomains, and DNS records.

```
┌──(root㉿kali)-[/home/tharusha]
└─# dnsrecon -d bumble.com
[*] std: Performing General Enumeration against: bumble.com...
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to bumble.com
[!] It is resolving to 31.222.67.113
[!] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for bumble.com
[*]      SOA ns2.bumble.com 31.222.75.253
[*]      NS ns7.bumble.com 31.222.78.39
[*]      NS ns2.bumble.com 31.222.75.253
[*]      NS ns2.bumble.com 64:ff9b::1fde:4bfd
[*]      NS ns1.bumble.com 31.222.73.253
[*]      NS ns1.bumble.com 64:ff9b::1fde:49fd
[*]      NS ns8.bumble.com 31.222.70.39
[*]      NS ns4.bumble.com 159.253.177.253
[*]      NS ns5.bumble.com 31.222.67.253
[*]      NS ns3.bumble.com 31.222.77.253
[*]      NS ns6.bumble.com 31.222.69.253
[*]      MX mailin1eu.monopost.com 159.253.176.122
[*]      MX mailin1us.monopost.com 31.222.73.202
[*]      MX mailin1eu.monopost.com 64:ff9b::9ffd:b07a
[*]      A bumble.com 31.222.67.113
[*]      TXT _dmarc.bumble.com v=DMARC1; p=reject; pct=100; fo=1; rua=mailto:dmarc-rua@corp.badoo.com
[*] Enumerating SRV Records
[-] No SRV Records Found for bumble.com
```

- **Wappalyzer**

A flexible web technology identification tool, Wappalyzer.com offers insightful information about the technologies that underpin webpages. Wappalyzer is a browser plugin and API that assists developers, marketers, and companies in determining the platforms, software tools, and frameworks that are used by a particular website. Through the analysis of several elements including content management systems, e-commerce platforms, analytics tools, and more, Wappalyzer helps customers to obtain competitive insights, optimize research procedures, and make well-informed judgments regarding the use of technology.

bumble.com

Technology stack

Static site generator

Next.js (12.3.4)

Documentation

Zendesk

Issue trackers

Zendesk

Programming languages

Node.js

Reverse proxies

Nginx

Web frameworks

Next.js (12.3.4)

JavaScript frameworks

React

Next.js (12.3.4)

AMP

Payment processors

PayPal

Web servers

Nginx

Next.js (12.3.4)

Advertising

Linkedin Ads

Taboola

Google AdSense

Analytics

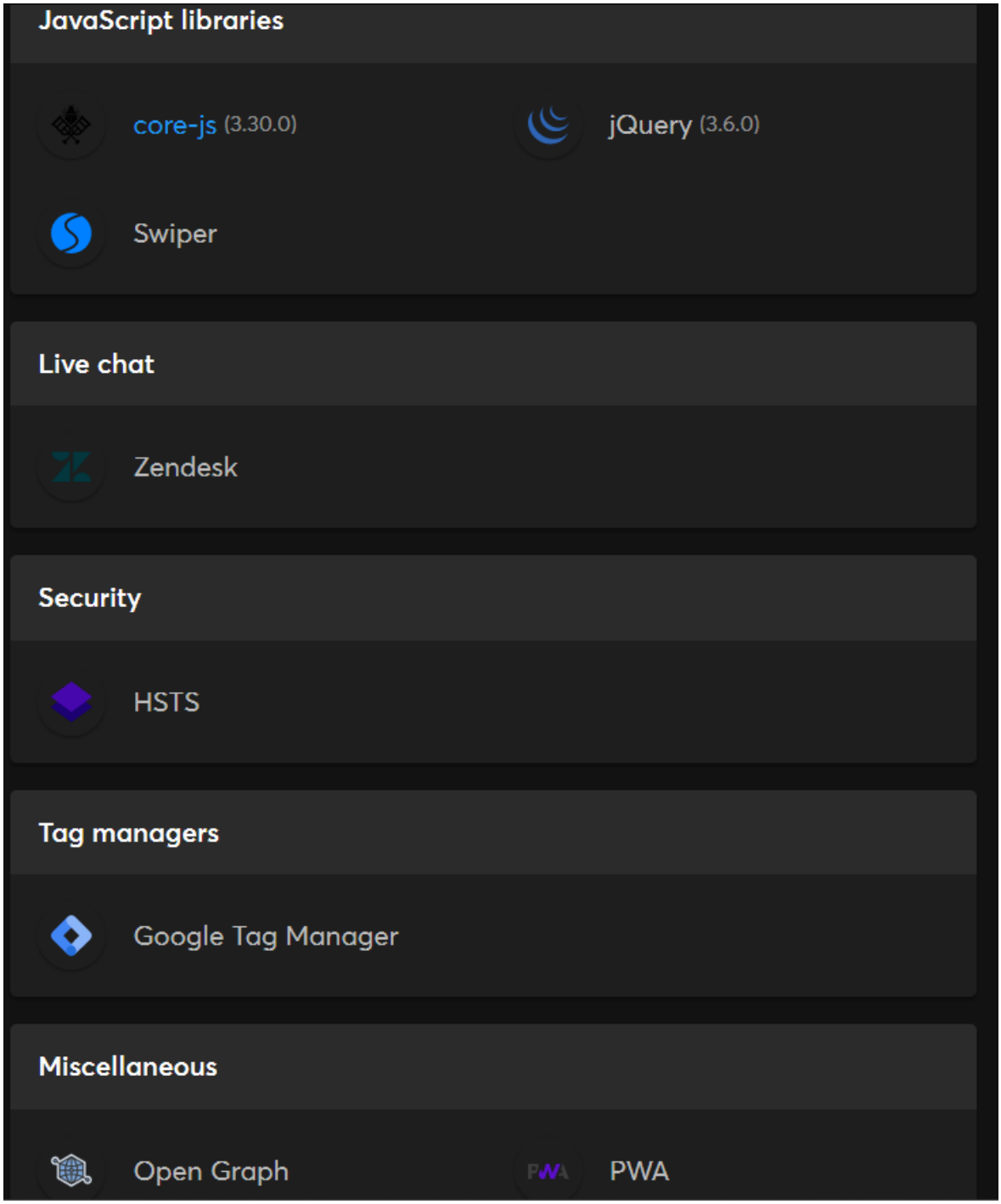
Google Analytics (UA)

Linkedin Insight Tag

Facebook Pixel (2.9.156)

Pinterest Conversion Tag

TikTok Pixel



- **Whatweb**

A web application's technology stack can be discovered with this open-source research tool. It analyzes HTTP answers from a target web server to collect further information about the web server, web framework, programming language, content management system (CMS), JavaScript libraries, and other technologies that the target site may be utilizing.

```
┌──(root㉿kali)-[/home/tharusha]
└─# whatweb bumble.com
http://bumble.com [302 Found] Country[UNITED KINGDOM][GB], HTTPServer[nginx], IP[31.222.67.113], RedirectLocation[https://bumble.com/], Title[302 Found], nginx
https://bumble.com/ [200 OK] Cookies[buzz_lang_code,device_id,first_web_visit_id,has_secure_session,session,session_cookie_name], Country[UNITED KINGDOM][GB], HTML5, HTTPServer[nginx], HttpOnly[session,session_cookie_name], IP[31.222.6
7.113], Open-Graph-Protocol[website][x2022001306556], Script[application/json], Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Bumble | Date, Chat, Meet New People &amp;amp; Network Better], UncommonHeaders
[content-security-policy-report-only,referrer-policy,x-content-type-options], X-UA-Compatible[IE=edge], nginx
```

- **Wafw00f**

An open-source program called Wafw00f is used to identify and fingerprint Web application firewalls (WAFs). Web application firewalls (WAFs), security solutions, defend against SQL injection, cross-site scripting (XSS), and other attacks.

```
┌──(root㉿kali)-[/home/tharusha]
└─# wafw00f bumble.com

                    ____
                   /    \
                  (  W00f! )
                   \  ____/
                   ,,    __           404 Hack Not Found
            |`-.__   / /
            /"  _/  /_/
           *===*    /
          /     )__//                          __     __
     /|  /     /___`                            \ \   / /
     \\/`   \ |                                 \ \_/ /   405 Not Allowed
     `\   /_\\_                                  \   /
       `  ___ ``  `                         403 Forbidden
                                                / _ \
                                502 Bad Gateway / / \ \   500 Internal Error
                                               /_/   \_\

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

[*] Checking https://bumble.com
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

- **Using nmap, open port enumeration**

Open port enumeration is a method for locating and classifying the open network ports on a target machine or network using the Nmap (Network Mapper) program. Nmap is an effective open-source tool for network scanning and host discovery that provides extensive information on the services and statuses that are running on various ports. This process involves sending specially made packets to a target system and analyzing the responses in order to determine which ports are open and what services are using them.

Nmap is a popular tool for network administrators and security specialists to assess system security, identify potential security flaws, and enhance network configurations due to its abundance of features and versatility. It's a helpful tool for enhancing security and computer network administration in general.

```
┌──(root㉿kali)-[/home/tharusha]
└─# nmap -sS bumble.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 06:38 EDT
Nmap scan report for bumble.com (31.222.67.113)
Host is up (0.022s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 10.33 seconds
```

- **Using Nikto to scan for vulnerabilities**

One method to check for vulnerabilities in Kali Linux is to use the powerful open-source tool Nikto web scanner, which is part of the popular operating system for penetration testing and ethical hacking. Nikto is specifically designed to identify and assess server and web application vulnerabilities.

When checking target web servers for known vulnerabilities, common security issues, and misconfigurations, Nikto can be used from the Kali Linux command line. Nikto searches for issues including outdated software, possibly unsafe scripts, security headers, and other online vulnerabilities. It helps ethical hackers and security professionals understand and reduce such threats by providing comprehensive information on the vulnerabilities discovered.

```
┌──(root㉿kali)-[/home/tharusha]
└─# nikto -h bumble.com
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          31.222.67.113
+ Target Hostname:    bumble.com
+ Target Port:        80
+ Start Time:         2024-05-10 07:04:40 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to th
sing-content-type-header/
+ Root page / redirects to: https://bumble.com/
^C
┌──(root㉿kali)-[/home/tharusha]
└─# nikto -h 31.222.67.113
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          31.222.67.113
+ Target Hostname:    31.222.67.113
+ Target Port:        80
+ Start Time:         2024-05-10 07:04:56 (GMT-4)
---------------------------------------------------------------------------
+ Server: nginx
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to th
sing-content-type-header/
+ All CGI directories 'found', use '-C none' to test none
```

Exploitation

I employed PWNXSS tool to identify cross-site vulnerabilities in the target web application for the exploitations.

- **PwnXSS**

PwnXSS is a free and open-source application that may be found on GitHub. This program especially detects cross-site scripting. I execute several payloads in numerous web application directories while testing my target domain for XSS vulnerabilities. After the test, I discovered that indrive.com had no XSS vulnerabilities.

```
┌──(tharusha㉿kali)-[~/PwnXSS]
└─$ python3 pwnxss.py -u https://bumble.shop/account/login?return_url=%2Faccount
PWNXSS
{v0.5 Final}
https://github.com/pwn0sec/PwnXSS

<<<<<<< STARTING >>>>>>>

[06:41:51] [INFO] Starting PwnXSS ...
***************
[06:41:51] [INFO] Checking connection to: https://bumble.shop/account/login?return_url=%2Faccount
[06:41:52] [INFO] Connection estabilished 200
[06:41:52] [WARNING] Target have form with POST method: https://bumble.shop/cart
[06:41:52] [INFO] Collecting form input key.....
[06:41:52] [INFO] Sending payload (POST) method ...
[06:41:53] [INFO] Parameter page using (POST) payloads but not 100% yet ...
[06:41:53] [WARNING] Target have form with POST method: https://bumble.shop/account/login
[06:41:53] [INFO] Collecting form input key.....
[06:41:53] [INFO] Form key name: form_type value: <script>alert(document.cookie)</script>
[06:41:53] [INFO] Form key name: utf8 value: <script>alert(document.cookie)</script>
[06:41:53] [INFO] Form key name: customer[email] value: <script>alert(document.cookie)</script>
[06:41:53] [INFO] Form key name: customer[password] value: <script>alert(document.cookie)</script>
[06:41:53] [INFO] Internal error: 'name'
[06:41:53] [INFO] Form key name: return_url value: <script>alert(document.cookie)</script>
[06:41:53] [INFO] Sending payload (POST) method ...
[06:41:54] [INFO] Parameter page using (POST) payloads but not 100% yet ...
[06:41:54] [WARNING] Target have form with POST method: https://bumble.shop/account/recover
[06:41:54] [INFO] Collecting form input key.....
[06:41:54] [INFO] Form key name: form_type value: <script>alert(document.cookie)</script>
[06:41:54] [INFO] Form key name: utf8 value: <script>alert(document.cookie)</script>
[06:41:54] [INFO] Form key name: email value: <script>alert(document.cookie)</script>
[06:41:54] [INFO] Internal error: 'name'
[06:41:54] [INFO] Sending payload (POST) method ...
[06:41:55] [INFO] Parameter page using (POST) payloads but not 100% yet ...
[06:41:55] [WARNING] Target have form with POST method: https://bumble.shop/cart
[06:41:55] [INFO] Collecting form input key.....
[06:41:55] [INFO] Form key name: checkout value: <Submit Confirm>
[06:41:55] [INFO] Internal error: 'name'
[06:41:55] [INFO] Sending payload (POST) method ...
[06:41:56] [INFO] Parameter page using (POST) payloads but not 100% yet ...
[06:41:56] [WARNING] Target have form with POST method: https://bumble.shop/cart
[06:41:56] [INFO] Collecting form input key.....
[06:41:56] [INFO] Form key name: checkout value: <Submit Confirm>
[06:41:56] [INFO] Internal error: 'name'
[06:41:56] [INFO] Sending payload (POST) method ...
[06:41:58] [INFO] Parameter page using (POST) payloads but not 100% yet ...
[06:41:58] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:41:58] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>#page-content
[06:41:58] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E#page-content
```

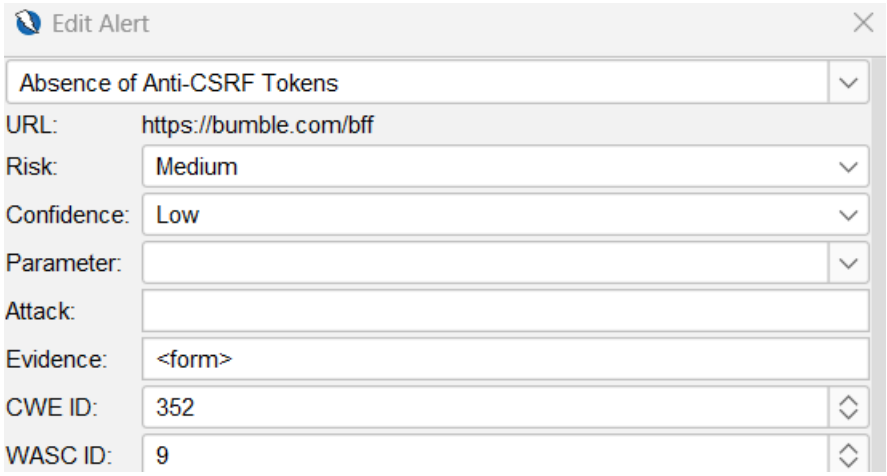
```
[06:41:58] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:41:58] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>#page-content
[06:41:58] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E#page-content
[06:42:00] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:00] [WARNING] Found link with query: mt=8 Maybe a vuln XSS point
[06:42:00] [INFO] Query (GET) : https://apps.apple.com/US/app/id930441707?mt=<script>alert(document.cookie)</script>
[06:42:00] [INFO] Query (GET) : https://apps.apple.com/US/app/id930441707?mt=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:07] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:07] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:07] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>#page-menu
[06:42:07] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E#page-menu
[06:42:08] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:08] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:08] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>
[06:42:08] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:09] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:09] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:09] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>
[06:42:09] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:11] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:11] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:11] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>
[06:42:11] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:12] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:12] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:12] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>
[06:42:12] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:14] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:14] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:14] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>
[06:42:14] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:16] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:16] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:16] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>
[06:42:16] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:18] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:18] [WARNING] Found link with query: return_url=%2Faccount Maybe a vuln XSS point
[06:42:18] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=<script>alert(document.cookie)</script>
[06:42:18] [INFO] Query (GET) : https://bumble.shop/account/login?return_url=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:19] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:19] [WARNING] Found link with query: mt=8 Maybe a vuln XSS point
[06:42:19] [INFO] Query (GET) : https://apps.apple.com/US/app/id930441707?mt=<script>alert(document.cookie)</script>
[06:42:19] [INFO] Query (GET) : https://apps.apple.com/US/app/id930441707?mt=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:21] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:21] [WARNING] Found link with query: hl=en Maybe a vuln XSS point
[06:42:21] [INFO] Query (GET) : https://www.instagram.com/bumble/?hl=<script>alert(document.cookie)</script>
[06:42:21] [INFO] Query (GET) : https://www.instagram.com/bumble/?hl=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
[06:42:27] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[06:42:27] [WARNING] Found link with query: lang=en Maybe a vuln XSS point
[06:42:27] [INFO] Query (GET) : https://www.tiktok.com/@bumble?lang=<script>alert(document.cookie)</script>
[06:42:27] [INFO] Query (GET) : https://www.tiktok.com/@bumble?lang=%3Cscript%3Ealert%28document.cookie%29%3C%2Fscript%3E
```

Vulnerabilities detect when Scanning

In order to process and find problems and vulnerabilities that are based on the OWASP top 10, I used tool like OWASP ZAP.

OWASP ZAP is a testing tool that may be used to identify potential security gaps in internet applications. OWASP ZAP can be used to find common vulnerabilities such as SQL injection and cross-site scripting (XSS).

1. Vulnerability Title



Vulnerability Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

* The victim has an active session on the target site.
* The victim is authenticated via HTTP auth on the target site.
* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

How to mitigate

Phase: Architecture and Design

- Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
  For example, use anti-CSRF packages such as the OWASP CSRFGuard.
- Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS.
- Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS.

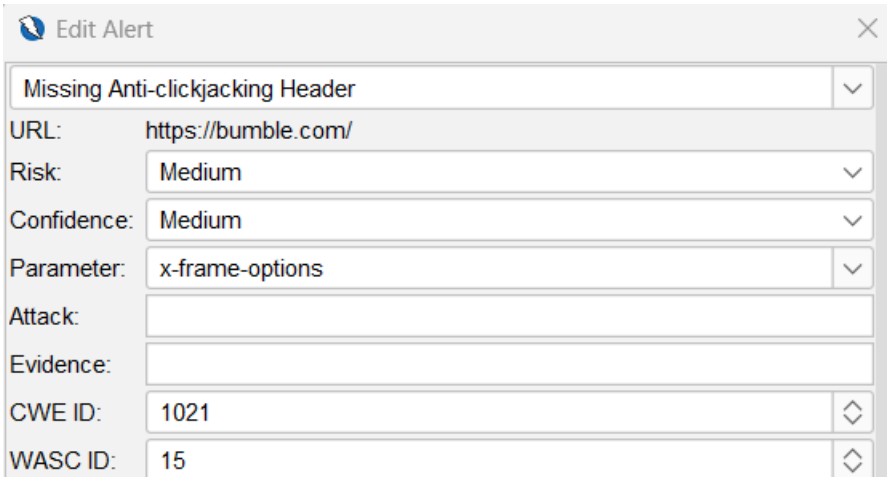
- Use the ESAPI Session Management control. This control includes a component for CSRF.
- Do not use the GET method for any request that triggers a state change.

Phase: Implementation

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

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

2. Vulnerability Title



Vulnerability Description

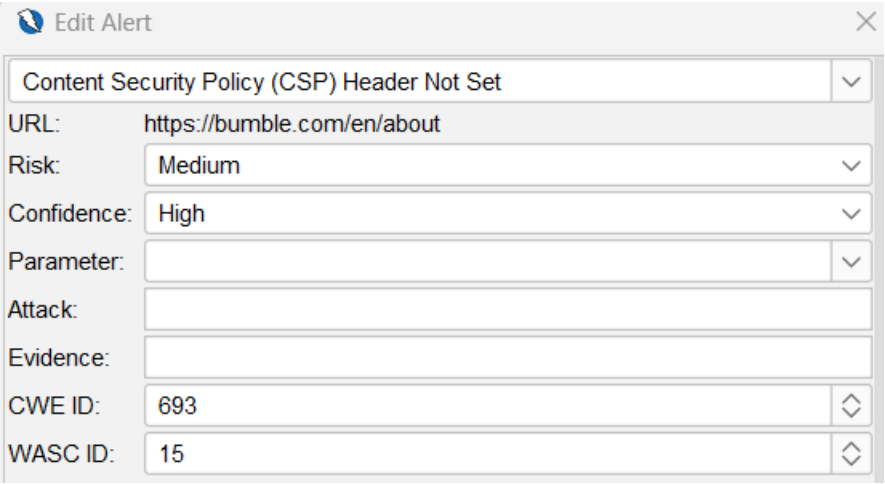
The response does not contain X-Frame-Options to prevent 'ClickJacking' attacks or Content-Security-Policy with 'frame-ancestors' directive.

How to mitigate

The HTTP headers X-Frame-Options and Content-Security-Policy are supported by most modern Web browsers. On every web page that your site or app returns, make sure that one of them is set.

If the page is part of a FRAMESET or other pages on your server that you anticipate will be the only ones framing it, then you should use SAMEORIGIN; if not, you should use DENY. Alternatively, think about putting the "frame-ancestors" requirement of the Content Security Policy into practice.

3. Vulnerability Title



Vulnerability Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

How to mitigate

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.