SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

WEB SECURITY (IE2062)

BUG BOUNTY ASSIGNMENT

IT20023614

WIJESINGHA W.M.P.M

Domain of Bug Bounty Test

https://www.reddit.com

Terms of Reference

This is report about bug bounty hunting. This web audit focusing on selected web domain, sub domains And complete web security (IE2062) module assignment. This project happens under Department of Computer Systems Engineering,
Sri Lanka Institute of Information Technology.

Acknowledgment

I give my special thanks to Dr. Lakmal Rupasinghe, head of web security (IE2062) module. And I want to give my gratitude to Ms. Chethana Liyanapathirana, our lecturer of Web Security Module. Both of you gave us most valuable knowledge, information and also study resources. Ms. Menaka Moonamaldeniya, and Ms. Chathu Udagedara for their immense support and guidance on this web audit. I really appreciate all your support

Table of Contents

Introduction

What is Computer Security?

An Italian inventor, Guglielmo Marconi, sent the first radio signal in 1895. But according to some scholars intellectuals it was invented by Nikola Tesla. However, because of Scholars and intellectuals like Alexander Graham Bell, Charles Babbage, Alan Turing, we achieve this current computing technology. With the improvement of Computer technology, threats and cyber-attacks are also improved. So, because of that reason cyber security also improved. Computer security, often known as cybersecurity, is the safeguarding of computer information and systems against injury, theft, and illegal access. Computer equipment is generally safeguarded using the same methods as other expensive or sensitive equipment, such as serial numbers, walls and locks, and sensors.

Web Technology

Website design deserves full credit to Mr Tim Berners-Lee. He is widely recognized as the creator of the World Wide Web, and he is a computer scientist. After his HTTP and HTML inventions, there are many technologies buildup with the help of that. To facilitate the creation of the Worldwide Web, many development tools, software packages, and environments have been developed. For a complete list of development tools, as well as links to a plethora of additional online resources, visit.

Web Security Audit

Performing a website security audit is the process of evaluating the web framework, including its vulnerabilities and security basis, as well as its extensions, templates, and other infrastructure. A thorough online security audit would often involve a static and dynamic examination of code, data model error checking, configuration verification, and other related activities. Website security audits involve the identification of hidden vulnerabilities on the website as well as the security architecture, and they are often followed by penetration tests. While the goal of a security audit is to identify and evaluate weak areas, the goal of a penetration test is to attack such vulnerabilities. Rather than simulating a hacker and a real-life assault, penetration tests are more like exploiting flaws in order to identify the risk associated with each weakness in the system under test.

Website Security Checklist

1. Look for flaws in the website's design.
2. Keep software up to date.
3. Validate user data.
2. Keep software up to date.
5. Make use of HTTPS.
6. Install a Web Application Firewall (WAF)
7. Keep an eye out for traffic jams.

Types of Web Security Audits

1. Vulnerability Scanner
2. Automated Security Audits
3. Manual Security Audits
4. Professional Security Audit

How to Start Bug Bounty

Bug Bounty Platform

As a starter, one should begin with bug bounty platforms and remain for an extended period to pick up on methods and tactics. Such sites attract not only novices but also a large number of skilled security specialists who routinely hack for them.

To do a bug bounty you need basic understand about

1. Internet, HTTP, TCP/IP
2. Networking
3. Linux Command-line
4. Web technologies, java-script, PHP, java
5. At least 1 programming language (Python/C/JAVA/Ruby.)
6. Owasp top 10
7. Testing tools like Burp.

Some many key elements and methods should be addressed while beginning and continuing a web security audit that is mentioned. Hosting discovery, inspection services, site structuring, website/app analysis, code assessment, vulnerability research, attack method selection, vulnerability confirmation, and remediation are all available.

Program Selection

There are many bug bounty platforms in the industry. Among those platforms, I choose Hacker One. There are many services including linking businesses with hackers and establishing your own bug bounty program provided by HackerOne, one of the top platforms for bug bounty programs. In order to utilize the platform, you have two options: either use the platform to handle vulnerability reports and deal with them yourself or have hackers at HackerOne deal with them on your behalf (triaging). As a result of triaging, security researchers are able to thoroughly examine all of the information they've received.

Platform / Companies

- HackerOne
- Bug Crowd
- Cobalt
- Synack
- Facebook
- Google

HackerOne

HackerOne was founded by a group of hackers and security experts who were motivated by a desire to make the internet a safer place. They are working to make the internet a more secure environment. Thousands of brilliant individuals — hackers, workers, and members of the community – have committed themselves to a single goal: hacking for the greater good.

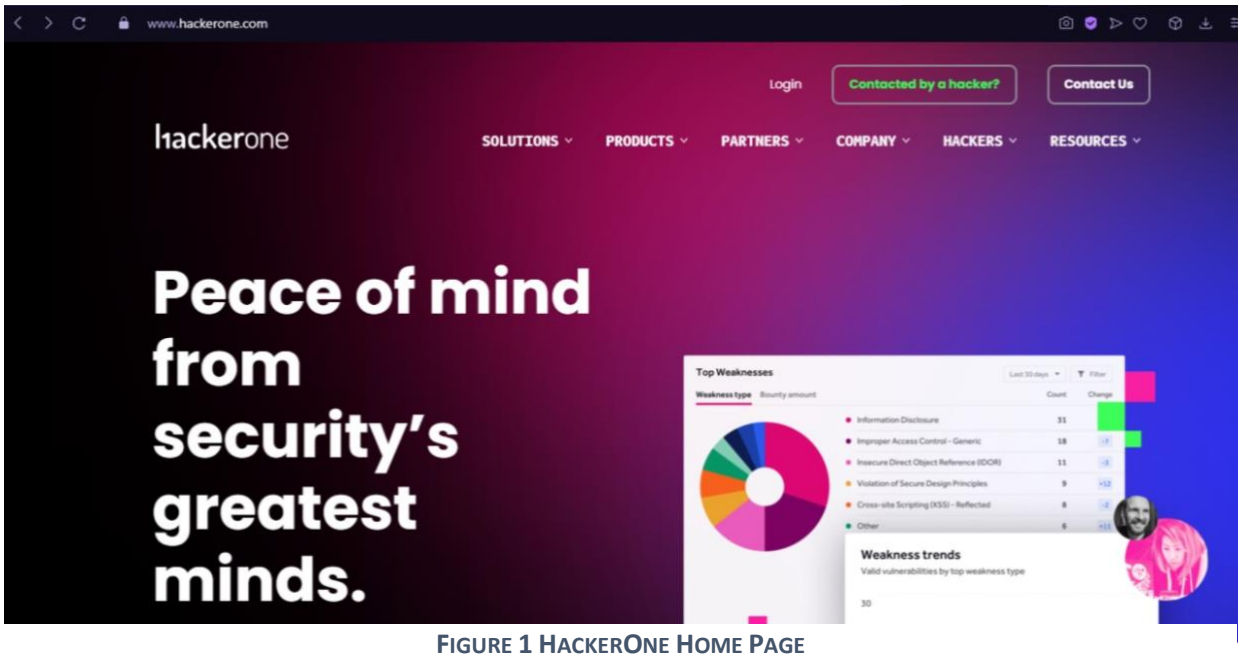


FIGURE 1 HACKERONE HOME PAGE

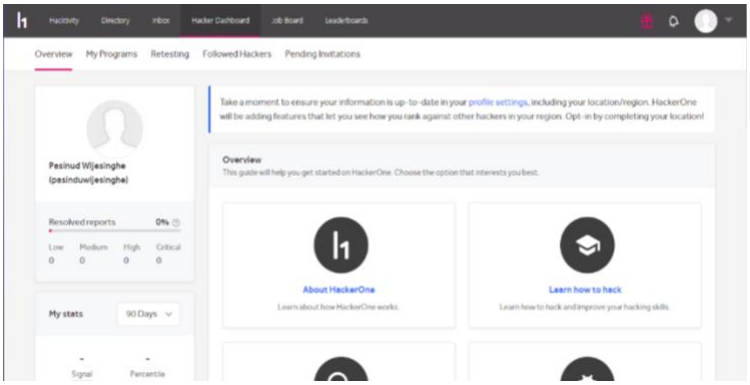


FIGURE 2 DASHBOARD

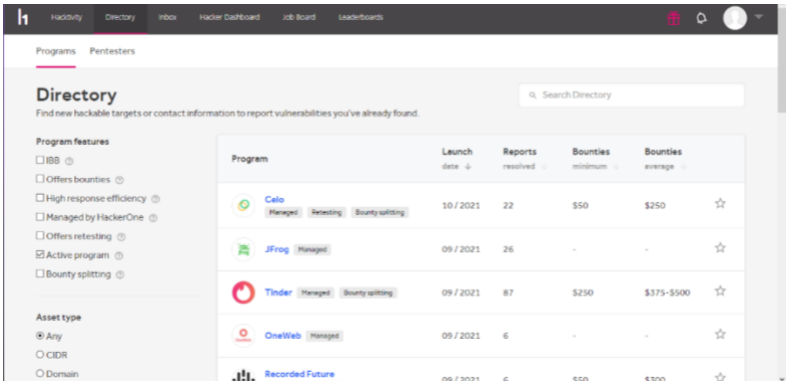
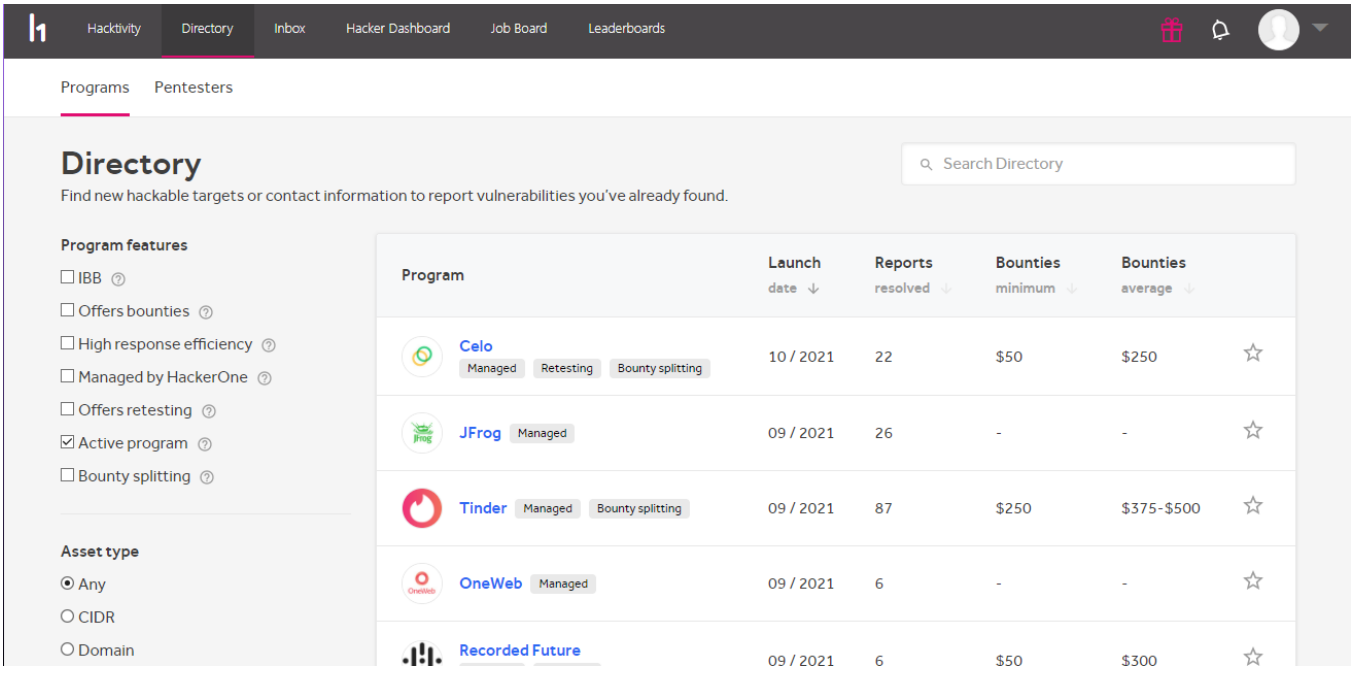


FIGURE 3 DIRECTORY

Domain Selection

First, we need to create an account in HackerOne and log in. After successful login, we can see a dashboard and we can see a navigation bar, so inside the navigation bar, there is a tab called “Directory” or else we can access it via this link. https://hackerone.com/directory/programs . On the Directory page, we can see the number of listed domains to bug bounty scans. Among those domains, we choose a domain we want. A few of the domains that show at the top of this page are listed below. Following the explicit intervention.

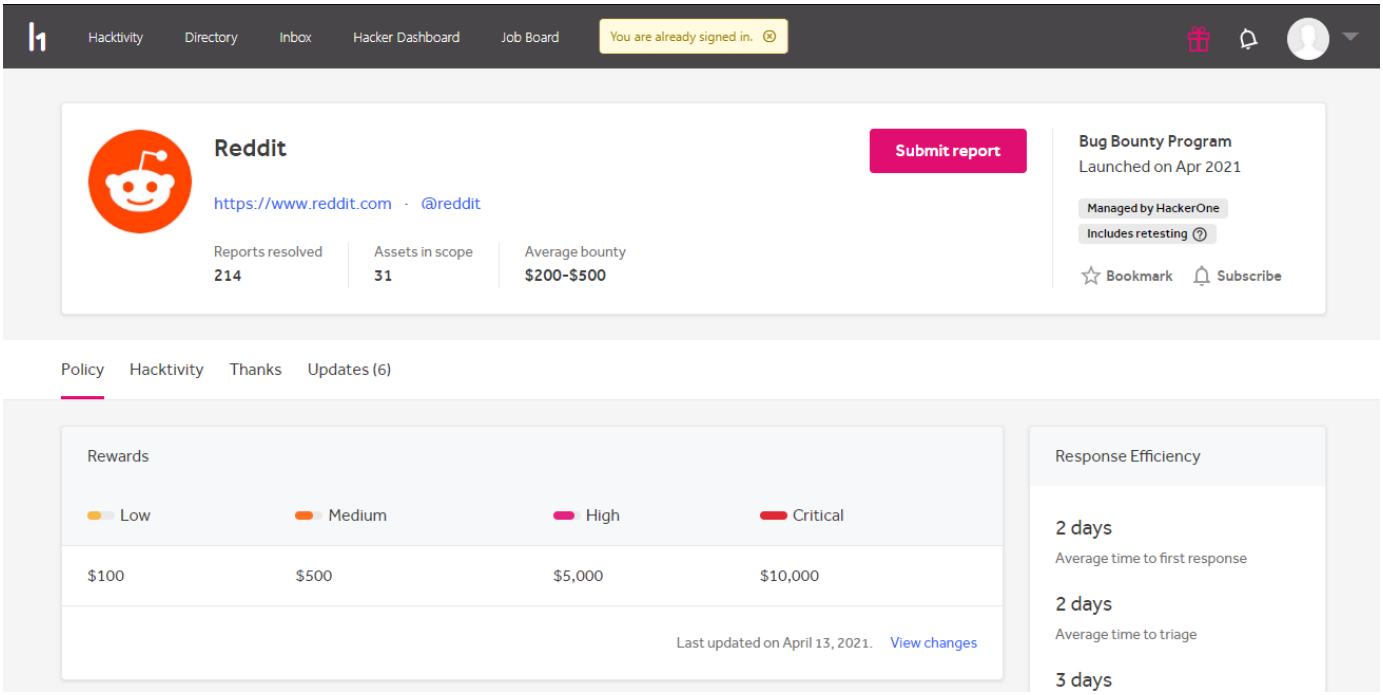


Always look for a goal that encompasses all you're trying to accomplish. What method will you use to locate it? You may locate in-scope items in the program rules by clicking on any of the listed programs and then scrolling

down to the rules, as illustrated in the picture below. There is only one domain in the scope item, so you only have to look for problems in one place. Because this software is now available to everyone, it will be used by many other hunters, reducing your success rate. We need a bigger target since so many individuals are currently hunting on this program. We must identify a more expansive goal. Consider what's shown in the illustration below.

Selected Domain

After successful research, I selected a domain **https://www.reddit.com**. They provide understandable information about their domain.



About Reddit

Reddit is a news aggregation, content rating, and conversation platform based in the United States. Site visitors vote up or down material submitted by registered users such as links, text entries, pictures, and video clips. Messages are categorized into "communities" or "subreddits" that are established by users and cover a wide range of subjects, including politics, religion, science, movies, video games (including online ones), music, literature,

sports, fitness, cuisine, and picture sharing. The more upvotes a post receives, the higher it will appear in the subreddit, and if there are enough of them, on the main page of the site itself. Reddit administrators monitor the communities and shut or limit them on occasion because of harassment, even though the site's rules forbid it. Reddit moderators, who are not regarded to be workers, may also be seen moderating in particular communities.

Policy Analyzing

In HackerOne they gave us what are the policies and other information. So before starting technical perspectives we have to analyze their terms and conditions. We need to gather the information about the website and study about their policy well because if we do some illegal thing, they might take some legal action against us.

Scope

All bug bounty programs have their own scope as a hunter we must know what the In-scope and Out-of-Scope is. This part explains how to report a problem and outline the program's disclosure policy, as well as other important information. Because incorrect disclosure (for example, publicly revealing a bug without authorization when authorization is needed) may result in unwelcome consequences for both you and the client, it is critical that you understand the policy statement of a system.

Out-of-Scope

1. Attacks requiring physical access to, root privileges on, or MITM of a user's device.
2. Account Oracles - the ability to determine if an email address or username is in use.
3. Attacks targeting outdated browsers or browsers other than Firefox, Chrome, or Safari.
4. Insecure cookie settings/flags on non-login cookies.
5. Missing HTTP security headers (CSP, HSTS, etc.).
6. Weak SSL/TLS/SSH algorithms or protocols.
7. Lack of certificate pinning (improper certificate validation still eligible)
8. CSRF with no security impact (unauthenticated/logout/login CSRF).
9. Best practices violations (password complexity, expiration, re-use, etc.).
10. Clickjacking on pages with no sensitive actions.
11. Component version disclosure without accompanying proof of the vulnerability.
12. Previously known vulnerable libraries without a working Proof of Concept.
13. 0-days in open source/vendor products - give us a chance to fix it on our own, if we missed it then it's fair game.
14. Disclosure of internal tracebacks (unless sensitive environment data is also leaked).
15. Comma Separated Values (CSV) injection.

16. Reflected file download.
17. Content spoofing and text injection issues without being able to modify HTML/CSS.
18. Re-usage of passwords from public dumps.
19. Homograph links.
20. Mobile app crashes.
21. Tab nabbing / window. Origin not being cleared on new tabs or windows
22. Deep links for Android missing auto Verify=true due to current Google limitation with AMP (may change in future)

Out-of-Scope Domains

Any SaaS or other service provider is not explicitly called out. If you think it's something owned by Reddit, you can send it along - we'll decide if it's out-of-scope.

In-Scope Domains (inclusive of all subdomains)

1. reddit.com
2. snooguts.net
3. redd.it
4. redditblog.com
5. redditmedia.com
6. redditstatic.com
7. redditgifts.com
8. reddituploads.com
9. redditinc.com
10. reddithelp.com (limited)
11. dubsmash.com
12. 1st party Android and iOS apps for Reddit and Dub smash

Information Gathering

The act of collecting various types of information on the intended victim or system is known as information gathering. ... Numerous tools, methods, and websites are available to hackers for information gathering, including Whois, nslookup, among others.

Information Gathering Types

There are two types of Information Gathering

1. Active Information Gathering

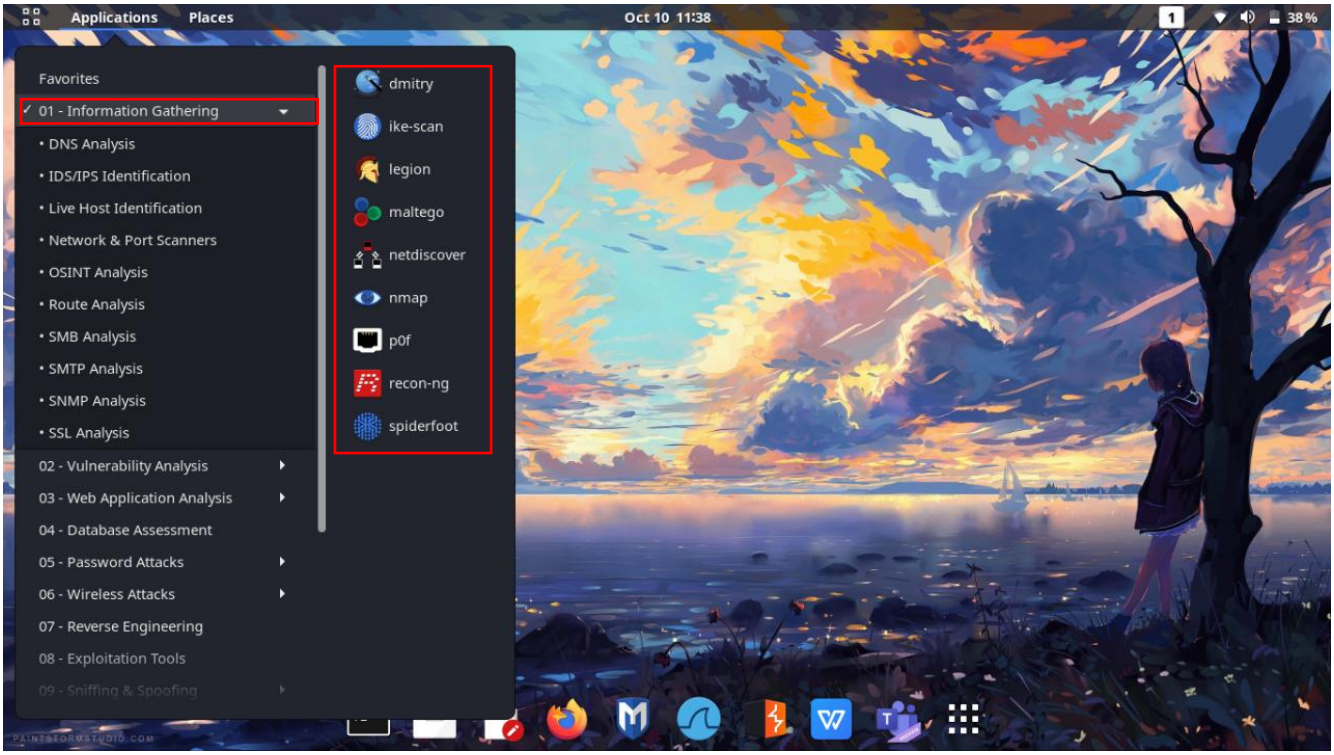
We can learn more about these targets by actively engaging with them, which is known as passive information gathering. Unlike passive information collecting, however, doing so without permission may be a criminal offence in certain countries. DNS Enumeration, Port Scanning, and OS Fingerprinting are all methods that may be used. Active information collecting aims to acquire as much information as possible, which is similar to passive information gathering.

2. Passive Information Gathering

Using publicly accessible information, we do passive information collection regarding our aims (resources). The search engine results and who-is information may be put to good use. In order to acquire as much knowledge about the subject as possible, the objective must be achieved.

Information Gathering Tools

There are Number of tools to information gathering tools in Kali Linux.

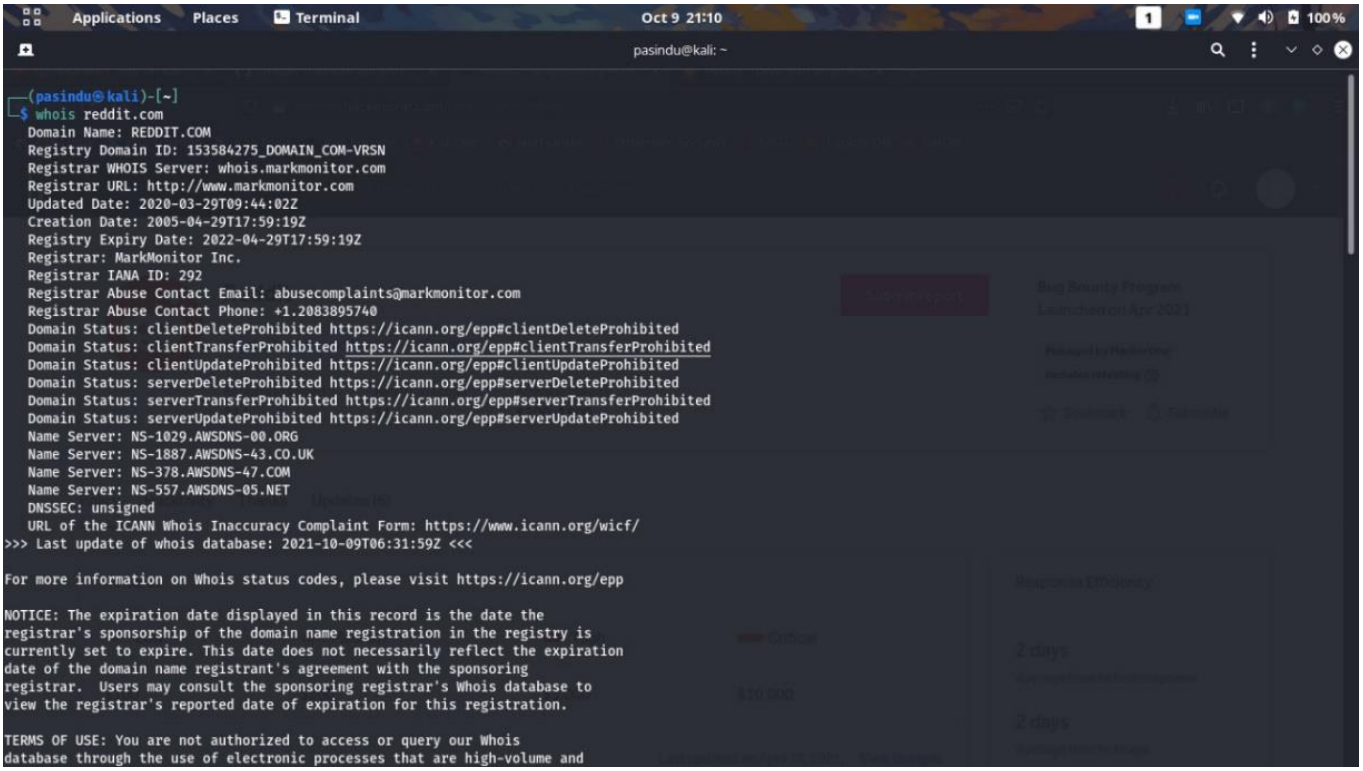


whois command

When it comes to providing Internet consumers with information services, WHOIS is a standard query and answer protocol built on top of TCP. Name Servers, IP address blocks, and a broad variety of other information services are included in the information returned by this service. In Linux, WHOIS is a client for connecting with the WHOIS server (or database server) through the well-known port number 43, which saves and understandably transmits database information for humans.

Results

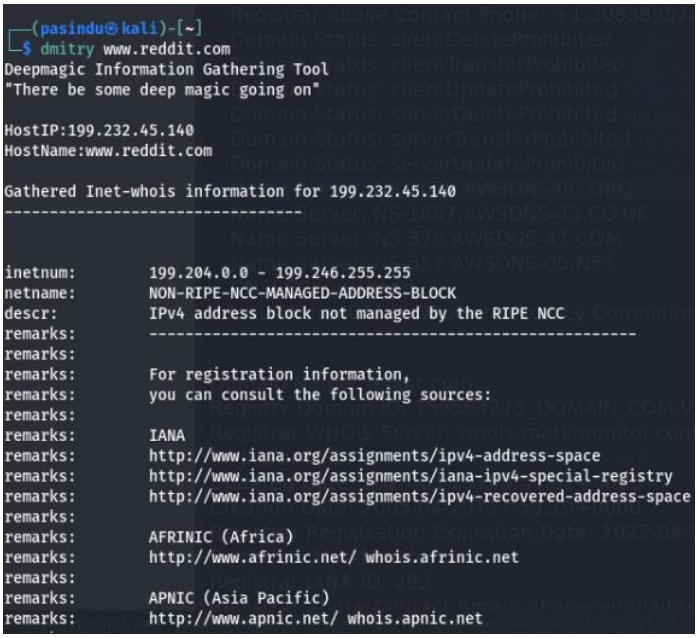
$ whois reddit.com



Dmitry Tool

To gather information about Deepmagic, you may use DMitry (Deepmagic Information Gathering Tool), a UNIX/(GNU)Linux Command Line Application written in C. There are no limits to what DMitry may learn about a host. Several built-in features may help you find potential subdomains, emails, uptime statistics, tcp port scans, and even whois lookups.

Results



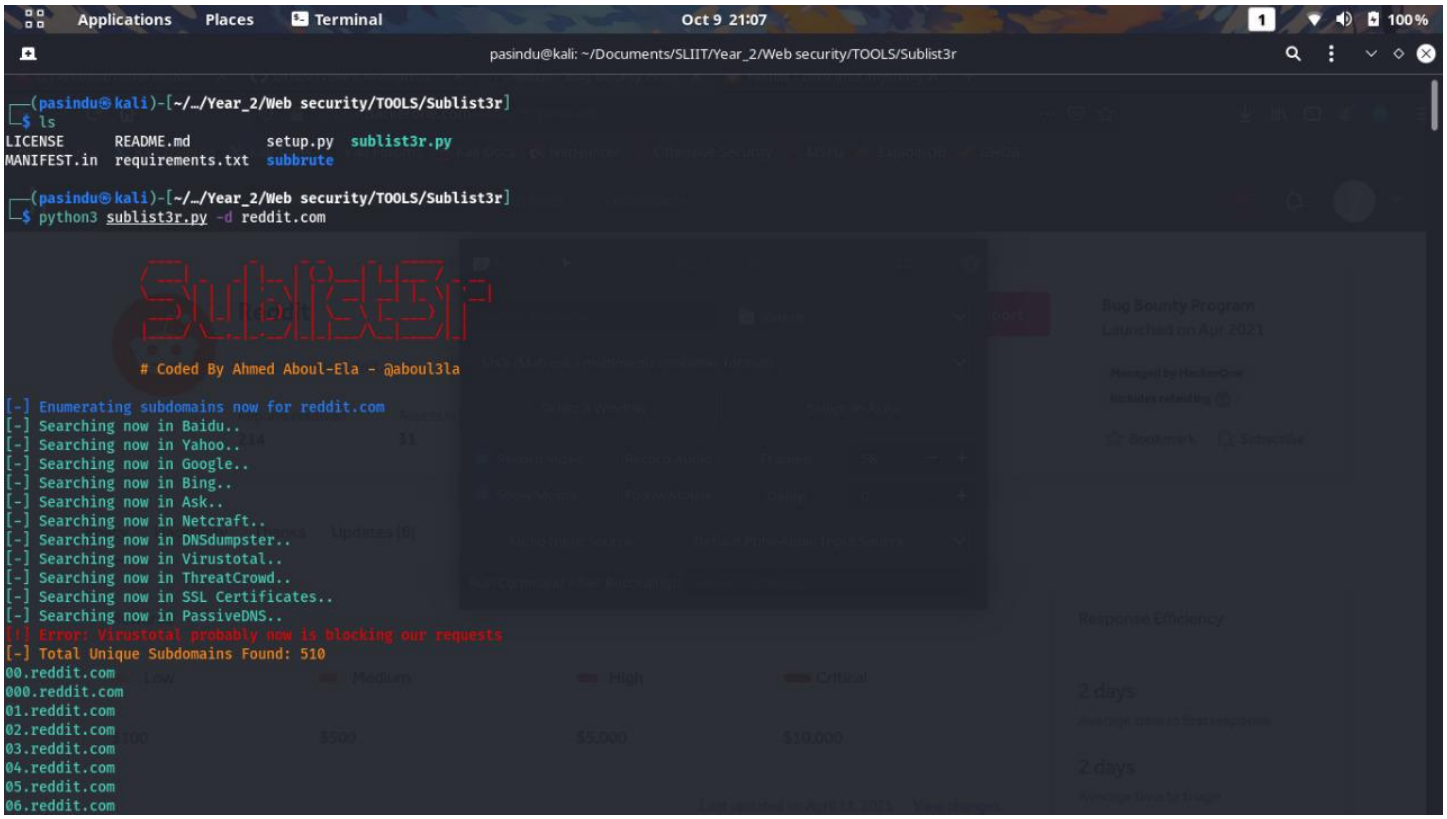
Sublister Tool

Sublist3r is a search and listing tool for subdomains that makes it simple to use. Virustotal and Netcraft are just a few of the search engines and databases that Sublist3r makes use of. DNSdumpster, ThreatCrowd, and ReverseDNS are some of the most well-known sources. Due to the integration of Sublist3r and subbrute, the option to use brute force has been introduced to Sublist3.

Sublisert Install & run

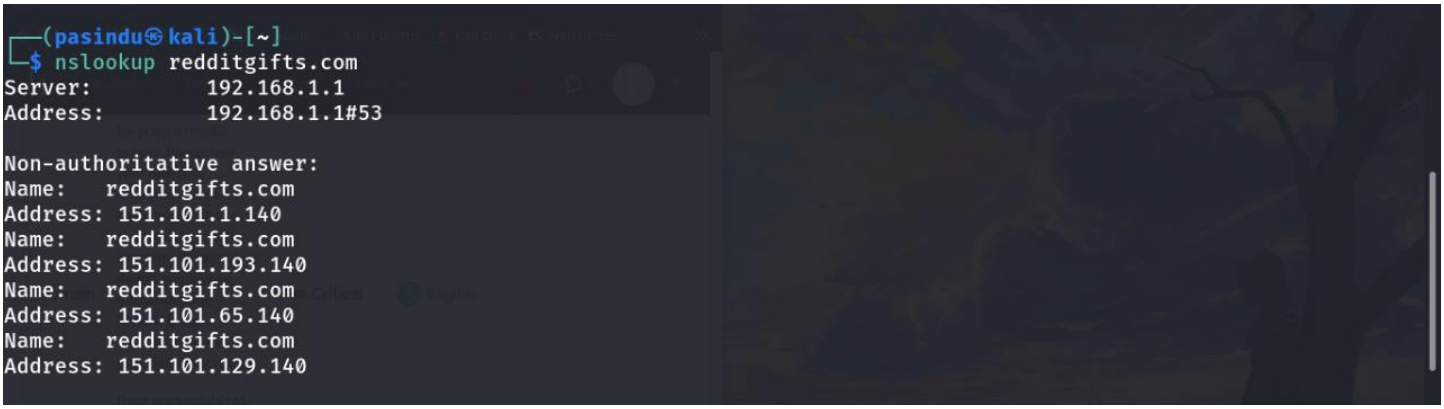
1. ***git clone https://github.com/aboul3la/Sublist3r.git***
2. ***cd Sublist3r/***
3. ***sudo pip install -r requirements.txt***
4. ***sudo apt-get install python-requests***
5. ***sudo apt-get install python-dnspython***
6. ***sudo apt-get install python-argparse***
7. ***python3 sublist3r.py -d reddit.com***

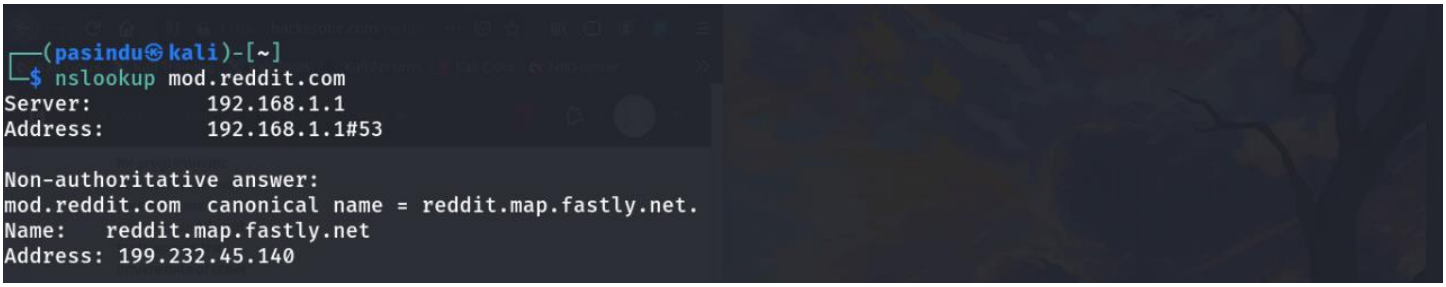
Results

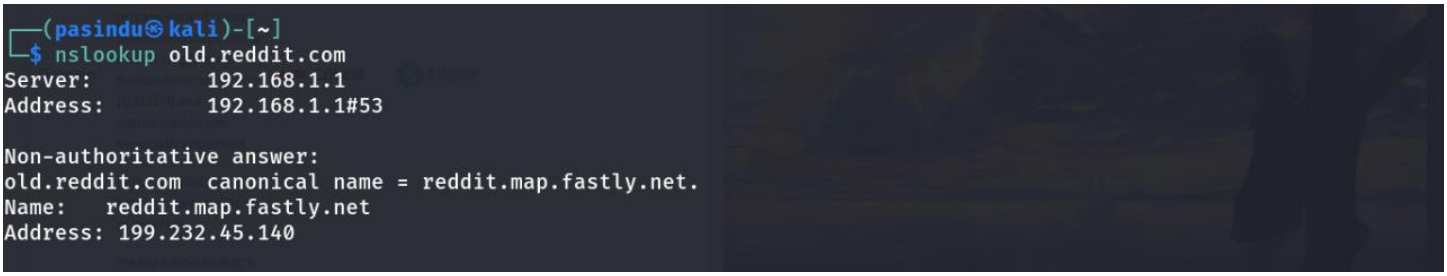


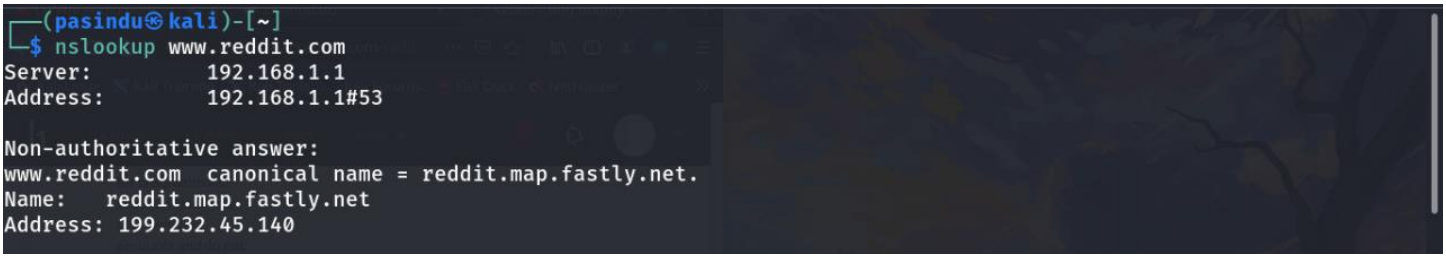
Nslookup

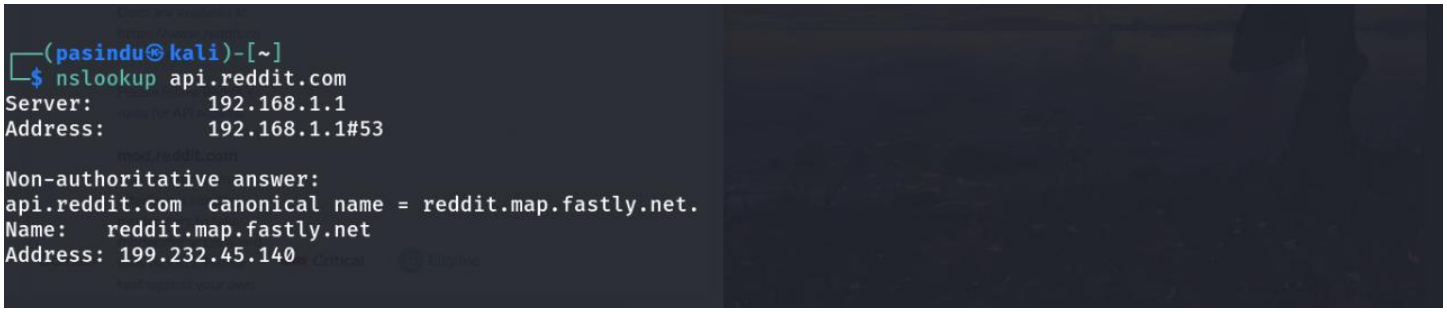
Nslookup is a command-line tool for network management that is tiny in size but packs a big punch. This app has a basic user interface, but it is very helpful, nevertheless. There are several common computer operating systems that include the Nslookup command, including as Windows, Mac OS X, and many Linux distributions. Domain names and IP addresses, as well as any other DNS Records, may be obtained by running queries against the DNS server.

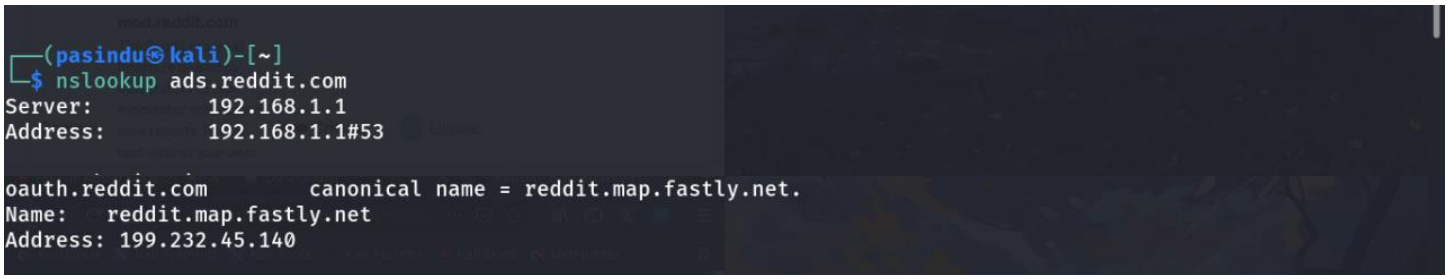


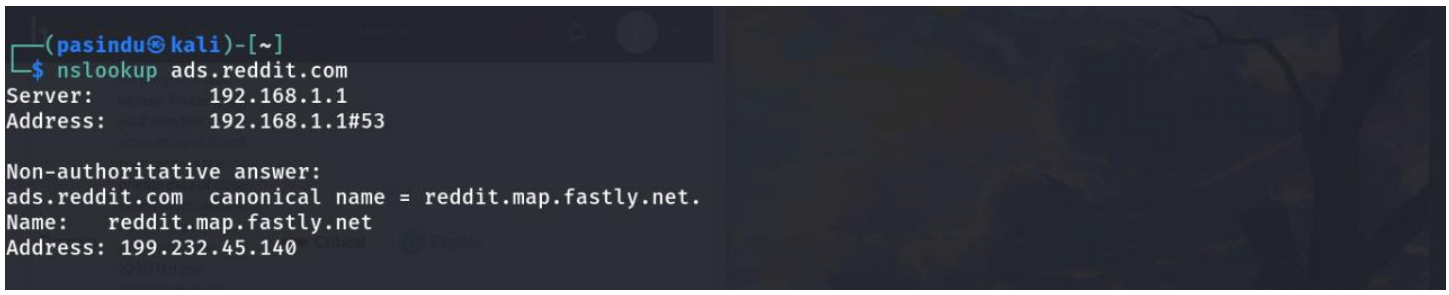


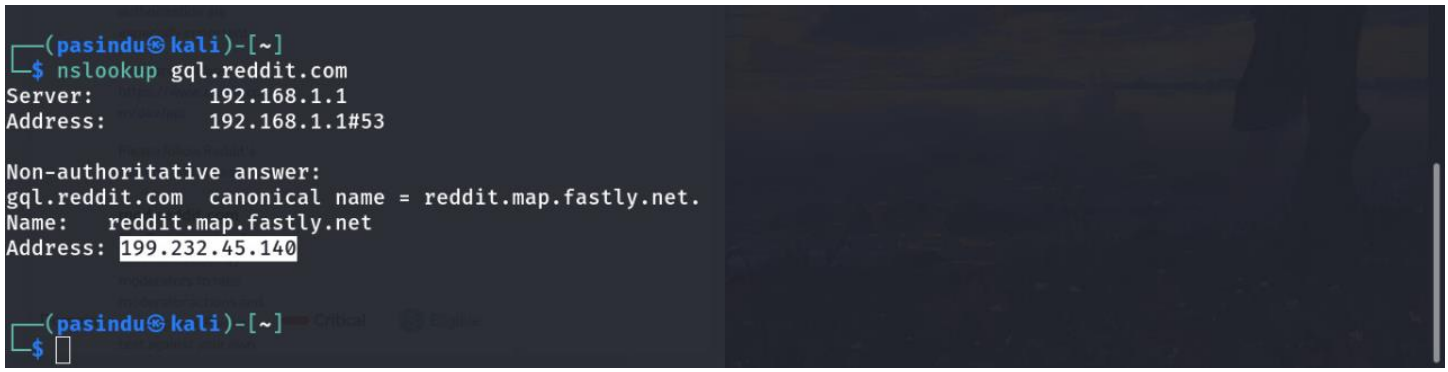












I scan number of domains with using nslookup command. All domains have same DNS server.

Whatweb Tool

WhatWeb is a website that recognizes webpages. In addition to content management systems (CMS), blogging platforms, statistical and analytic packages, JavaScript libraries, web servers, and embedded devices are all recognized by the standards body. WhatWeb offers approximately 900 plugins, each of which is designed to recognize something specific. Other information that is identified includes version numbers, email addresses, account IDs, web framework modules, SQL problems, and other information about the application.

```
┌──(pasindu㉿kali)-[~]
└─$ whatweb old.reddit.com
http://old.reddit.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[snooserv], IP[199.232.45.14
0], RedirectLocation[https://old.reddit.com/], UncommonHeaders[retry-after], Via-Proxy[1.1 varnish]
https://old.reddit.com/ [200 OK] Cookies[csv,edgebucket,loid,session_tracker], Country[UNITED STATES][US], HTML5
, HTTPServer[snooserv], IP[199.232.45.140], OpenSearch[/static/opensearch.xml], PasswordField[passwd], Script[te
xt/javascript,text/template], Strict-Transport-Security[max-age=15768000, max-age=15552000; includeSubDomains; p
reload], Title[reddit: the front page of the internet], UncommonHeaders[x-content-type-options,x-moose], Via-Pro
xy[1.1 varnish], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block]
http://redditgifts.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[151.101.65.14
0], RedirectLocation[https://www.redditgifts.com/], Strict-Transport-Security[max-age=31536000; includeSubdomain
s], UncommonHeaders[retry-after,x-content-type-options], Varnish, Via-Proxy[1.1 varnish], X-Frame-Options[SAMEOR
IGIN], X-XSS-Protection[1; mode=block]
https://www.redditgifts.com/ [200 OK] Cookies[ause,csrftoken,sessionid], Country[UNITED STATES][US], Django, Goo
gle-Analytics[UA-11645097-1], HTML5, HttpOnly[sessionid], IP[199.232.45.140], JQuery[2.0.3], Open-Graph-Protocol
[website][291585047533359], Script[text/javascript], Strict-Transport-Security[max-age=31536000; includeSubdomai
ns], Title[reddit gift exchanges and more! - redditgifts], UncommonHeaders[x-content-type-options], Via-Proxy[1.
1 varnish], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
```

```
┌──(pasindu㉿kali)-[~]
└─$ whatweb redditgifts.com
http://redditgifts.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[151.101.65.14
0], RedirectLocation[https://www.redditgifts.com/], Strict-Transport-Security[max-age=31536000; includeSubdomain
```

```
┌──(pasindu㉿kali)-[~]
└─$ whatweb new.reddit.com
http://new.reddit.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[199.232.45.140
], RedirectLocation[https://new.reddit.com/], UncommonHeaders[retry-after], Varnish, Via-Proxy[1.1 varnish]
https://new.reddit.com/ [200 OK] Cookies[csv,loid,session_tracker,token_v2], Country[UNITED STATES][US], HTML5,
HttpOnly[token_v2], IP[199.232.45.140], Open-Graph-Protocol[website], Script[application/json,application/ld+jso
n], Title[Reddit - Dive into anything], Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN]
```

```
┌──(pasindu㉿kali)-[~]
└─$ whatweb www.reddit.com
http://www.reddit.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[snooserv], IP[199.232.45.14
0], RedirectLocation[https://www.reddit.com/], UncommonHeaders[retry-after,x-clacks-overhead], Via-Proxy[1.1 var
nish]
```

```
┌──(pasindu㉿kali)-[~]
└─$ whatweb api.reddit.com
http://api.reddit.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[snooserv], IP[199.232.45.14
0], RedirectLocation[https://api.reddit.com/], UncommonHeaders[retry-after,x-clacks-overhead], Via-Proxy[1.1 var
nish]
https://api.reddit.com/ [200 OK] Cookies[csv,edgebucket,loid,session_tracker], Country[UNITED STATES][US], HTTPS
erver[snooserv], IP[199.232.45.140], Strict-Transport-Security[max-age=15552000; includeSubDomains; preload], Un
commonHeaders[x-content-type-options,x-ratelimit-remaining,x-ratelimit-used,x-ratelimit-reset,access-control-all
ow-origin,access-control-expose-headers,x-moose,x-clacks-overhead], Via-Proxy[1.1 varnish], X-Frame-Options[SAME
ORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block]
```

```
Applications  Places  Terminal   Oct 13 23:06   1   96%
pasindu@kali: ~
┌──(pasindu㉿kali)-[~]
└─$ whatweb oauth.reddit.com
http://oauth.reddit.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[snooserv], IP[199.232.45.
140], RedirectLocation[https://oauth.reddit.com/], UncommonHeaders[retry-after,x-clacks-overhead], Via-Proxy[1.1
 varnish]
https://oauth.reddit.com/ [403 Forbidden] Cookies[csv,edgebucket], Country[UNITED STATES][US], HTTPServer[snoose
rv], IP[199.232.45.140], Strict-Transport-Security[max-age=15552000; includeSubDomains; preload], UncommonHeader
s[x-clacks-overhead], Via-Proxy[1.1 varnish]
```

```
┌──(pasindu㉿kali)-[~]
└─$ whatweb gql.reddit.com
http://gql.reddit.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[199.232.45.140
], RedirectLocation[https://graphql.kubernetes.ue1.snooguts.net/], Strict-Transport-Security[max-age=31536000; i
ncludeSubdomains], UncommonHeaders[retry-after,x-content-type-options], Varnish, Via-Proxy[1.1 varnish], X-Frame
-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
https://graphql.kubernetes.ue1.snooguts.net/ [303 See Other] Country[UNITED STATES][US], HTTPServer[nginx], IP[3
.233.173.237], RedirectLocation[https://auth-all.kubernetes.ue1.snooguts.net/oauth2/start?rd=%2Fgraphql.kubernet
es.ue1.snooguts.net/], Strict-Transport-Security[max-age=16070400; includeSubDomains], Title[303 See Other], X-F
rame-Options[SAMEORIGIN], nginx
https://auth-all.kubernetes.ue1.snooguts.net/oauth2/start?rd=%2Fgraphql.kubernetes.ue1.snooguts.net/ [302 Found]
 Country[UNITED STATES][US], HTTPServer[nginx], IP[3.233.173.237], RedirectLocation[https://accounts.google.com/
o/oauth2/auth?access_type=offline&approval_prompt=force&client_id=531682288848-oulcmcmfq2jmmecb7pp9kobdmrutqhq6.
apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fauth-all.kubernetes.ue1.snooguts.net%2Foauth2%2Fcallback&r
esponse_type=code&scope=profile+email], Strict-Transport-Security[max-age=16070400; includeSubDomains], X-Frame-
Options[DENY], nginx
https://accounts.google.com/o/oauth2/auth?access_type=offline&approval_prompt=force&client_id=531682288848-oulcm
cmfq2jmmecb7pp9kobdmrutqhq6.apps.googleusercontent.com&redirect_uri=https%3A%2F%2Fauth-all.kubernetes.ue1.snoogu
ts.net%2Foauth2%2Fcallback&response_type=code&scope=profile+email [302 Found] Cookies[__Host-GAPS], Country[UNIT
ED STATES][US], probably Google-Search-Appliance, HTTPServer[GSE], HttpOnly[__Host-GAPS], IP[74.125.24.84], Redi
rectLocation[https://accounts.google.com/signin/oauth/error?authError=Cg9pbnZhbGlkX3JlcXVlc3QS3gEKWW91IGNhbid0IH
NpZ24gaW4gdG8gdGhpcyBhcHAgYmVjYXVzZSBpdCBkb2Vzbid0IGNvbXBseSB3aXRoIEdvb2dsZSdzIE9BdXRoIDIuMCBwb2xpY3kgZm9yIGtlZX
BpbmcgYXBwcyBzZWN1cmUuCgpZb3UgY2FuIGxldCB0aGUgYXBwIGRldmVsb3BlciBrbm93IHRoYXQgdGhpcyBhcHAgZG9lc24ndCBjb21wbHkgd2
l0aCBvbmUgb3IgbW9yZSBHb29nbGUgdmFsaWRhdGlvbiBydWxlcy4KICAaWWh0dHBzOi8vZGV2ZWxvcGVycy5nb29nbGUuY29tL2lkZW50aXR5L3
Byb3RvY29scy9vYXV0aDIvcG9saWNpZXMjc2VjdXJlLXJlc3BvbnNlLWhhbmRsaW5nIJADKlYKDHJlZGlyZWN0X3VyaRJGaHR0cHMlM0ElMkYlMk
ZhdXRoLWFsbC5rdWJlcm5ldGVzLnVlMS5zbm9vZ3V0cy5uZXQlMkZvYXV0aDIlMkZjYWxsYmFjaw%3D%3D&client_id=531682288848-oulcmc
mfq2jmmecb7pp9kobdmrutqhq6.apps.googleusercontent.com], Strict-Transport-Security[max-age=31536000; includeSubDo
mains], Title[Moved Temporarily], UncommonHeaders[content-security-policy,x-content-type-options,alt-svc], X-Fra
```

```
┌──(pasindu㉿kali)-[~]
└─$ whatweb ads.reddit.com
http://ads.reddit.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Varnish], IP[199.232.45.140
], RedirectLocation[https://ads.reddit.com/], Strict-Transport-Security[max-age=31536000; includeSubdomains], Un
commonHeaders[retry-after,x-content-type-options], Varnish, Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN],
 X-XSS-Protection[1; mode=block]
https://ads.reddit.com/ [502 Bad Gateway] Cookies[csv], Country[UNITED STATES][US], IP[199.232.45.140], Strict-T
ransport-Security[max-age=31536000; includeSubdomains], Title[502 Bad Gateway], UncommonHeaders[x-content-type-o
ptions], Via-Proxy[1.1 varnish], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
```

Analyze Information

According to the information, I gathered, hear I mention some important things that can be useful.

sublister

Total Unique Subdomains Found: 510 (Assets in scope 31)

nslookup

Server: 192.168.1.1

Address: 192.168.1.1#53

Deepmagic Information Gathering Tool

HostIP:199.232.45.140
Hostname: www.reddit.com

Gathered TCP Port information for 199.232.45.140

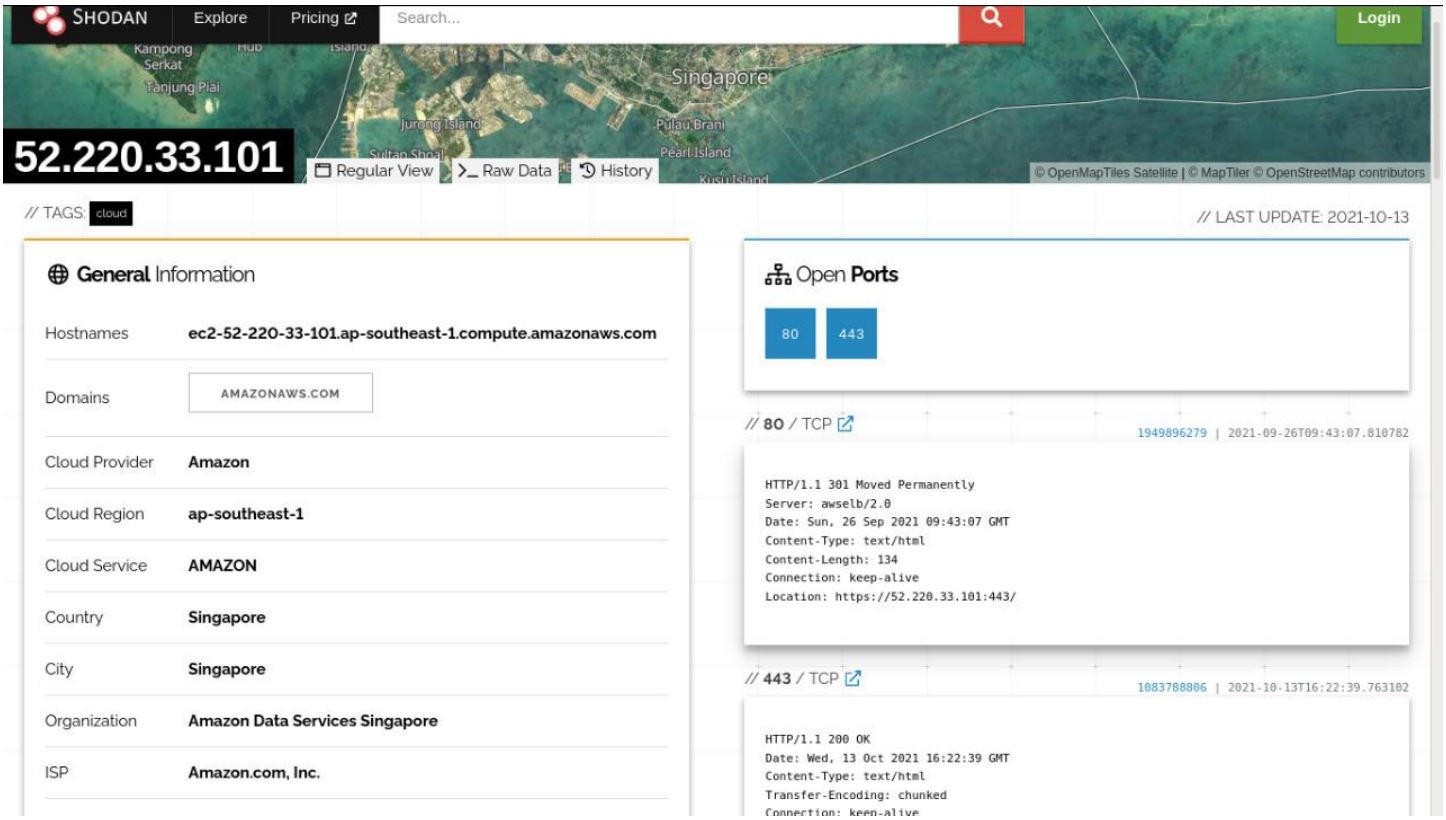
Port	State
25/tcp	open
80/tcp	open

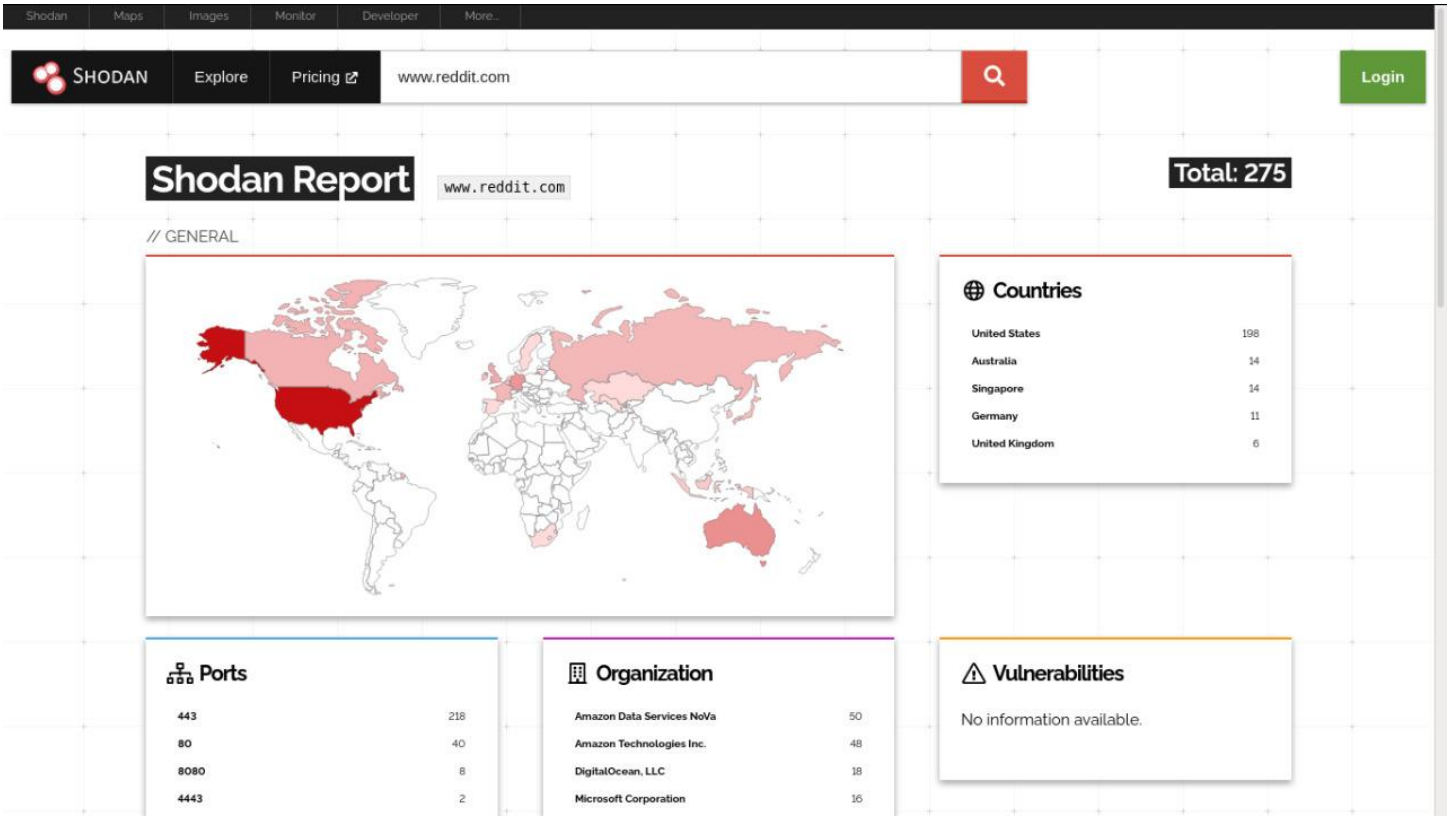
Port scan Finished: Scanned 150 ports, 0 ports were in state closed

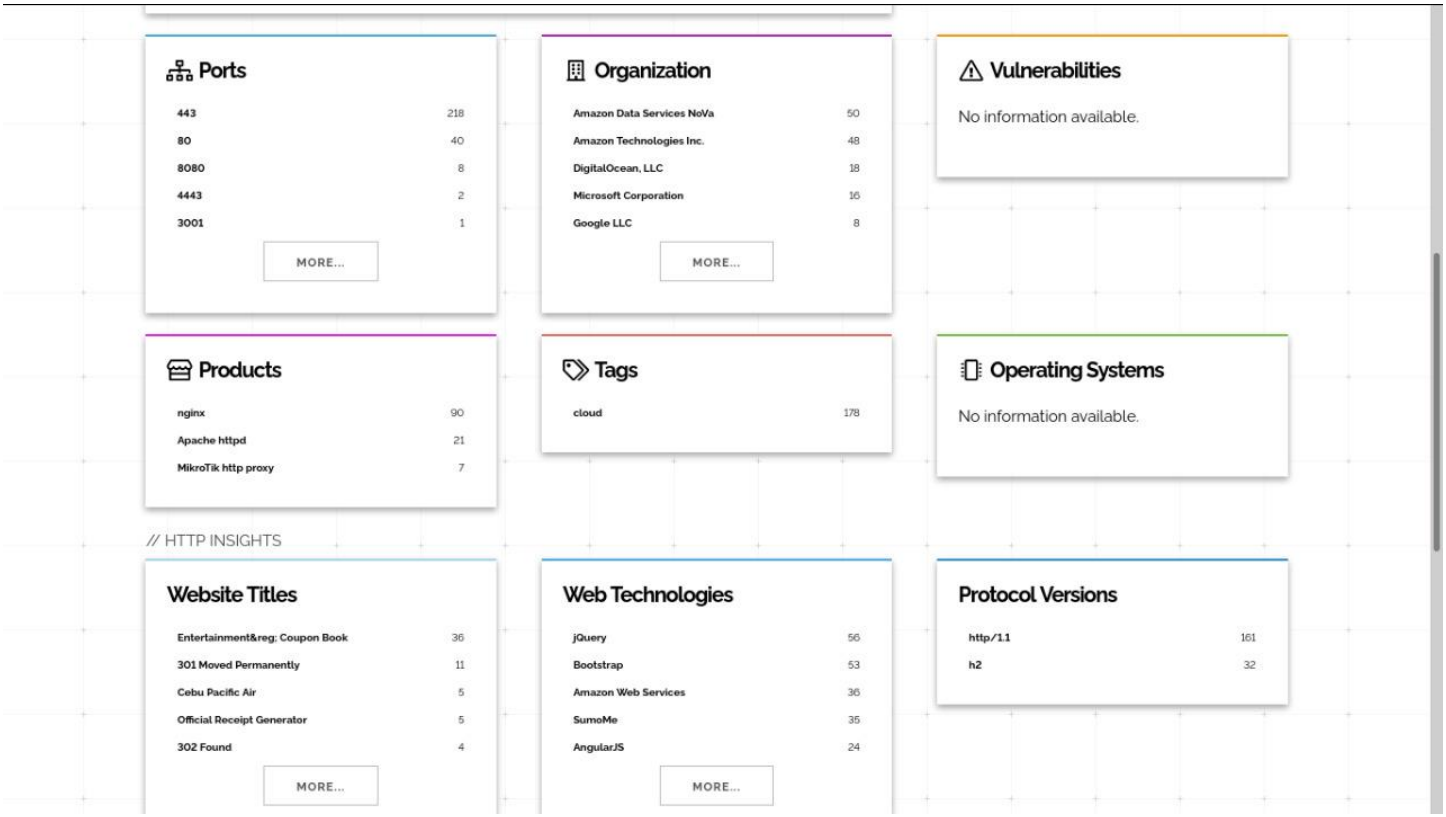
Shodan Report

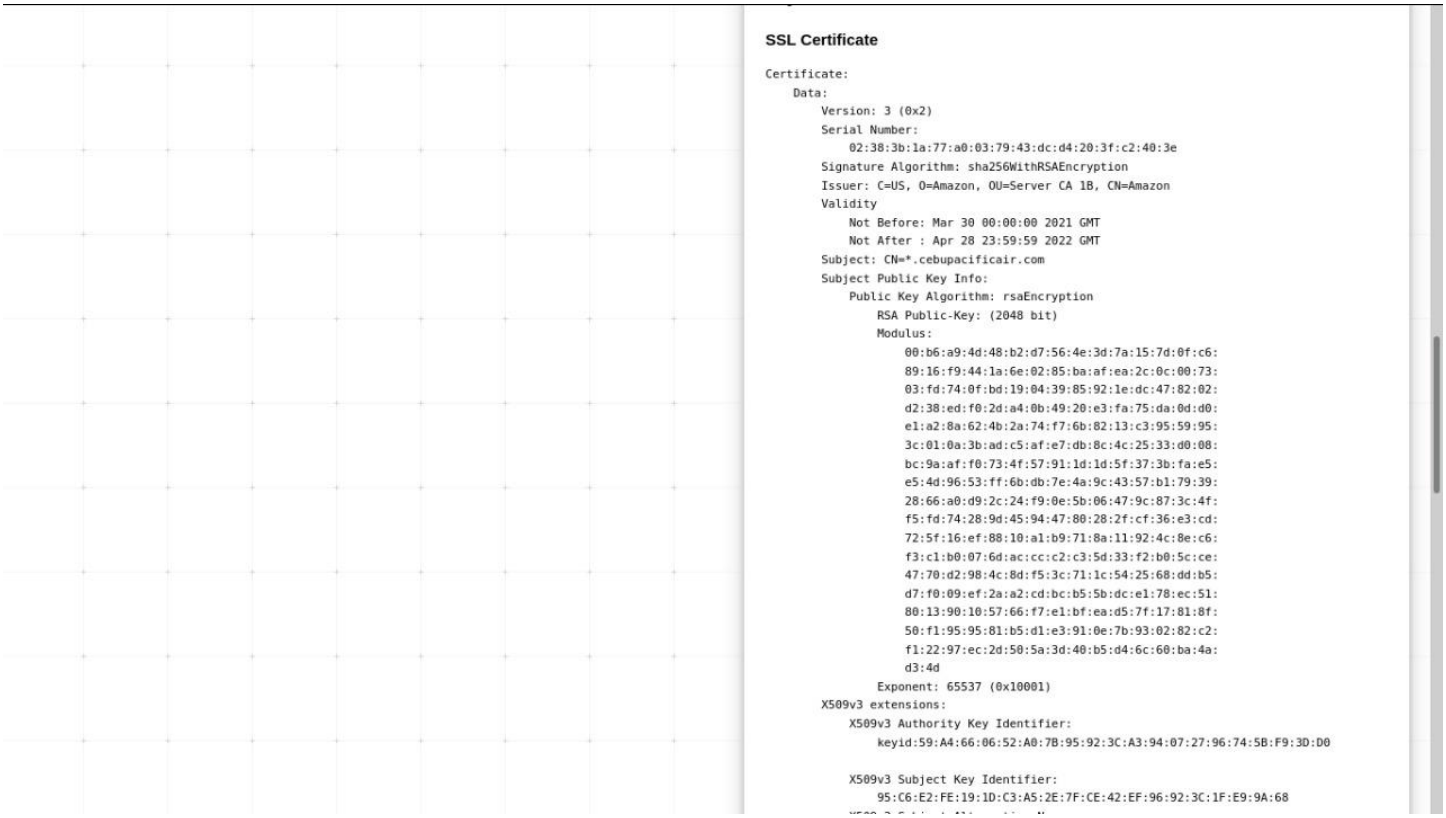
The Internet is made up of many different components, including websites. Power plants, cell phones, refrigerators, and Minecraft servers may all be found with Shodan. Exposure to the Network should be monitored. Always be aware of which gadgets are connected to the Internet and which are not. Shodan helps you remain safe by giving you a complete picture of all exposed services.

Shodan is an online platform that allows users to utilize a number of criteria to find different kinds of internet-connected servers (such as cameras, routers, and servers). Information that the server provides back to the client has also been characterized as a search engine for service banners. A welcome message, server software information, or any other information that the client may discover before communicating with the server might be included in this section.


SHODAN
Explore
Pricing
Search...
Login
Singapore
52.220.33.101
Regular View
Raw Data
History
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
// TAGS: cloud
// LAST UPDATE: 2021-10-13
General Information
Hostnames ec2-52-220-33-101.ap-southeast-1.compute.amazonaws.com
Domains AMAZONAWS.COM
Cloud Provider Amazon
Cloud Region ap-southeast-1
Cloud Service AMAZON
Country Singapore
City Singapore
Organization Amazon Data Services Singapore
ISP Amazon.com, Inc.
Open Ports
80
443
// 80 / TCP
1949896279 | 2021-09-26T09:43:07.810782
HTTP/1.1 301 Moved Permanently
Server: awselb/2.0
Date: Sun, 26 Sep 2021 09:43:07 GMT
Content-Type: text/html
Content-Length: 134
Connection: keep-alive
Location: https://52.220.33.101:443/
// 443 / TCP
1083788806 | 2021-10-13T16:22:39.763102
HTTP/1.1 200 OK
Date: Wed, 13 Oct 2021 16:22:39 GMT
Content-Type: text/html
Transfer-Encoding: chunked


Shodan
Maps
Images
Monitor
Developer
More..
SHODAN
Explore
Pricing
www.reddit.com
Login
Shodan Report
www.reddit.com
Total: 275
// GENERAL
Countries
United States 198
Australia 14
Singapore 14
Germany 11
United Kingdom 6
Ports
443 218
80 40
8080 8
4443 2
Organization
Amazon Data Services NoVa 50
Amazon Technologies Inc. 48
DigitalOcean, LLC 18
Microsoft Corporation 16
Vulnerabilities
No information available.





In showdan report we can see they don't have any vulnerability information. And there is some information about SSL Certificate.

Vulnerability Scanning

When a system or piece of software that runs on it is subjected to vulnerability scanning, security vulnerabilities and weaknesses are discovered. When it comes to vulnerability management, this is an essential part of the overall strategy: protecting the business against data breaches and leaks. Vulnerability scanners work by scanning the attack surface from the person examining it. Using a database of known security vulnerabilities in services and ports, packet building abnormalities, and possible routes to vulnerable applications or scripts, the software checks the attack surface details against the database. The scanning program makes an effort to take advantage of any flaw it finds.

Vulnerability scanning is fundamentally invasive on the running code of the target computer; thus it comes with its own set of dangers when performed. Therefore, problems like failures and reboots may occur throughout the scan, which reduces productivity.

Vulnerability scanning may be done in two ways: authenticated or unauthenticated. An intruder-style scan is used in the unauthenticated technique since the tester has no access to the network. Vulnerabilities found by such an audit are accessible from outside of the network, without having to log in. An authenticated scan reveals vulnerabilities that may be accessed by a trusted user or an invader who has obtained access as a trusted user when the tester signs in as a network user.

Vulnerability Scanning Tools

Vulnerability in web applications There are many types of scanning software available. Scanners scan online applications from the outside in search of security vulnerabilities such as XSS, SQL Injection, CGI-Binding, and Path Traversal.

There are number of tools

- Netsparker
- Rapid7 insightAppSec
- Acunetix Web Vulnerability Scanner
- PortSwigger Burp Suite
- HCL AppScan
- Qualys Web Application Scanner
- Tenable Nessus
- Mister Scanner
- Zap
- Legion
- nmap

Among those number of tools, I focused on Netspaker, Zap, nmap Legion etc.

Nmap Scan

Nmap is the abbreviation for Nmap, which stands for Network Mapper. A Linux command-line program that scans IP addresses and ports in a network and detects installed apps is available as an open-source project. Nmap is a network administration tool that finds out what devices are connected to a network, what ports and services are open, and whether there are any security flaws. Nmap was created by Gordon Lyon (a.k.a. Fyodor) as a tool to help map a network's complete topology and discover open ports and services. Nmap has risen to prominence because of its appearances in films and television shows alike, including The Matrix and Mr. Robot.

Nmap is the scanning tool of choice for security professionals for a variety of reasons. You can rapidly map a network using Nmap since it does not need complicated commands or settings. Simple commands (such checking whether a host is up) and sophisticated programming using the Nmap scripting engine are also supported.

Here is the scan report:

```
# Nmap 7.91 scan initiated Thu Oct 14 00:33:22 2021 as: nmap -sS -iL nmapDomainInScope.txt -oN
nmapscan.txt www.reddit.com
Failed to resolve "snooguts.net".
Failed to resolve "redditstatic.com".
Failed to resolve "reddituploads.com".
Nmap scan report for reddit.com (151.101.193.140)
Host is up (0.010s latency).
Other addresses for reddit.com (not scanned): 151.101.129.140 151.101.1.140 151.101.65.140
Not shown: 997 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap scan report for redd.it (151.101.65.140)
Host is up (0.010s latency).
Other addresses for redd.it (not scanned): 151.101.1.140 151.101.193.140 151.101.129.140
Not shown: 997 filtered ports
PORT    STATE SERVICE
25/tcp  open  smtp
80/tcp  open  http
443/tcp open  https

Nmap scan report for redditmedia.com (3.215.169.224)
Host is up (0.021s latency).
```

rDNS record for 3.215.169.224: ec2-3-215-169-224.compute-1.amazonaws.com
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for reddithelp.com (151.101.1.140)
Host is up (0.010s latency).
Other addresses for reddithelp.com (not scanned): 151.101.65.140 151.101.193.140 151.101.129.140
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for dubsmash.com (104.22.2.66)
Host is up (0.0074s latency).
Other addresses for dubsmash.com (not scanned): 172.67.40.141 104.22.3.66 2606:4700:10::6816:342
2606:4700:10::6816:242 2606:4700:10::ac43:288d
Not shown: 995 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https
8080/tcp open http-proxy
8443/tcp open https-alt

Nmap scan report for api.reddit.com (199.232.45.140)
Host is up (0.0092s latency).
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for redditblog.com (151.101.193.140)
Host is up (0.012s latency).
Other addresses for redditblog.com (not scanned): 151.101.129.140 151.101.1.140 151.101.65.140
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for redditgifts.com (151.101.65.140)
Host is up (0.013s latency).
Other addresses for redditgifts.com (not scanned): 151.101.1.140 151.101.193.140 151.101.129.140
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for mod.reddit.com (199.232.45.140)
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for redditinc.com (151.101.193.140)
Host is up (0.015s latency).
Other addresses for redditinc.com (not scanned): 151.101.129.140 151.101.65.140 151.101.1.140
2a04:4e42:200::396 2a04:4e42:600::396 2a04:4e42::396 2a04:4e42:400::396
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for ads.reddit.com (199.232.45.140)
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for gql.reddit.com (199.232.45.140)
Host is up (0.014s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for accounts.reddit.com (199.232.45.140)
Host is up (0.014s latency).

Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for gateway.reddit.com (199.232.45.140)
Host is up (0.015s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for strapi.reddit.com (199.232.45.140)
Host is up (0.014s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

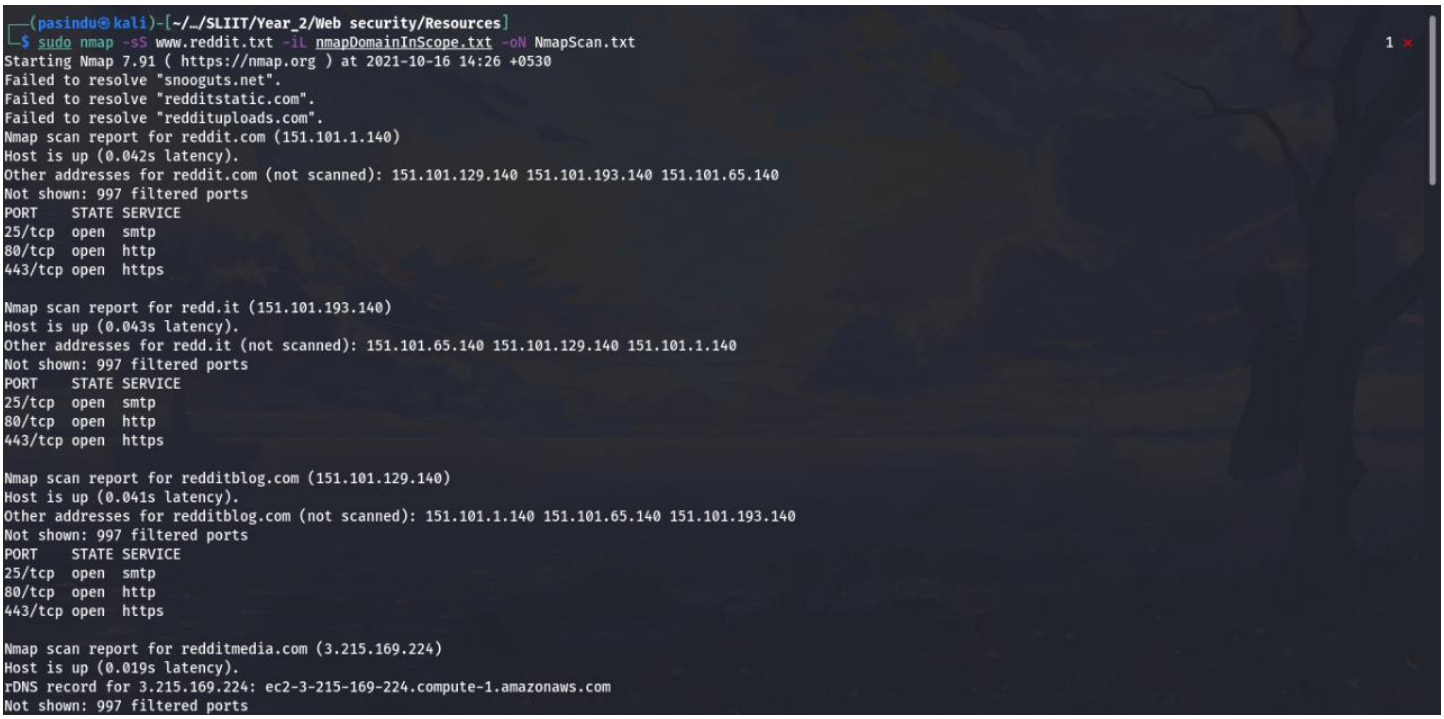
Nmap scan report for m.reddit.com (199.232.45.140)
Host is up (0.014s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for amp.reddit.com (199.232.45.140)
Host is up (0.013s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap done at Thu Oct 14 00:34:29 2021 -- 17 IP addresses (17 hosts up) scanned in 67.17 seconds

Hear, I scan 17 Domains in my scope, and I identified 25, 80, 443 are opened. I input all domains at ones with using this command,

nmap -sS www.reddit.com -iL inscopedomain.txt -oN nampresult.txt



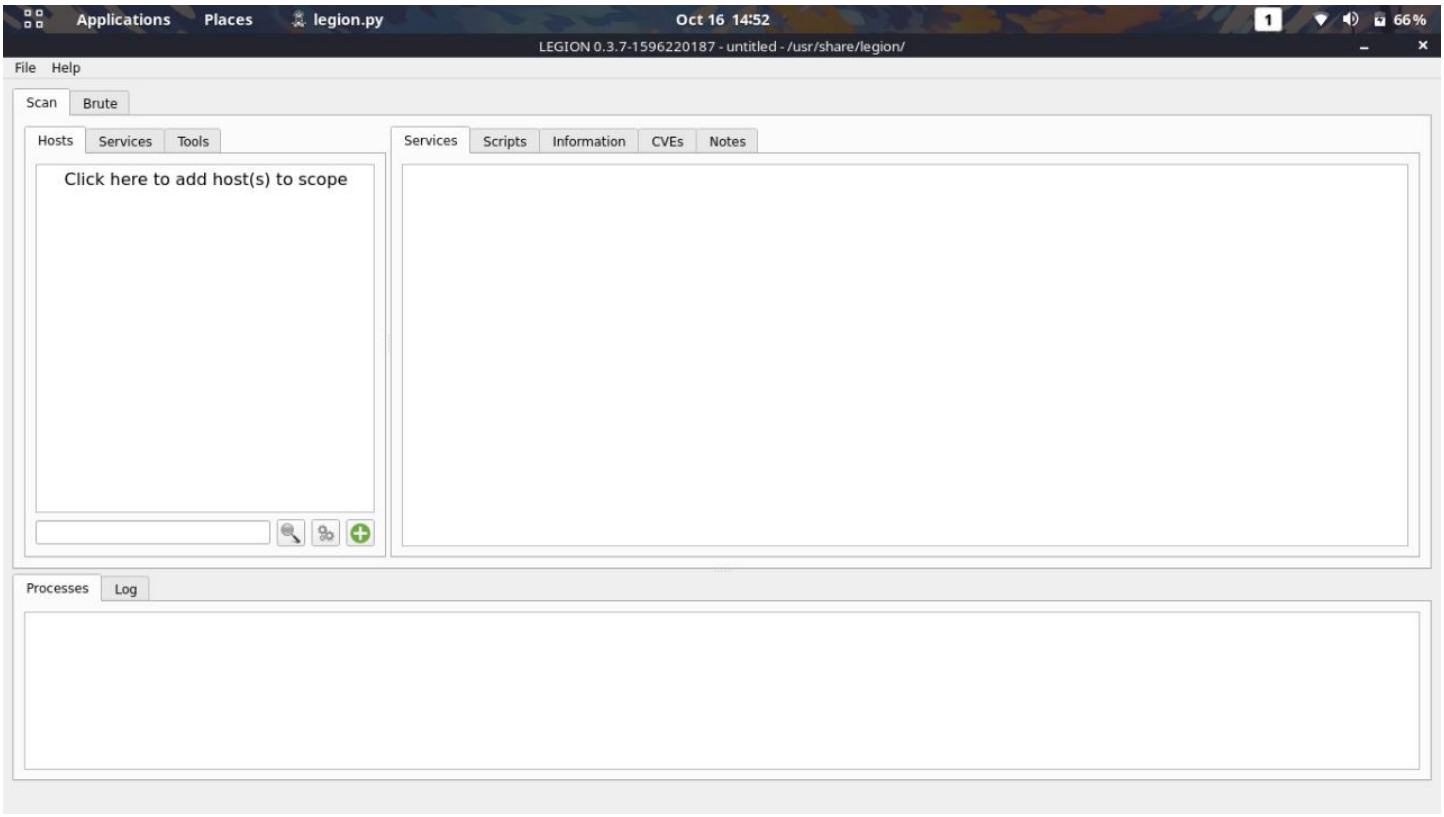
Legion Tool

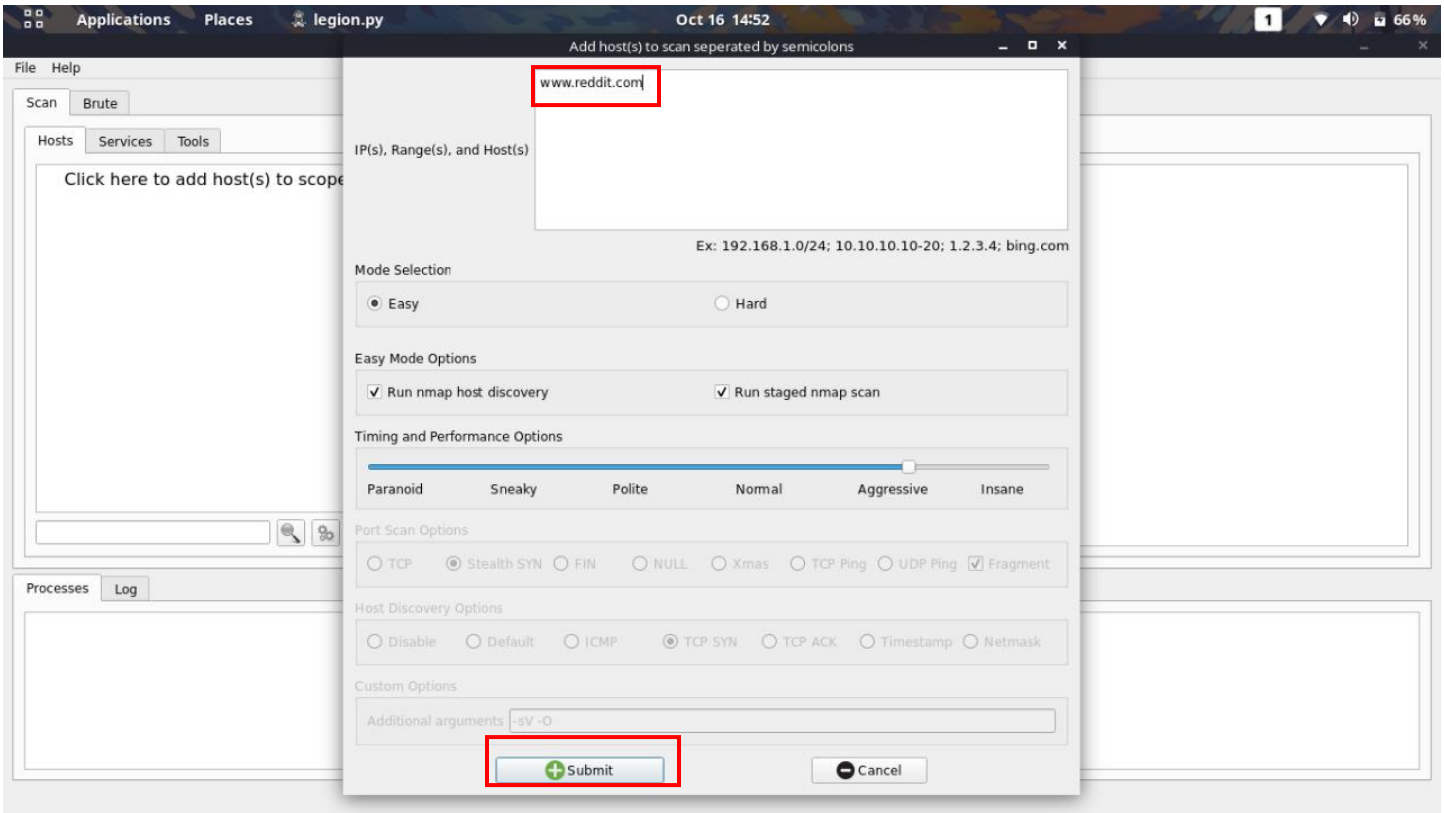
Legion is a network penetration testing platform that is super-extensible and semi-automated. Legion is incredibly simple to use. Pen testers may easily discover and exploit attack vectors on hosts using a GUI with panels and a vast number of options. It features a function that saves project outcomes and tasks in real time.

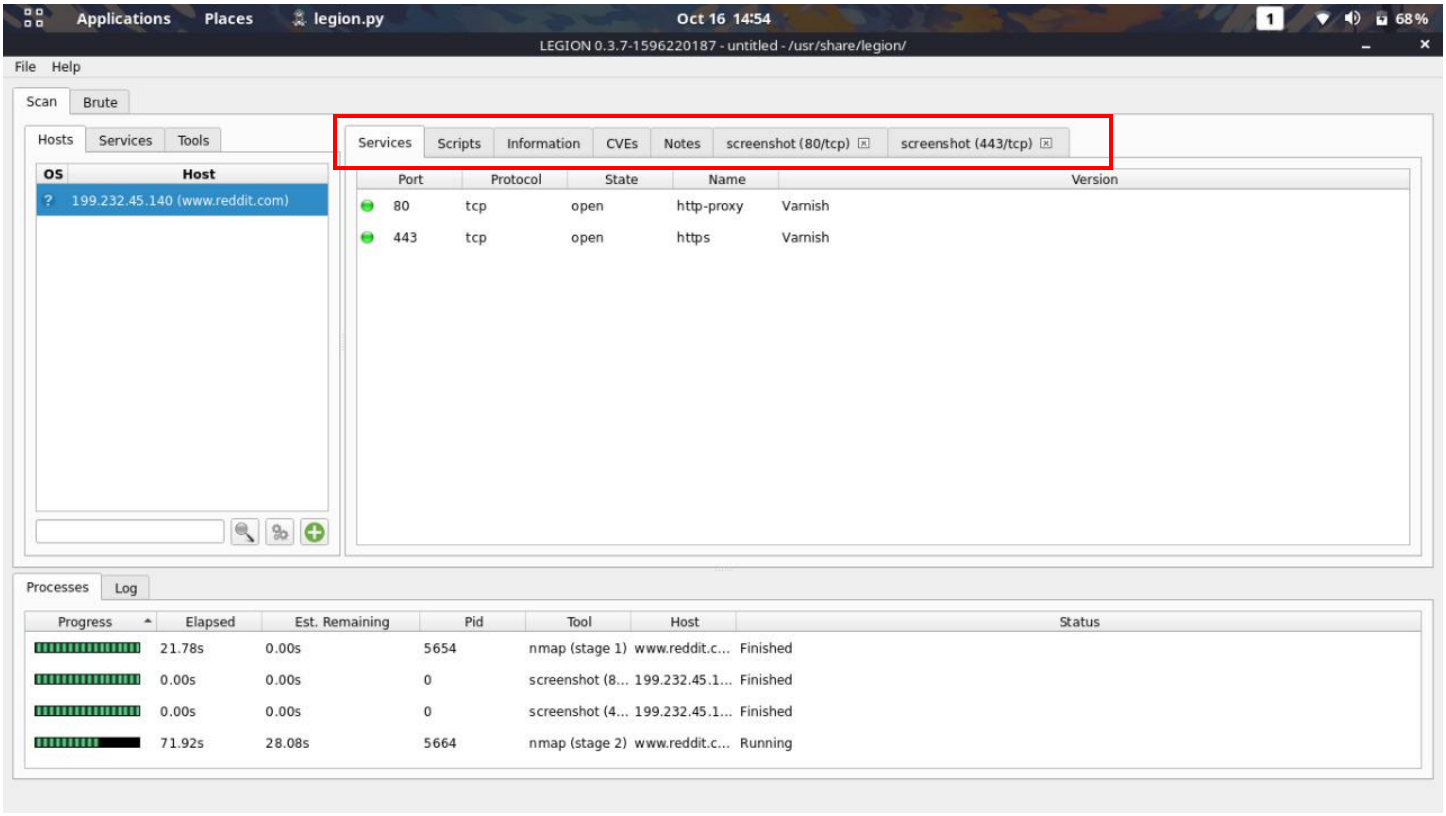
Legion also includes features like as automatic recon and scanning using

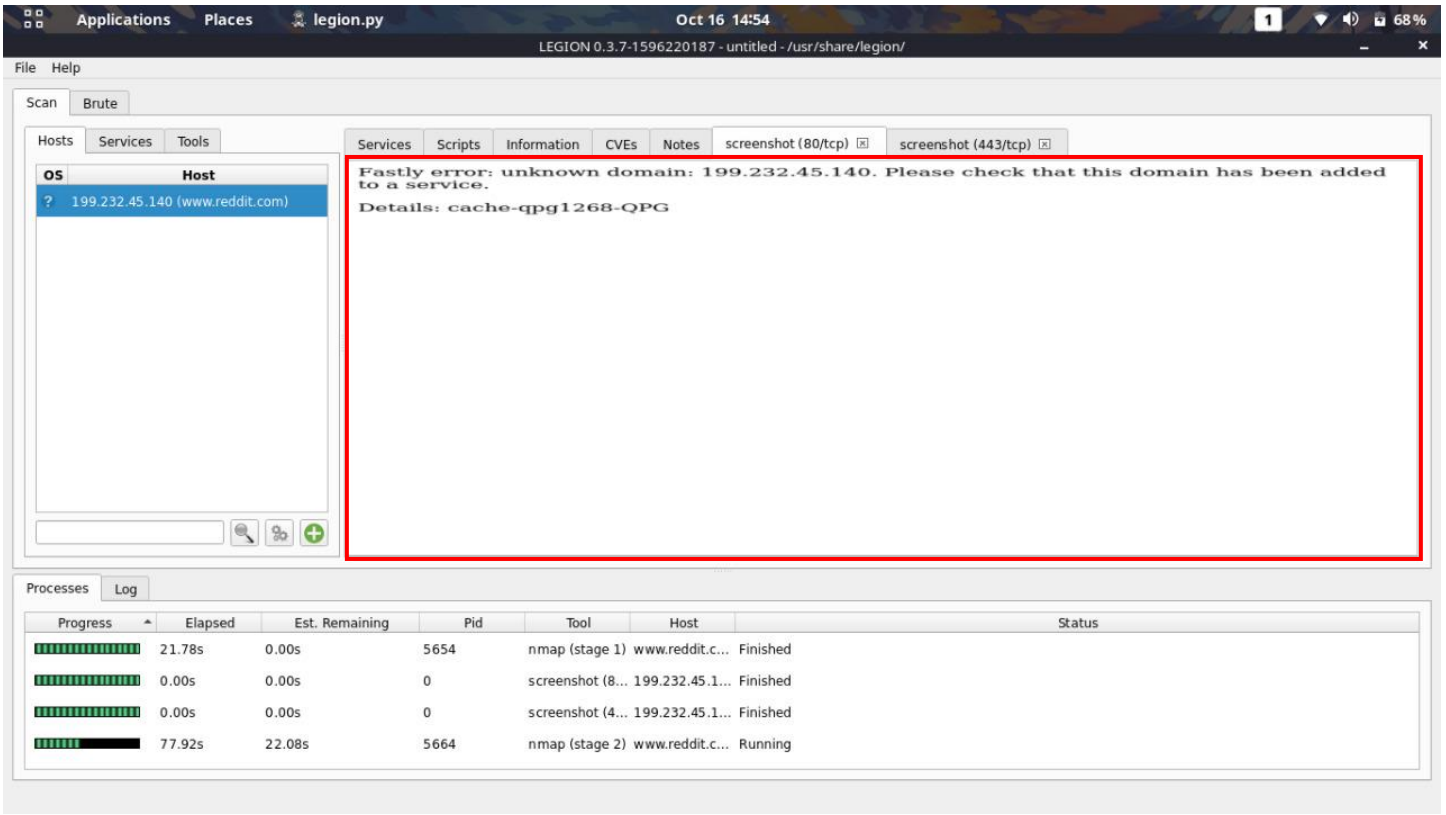
- NMAP
- whataweb
- sslyzer
- Vulners
- webslayer
- SMBenum
- dirbuster
- nikto
- Hydra, as well as almost 100 auto-scheduled scripts.

Legion Tool's modular feature allows users to quickly personalize Legion.


Applications
Places
legion.py
Oct 16 14:52
66%
LEGION 0.3.7-1596220187 - untitled - /usr/share/legion/
File
Help
Scan
Brute
Hosts
Services
Tools
Click here to add host(s) to scope
Services
Scripts
Information
CVEs
Notes
Processes
Log


Applications
Places
legion.py
Oct 16 14:52
66%
Add host(s) to scan seperated by semicolons
www.reddit.com
IP(s), Range(s), and Host(s)
Ex: 192.168.1.0/24; 10.10.10.10-20; 1.2.3.4; bing.com
Mode Selection
Easy
Hard
Easy Mode Options
Run nmap host discovery
Run staged nmap scan
Timing and Performance Options
Paranoid
Sneaky
Polite
Normal
Aggressive
Insane
Port Scan Options
TCP
Stealth SYN
FIN
NULL
Xmas
TCP Ping
UDP Ping
Fragment
Host Discovery Options
Disable
Default
ICMP
TCP SYN
TCP ACK
Timestamp
Netmask
Custom Options
Additional arguments
-sV -O
Submit
Cancel



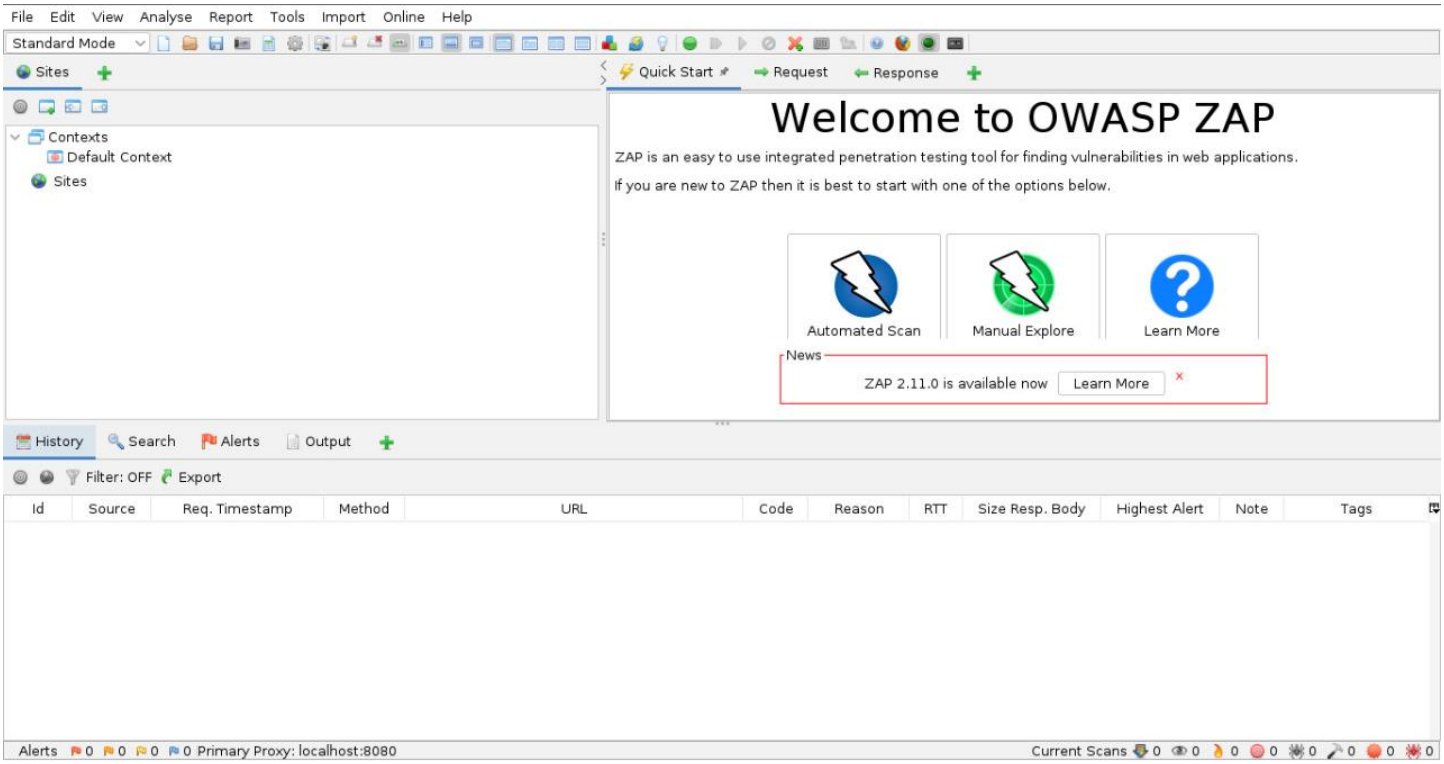


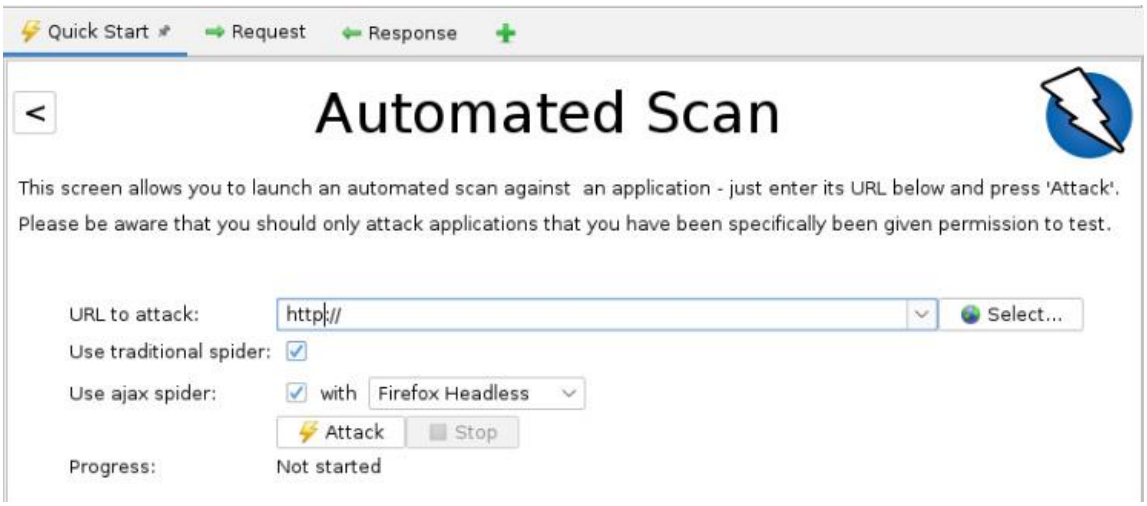
Hear we can identify vulnerabilities and their CVE number and also screenshot of webpage. So we can easily defense that vulnerability.

ZAP OWZAP

The open-source web application security scanner OWASP ZAP (short for Zed Attack Proxy) was developed by OWASP. It is designed to be utilized by both newcomers to application security and experienced penetration testers. It is one of the most active initiatives under the Open Web Application Security Project (OWASP).

Intercepting proxy server, Traditional and AJAX Web crawlers, Automated scanner, Passive scanner, forced browsing, Fuzzer, WebSocket support, Scripting languages, and Plug-n-Hack support are just a few of the built-in capabilities. It includes a plugin-based design and an online "marketplace" where users may contribute new or updated functionality. The graphical user interface (GUI) control panel is simple to use.





ZAP Scanning Report

Summary of Alerts

Generated on Sat, 16 Oct 2021 15:44:57

Risk Level	Number of Alerts
High	0
Medium	3
Low	7
Informational	3

Alerts

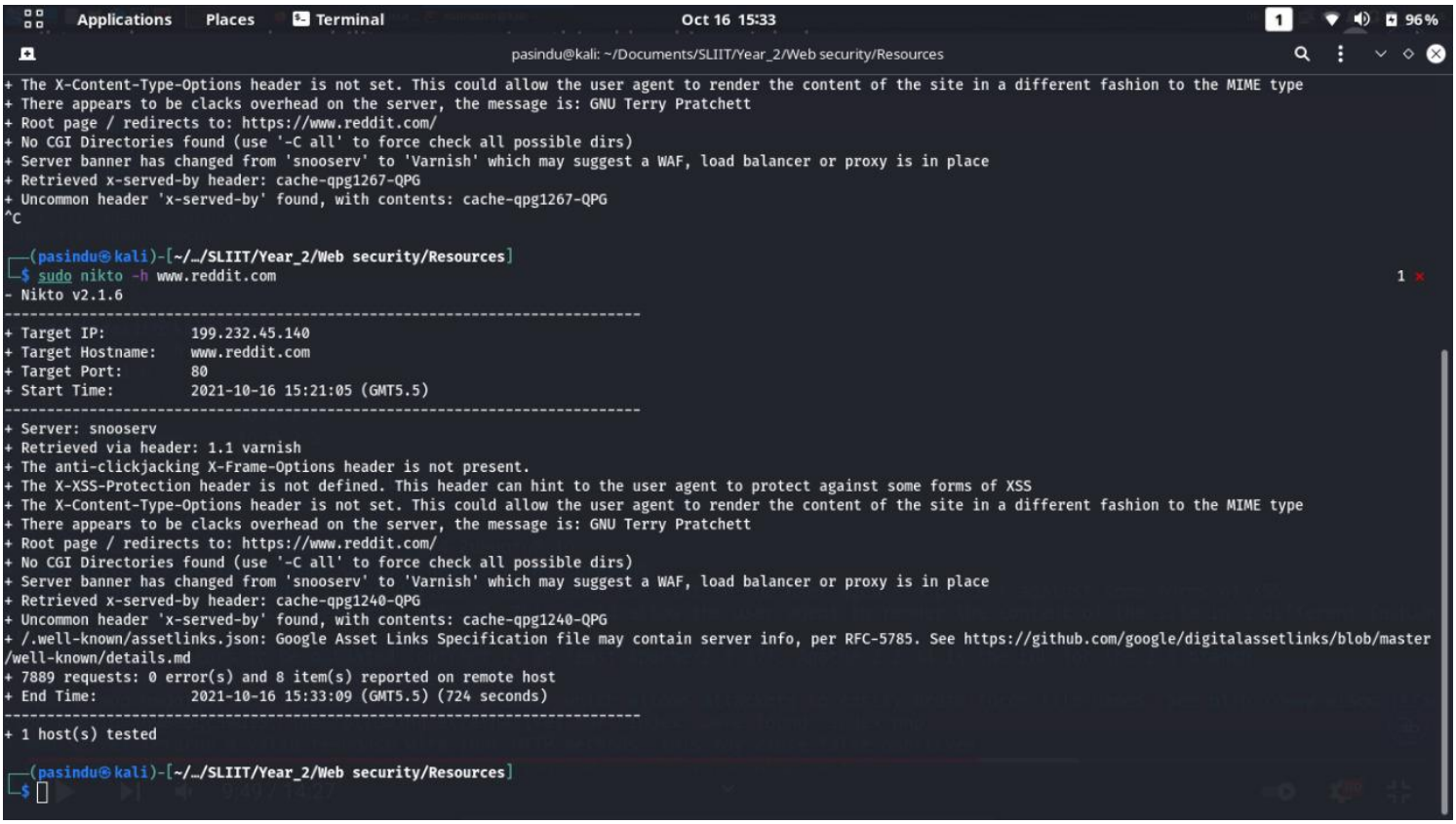
Name	Risk Level	Number of Instances
Cross-Domain Misconfiguration	Medium	1
CSP: Wildcard Directive	Medium	3
X-Frame-Options Header Not Set	Medium	6
Absence of Anti-CSRF Tokens	Low	128
Cookie No HttpOnly Flag	Low	98
Cookie without SameSite Attribute	Low	4
Cookie with SameSite Attribute None	Low	94
Cross-Domain JavaScript Source File Inclusion	Low	1901
Incomplete or No Cache-control Header Set	Low	82
X-Content-Type-Options Header Missing	Low	79
Information Disclosure - Suspicious Comments	Informational	112

Hear I found some medium level and low-level vulnerabilities. We can do automated and manual scan with using ZAP. I will talk about this output repot with more information in latter part of this. I analyze all of this information there.

Nikto Tool

Nikto is not intended to be a stealthy tool. It will test a web server as quickly as possible and will be visible in log files or to an IPS/IDS. However, LibWhisker's anti-IDS techniques are supported if you wish to give them a shot (or test your IDS system).

Not every check is a security risk, but the majority of them are. Some items are "info only" tests that look for things that may or may not have a security problem, but that the webmaster or security engineer may not be aware are there on the server. These things are generally labeled correctly in the written content. There are also some checks for unknown things that have been spotted in log files that have been searched for.



Hear we can see some vulnerabilities; I will talk about these things in vulnerability analysis part.

Netspaker

Netsparker is an automated, but completely customizable, online application security scanner that allows you to scan websites, web apps, and web services for security problems. It can be used to scan websites, web applications, and web services for security vulnerabilities. Netsparker can scan all kinds of online applications, independent of the platform on which they are constructed or the programming language in which they are written.

When Netsparker scanners detect the following vulnerability categories, they can create a proof:

- SQL Injection
- Boolean SQL Injection
- Blind SQL Injection
- Remote File Inclusion (RFI)
- Command Injection
- Blind Command Injection
- XML External Entity (XXE) Injection
- Remote Code Evaluation
- Local File Inclusion (LFI)
- Server-side Template Injection
- Remote Code Execution
- Injection via Local File Inclusion

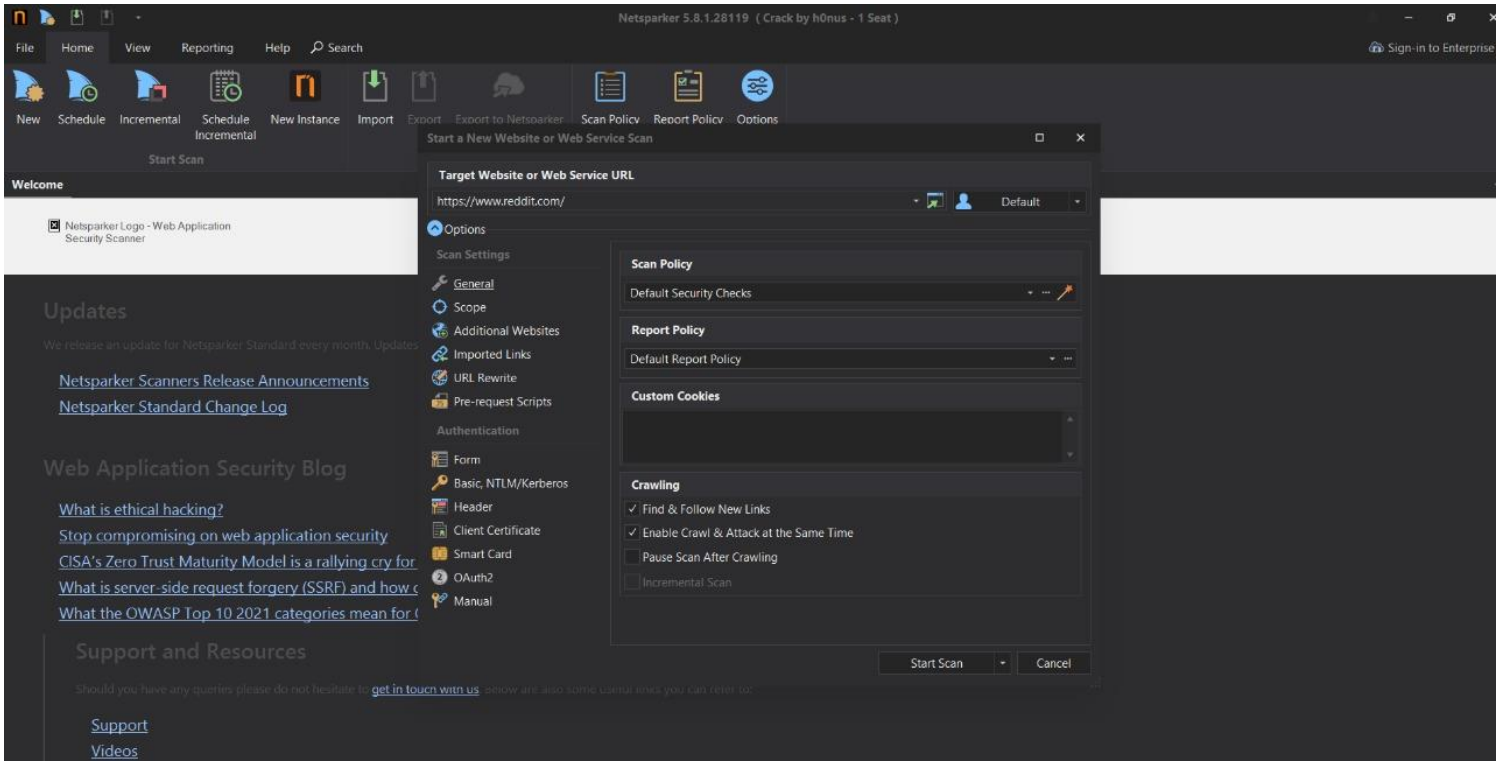
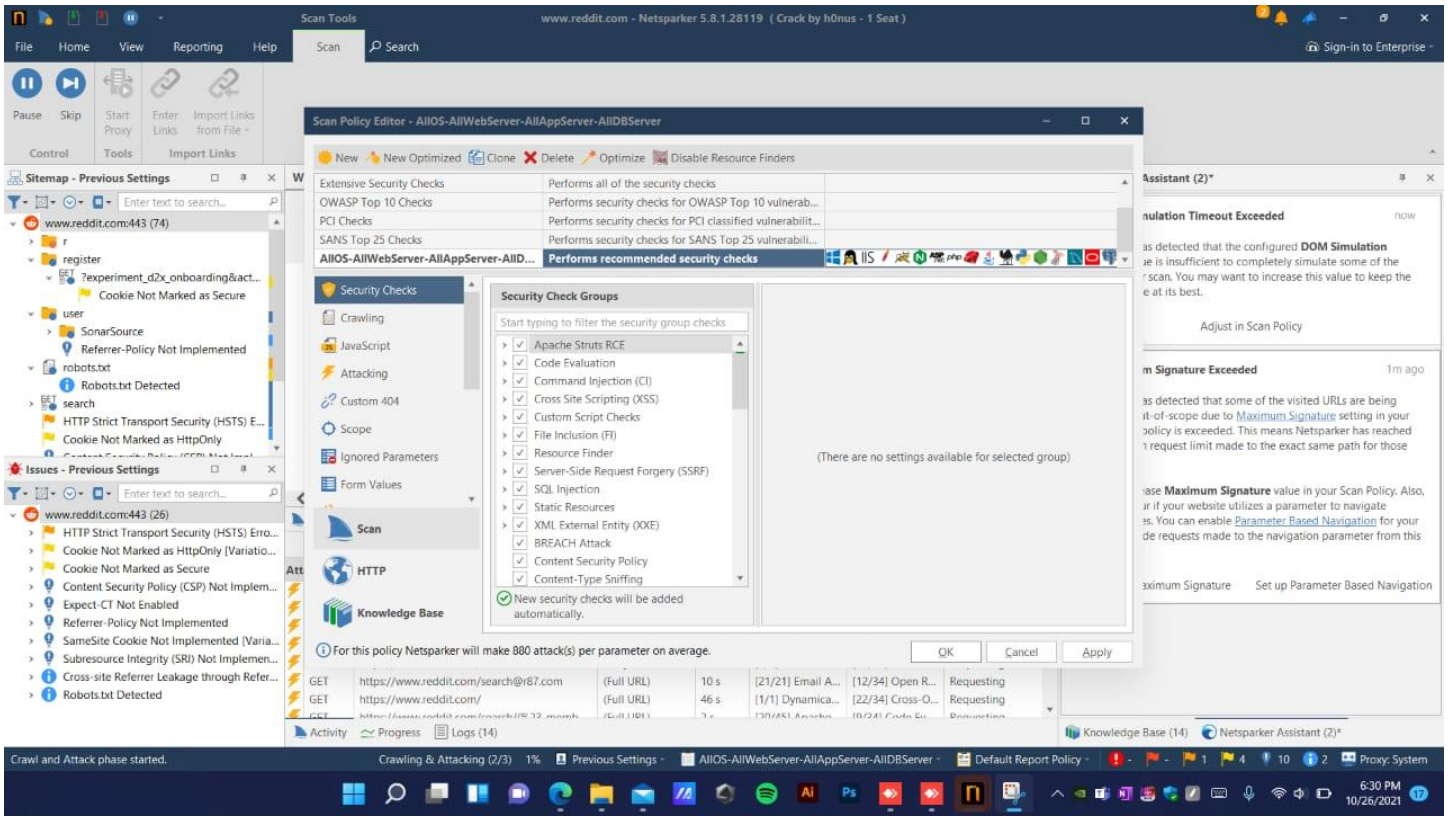
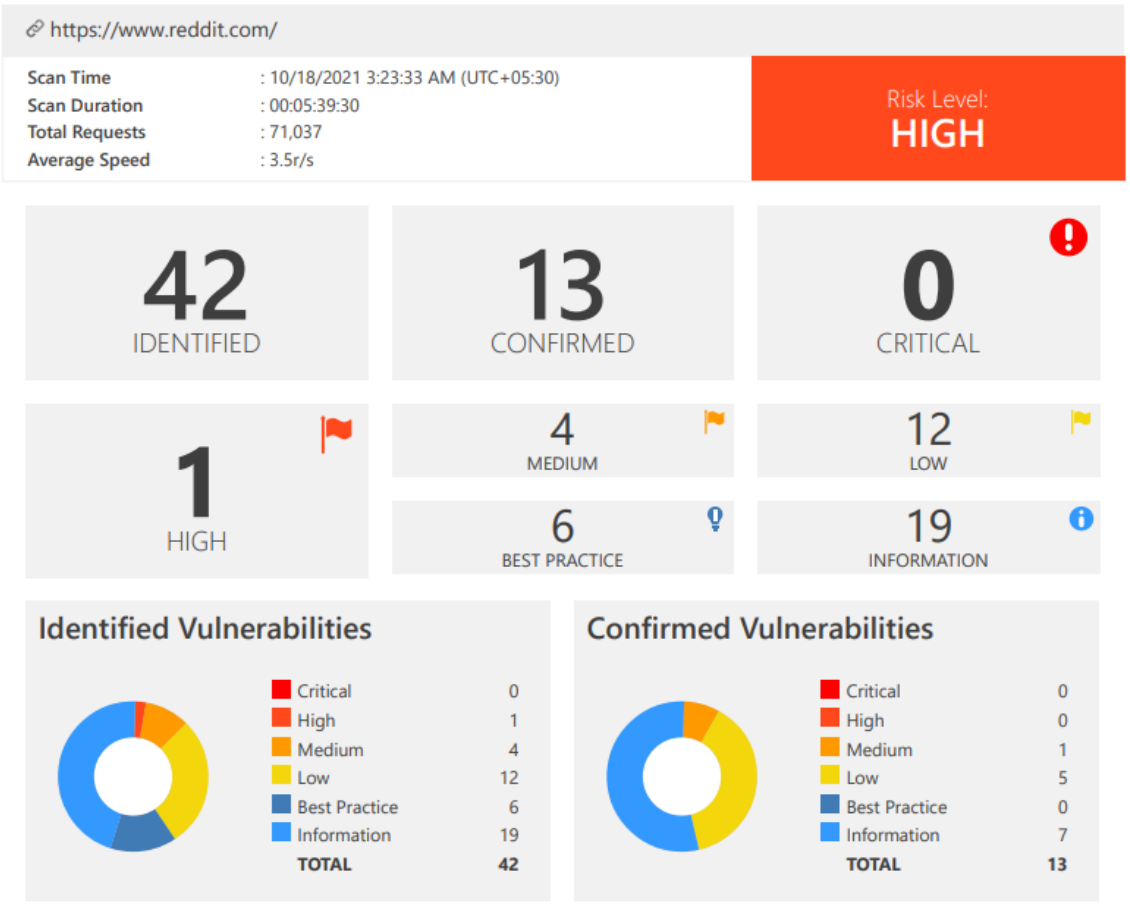


FIGURE 4 MAIN INTERFACE



Hear I scan number of domains in my scope in my and hear is the results.

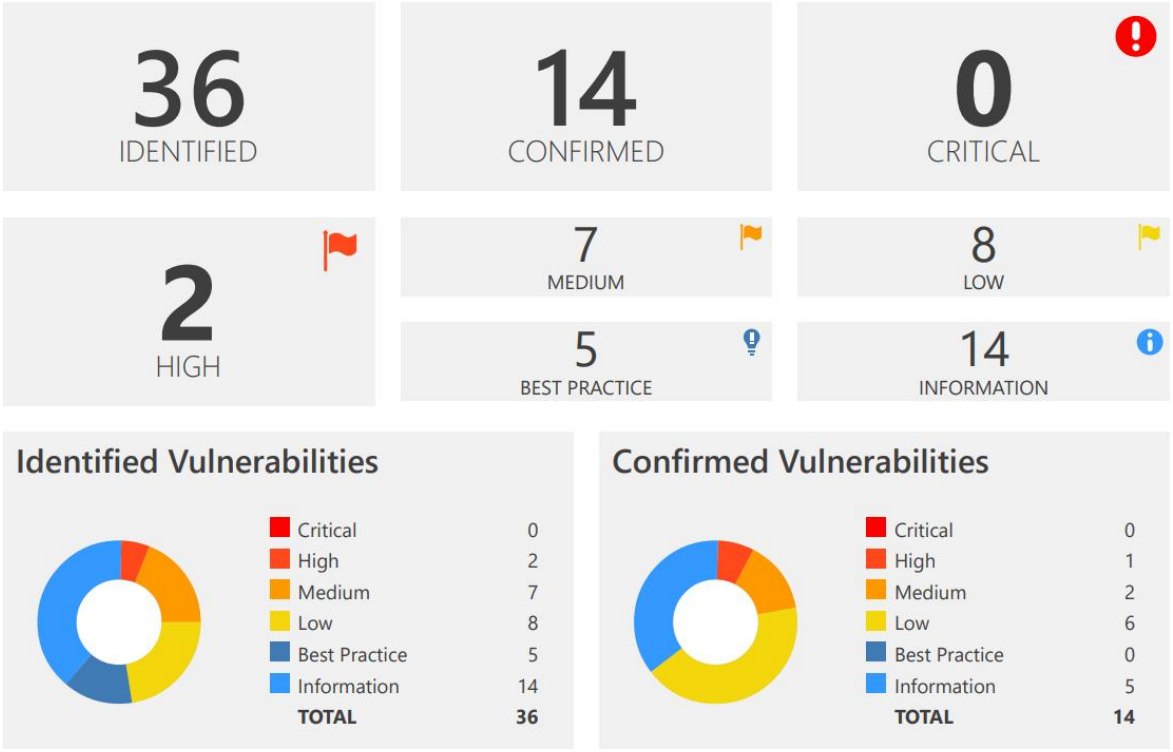
https://www.reddit.com



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Modernizr)	GET	https://www.reddit.com/r/PS5/comments/	
	[Possible] BREACH Attack Detected	GET	https://www.reddit.com/search?q=3	
	[Possible] Password Transmitted over Query String	GET	https://www.reddit.com/register/?dest=https%3A%2F%2Fwww.reddit.com%2F	
	Out-of-date Version (jQuery)	GET	https://www.reddit.com/r/PS5/comments/	
	Weak Ciphers Enabled	GET	https://www.reddit.com/	

https://www.redditgifts.com/



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (AngularJS)	GET	https://www.redditgifts.com/gallery/secret-santa-2015/gift/these-wonderful-secret-santa-gifts-my/	
	Session Cookie Not Marked as Secure	GET	https://www.redditgifts.com/profiles/login/	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.redditgifts.com/	
	Out-of-date Version (jQuery UI Autocomplete)	GET	https://www.redditgifts.com/	
	Out-of-date Version (jQuery UI Dialog)	GET	https://www.redditgifts.com/	
	Out-of-date Version	GET	https://www.redditgifts.com/	

https://m.reddit.com/

Scan Time	: 10/14/2021 6:36:01 AM (UTC+05:30)
Scan Duration	: 00:00:03:02
Total Requests	: 4,827
Average Speed	: 26.5r/s

Risk Level: MEDIUM

5 IDENTIFIED	1 CONFIRMED	0 CRITICAL
0 HIGH	1 MEDIUM	0 LOW
	2 BEST PRACTICE	2 INFORMATION

Identified Vulnerabilities

Critical	0
High	0
Medium	1
Low	0
Best Practice	2
Information	2
TOTAL	5

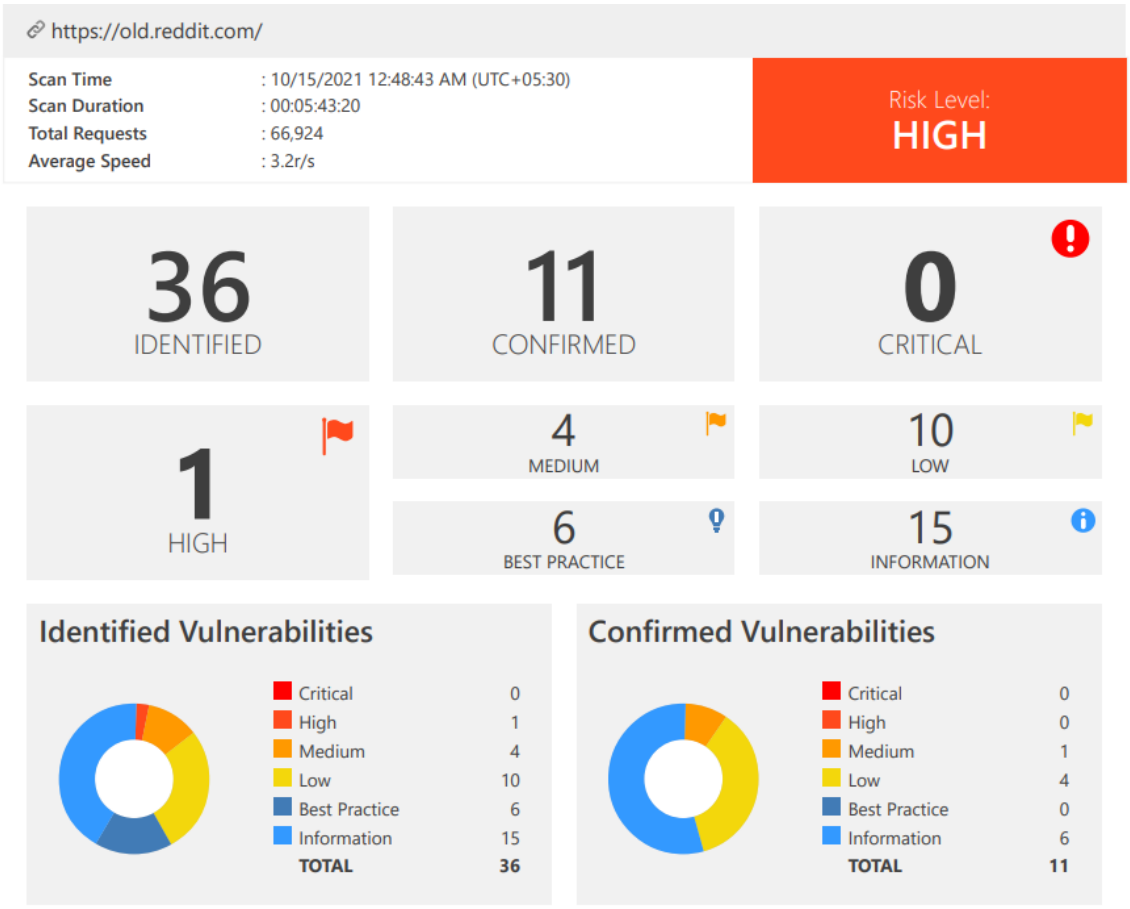
Confirmed Vulnerabilities

Critical	0
High	0
Medium	1
Low	0
Best Practice	0
Information	0
TOTAL	1

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Weak Ciphers Enabled	GET	https://m.reddit.com/	
	Expect-CT Not Enabled	GET	https://m.reddit.com/	
	Missing X-XSS-Protection Header	GET	https://m.reddit.com/.well-known/apple-app-site-association	
	Apple's App-Site Association (AASA) Detected	GET	https://m.reddit.com/.well-known/apple-app-site-association	
	HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	GET	https://m.reddit.com/	

https://old.reddit.com/



Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Modernizr)	GET	https://old.reddit.com/	
	[Possible] BREACH Attack Detected	GET	https://old.reddit.com/r/AskReddit/	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://old.reddit.com/	
	Out-of-date Version (jQuery)	GET	https://old.reddit.com/	
	Weak Ciphers Enabled	GET	https://old.reddit.com/	
	[Possible] Cross-site Request Forgery	GET	https://old.reddit.com/	
	[Possible] Cross-site	GET	https://old.reddit.com/	

https://www.dubsmash.com/

https://www.dubsmash.com/

Scan Time	: 10/18/2021 11:21:30 AM (UTC+05:30)
Scan Duration	: 00:00:01:28
Total Requests	: 676
Average Speed	: 7.6r/s

Risk Level:
MEDIUM

Your website is fairly insecure!

There are some problems on the application that need to be addressed but nothing that requires you to panic. Address the identified issues in timely manner.

Vulnerabilities

Critical	0
High	0
Medium	2
Low	1
Best Practice	1
Information	1
TOTAL	**5**

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.
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.
Expect-CT in Report Only Mode	**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 Analytics

In this section I am consider about some vulnerabilities we found in our scans. Their risk level, and other details. Feather We are focusing number of vulnerabilities, types as so on.

Nmap Scan Analytics

Total Number of scanned domains = 17 (17 hosts up)

Open Ports each domain

Domain Name	Open Ports
1. www.reddit.com 2. www.redd.it 3. redditmedia.com 4. redditthelp.com 5. api.reddit.com 6. redditblog.com 7. redditgifts.com 8. mod.reddit.com 9. redditinc.com 10. ads.reddit.com 11. gql.reddit.com 12. accounts.reddit.com 13. gateway.reddit.com 14. strapi.reddit.com 15. m.reddit.com 16. amp.reddit.com	25/tcp open smtp 80/tcp open http 443/tcp open https
17. dubsmash.com	25/tcp open smtp 80/tcp open http 443/tcp open https 8080/tcp open http-proxy 8443/tcp open https-alt

Netspaker Scan Analytics

Hear I scan 5 domains in my scope, and I found medium level and low-level vulnerabilities.

Domain Name	**High Risks**	**Medium Risks**	**Low Risks**	**Total**
www.reddit.com	1	4	12	**17**
redditgifts.com	2	7	12	**21**
m.reddit.com	-	1	-	**1**
old.reddit.com	1	4	10	**15**
www.dubsmash.com	-	2	1	**3**
Total	**4**	**18**	**35**	**57**

Vulnerability Assessment and Evaluation

The process of defining, detecting, categorizing, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures is known as vulnerability assessment. Vulnerability assessments also provide organizations with the information, awareness, and risk backgrounds they need to recognize and respond to threats to their environment.

Importance of vulnerability assessments

A vulnerability assessment offers information on any security flaws in an organization's environment. It also instructs on how to evaluate the dangers connected with certain flaws. This procedure gives the company a greater knowledge of its assets, security vulnerabilities, and overall risk, lowering the chances of a cybercriminal breaking into its systems and catching the company off guard.

Identify Vulnerabilities in https://www.reddit.com

Out-of-date Version (Modernizr)

Modernizr is a JavaScript package that determines whether your visitor's browser supports HTML5 and CSS3 capabilities. It allows developers to test new technologies and give fallbacks for browsers that do not support them by detecting feature support. Feature detection is a significantly more efficient method than browser sniffing**.**

Netsparker discovered that the target website was using Modernizr and that it was outdated.

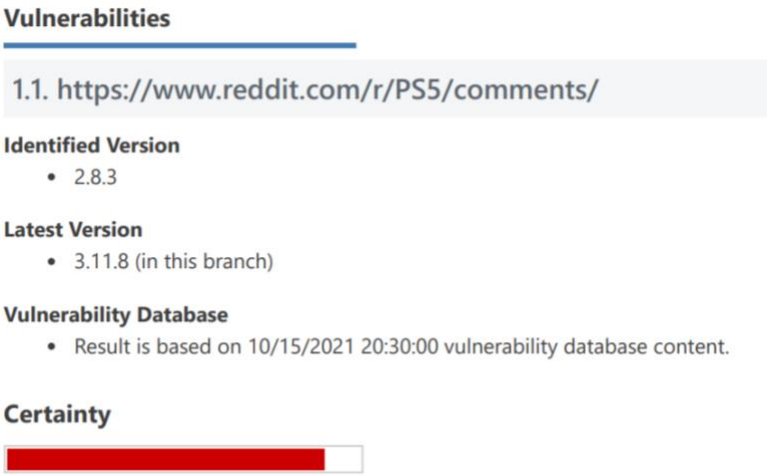
Impact

Since this is an old version of the software, it may be vulnerable to attacks.

Modernizr Sanitization bypass using HTML Entities

https://github.com/Modernizr/Modernizr/issues/2158

Affected Versions 1.1 to 3.3.1



Request

```
GET /r/PS5/comments/ HTTP/1.1
Host: www.reddit.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: loid=0000000000fl9stjaa.2.1634507616000.Z0FBQUFBQmhiSnRnb0Y4NEhEb2lLOHFqX1U1VDZ4TXRwVUNhYl80VG1
oM1pVeHdzZEhZdWo2TkxfUWtMd1IzRnZvOW9RbjdUSTZaUXJ1SVZRUWNpem5qTTFQcm8zWTRoQTFHWkNRR1lPMlJCaFQxcy1FOUxfMH
V0TFZKQ0JpQU5sR19tQkx3UlFJOXc; csv=1; edgebucket=VxrPKEYx2VeuevM9Ws; token_v2=eyJhbGciOiJIUzI1NiIsInR5c
CI6IkpXVCJ9.eyJleHAiOjE2MzQ1MTEwOTYsInN1YiI6Ii1TVlduSGFLUzJTY0N4TG1zb2twMjFxSy0wSFp6VnciLCJsb2dnZWRJbiI
6ZmFsc2UsInNjb3BlcyI6WyIqIiwiZW1haWwiLCJwaWkiXX0.qz8jOZKVJ7CVvJrTka85dEfLbTPs6xKST0zBW44DMnI; session=5
bceb779bd396322d0c1cab78998463dc2dd9d79gASVSQAAAAAAAABKfZtsYUdB2Fsm30PHK32UjAdfY3NyZnRflIwoZTU4NDgzOWZm
MzQzYzRhMjI4MmNhMjY0YjQ4ZjMzYjIwOWJjM2M1NJRzh5Qu; session_tracker=onqodqlbpirgapakqg.0.1634507664130.Z0
FBQUFBQmhiSnVRWDl1VVJJc1JTMHdPWGJ5Nk1hdVpSZG1VbUoxWDNpNXJ5cHNhLVRjODd1alhRSk5OYUtub2xwOENlRkRuVHkzajh0W
Wd0anZXSi1Uekp4V3dHUDhjUzBKNGhMYkFic3pxcV9mR0N6SC1OMW5YZENLQjdVRlg3UWQ3b2RhMVlHNmI
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1318.3551 Total Bytes Received : 142217 Body Length : 141314 Is Compressed : No

```
HTTP/1.1 200 OK
X-Moose: majestic
cache-control: max-age=0, must-revalidate
Set-Cookie: session_tracker=onqodqlbpirgapakqg.0.1634507664643.Z0FBQUFBQmhiSnVRTkEwd0ZxZW5NdHJLWXpKUXhi
NEVmQnh4d1FOSUxjUTFpZFdlb0tjSTRXNFdGYmltRjhSOUwxa3Jrc3BpN0lOaGdaUkh4N3o1Mk1KcGRvWDRtcm9XZTBCSUE4U1p3cTh
pbHRJSTFuNU96NW0xdmZENDQzZjJ1SXo4eXluREt3RTY; Domain=reddit.com; Max-Age=7199; Path=/; expires=Sun, 17-
Oct-2021 23:54:24 GMT; secure; SameSite=None; Secure
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Server: snooserv
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
Accept-Ranges: bytes
Connection: keep-alive
x-frame-options: SAMEORIGIN
Vary: accept-encoding
Content-Length: 21244
Via: 1.1 varnish
X-Clacks-Overhead: GNU Terry Pratchett
Content-Type: text/html; charset=UTF-8
x-ua-compatible: IE=edge
Date: Sun, 17 Oct 2021 21:54:25 GMT
content-encoding:

<!doctype html><html xmlns="http://www.w3.org/1999/xhtml" lang="en-us" xml:lang="en-us"><head><title>co
mments : PS5</title><meta name="keywords" content=" reddit, reddit.com, vote, comment, submit " /><meta
 name="description" content="The Reddit home for PlayStation 5. Your hub for everything related to PS5
 including news, games and discussion. Consider joining r/PlayStation for..." /><meta name="referrer" c
ontent="always"><meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /><link type="applic
ation/opensearchdescription+xml" rel="search" href="/static/opensearch.xml"/><link rel="canonical" href
="https://www.reddit.com/r/PS5/" /><meta name="viewport" content="width=1024"><link rel="dns-prefetch"
 href="//out.reddit.com"><link rel="preconnect" href="//out.reddit.com"><meta property="og:image" conte
nt="https://styles.redditmedia.com/t5_2s887/styles/bannerBackgroundImage_7u1b96w0nj651.png"><meta prope
rty="og:site_name" content="reddit"><meta property="og:description" content="The Reddit home for PlaySt
ation 5. Your hub for everything related to PS5 including news, games
```

BREACH Attack Detected

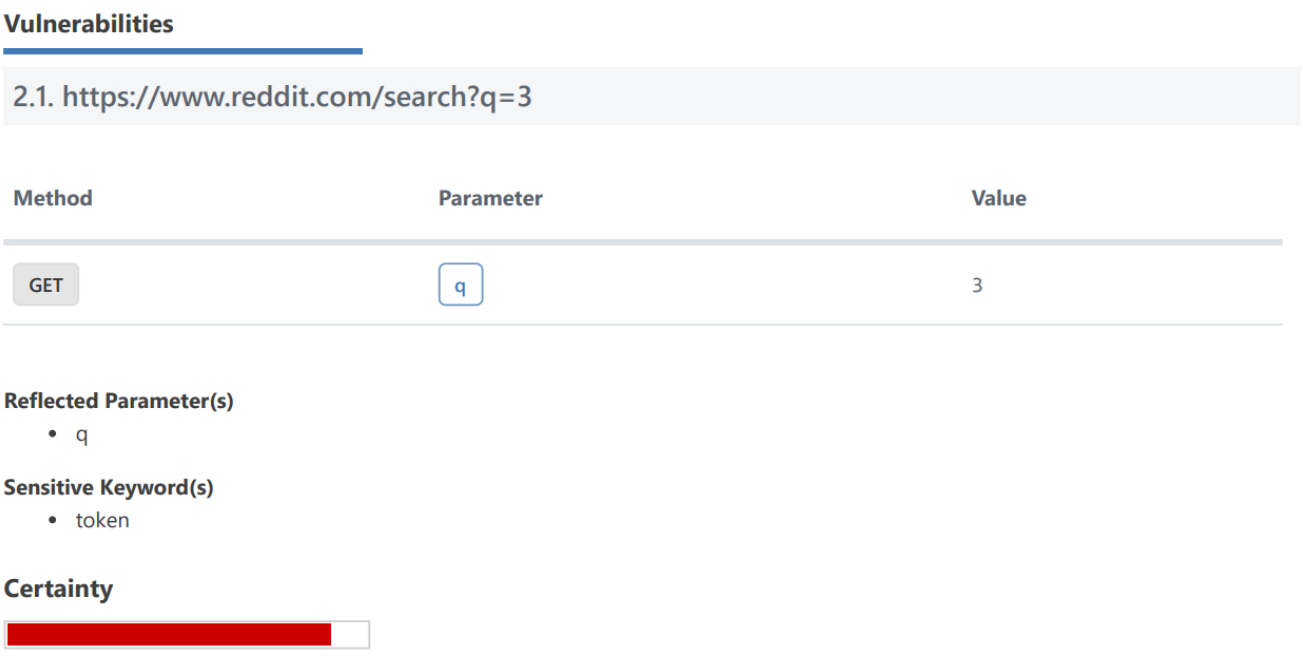
BREACH Detection is a security check that looks at a variety of factors. BREACH Attack detection looks for secured connections where attackers may still see the encrypted communication of the victim.

Netsparker detected that BREACH (Browser Reconnaissance & Exfiltration via Adaptive Compression of Hypertext) attack is possible on this website. Due to elements that make BREACH attack possible, SSL/TLS protected traffic remains vulnerable and can be attacked to uncover information from the website. Regardless of which version of SSL/TLS you use, attacks are still possible. Attacks do not require TLS-layer compression and they can work against any cipher suite.

Impact

An attacker can observe the victim's encrypted traffic and cause the victim to submit HTTP requests to the vulnerable web server even if the connection is SSL/TLS secured (by using invisible frames). An attacker might take information from the website and perform the following with it if they followed these steps:

- Inject partial plaintext into a victim's requests that they have discovered.
- Calculate the volume of encrypted traffic.



Request

```
GET /search?q=3 HTTP/1.1
Host: www.reddit.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: loid=0000000000fl9stjaa.2.1634507616000.Z0FBQUFBQmhiSnRnb0Y4NEhEb2lLOHFqX1U1VDZ4TXRwVUNhYl80VG1
oM1pVeHdzZEhZdWo2TkxfUWtMd1IzRnZvOW9RbjdUSTZaUXJ1SVZRUWNpem5qTTFQcm8zWTRoQTFHWkNRR1lPMlJCaFQxcy1FOUxfMH
V0TFZKQ0JpQU5sR19tQkx3UlFJOXc; csv=1; edgebucket=VxrPKEYx2VeuevM9Ws; token_v2=eyJhbGciOiJIUzI1NiIsInR5c
CI6IkpXVCJ9.eyJleHAiOjE2MzQ1MTEwOTYsInN1YiI6Ii1TVlduSGFLUzJTY0N4TG1zb2twMjFxSy0wSFp6VnciLCJsb2dnZWRJbiI
6ZmFsc2UsInNjb3BlcyI6WyIqIiwiZW1haWwiLCJwaWkiXX0.qz8jOZKVJ7CVvJrTka85dEfLbTPs6xKST0zBW44DMnI; session=5
bceb779bd396322d0c1cab78998463dc2dd9d79gASVSQAAAAAAAABKfZtsYUdB2Fsm30PHK32UjAdfY3NyZnRflIwoZTU4NDgzOWZm
MzQzYzRhMjI4MmNhMjY0YjQ4ZjMzYjIwOWJjM2M1NJRzh5Qu; session_tracker=onqodqlbpirgapakqg.0.1634507649387.Z0
FBQUFBQmhiSnVCbTJKZ01HeWk2ekw2anZPYjlUNUpuS2VNN2JXV1pQU0s0aXprSmp4MGJuTmlLU1lhbDNUSnpveVZ6aVhIRTJBRnpYM
EV0OTNSN21pa0Y0ZmV0VHd1cWI2MGwxOHdXUGhwS29IVmRyMUlRYTNlZWk2SldKVW5qcHowUzVxQzJ4RTU
Referer: https://www.reddit.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 5960.0601 **Total Bytes Received** : 654195 **Body Length** : 653419 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: session_tracker=onqodqlbpirgapakqg.0.1634507650935.Z0FBQUFBQmhiSnVDRG1EWHlkdVZuUk5zeVg3Z0E5
amVHRkhQVk0wNDM4VTM4NFgxYk9zVVVDeUJsTWswZWRxM2diUHpUWUQtOTRZLTRMVE5qMW1rR21yM2xKSEI1a2V0VnlWXy1NNWY1TVd
wRFFLeXkyNXZ2bVFtaEM1UTZPdlBMRzdQTFZuYUpxemE; path=/; domain=.reddit.com; secure; SameSite=None; Secure
Server: snooserv
transfer-encoding: chunked
X-Clacks-Overhead: GNU Terry Pratchett
Connection: keep-alive
Via: 1.1 varnish
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
Vary: Accept-Encoding
Strict-Transport-Security: max-age=15552000; includeSubDomains; preload
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Sun, 17 Oct 2021 21:54:11 GMT
Cache-control: private, s-maxage=0, max-age=0, must-revalidate, no-store
```

Identify Vulnerabilities https://www.redditgifts.com/

Out-of-date Version (AngularJS)

AngularJS is an open-source front-end web framework for creating single-page apps based on JavaScript. It is mostly managed by Google and a community of individuals and businesses. By offering a framework for client-side model–view–controller (MVC) and model–view–viewmodel (MVVM) architectures, as well as components widely used in web applications and progressive web apps, it promises to ease both the creation and testing of such systems.

Impact

Due to the fact that this is an older version of the program, it might be exposed to assaults.
Incorrect Neutralization of Input by AngularJS During Web Page Generation ('Cross-site Scripting') Vulnerability Prior to 1.8.0, angular.js allowed cross-site scripting. The regex-based HTML input replacement has the potential to transform sanitized code into unsanitized code.Wrapping "<option>" elements in "<select>" ones changes parsing behavior, leading to possibly unsanitizing code.

Affected Versions = 0.9.0 to 1.7.9

CVE ID = CVE-2020-7676

AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability There is a vulnerability in all angular versions before 1.5.0-beta.0, where after escaping the context of the web application, the web application delivers data to its users along with other trusted dynamic content, without validating it.

Affected Versions 1.0.0 to 1.4.14

CVE References CVE-2019-14863

AngularJS Improper Input Validation Vulnerability

In AngularJS before 1.7.9 the function `merge () ` could be tricked into adding or modifying properties of `Object.prototype` using a `__proto__` payload

Affected Versions 0.9.0 to 1.7.8

CVE References CVE-2019-10768

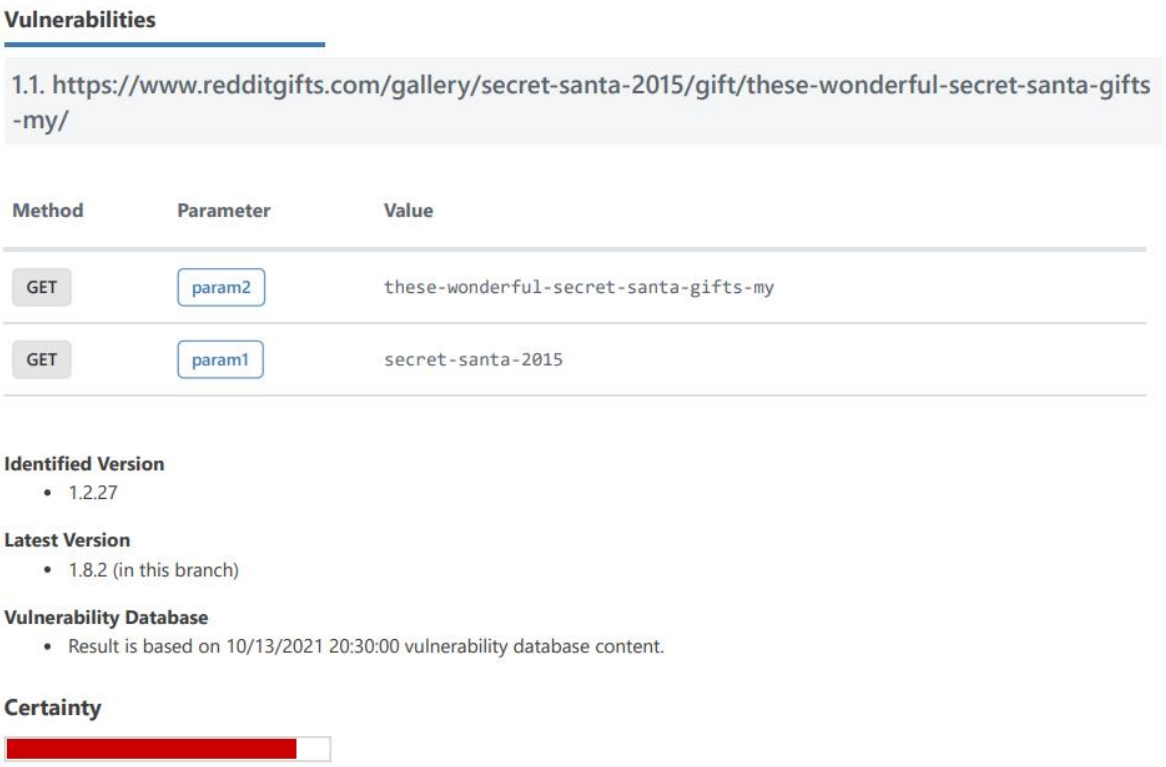
AngularJS Denial of Service (DoS)

AngularJS.Core is an AngularJS. * Package for other Angular modules within .NET.Affected versions of this package are vulnerable to Denial of Service (DoS). https://snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-471886

Affected Versions 0.9.0 to 1.6.2

AngularJS Cross-site Scripting (XSS) Vulnerability

AngularJS.Core is an AngularJS.* package for other Angular modules within .NET.Affected versions of this package are vulnerable to Cross-site Scripting (XSS)https://snyk.io/vuln/SNYK-DOTNET-ANGULARJSCORE-471883



Request

```
GET /gallery/secret-santa-2015/gift/these-wonderful-secret-santa-gifts-my/ HTTP/1.1
Host: www.redditgifts.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ause=dc55a806d28066e8c428137f61b24a73; sessionid=xtqdk40pm71i45dq2h809x3px54wloah; announcement
_2021=1; csrftoken=IhDfBRCamRNN3Kh357BtbDy8EoKMYR1CHPqNeWv4BAfdEwG0FJeqeFma5fD3OXfC
Referer: https://www.redditgifts.com/blog/view/best-secret-santa-2015-so-far/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 754.8162 Total Bytes Received : 35352 Body Length : 34799 Is Compressed : No

```
HTTP/1.1 200 OK
Set-Cookie: csrftoken=IhDfBRCamRNN3Kh357BtbDy8EoKMYR1CHPqNeWv4BAfdEwG0FJeqeFma5fD3OXfC; expires=Wed, 12
-Oct-2022 20:39:03 GMT; Max-Age=31449600; Path=/; secure
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 varnish
X-XSS-Protection: 1; mode=block
Content-Length: 7071
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Wed, 13 Oct 2021 20:39:03 GMT
Vary: Cookie, Accept-Encoding
```

```
<!doctype html>
<html lang="en" class="no-font">
<head>

<script type="text/javascript">
function trackOutboundLink(link, category, action, label) {
if (label) {
try {
_gaq.push(['_trackEvent', category, action, label]);
} catch (err) {}
} else {
try {
_gaq.push(['_trackEvent', category, action]);
} catch (err) {}
}

setTimeout(function () {
document.location.href = link.href;
}, 100);
}
</script>
```

```
<script type="text/javascript">
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-11645097-1']);
_gaq.push(['_setDomainName', 'redditgifts.com']);
_gaq.push(['_setCustomVar', 1, 'VisitorType', 'Member', 2]);
_gaq.push(['_trackPageview']);
_gaq.push(['_trackPageLoadTime']);
(function() {
```

```
var ga = document.createElement('script');
ga.type = 'text/javascript';
ga.async = true;
ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.c
om/ga.js';
var s = document.getElementsByTagName('script')[0];
s.parentNode.insertBefore(ga, s);
})();
</script>


<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>These wonderful Secret Santa gifts brough
…
```

Session Cookie Not Marked as Secure

Netsparker discovered an HTTPS session cookie that was not designated as secure. Following a successful man-in-the-middle assault, an attacker who can successfully intercept the communication might possibly steal the cookie. It is worth noting that Netsparker deduced that the cookie in issue is session-related based on its name.

Impact

Because this cookie will be sent via an HTTP connection, an attacker may intercept it and use it to hijack a victim's session. If a man-in-the-middle attack is successful, the attacker can force the victim to make an HTTP request to your website in order to steal the cookie.

Vulnerabilities

2.1. https://www.redditgifts.com/profiles/login/

CONFIRMED

Identified Cookie(s)

- sessionid

Cookie Source

- HTTP Header

Request

```
GET /profiles/login/ HTTP/1.1
Host: www.redditgifts.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: ause=65119c699215f79ee6cb002b115d8b4e; csrftoken=IhDfBRCamRNN3Kh357BtbDy8EoKMYR1CHPqNeWv4BAfdEw
G0FJeqeFma5fD3OXfC; sessionid=eiu067x626eumdyggqio8ypgabiz61ef
Referer: https://www.redditgifts.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1318.0216 **Total Bytes Received** : 10045 **Body Length** : 9282 **Is Compressed** : No

```
HTTP/1.1 200 OK
Set-Cookie: csrftoken=IhDfBRCamRNN3Kh357BtbDy8EoKMYR1CHPqNeWv4BAfdEwG0FJeqeFma5fD3OXfC; expires=Wed, 12
-Oct-2022 20:32:54 GMT; Max-Age=31449600; Path=/; secure
Set-Cookie: sessionid=; Domain=.redditgifts.com; expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0; Path
=/
Expires: Wed, 13 Oct 2021 20:32:54 GMT
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 varnish
X-XSS-Protection: 1; mode=block
Content-Length: 2877
X-Frame-Options: SAMEORIGIN
Accept-Ranges: bytes
Vary: Cookie, Accept-Encoding
Strict-Transport-Security: max-age=31536000; includeSubdomains
Content-Type: text/html; charset=utf-8
Content-Encoding:
Date: Wed, 13 Oct 2021 20:32:54 GMT
Cache-Control: no-cache, no-storeHTTP/1.1 200 OK
Set-Cookie: csrftoken=IhDfBRCamRNN3Kh357BtbDy8EoKMYR1CHPqNeWv4BAfdEwG0FJeqeFma5fD3OXfC; expires=Wed, 12
-Oct-2022 20:32:54 GMT; Max-Age=31449600; Path=/; secure
Set-Cookie: sessionid=; Domain=.redditgifts.com; expires=Thu, 01-Jan-1970 00:00:00 GMT; Max-Age=0; Path
=/

Expires: Wed, 13 Oct 2021 20:32:54 GMT
X-Content-Type-Options: nosniff
Connection: keep-alive
Via: 1.1 varnish
X-XSS-Protection: 1; mode=block
Content-Length: 2877
X-Frame-Options: SAMEORIGIN
```

Identify Vulnerabilities https://m.reddit.com/

Weak Ciphers Enabled

During secure connection, Netsparker discovered that weak ciphers are enabled (SSL). To protect safe communication with your visitors, only strong ciphers should be allowed on your web server.

Vulnerabilities

1.1. https://m.reddit.com/

CONFIRMED

List of Supported Weak Ciphers

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

Request

```
[NETSPARKER] SSL Connection
```

Response

Response Time (ms) : 1 Total Bytes Received : 27 Body Length : 0 Is Compressed : No

```
[NETSPARKER] SSL Connection
```

Identify Vulnerabilities https://old.reddit.com/

Out-of-date Version (Modernizr)

Modernizr is a JavaScript package that determines whether your visitor's browser supports HTML5 and CSS3 capabilities. It allows developers to test new technologies and give fallbacks for browsers that do not support them by detecting feature support. Feature detection is a significantly more efficient method than browser sniffing**.**

Netsparker discovered that the target website was using Modernizr and that it was outdated.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.
Modernizr Sanitization bypass using HTML Entities https://github.com/Modernizr/Modernizr/issues/2158
Affected Versions 1.1 to 3.3.1

Vulnerabilities

1.1. https://old.reddit.com/

Identified Version

- 2.8.3

Latest Version

- 3.11.8 (in this branch)

Vulnerability Database

- Result is based on 10/13/2021 20:30:00 vulnerability database content.

Certainty

Request

```
GET / HTTP/1.1
Host: old.reddit.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4221.6012 Total Bytes Received : 402141 Body Length : 400691 Is Compressed : No

```
HTTP/1.1 200 OK
X-Moose: majestic
cache-control: max-age=0, must-revalidate
Set-Cookie: loid=0000000000fhbrxs7n.2.1634239127052.Z0FBQUFBQmhhSUtYQjBQY3lzeHZfV0UzcFAtY0hkRm15Nk1CQVN
IYzhXZjZHT29LemZDaHFmZU5OWEhYaFpnTG8zbXYzRFhFLWJOVmhLQnpLaF9IYnRxNzlhM1VRLUFxWFpKNUFkWGJRcnlrd0g4MVV0Rz
B2M3ZobGVmTTJuSGVhT3ZUZFlyNnRRNTg; Domain=reddit.com; Max-Age=63071999; Path=/; expires=Sat, 14-Oct-202
3 19:18:47 GMT; secure; SameSite=None; Secure
Set-Cookie: session_tracker=8tN0RLZanzdQv3ByAb.0.1634239127052.Z0FBQUFBQmhhSUtYVXBJbEhCbUdHLXhEMldEd3Vk
T2NFZGFvX3FMRENNWGxBU3Y5cUNFWVZqSVMyajlPalBMTm1LUU11S1lidGxmRWhGYXBJZXpjVmhFLUxxTGl0SWhia0l0WHRhUWhtdGV
VWGE0UHdzREphZG9QYW1vMFYzdERtRlNmcVFndW80b2g; Domain=reddit.com; Max-Age=7199; Path=/; expires=Thu, 14-
Oct-2021 21:18:47 GMT; secure; SameSite=None; Secure
Set-Cookie: csv=1; Max-Age=63072000; Domain=.reddit.com; Path=/; Secure; SameSite=None
Set-Cookie: edgebucket=N6rljStre1IS4YRolQ; Domain=reddit.com; Max-Age=63071999; Path=/;  secure
strict-transport-security: max-age=15768000
strict-transport-security: max-age=15552000; includeSubDomains; preload
Server: snooserv
```

```
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
Vary: accept-encoding
Connection: keep-alive
x-frame-options: SAMEORIGIN
Accept-Ranges: bytes
Content-Length: 111990
Via: 1.1 varnish
Content-Type: text/html; charset=UTF-8
x-ua-compatible: IE=edge
Date: Thu, 14 Oct 2021 19:18:48 GMT
content-encoding:

<!doctype html><html xmlns="http://www.w3.org/1999/xhtml" lang="en-us" xml:lang="en-us"><head><title>re
ddit: the front page of the internet</title><meta name="keywords" content=" reddit, reddit.com, vote, c
omment, submit " /><meta name="description" content="Reddit gives you the best of the internet in one p
lace. Get a constantly updating feed of breaking news, fun stories, pics, memes, and videos just for yo
u. Passionate about something niche? Reddit has thousands of vibrant communities with people that share
 your interests. Alternatively, fin
…
```

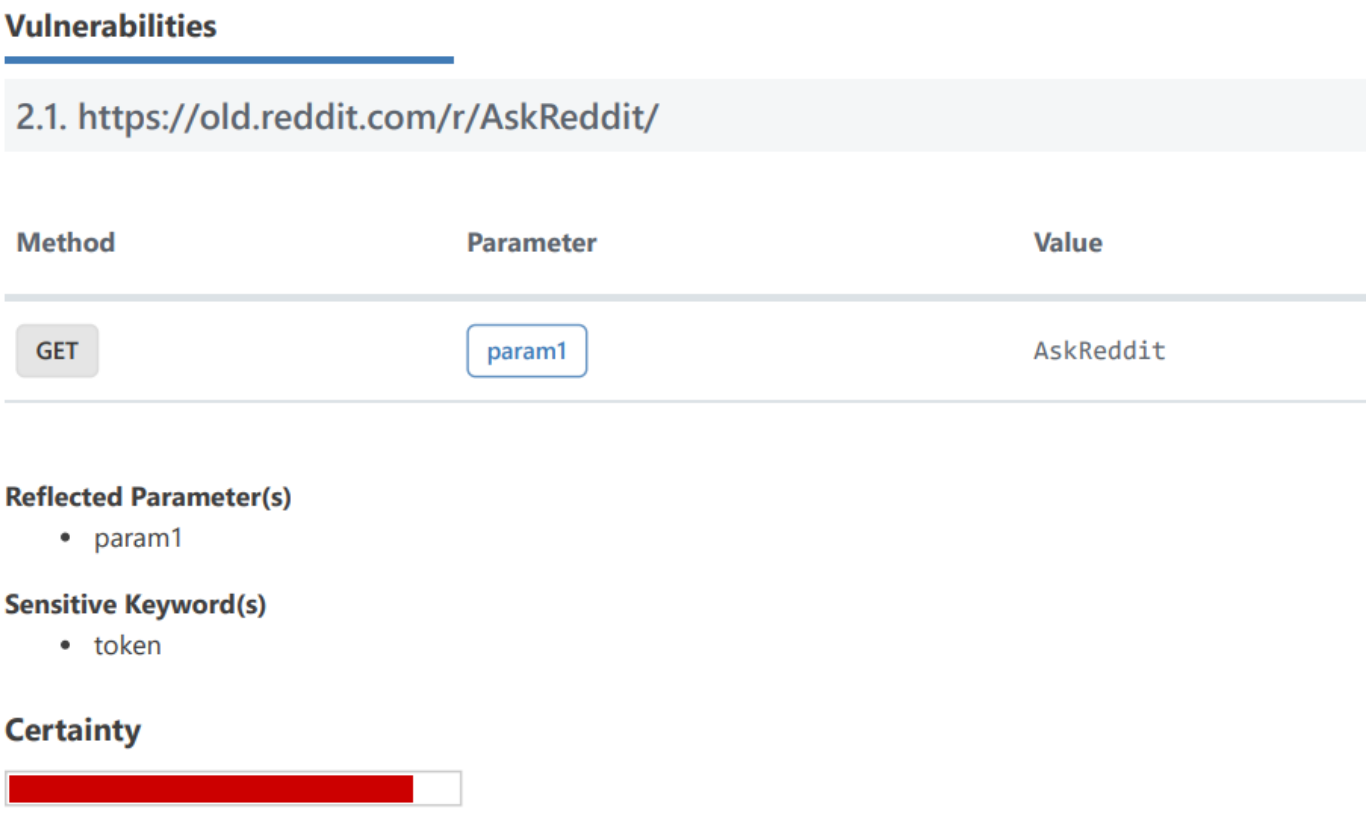
BREACH Attack Detected

This website may be vulnerable to a BREACH (Browser Reconnaissance & Exfiltration through Adaptive Compression of Hypertext) attack, according to Netsparker. SSL/TLS encrypted traffic remains susceptible and can be exploited to extract information from the website due to components that enable BREACH attacks possible. Attacks are feasible regardless of the version of SSL/TLS you use. TLS-layer compression is not required for attacks, and they may be used with any cipher suite.

Impact

Even if you use an SSL/TLS protected connection, an attacker can still view the victim's encrypted traffic and cause the victim to send HTTP requests to the vulnerable web server (by using invisible frames). Following these steps, an attacker could steal information from the website and do the following:

- Inject partial plaintext they have uncovered into a victim's requests
- Measure the size of encrypted traffic



Request

```
GET /r/AskReddit/ HTTP/1.1
Host: old.reddit.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: loid=0000000000fhbrxs7n.2.1634239127052.Z0FBQUFBQmhhSUtYQjBQY3lzeHZfV0UzcFAtY0hkRm15Nk1CQVNIYzh
XZjZHT29LemZDaHFmZU5OWEhYaFpnTG8zbXYzRFhFLWJOVmhLQnpLaF9IYnRxNzlhM1VRLUFxWFpKNUFkWGJRcnlrd0g4MVV0RzB2M3
ZobGVmTTJuSGVhT3ZUZFlyNnRRNTg; csv=1; edgebucket=N6rljStre1IS4YRolQ; pc=ou; session_tracker=8tN0RLZanzd
Qv3ByAb.0.1634239206556.Z0FBQUFBQmhhSUxtZF9TcW9MUktsMlFidVgwYUxiWWZYbEpOYUpUa192WFRJc2U2RDZXS0pLVUlDYlA
wR25ZcGlUTDAza0tQME9jMnpUSHdib1h1cWhGd0RuRmJCempLNlRHTk5YVFkwSVQ3ZFJGSERvdUZhSV9wRXZyZ1VzVXNZN0hzSXFGQX
Ftby0
Referer: https://old.reddit.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 4297.7021 **Total Bytes Received** : 258750 **Body Length** : 257799 **Is Compressed** : No

```
HTTP/1.1 200 OK
x-datadome: protected
X-Moose: majestic
cache-control: max-age=0, must-revalidate
Set-Cookie: session_tracker=8tN0RLZanzdQv3ByAb.0.1634239207215.Z0FBQUFBQmhhSUxuVURTdHI3MGpjOWlETHJXVnY3
aHhNQi1iQzFhQ1hKMzVpNDhiUjBPbVhoUXZxeVl0cUEyeGowWkpTbWc3WXhES0x1Mkx4NkFqODBGaEd2Z1JyRHpWb0wzQVFJM1kxVHB
uS0xhdUFnSnBGT3FxN2xVaHdQVnVTRTZ5dGlKVWxlaGc; Domain=reddit.com; Max-Age=7199; Path=/; expires=Thu, 14-
Oct-2021 21:20:07 GMT; secure; SameSite=None; Secure
strict-transport-security: max-age=15768000
strict-transport-security: max-age=15552000; includeSubDomains; preload
Fastly-Restarts: 1
Server: snooserv
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
```

```
x-xss-protection: 1; mode=block
Connection: keep-alive
x-frame-options: SAMEORIGIN
Accept-Ranges: bytes
Content-Length: 92486
Vary: accept-encoding
Via: 1.1 varnish
Content-Type: text/html; charset=UTF-8
x-ua-compatible: IE=edge
Date: Thu, 14 Oct 2021 19:20:07 GMT
content-encoding:
```

<!doctype html><html xmlns="http://www.w3.org/1999/xhtml" lang="en-us" xml:lang="en-us"><head><title>As
k Reddit...</title><meta name="keywords" content=" reddit, reddit.com, vote, comment, submit " /><meta
 name="description" content="r/AskReddit is the place to ask and answer thought-provoking questions." /
><meta name="referrer" content="always"><meta http-equiv="Content-Type" content="text/html; charset=UTF
-8" /><link type="application/opensearchdescription+xml" rel="search" href="/static/opensearch.xml"/><l
ink rel="canonical" href="https://www.reddit.com/r/AskReddit/" /><meta name="viewport" content="width=1
024"><link rel="dns-prefetch" href="//out.reddit.com"><link rel="preconnect" href="//out.reddit.com"><m
eta property="og:image" content="https://b.thumbs.redditmedia.com/PXt8GnqdYu-9lgzb3iesJBLN21bXExRV1A45z
dw4sYE.png"><meta property="og:site_name" content="reddit"><meta property="og:description" content="r/A
skReddit is the place to ask and answer thought-provoking questions."><meta property="og:title" content
="Ask Reddit... • r/
…

Identify Vulnerabilities https://www.dubsmash.com/

HTTP Strict Transport Security (HSTS) Errors and Warnings

HTTP Strict Transport Security (HSTS) is a strategy that helps protect websites from man-in-the-middle attacks including protocol downgrades and cookie hijacking. It enables web servers to declare that web browsers (or other conforming user agents) should communicate with them using only HTTPS connections, which offer Transport Layer Security (TLS/SSL), rather to the unsecured HTTP. RFC 6797 specifies the HSTS protocol, which is an IETF standards track protocol.

Weak Ciphers Enabled

During secure connection, Netsparker discovered that weak ciphers are enabled (SSL).

To protect safe communication with your visitors, only strong ciphers should be allowed on your web server.

Insecure Transportation Security Protocol Supported (TLS 1.0)

These flaws are not particularly serious, but they might aid an attacker. You should consider repairing them.

Mitigate Identified Vulnerabilities

Mitigating a vulnerability, on the other hand, is devising a temporary remedy or workaround to reduce the likelihood of exploitation. In this case, the optimal strategy is to patch or remediate a vulnerability as soon as it is found before it becomes a security concern.

Fixing or removing a vulnerability, or dealing with the fundamental cause of the vulnerability, is referred to as "remediation." Mitigating a vulnerability, on the other hand, is devising a temporary remedy or workaround to reduce the likelihood of exploitation.

What are the vulnerabilities we identified?

- Out-of-date Version (Modernizr)
- Session Cookie Not Marked as Secure
- BREACH Attack Detected
- Out-of-date Version (AngularJS)
- AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability
    a. AngularJS Improper Input Validation Vulnerability
    b. AngularJS Denial of Service (DoS)
    c. AngularJS Cross-site Scripting (XSS) Vulnerability
- Weak Ciphers Enabled
- HTTP Strict Transport Security (HSTS) Errors and Warnings
- Insecure Transportation Security Protocol Supported (TLS 1.0)

Mitigation

Now let’s consider how to mitigate these vulnerabilities.

Out-of-date Version (Modernizr)

Upgrade web site installation of Modernizr to the latest stable version.

BREACH Attack Detected

The target web page matches the following criteria that allow a Possible BREACH Attack, according to Netsparker:

- Served from a server that compresses data at the HTTP level (ie. gzip)
- User input is reflected in the HTTP response body.
- HTTP response bodies include sensitive information (such as a CSRF token).

propose the following ways to alleviate the problem:

1. Disable HTTP level compression if at all feasible.
2. Keep critical data separate from user input.
3. Use a CSRF token to protect vulnerable websites. Because an attacker exploits this flaw by forcing the user to visit a target website using invisible frames, the SameSite Cookie property will prevent the problem. Cookies belonging to the target will not be transmitted with a request that does not include top level navigation now that the SameSite cookie property has been introduced.
4. Hide the length of the transmission by padding the answers with a random amount of bytes.
5. Set a rate limit of five times per minute to meet the page maximum.

Session Cookie Not Marked as Secure

Mark all cookies used within the application as secure.

Required Skills for Successful Exploitation

To take use of this flaw, the attacker must be able to intercept traffic. This usually necessitates local access to the victim's web server or network. Attackers must be familiar with layer 2 and have access to a system that connects the victim to the web server.

AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

Upgrade web site installation of AngularJS to the latest stable version

Other configurations for Improve Security

- should take care of them as quickly as possible. You might wish to rescan once you have done this to be sure they are gone.
- should take care of them as quickly as possible. You might wish to rescan once you have done this to be sure they are gone.

Try SQL Injection Attack on www.reddit.com

What is SQL Injection?

SQL injection is a well-known attack method that enables users to manipulate databases' backends and get access to otherwise restricted data. Customers' private information, sensitive company information, or user lists are examples of the types of data that might be included in this category. Unauthorized usage of sensitive data and unexpected provision of administrative access to a database are all possible outcomes of a successful SQL injection. SQL injection attacks are a severe security issue to Web applications because they enable attackers to get uncontrolled access to the data contained inside the application.

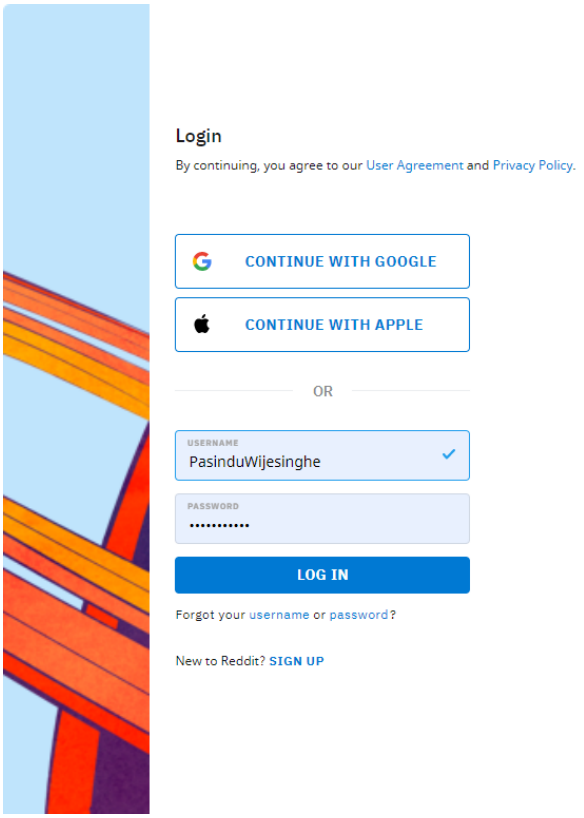
Access to the databases that underpin the apps, and to the potentially sensitive information contained inside these databases Despite the fact that researchers and Several techniques have been developed by practitioners to deal with the SQL problem. Current options either fail to address the entire scope of the injection issue or do so ineffectively. They either do not address the full breadth of the issue or have constraints that preclude their utilization. adoption. Many scholars and practitioners are only acquainted with one or two of these terms.

attack tactics are a subset of the vast array of strategies accessible to attackers that use is attempting to exploit SQL injection flaws in order to get access. As a result, many of the remedies described in the literature are aimed upon SQL injection is merely one of the problems that might arise. In order to deal with this, in this problem, we give an in-depth examination of the many forms of The SQL injection attacks that have been discovered so far. We have a different form of attack for each type of assault. offer explanations and instances of how assaults of such kind may manifest themselves should be carried out in addition, we discuss and assess current detection and monitoring systems. SQL injection attacks are prevented by using several approaches. We explore the advantages and disadvantages of each technique in terms of tackling the problem. SQL injection attacks include the complete spectrum of possibilities.

Attack To Reddit (SQL Injection)

In order to do this first I Created an account in Reddit and try to hack it using SQL Injection.

Login screen



I tried some command hear.

1. Adding a boolean to a where clause that is always true like ' OR 1=1
2. Escaping part of query by entering line comments --
3. Ending the initial query and start a new query '; DROP TABLE USERS.
4. Connecting data from multiple tables by using UNION

I try most of command and study those things well but reddit is secured from SQL injection attack

Conclusion

I choose Reddit web domain from HackerOne platform. First, I gather some information about reddit, and I used tools like Nikto, Whatweb, Dmitry, etc. after I analyzed that information. I scan reddit domain with using Netspaker, Nmap, Legion, and ZAP. Overall, they have good security defenses.