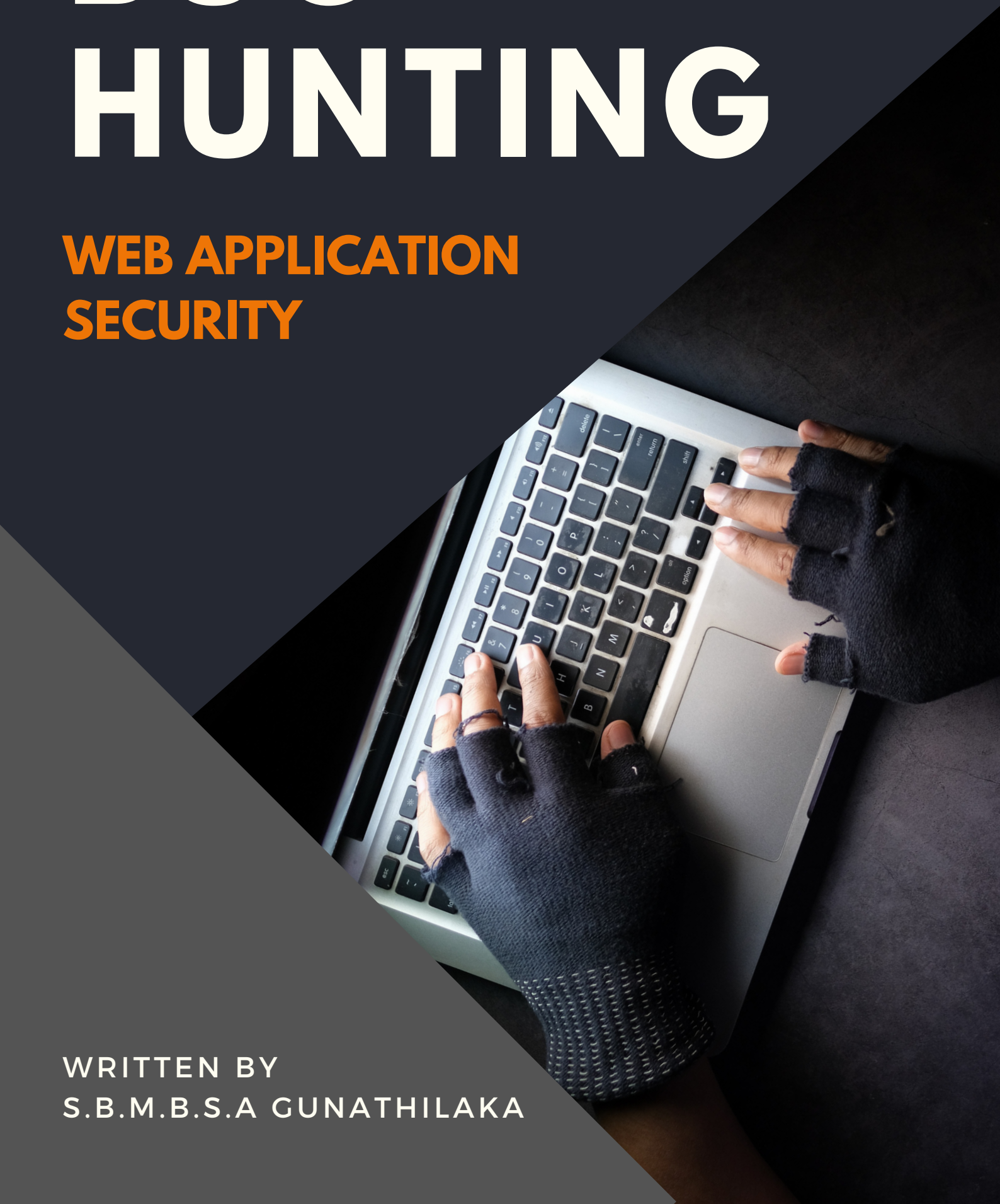
BUG HUNTING

WEB APPLICATION SECURITY



WRITTEN BY
S.B.M.B.S.A GUNATHILAKA

Preface

Prominent companies worldwide start bug bounty programs, and they need to get service from white hat hackers to find bugs in their web applications and who is capable of finding a bug that that company will reward the person. Day by day, the no of bug bounty programs has been increased because of that, and there is a huge opportunity for ethical hackers nowadays.

This book simply covers what bug bounty hunting is. After that, we will discuss what tools we can use when we are doing bug bounties and I put five reports that include how I started bug bounty and how I analyse web applications as a university student and so on.

This book will help you to get an idea about how bug bounty hunting is happening.

For whom I wrote this book

This book targets people who need to be ethical hackers, in other words. This book is suitable for bug bounty hunting beginners who want to understand what is happening behind bug bounty hunting.

What is a bug bounty program?

The main purpose of the bug bounty program is to allow ethical hackers to analyze a web application that own by another party and reporting bugs, in other words, vulnerabilities, weaknesses, and possible exploitations in the web application's hardware, software, and firmware. For that service, they are willing to provide rewards according to the ethical hackers' service.

These companies and organizations allow using external resources to scan into their systems with the intention of find vulnerabilities and disclose those vulnerabilities to the corresponding company. They are expected by launching a bug bounty program with the help of ethical hackers worldwide, fixing their web application weaknesses, and preventing the black hat and grey hat hackers from hacking into their systems and compromising their systems.

Nowadays, we can see many bug bounty programs have grown rapidly from small companies to large companies and government organizations.

Bug bounty websites

First, if someone needs to be a bug bounty hunter, that person should read a lot of books and watch enough courses or participating in programs. After doing those things, it's time to get into the actual work in the field. Everyone needs to deal with real-world applications to get experiences and understand the concepts they have learned before. For that, there are bug bounty websites that allow you to hack into their application legally, and they have few levels you can hack. Using those websites, you can improve your cybersecurity knowledge and skillset. I have given some bug bounty websites and sites you can learn more about cybersecurity.

- Google Gruyere
- HackThis!!
- Penester Lab
- Hack The Box
- GitHub WebGoat
- OWASP Juice Shop
- PortSwigger
- Hacker101
- Bugcrowd University
- Web Hacking 101

Bug hunter toolkit

Web browser

You can install whatever browser you like and suitable for works you are going to do, but most of the time, bug bounty hunters use Google Chrome or Firefox, and then you can install addons and change settings as you want and weaponize it.

Virtual machine

Instead of installing an operating system directly into your machine to practice, you can use virtual machine software and install your testing operating systems and tools. Virtual machine software is helpful for two reasons. You can isolate your testing environment from your original operating system, then something happens to your testing background you can easily repair it without effecting your original OS.second reason is that sometimes you have to practice with vulnerable applications like Metasploitable and applications published in VulnHub then

virtual machine software makes easy those works. In addition, you can install few operating systems in virtual machine software.

Proxy

In some cases, you have to trap all the traffic between your browser and the target website, and then you can use an interception proxy like burp proxy. Also, it allows you to automate attacks or use some other features like encoding/decoding.

These are the three major things that need to use as a bug bounty hunter, and there is no specific toolset for bug bounty hunters. You can install whatever the tool in your testing background, but some of the tools I have given here.

- Burp
- Project Zap
- FFUF
- DirBuster Project
- Amass
- Reconless
- InsiderPHD
- Assetnote Wordlists

When you are reading this book, you can learn about some of major tools in detail so if you have no idea, don't worry; you can understand everything.

Tools for bug bounty hunting

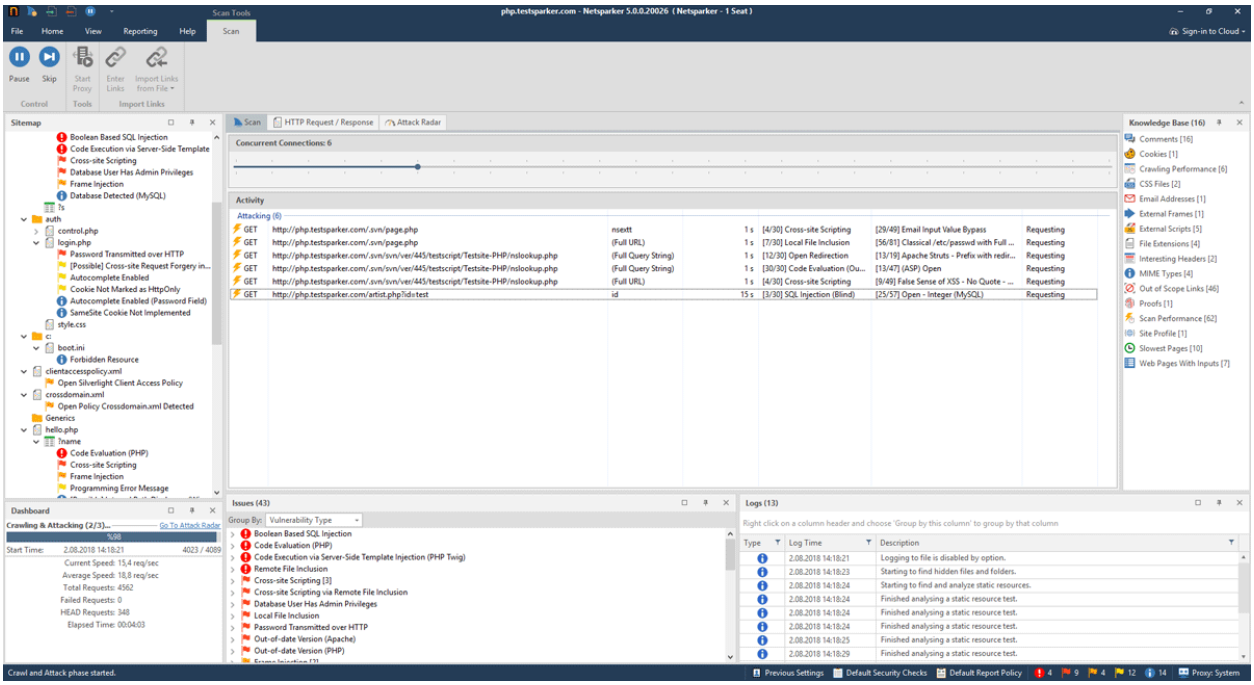
Before starting bug bounty hunting, we need knowledge about what tools we can use for that. When we do bug bounty hunting activities, the tools that we are using are also important as our knowledge and experience we obtained. in this chapter, we will learn the most commonly used tools for bug bounty hunting and other web application security assessments. We can use most of the tools freely, but sometimes we have to spend some money to get the best use.

1. Netsparker

Netsparker is a vulnerability scanner, and it is an automated and highly configurable tool. netsaprker can scan web applications, web services, and whatever the platform or language regardless it scan all types of web applications. Also, it uses proprietary proof-based scanning technology to identify vulnerabilities and verify them by exploiting and proof them in a read-only way.

features

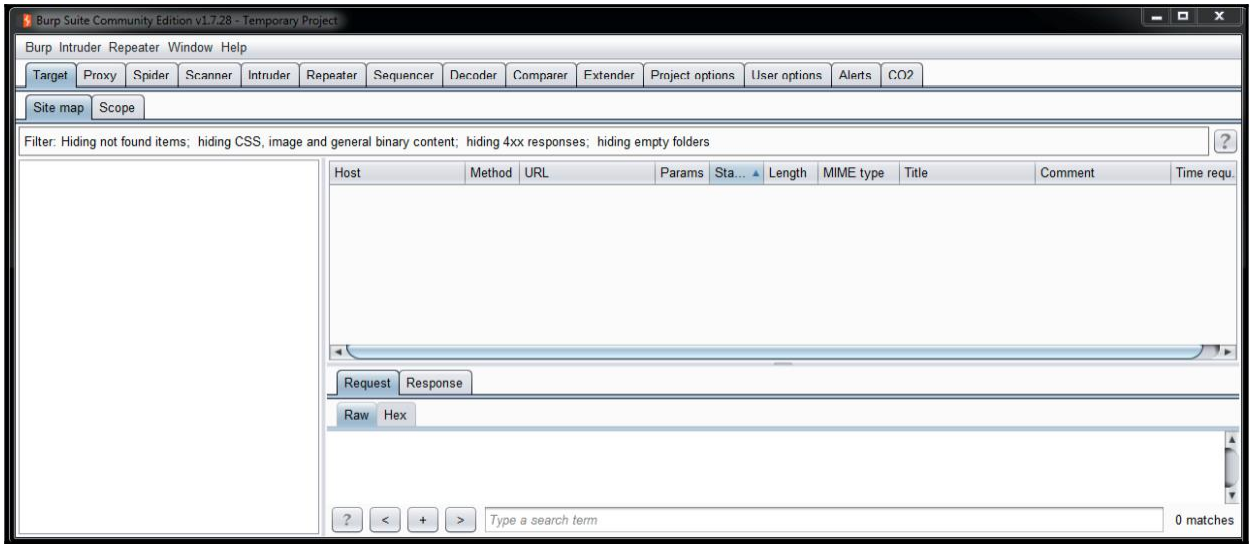
- Proof-based scanning technology is used to detect vulnerabilities.
- Automatically detects custom 404 error pages and other related URL rules.
- REST API, bug tracking.
- Give more flexible solutions.
- Scan bulk of web application in minimum time.
- Netspaker has a commercial license.



2. Burp Suite

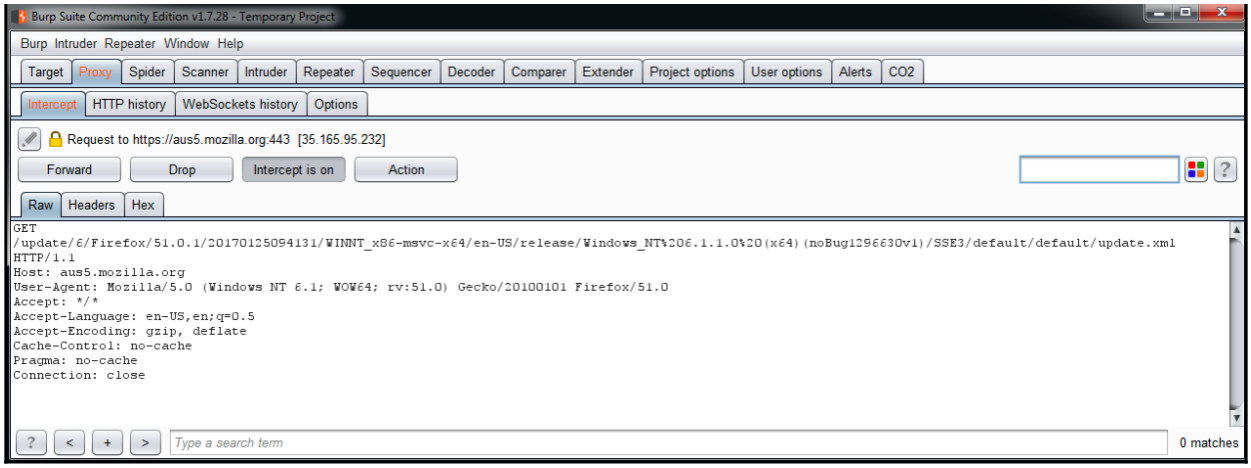
Burp Suite is also a vulnerability scanner used among many bug bounty hunters, and it is a collection of tools. We can download and use it freely, but it has limited functionality and no automation capabilities. To get the professional version, we have to spend some money. Burp Suite is an HTTP proxy and a fundamental tool for all security professionals and bug bounty hunters focused on web application security.

When you open the burp suite community edition, you can see the below window.



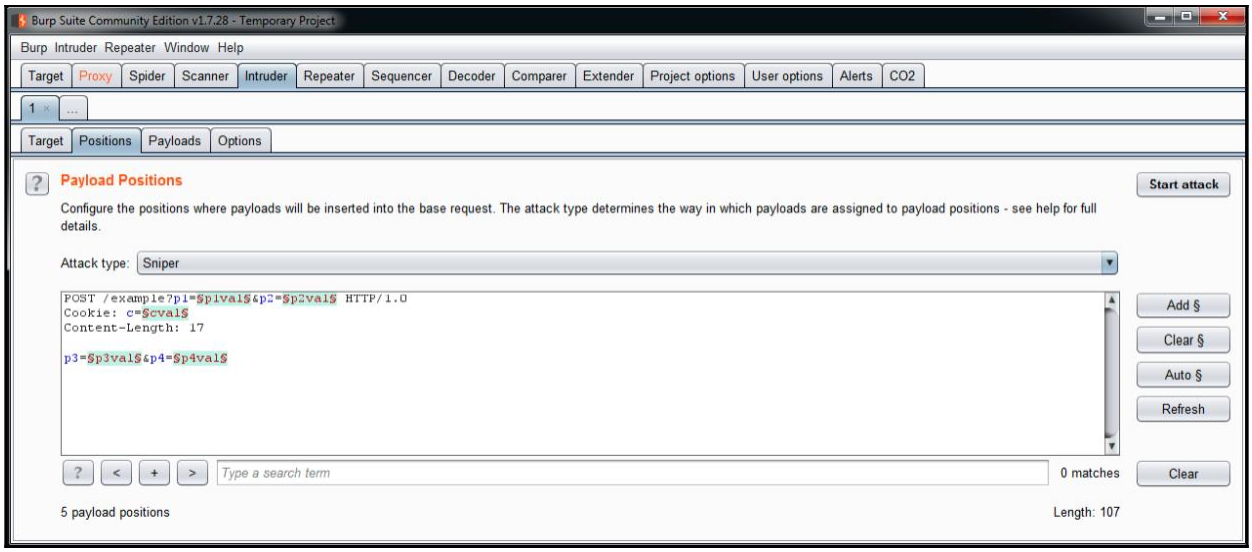
When we see the burp suite for the first time, it looks a bit complex because many tools are coming with the burp suite as a collection of tools. In addition, you can add new tools as plugins into the burp suite, but it is only available for the pro version. We can see some tabs, and these are the tools coming inbuilt, and every and each tool has configuration options. In this chapter, I will give a brief idea about the burp suite and its basics.

Proxy tab

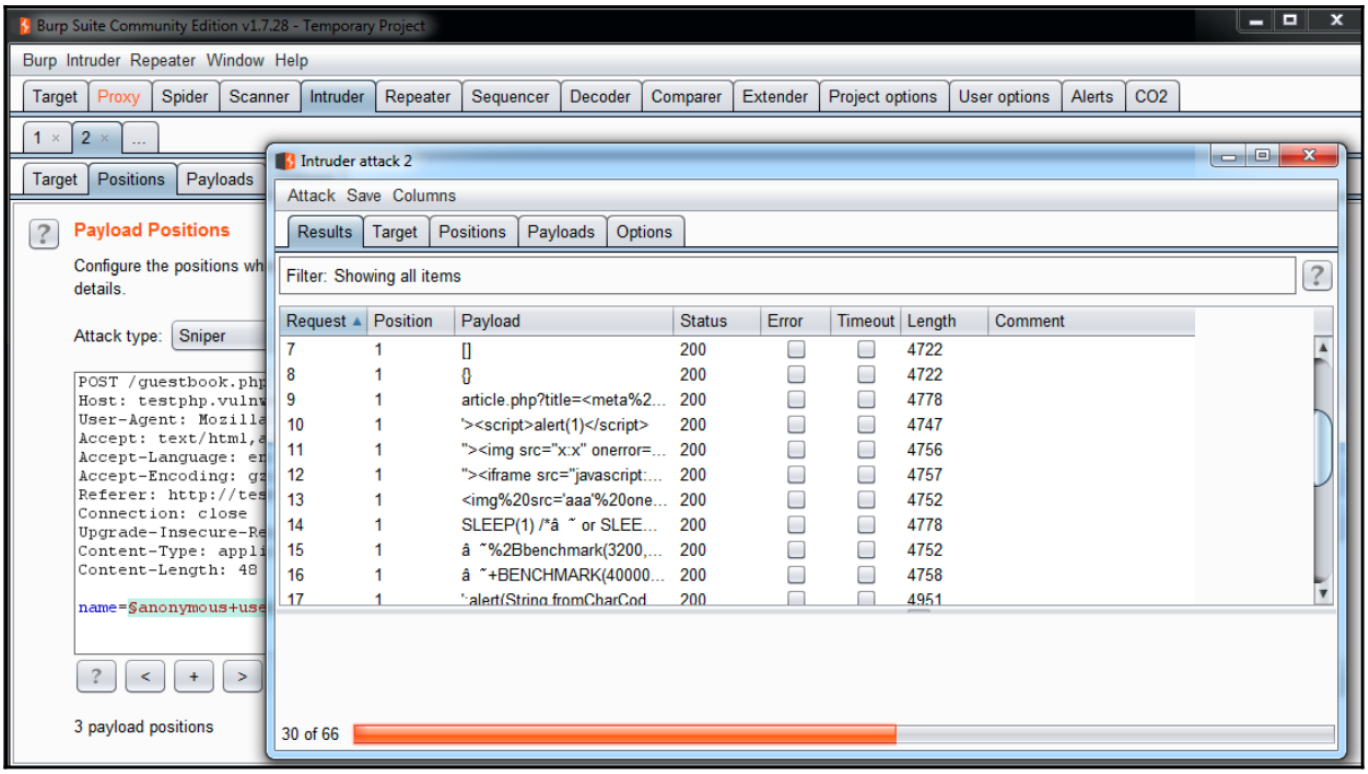


In this tab, you can see several buttons call forward, drop, intercept is on, and action. These buttons are for edit and manipulate requests. You can intercept and see requests that your browser makes. You can also analyze them easily, modify them as you want, and send them back to the web application.these are the most commonly used buttons in this proxy tab. You can do interesting things using this proxy tab.

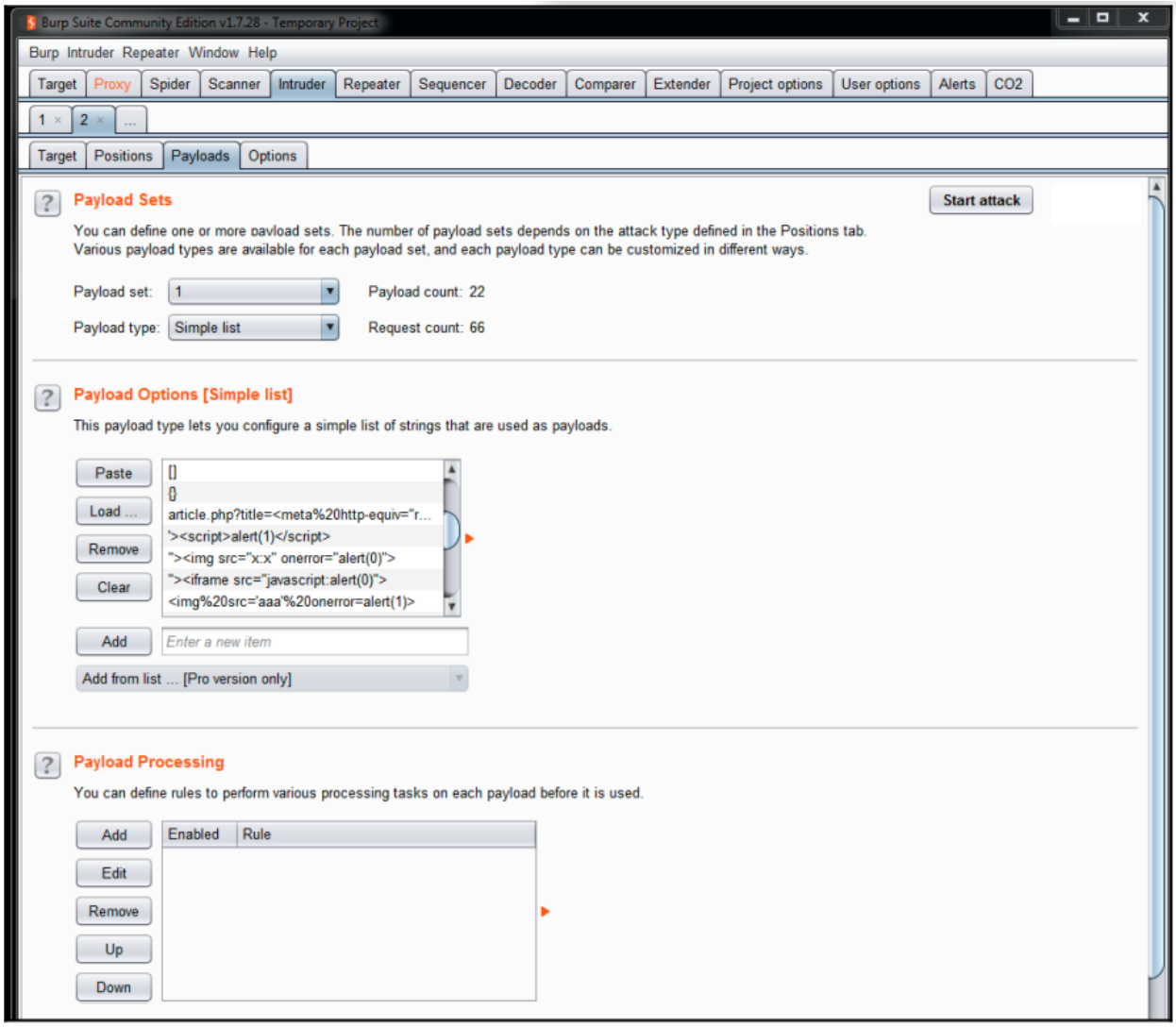
Intruder tab



When you click on the intruder tab, you can see the foregoing view. the use of this tab is you can automate the modified requests using this intruder tab. It is also capable of sending a lot of requests with different values. After sending the requests, you can also see the corresponding responses, analyze them, and find vulnerabilities. You can launch an intruder attack from this tab, and it will take you to another new window, and then it will show HTTP responses.

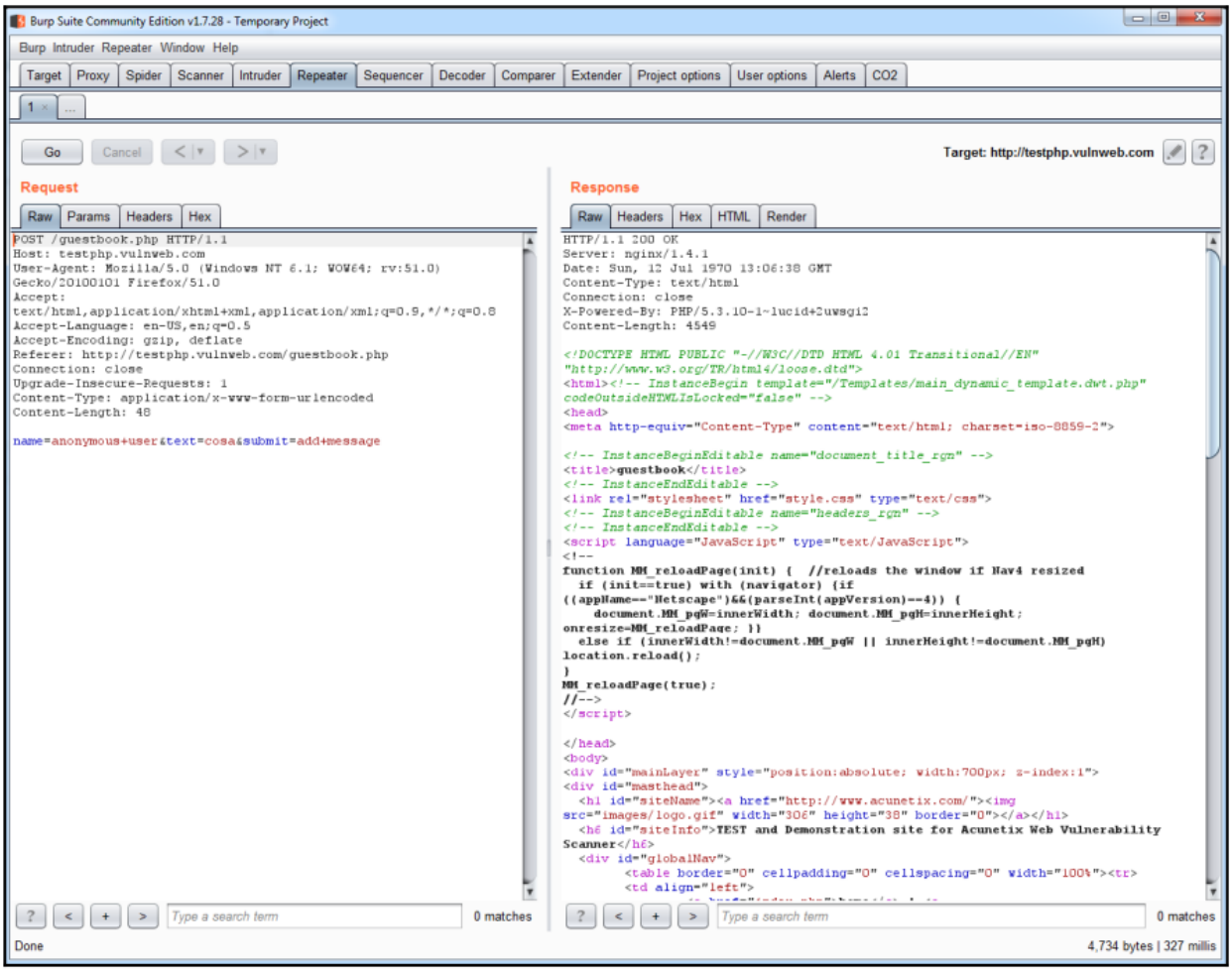


You can create your own payload, or there are a lot of word lists available on the internet with different types of testing strings, then we can load them into payload in intruder.



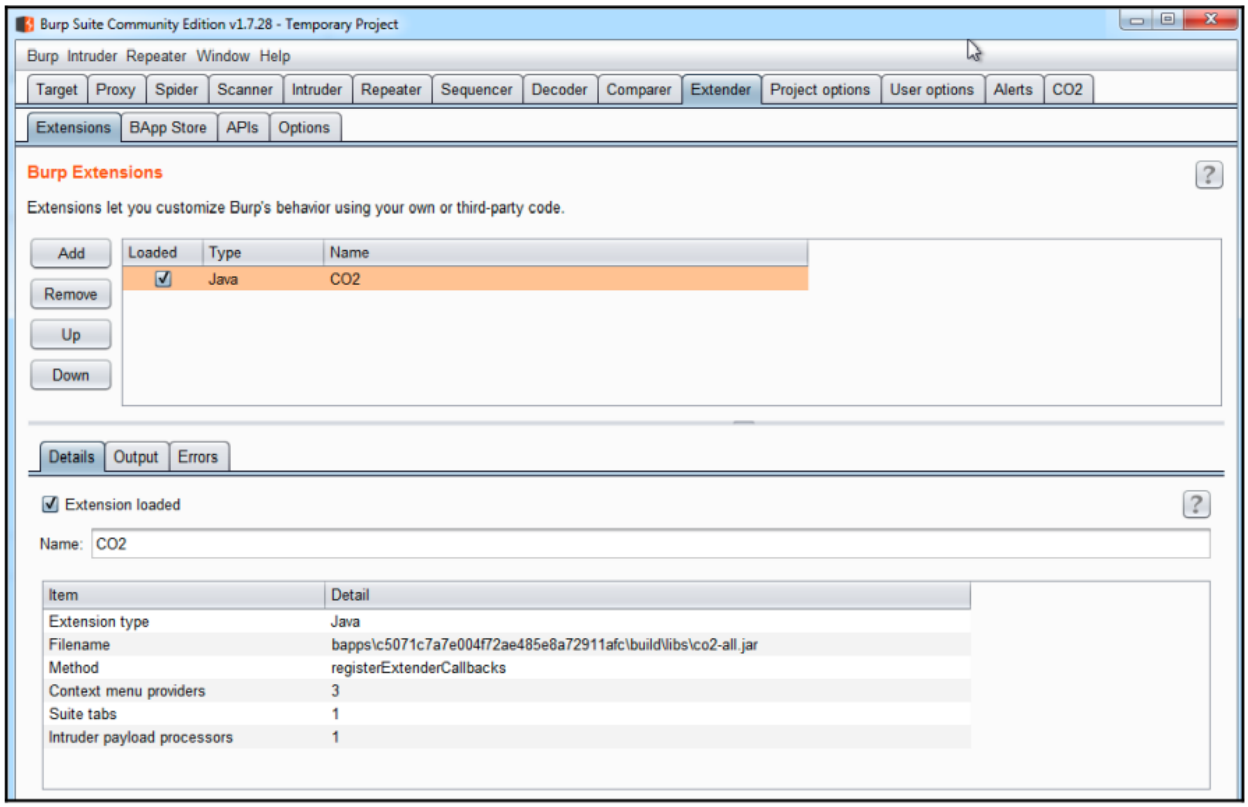
Repeater

Repeater is a useful tool in bup suite when we have to interact with the web application's backend or we can use it to edit a particular request .you can view both request and the response in the same window. It makes the analysis much easier. On the request side, we can see the original HTTP request, and on the response side, we can get results by modifying the request on the other side .also we can see the actual webpage in the render option. With this tool, we can try amazing things.



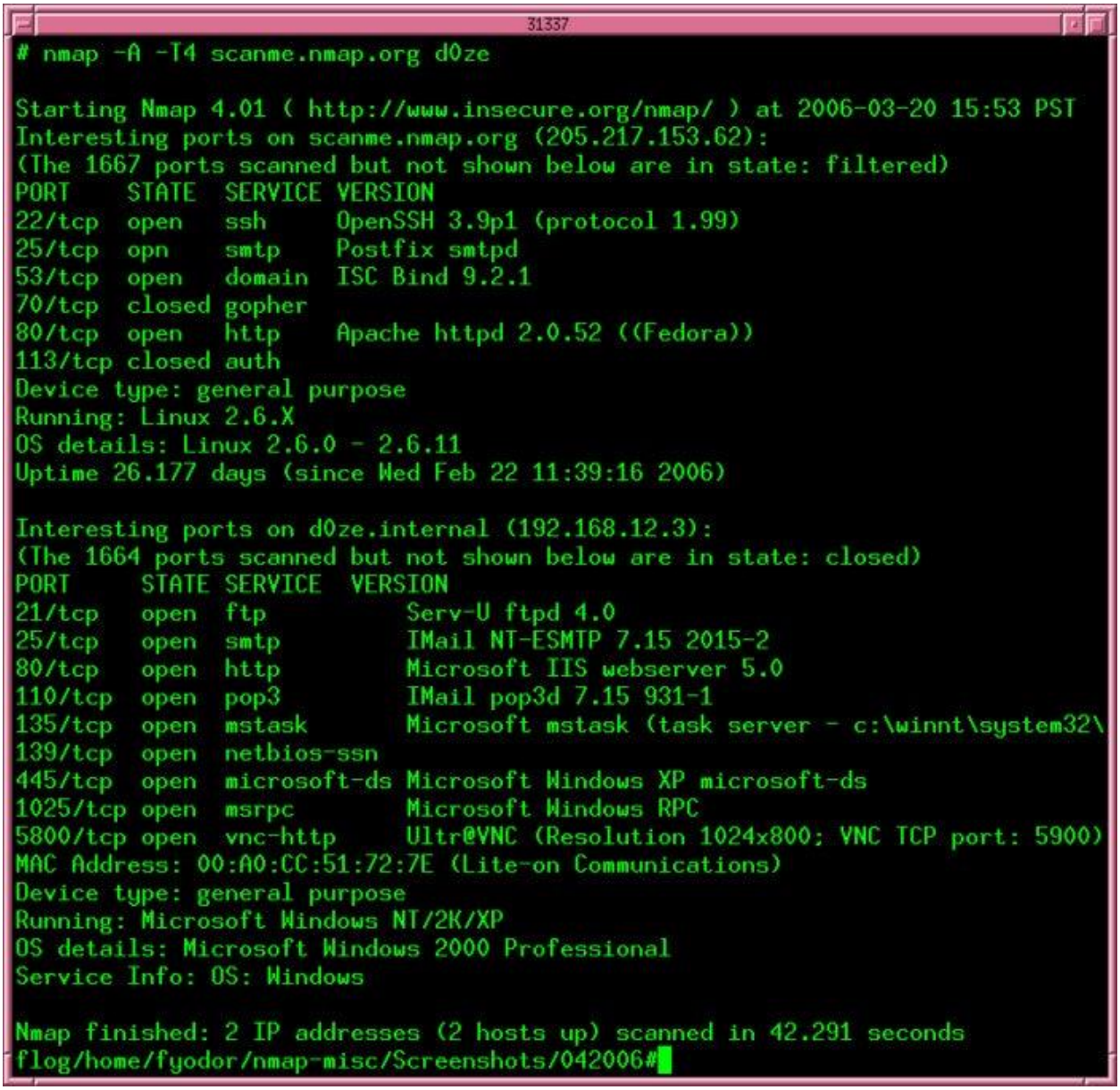
Extender

This tab lets you add more tools like plugins and extensions, and you can go to the BApp store to add plugins.



You can learn more things about the burp suite from the official portswigger site, and they give links for download the burp suite to your machine.

3. Nmap



Nmap is short for network mapper, and it is a very powerful port scanner and also a service enumerator and vulnerability scanning capabilities. Nmap can use for what kind of devices are running in a particular network and identify hosts and their services that they are offering and ports.

Nmap is capable of monitoring a single host as well as huge networks that are consisting a very large number of devices. Basically, in Nmap, it listens for responses and checks whether which ports are opened and which ports are closed, and also they use filtering or not.

Common functions in Nmap

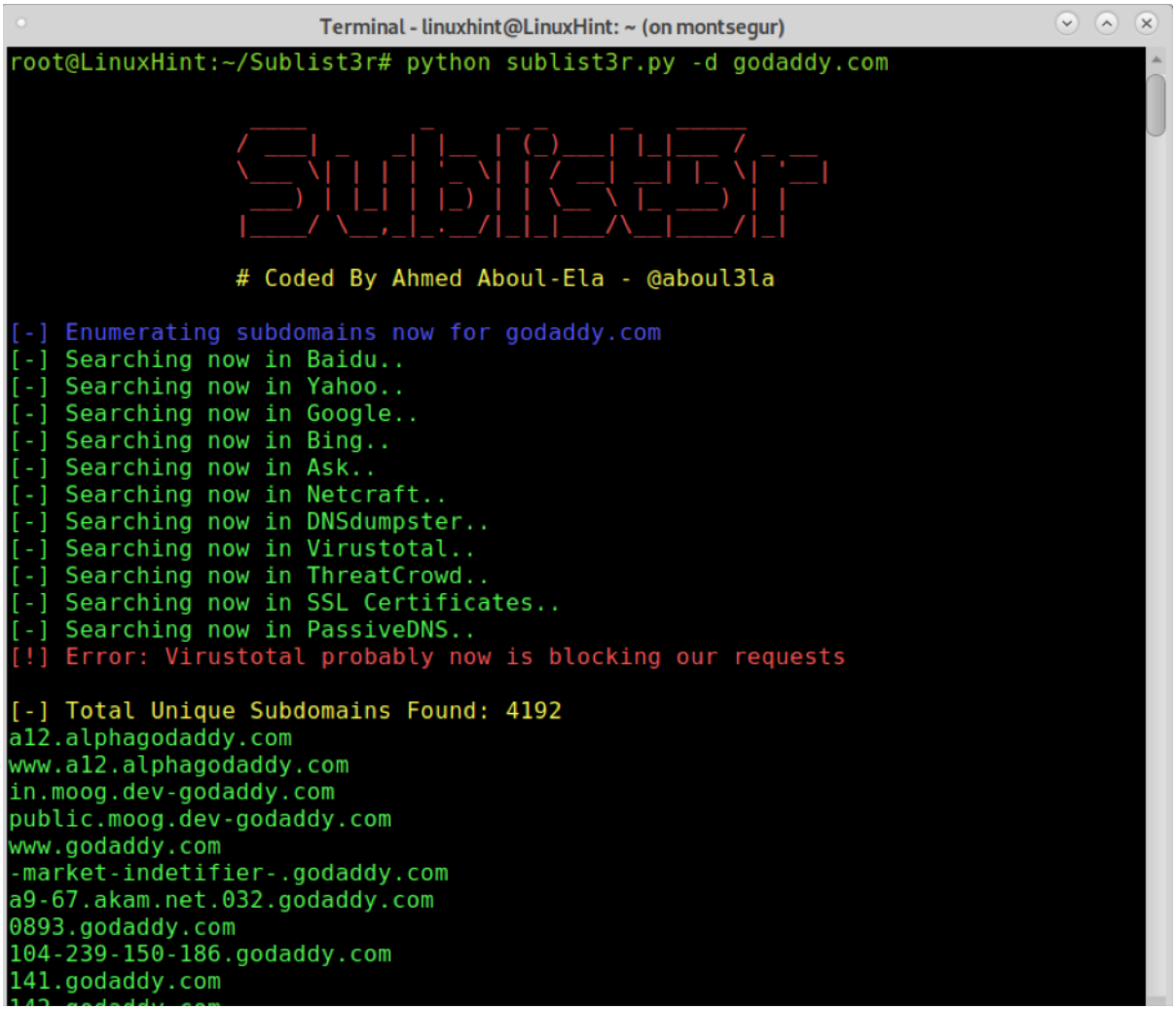
- Port scanning
- Host scanning
- Os scanning
- Ping scanning
- Scan top ports

4. Gobuster

```
└─$ $gobuster --help
Usage:
  gobuster [command]

Available Commands:
  dir         Uses directory/file brutceforcing mode
  dns         Uses DNS subdomain bruteforcing mode
  help        Help about any command
  vhost       Uses VHOST bruteforcing mode

Flags:
  -h, --help              help for gobuster
  -z, --noprogress        Don't display progress
  -o, --output string     Output file to write results to (defaults to stdout)
  -q, --quiet             Don't print the banner and other noise
  -t, --threads int       Number of concurrent threads (default 10)
  -v, --verbose           Verbose output (errors)
  -w, --wordlist string   Path to the wordlist

Use "gobuster [command] --help" for more information about a command.
```

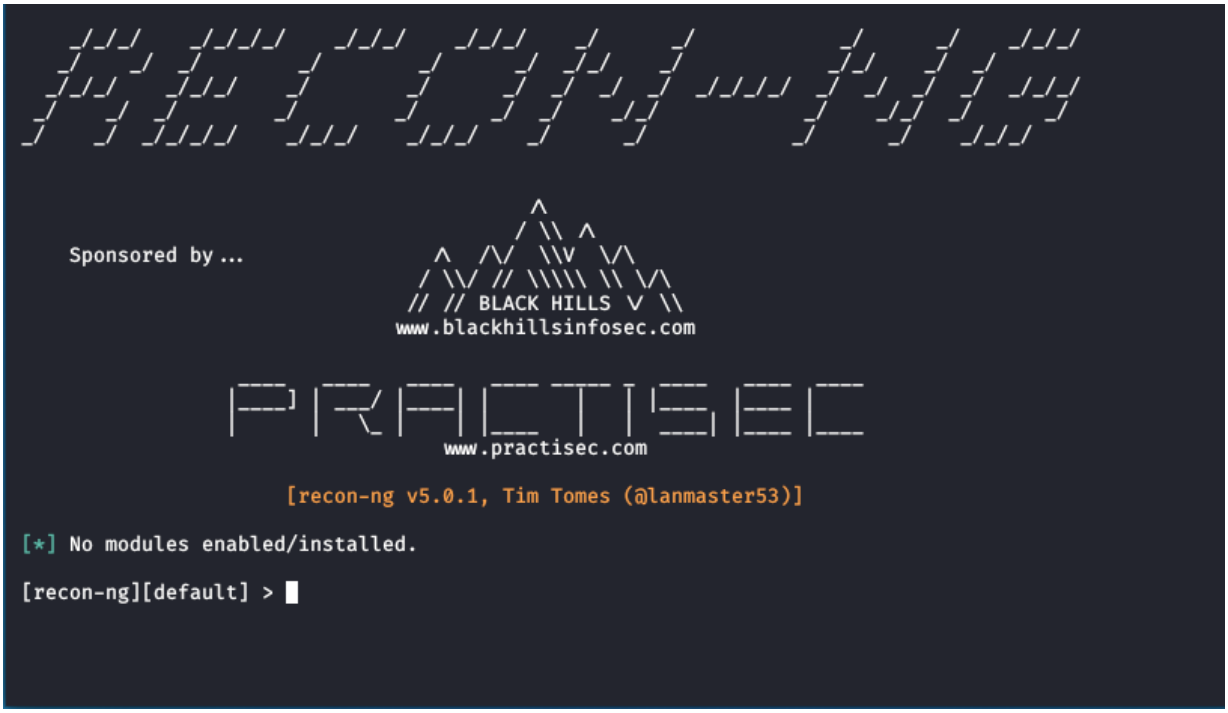
Gobuster is a record scanner, and it is used for brute force directories and files in a web application. And also, it can brute force on wildcard support DNS subdomains. This tool is written in the Go language, and it is speed than other directory scanners because the GO language is known to be fast.

5. Sublist3r



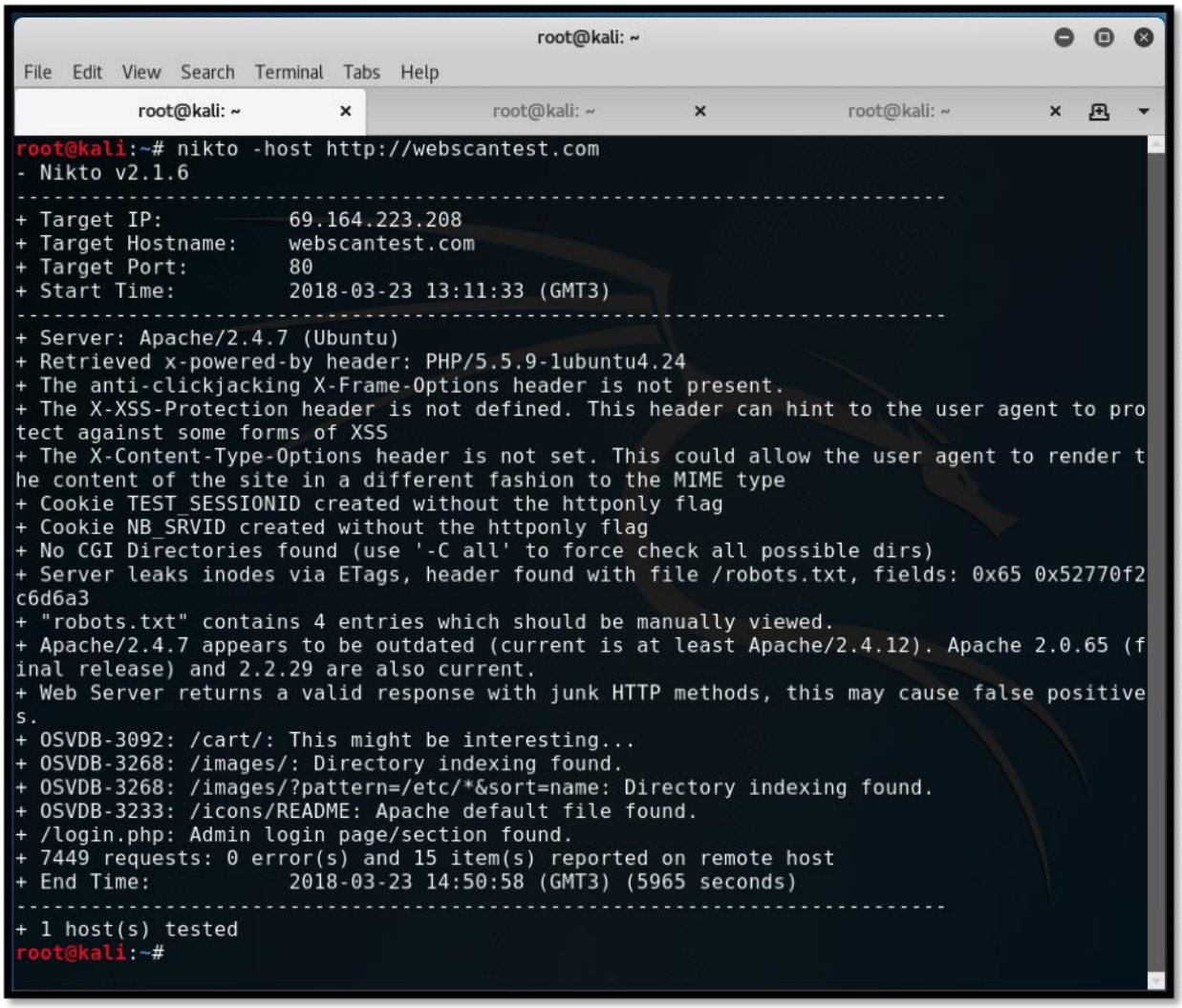
Sublist3r is written in python language, and it uses for enumerating subdomains of a particular website. It helps professionals in web application security to gather subdomains of a specific domain. To get more accurate search results, sublist3r uses search engines and some tools like Netcraft,virustotal.

6. Recon-ng



Recon-ng is an open-source reconnaissance tool, and anyone can download it without paying. It is written in python, and this tool is based on Open Source Intelligence (OSINT). It has a similar interface to Metasploit and is very easy to use for anyone. It provides a lot of helpful features and tools. What you have to do is using the command line to give the necessary commands. You can do any recon, and it provides many file types to output your report.

7. Nikto



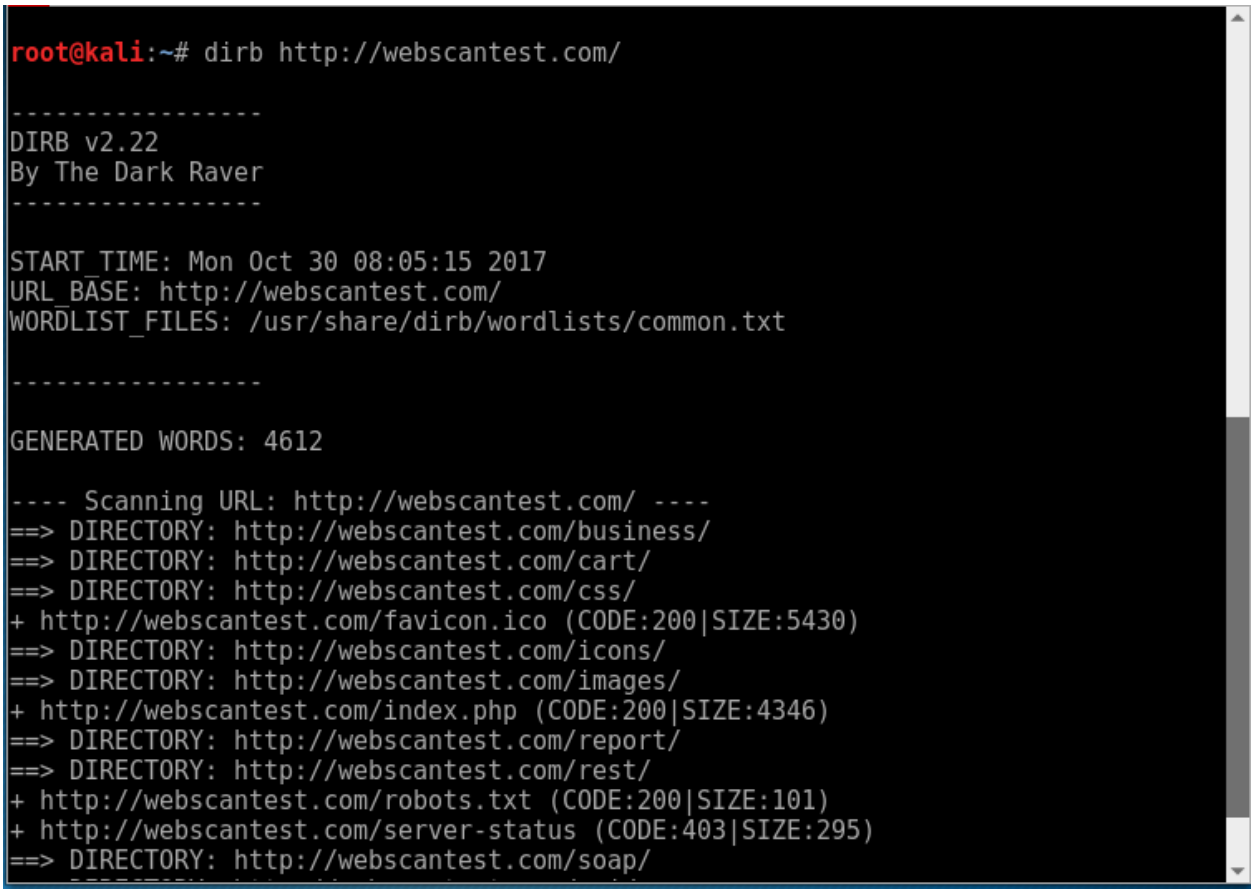
This tool is also freely available for anyone, and it is a vulnerability scanner .nikto can identify outdated software versions, dangerous files, and more other problems in a webserver. Nikto is able to scan a particular server in less time because it is designed as a stealthy tool so it can prevent from being spotted by others when we are performing a scan.

Main features

- SSL support and full HTTP proxy support
- Checks for outdated server software and components
- Scan multiple ports on a server

- Easily update
- Subdomain guessing

8. Dirb

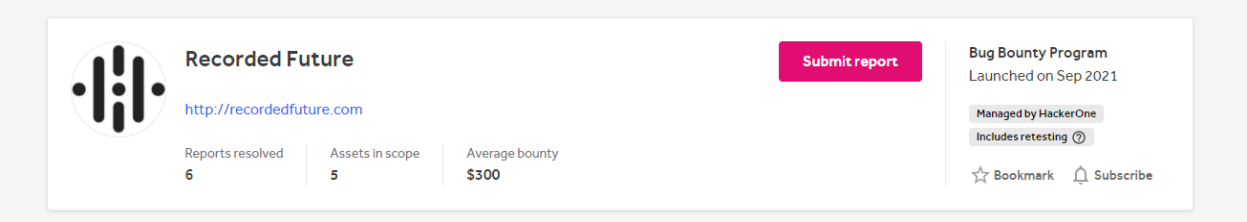


Dirb is a web content scanner with a simple interface. It scans a given domain for existing or hidden web objectives. It works based on a brute force attack, so you can also give a custom wordlist for the dictionary attack. It is not a vulnerability scanner, but it scans for identify files and directories.

REPORT 01

Getting start

Before starting the journey of bug bounty hunting, we first need to select a bug bounty program from a reliable website like HackerOne, Bugcrowd, etc., so I selected a program from HackerOne, and the company name is "recorded future" it is a privately held cybersecurity company in united states.



The Recorded Future Intelligence Platform produces accurate and actionable intelligence at scale, delivered in real-time. It combines automated analytics with human expertise to unite an unrivalled variety of open source, dark web, technical sources, and original research.

First of all, we must read the policies and other details given in the description .then we can get a better idea of what happens in this company and what our scope is and so on. they have first given the rewards according to the vulnerability level. Low low-level bugs give $100, a medium-level $300, a high-level $750, and critical bugs give $2000 as a reward. Then they tell their program rules. This is very important to us because we will analyze their web application, so we must behave according to these given rules.

Program Rules

Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be eligible for a reward.

- Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
- When duplicates occur, we only award the first report that was received (provided that it can be fully reproduced).
- Multiple vulnerabilities caused by one underlying issue will be awarded one bounty.
- Social engineering (e.g. phishing, vishing, smishing) is prohibited.
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with explicit permission of the account holder.

This program is aimed at unauthenticated access only. Recorded Future will not be able to provide accounts to the services to any would be pentesters.

Then are given the rewards based on severity per CVSS (the Common Vulnerability Scoring Standard), and they are given the score range and the reward they are given for each range.

Critical (9.0 - 10.0)	High (7.0 - 8.9)	Medium (4.0 - 6.9)	Low (0.1 - 3.9)
$2,000	$750	$300	$100

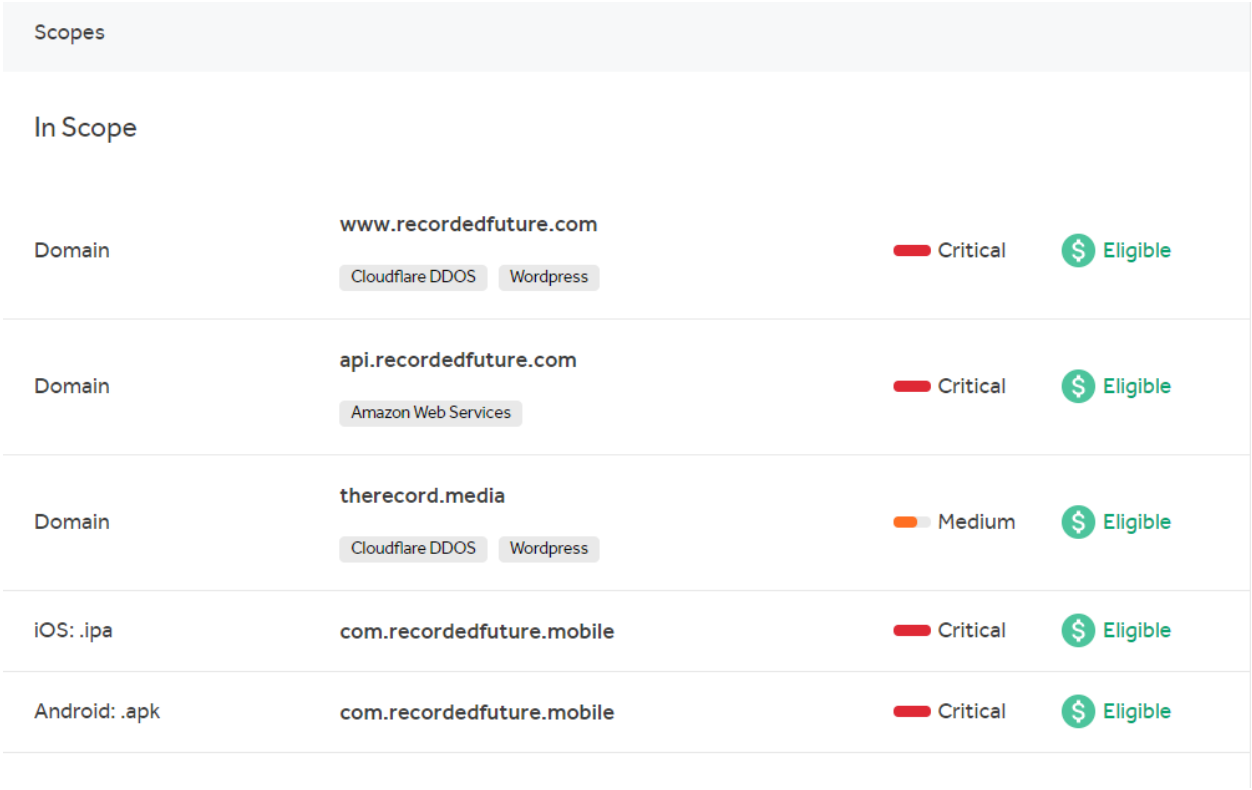
Next, they give the out-of-scope vulnerabilities. We cannot try to find a bug or put them into our report using these vulnerabilities. We have to find a bug that should not be in this given list.

Out of scope vulnerabilities

When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug. The following issues are considered out of scope:

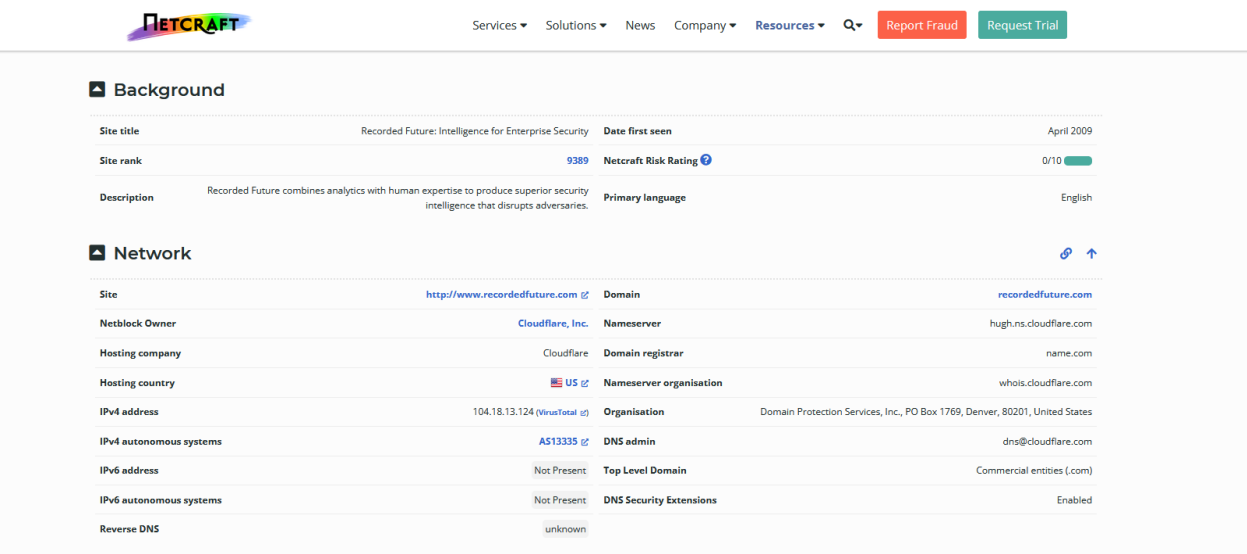
- Clickjacking on pages with no sensitive actions
- Cross-Site Request Forgery (CSRF) on unauthenticated forms or forms with no sensitive actions
- Attacks requiring MITM or physical access to a user's device.
- Previously known vulnerable libraries without a working Proof of Concept.
- Comma Separated Values (CSV) injection without demonstrating a vulnerability.
- Missing best practices in SSL/TLS configuration.
- Any activity that could lead to the disruption of our service (DoS).
- Content spoofing and text injection issues without showing an attack vector/without being able to modify HTML/CSS
- Rate limiting or bruteforce issues on non-authentication endpoints
- Missing best practices in Content Security Policy.
- Missing HttpOnly or Secure flags on cookies
- Missing email best practices (Invalid, incomplete or missing SPF/DKIM/DMARC records, etc.)
- Vulnerabilities only affecting users of outdated or unpatched browsers [Less than 2 stable versions behind the latest released stable version]
- Software version disclosure / Banner identification issues / Descriptive error messages or headers (e.g. stack traces, application or server errors).
- Public Zero-day vulnerabilities that have had an official patch for less than 1 month will be awarded on a case by case basis.
- Tabnabbing
- Open redirect - unless an additional security impact can be demonstrated
- Issues that require unlikely user interaction
- Broken links links on www.recordedfuture.com or therecord.media

The in-scope area is very important to us for bug bounty hunting because every scan we are done is only for these in-scope domains. Otherwise, we have to face many problems.

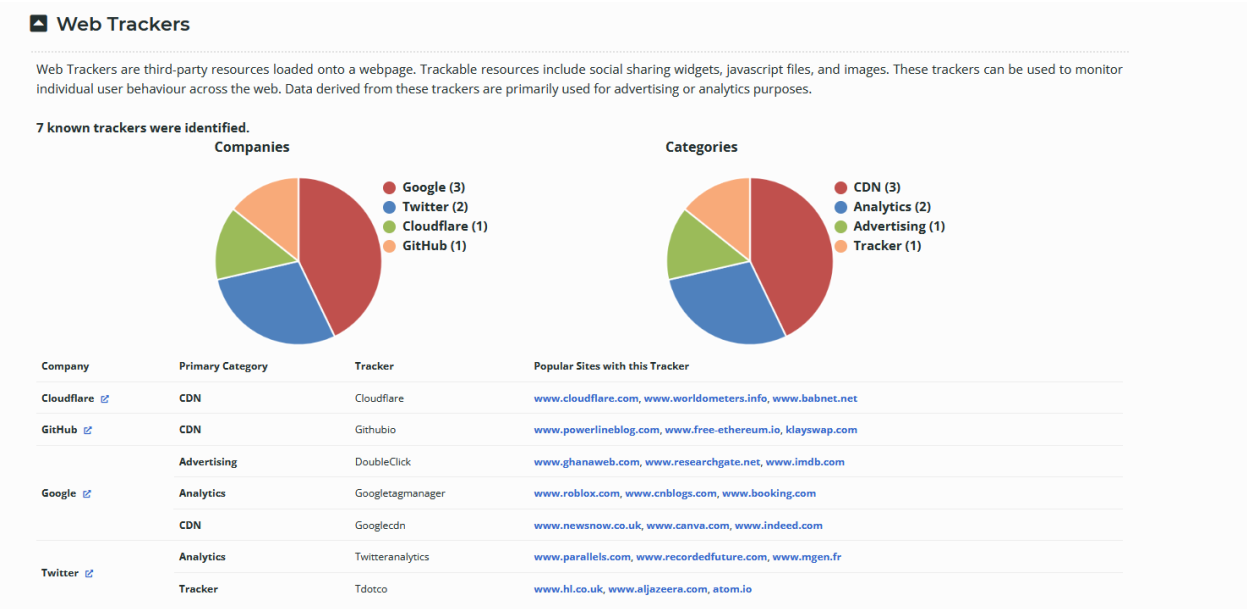


Information Gathering

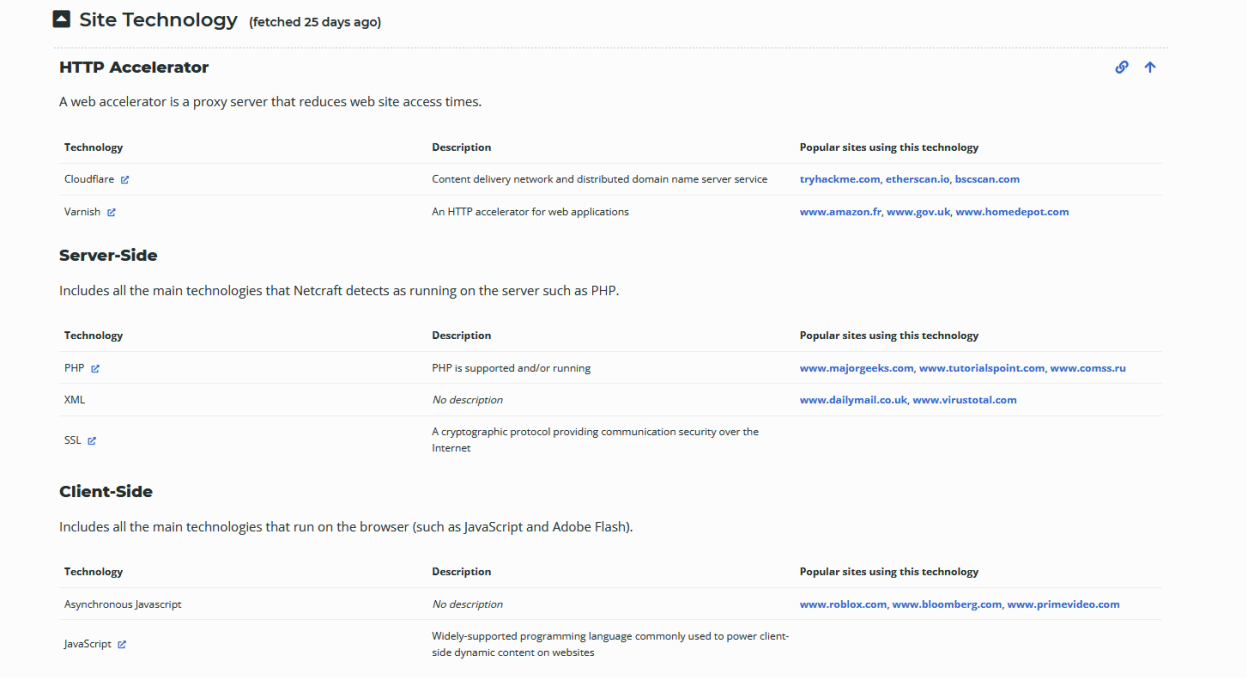
Let's look at how we can gather information about technologies and other useful information about recordedfuture.com.there are a lot of tools and websites for this, but here we are only using Netcraft, so let's put our domain and see what we can capture from Netcraft.



At the top, It shows some basic things such as site title, when the website was created, and site rank. Then we can see site URL and Cloudflare as the hosting company and its hosting country. And again, we can see the IP address of our target .in the black hat hacker point of view, we can use the name server to launch a spear-phishing attack to obtain the target domain, but we cannot do things like that because we are just finding a vulnerability in a legal manner.



On the web trackers, it shows third-party resources or applications used on our target domain. We can see it uses Cloudflare CDN, google CDN, some advertising services and analytics are using in this domain.



Site Technology (fetched 25 days ago)

HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

Technology	Description	Popular sites using this technology
Cloudflare	Content delivery network and distributed domain name server service	tryhackme.com, etherscan.io, bscscan.com
Varnish	An HTTP accelerator for web applications	www.amazon.fr, www.gov.uk, www.homedepot.com

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
PHP	PHP is supported and/or running	www.majorgeeks.com, www.tutorialspoint.com, www.comss.ru
XML	*No description*	www.dailymail.co.uk, www.virustotal.com
SSL	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Asynchronous Javascript	*No description*	www.roblox.com, www.bloomberg.com, www.primevideo.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

The site technology is one of the most important areas to us because it shows a lot of technologies used in our target domain. We can see the Cloudflare hosting company and an HTTP accelerator called varnish. We can see it uses PHP on the server-side area so the website can understand and execute PHP code. This can be useful if we manage to execute some code on our domain, then we can create payloads in Metasploit using PHP.also we can see it uses SSL to create an encrypted communication between the web server and the web browser.

It uses javascript as a client-side technology, so if we manage to come up with javascript code, it will affect the users or the people who visit the website.

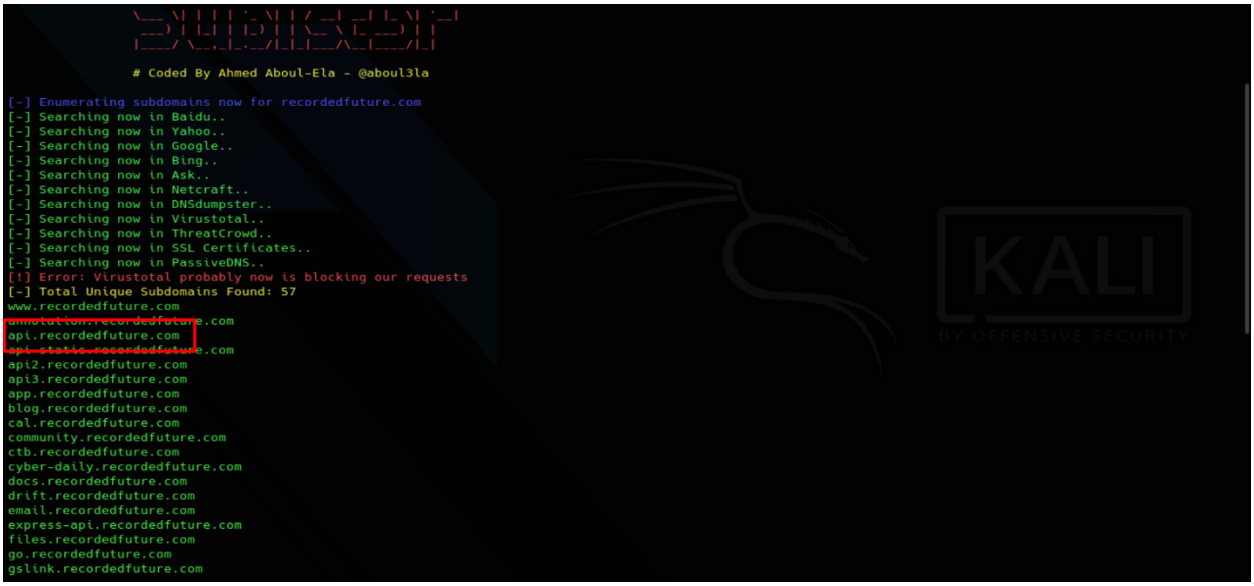
Gathering subdomain info

Then we are going to find what are the subdomains of our target domain

Why the subdomains are important for us .becuase they maintain several domains for their customers, employees, VIP users, and for new beta versions .they not reveal these domains for you unless you are a customer or an employee of that company. So sometimes, that domains could include some vulnerabilities. If it a company is going to update their web application first, they give it for the beta version. So definitely beta version has some vulnerabilities or exploits because it includes some experimental features, and they are still under development .people don't know these other domains because these are not advertised. So we can enumerate subdomains, and it can be useful to try and hack into them.

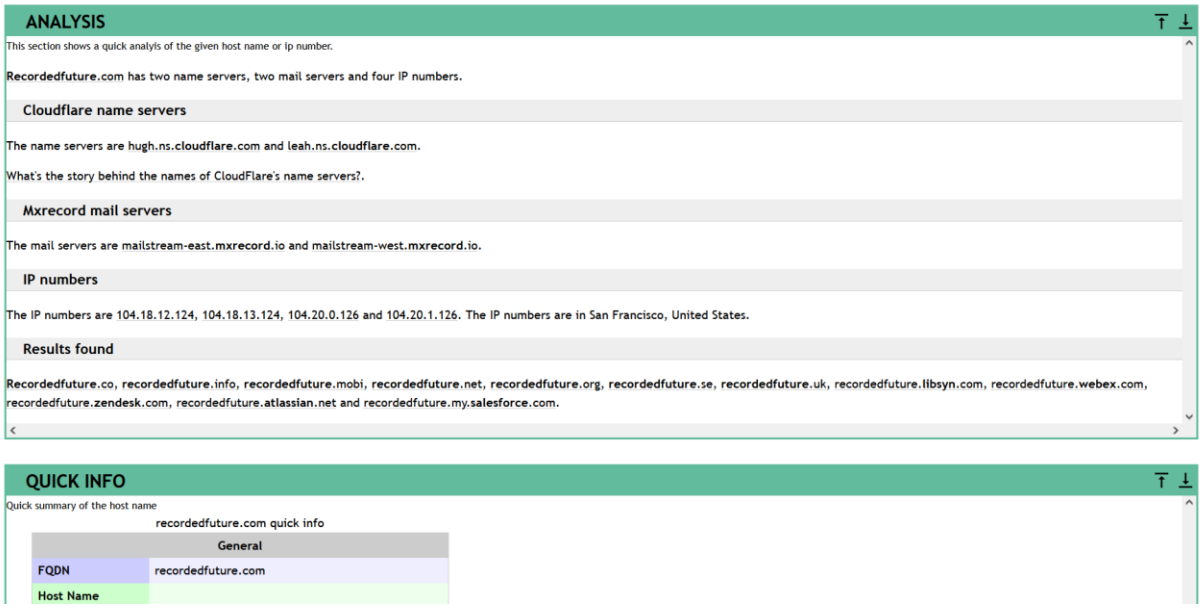
So we can do some domain scans using several tools. There are few tools we can use to enumerate subdomains.

- Sublist3r
  Basic command
  python sublist3r.py -d example.com

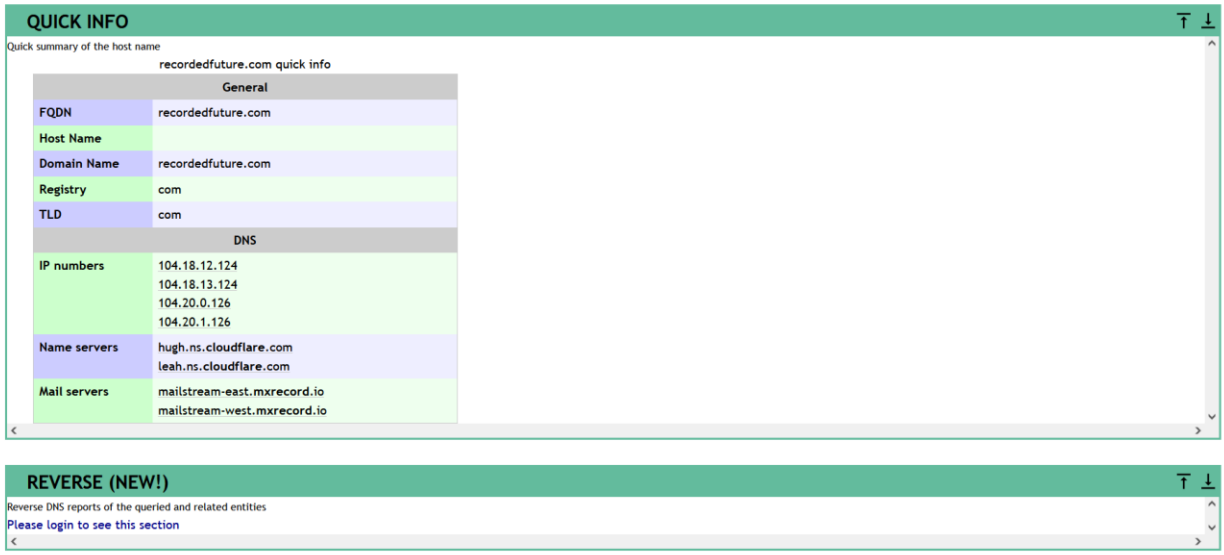


Now we can see sublister giving 57 unique domains for our target domain. We can also see some domains in the in-scope domains given in the bug bounty program description. If we are unable to find a bug using our target domain, we can try to hack into these domains and get access to whatever domain we want .beacuse all domains are located in the same server, and all domains have the exact same IP address.

Earlier, we found recordedfuture.com domains IP address, technologies it uses, and some subdomains. Now we are going to gather more details about our domain. So we are going to use a website called robtex.com to collect some information.



After giving the domain name, we got a lot of details. We can see the domain has two name servers. We can also see the Cloudflare name servers, and It is the hosting company of recordedfuture.com.it is very important information for bad hackers because they can pretend like Cloudflare hosting company and say an interesting thing for recordedfuture.com and ask to login to a fake page that the attacker created then he will steal their information. Also, we can see a mail server and the IP address again, so we can use this IP address to find other domains in the same server we did earlier.



QUICK INFO

Quick summary of the host name

recordedfuture.com quick info

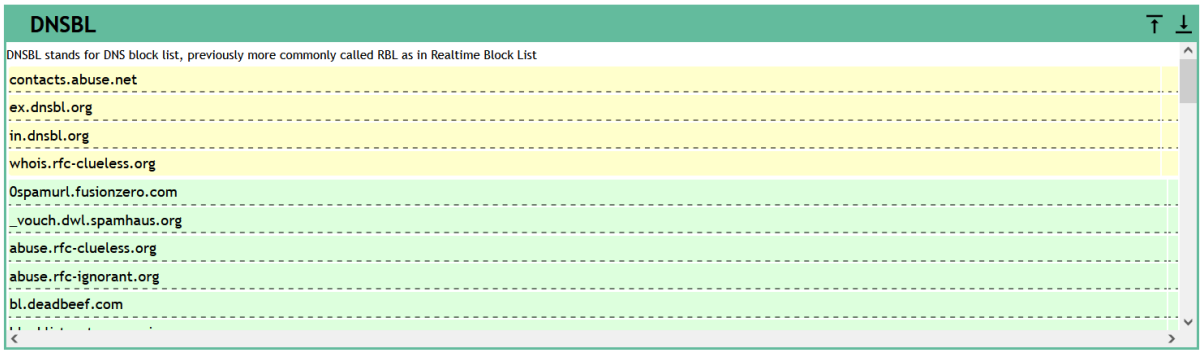
General	
FQDN	recordedfuture.com
Host Name	
Domain Name	recordedfuture.com
Registry	com
TLD	com
DNS	
IP numbers	104.18.12.124 104.18.13.124 104.20.0.126 104.20.1.126
Name servers	hugh.ns.cloudflare.com leah.ns.cloudflare.com
Mail servers	mailstream-east.mxrecord.io mailstream-west.mxrecord.io

REVERSE (NEW!)

Reverse DNS reports of the queried and related entities

Please login to see this section

On the quick info, we can see a summary of the things we saw before, and in the reverse section, we give the reverse DNS lookup, but we have to log in to the robtex site. We can use that to translate the IP address to the domain name or all the linked domain names.



DNSBL

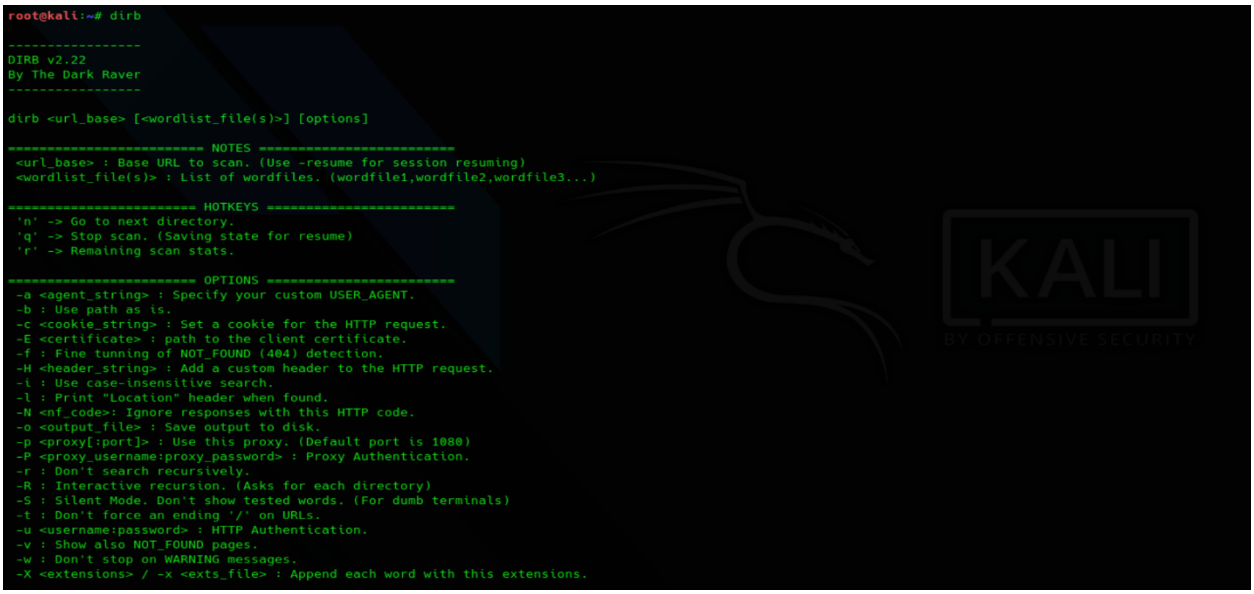
DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List

contacts.abuse.net
ex.dnsbl.org
in.dnsbl.org
whois.rfc-clueless.org
0spamurl.fusionzero.com
_vouch.dwl.spamhaus.org
abuse.rfc-clueless.org
abuse.rfc-ignorant.org
bl.deadbeef.com

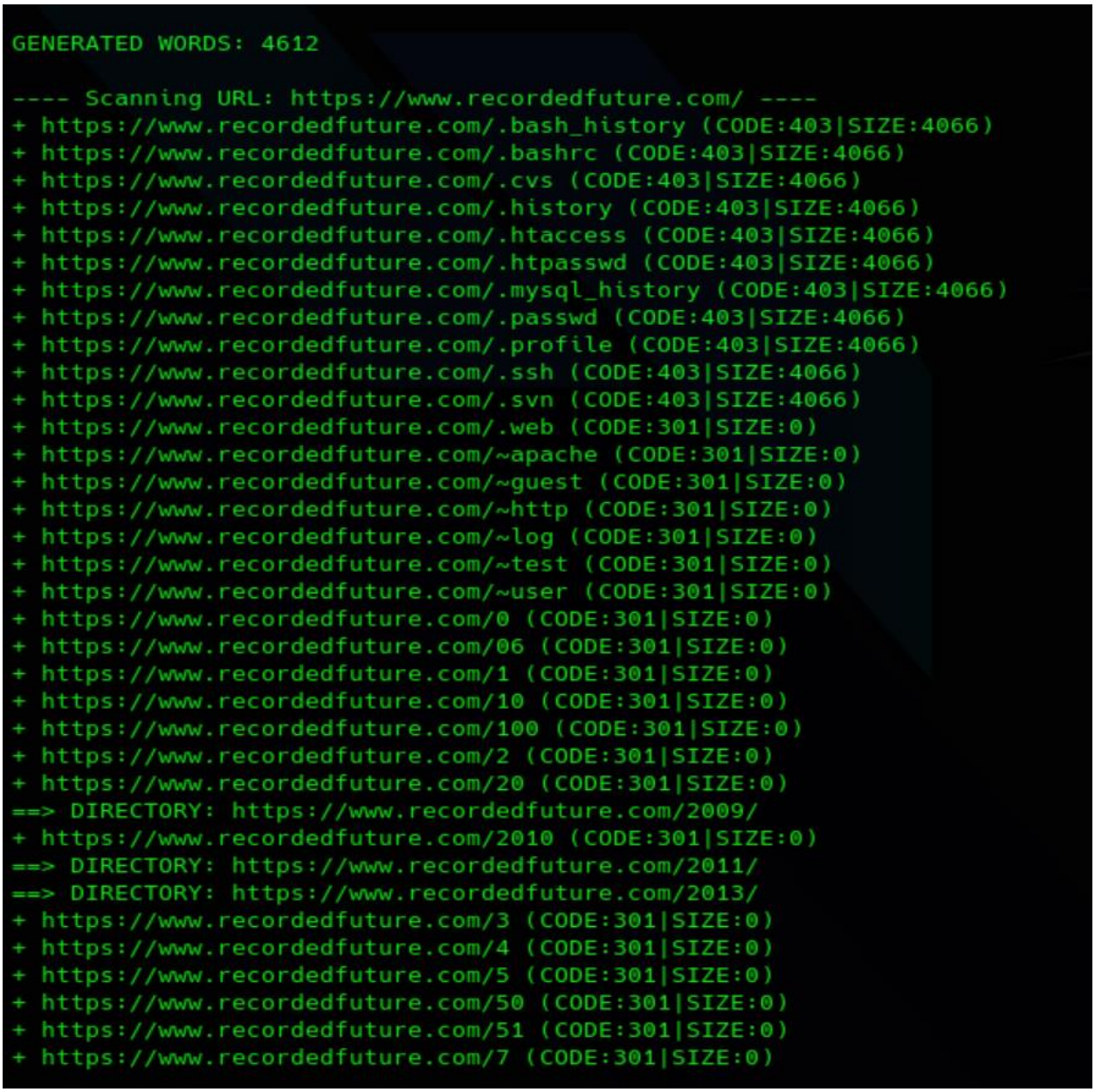
And finally, we have the DNS block information. It is a list that consisting websites to use send spam. Simply it means emails sent from these sites are considered spam by recordedfuture.com.

Gather information about files and directories

So far, we have a look at the basic information we can gather, some tools, and websites. Now we are going to find files or directories stored in the recordedfuture.com domain's server. This is very important because these files can be included passwords, config information, and some clues to access the target server, which will help us find a vulnerability. The tool we are going to use is called dirb.



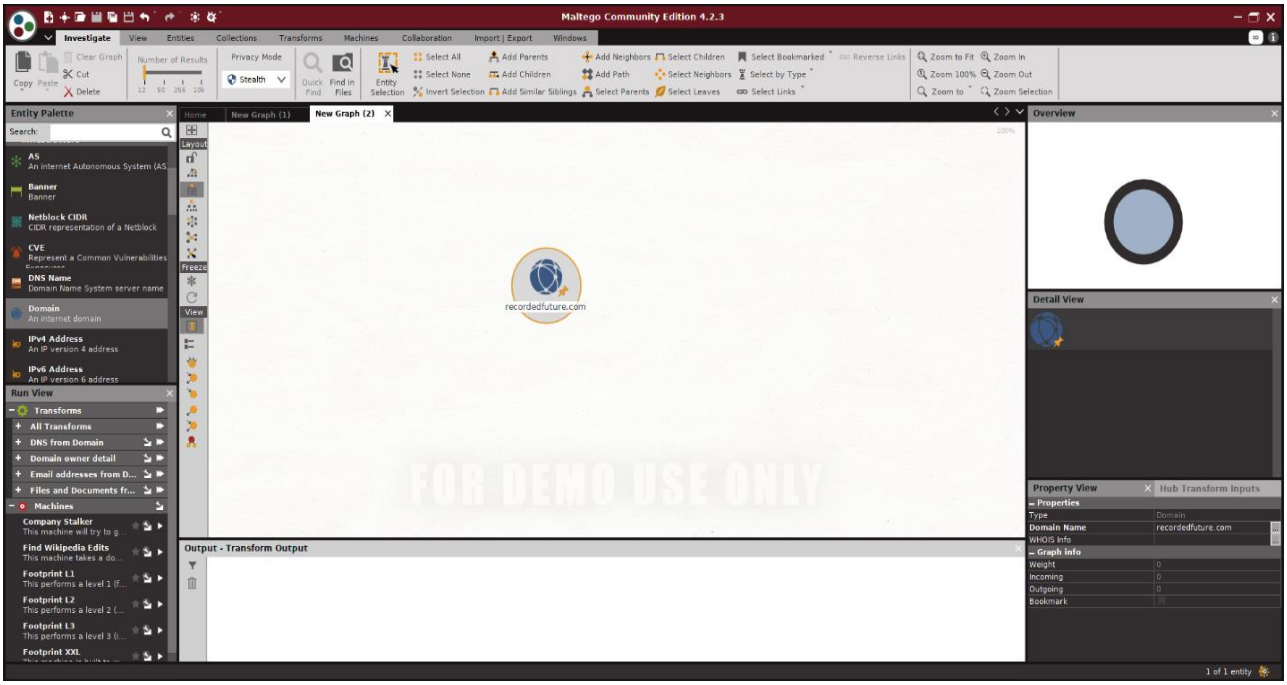
To use this tool, you have to type dirb then the URL, and it asks for a wordlist. It works based on a brute force attack, and it uses the wordlist and sends requests with those names to find a matching file or directory from the target server. It only gives you the matching files or directories that match the wordlist names. But you can try with custom wordlists.



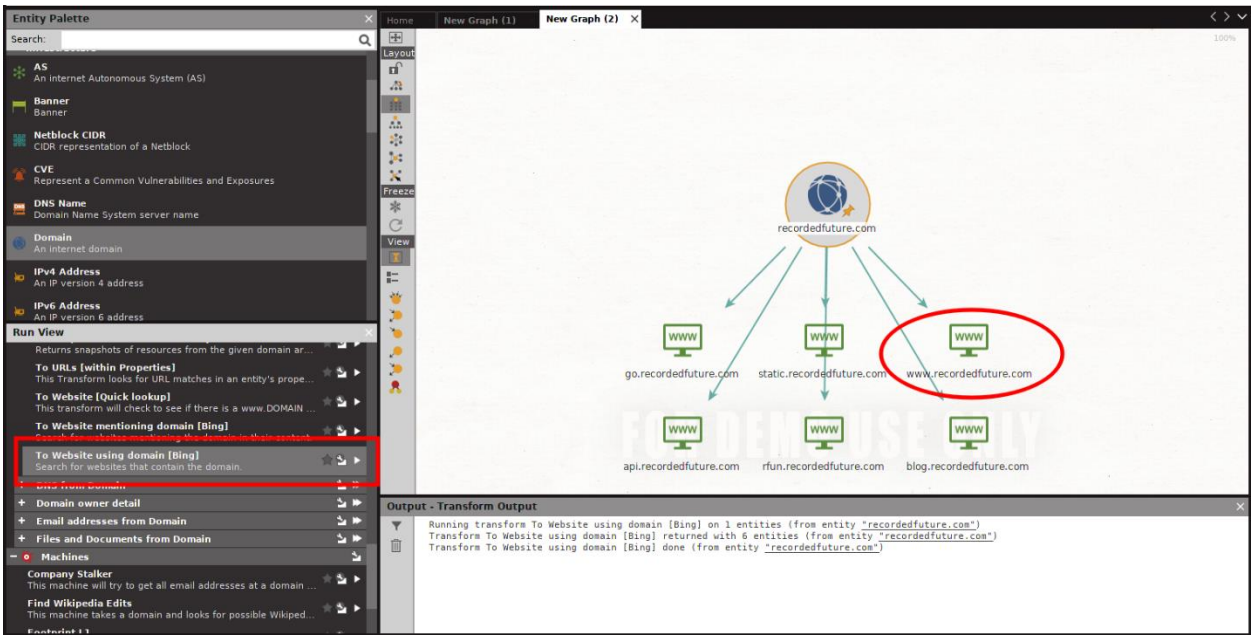
We can see It found some interesting files and directives in our target domain. So we can go through each one and see if there are any important things in that files. It should definitely be something important. It also shows the status code so we can save time by avoiding opening the blocked directories. We can see code 403 that means the server understood the request but refused to authorize it. So we cannot get any information from that files.

Next, we are going to look at another tool called maltego. We can use this tool to gather information on pretty much everything. But we only use it to gather information about our

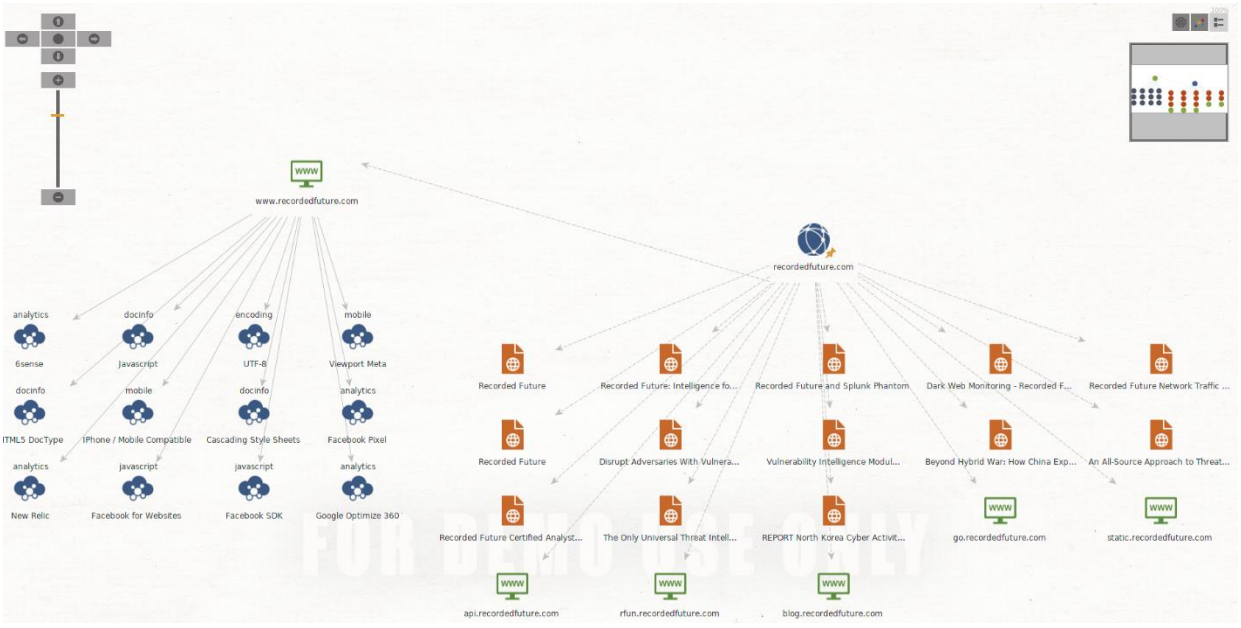
target. First, we can go to the entity palette and drag and drop the domain into the white area. Then we can change the domain to recordedfuture.com.



Then we can select a suitable transform from the run view section or transform tab. as the first transform; we can run the website using domain transform.



Now we can see our target domain that is recordedfuture.com and other subdomains. These are we found earlier as well. Let's run a transform to find the files and other technologies in this domain.

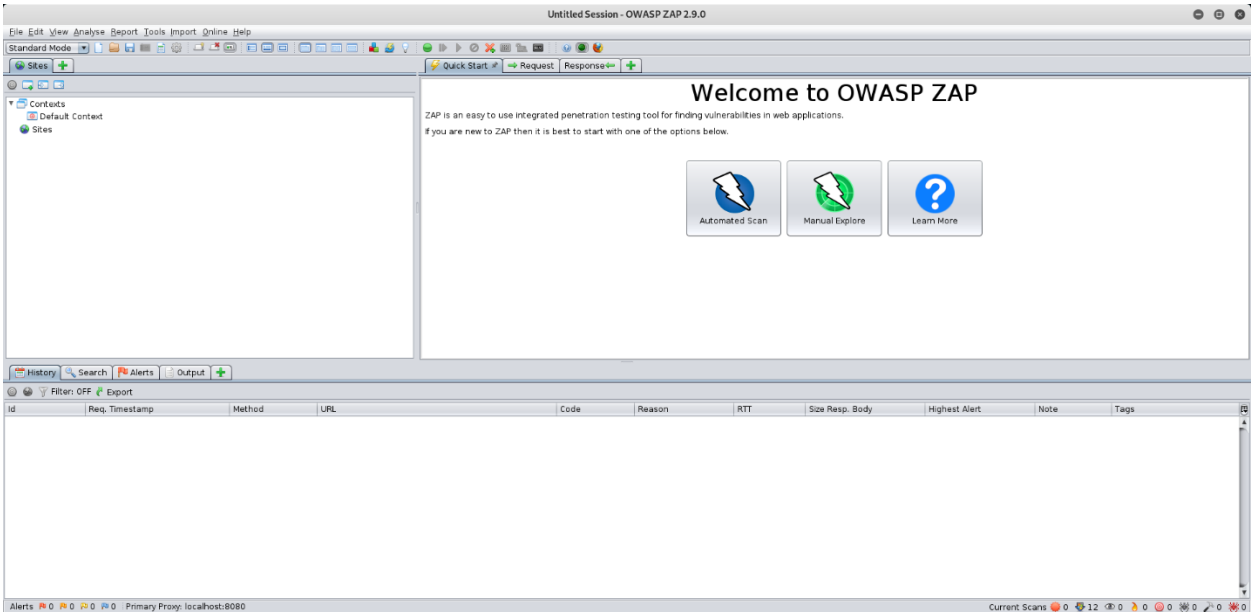


Now we can see all the technologies uses inside the domain and some files stored in the server. We can see recordedfuture has a mobile version that may be a mobile app. It uses google analytics services and some encoding mechanisms; these things may be useful in our further analysis.

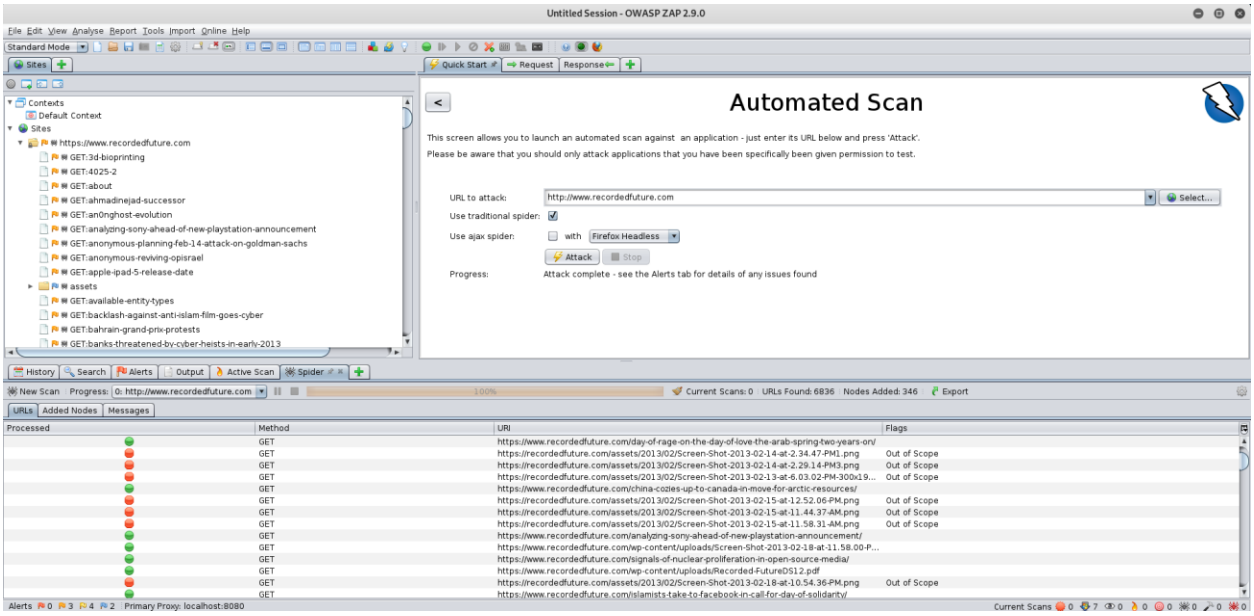
Now we have an idea about recordedfuture.com, and we gathered some data. now we can move to the vulnerability

Vulnerability assessment

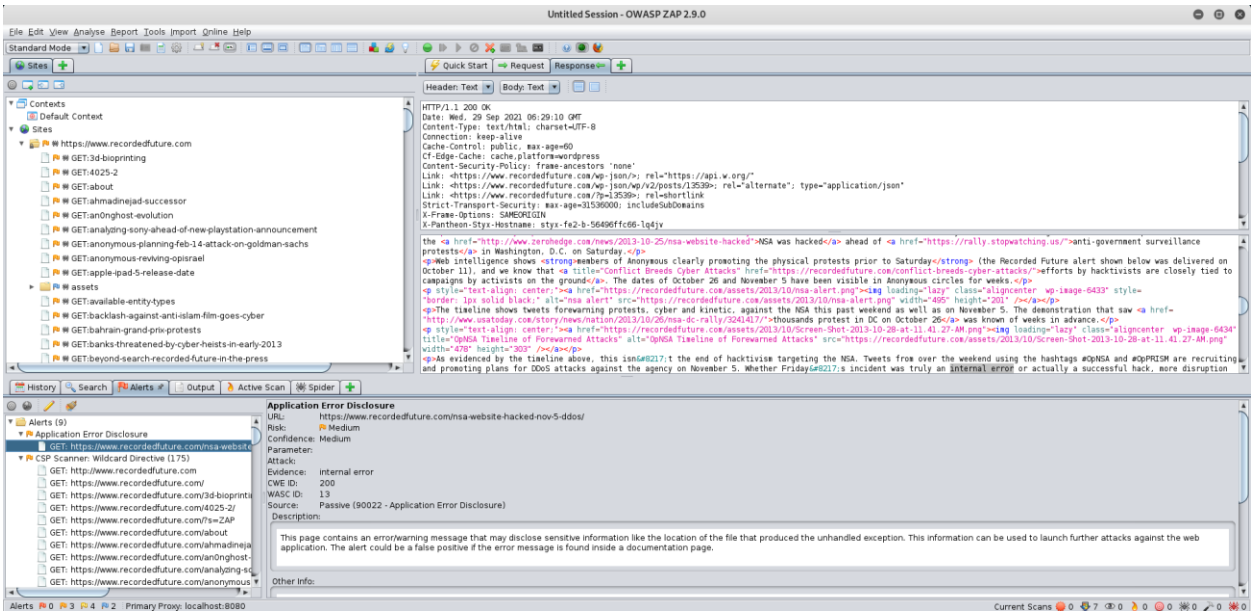
In this chapter, we are mainly trying to gain initial knowledge and identify any potential security weakness that could allow an outside attacker to hack and gain access into the target domain. So we need some tools to automate the vulnerability scan procedure; it will allow us to automatically discover vulnerabilities in web applications. But we know these are just tools; they make mistakes and miss some vulnerabilities. We can use these tools as a backup or help us with our penetration testing. So now we are going to use the owasp zap tool for a vulnerability scan.



This is the main view of the tool, and on the left side, you will see the websites you are targeting, and on the right side, you can attack by setting the URL. You can also see your attack result for your scan at the bottom of the window .so now we can click on the green plus, and in the dropdown menu, we can select active scan. And we need to set our scan policy manager, and if you want, you can add a scan policy or use the default one. Also, you can edit it and set the attack strength as you want. When we click on the attack first, it will find all related URLs, and it will try to attack those URLs according to the scan policy we set before.



After finishing the process, we can see on the left that we have our website and click on it to see results. We can see very important things on the alert tab at the bottom of the window. In there, you can see all the vulnerabilities that have been discovered. We can click one of those and see further details about the given vulnerability.



If we click on any of them, we can see the risk level and a description of the vulnerability, the HTTP request sent to discover, and the corresponding response.

Vulnerabilities we found

In this vulnerability scan, we did not get any high-priority alerts, but we got several low-priority alerts. Among those, I chose one and tried to find a bug using that vulnerability.

- Strict transport security not enforced

Description

- This domain is unable to prevent clients from connecting through an unsecured channel that is an HTTP connection. It can modify the legitimate user's network traffic by making a downgrade attack, bypassing the application's encryption mechanisms, and grabbing sensitive data from legitimate users. In this situation, the attack will convert the HTTPS link as HTTP then the user follows the modified link and browses the site from an unencrypted HTTP page. Then an attacker can easily capture the legitimate user's sensitive data.

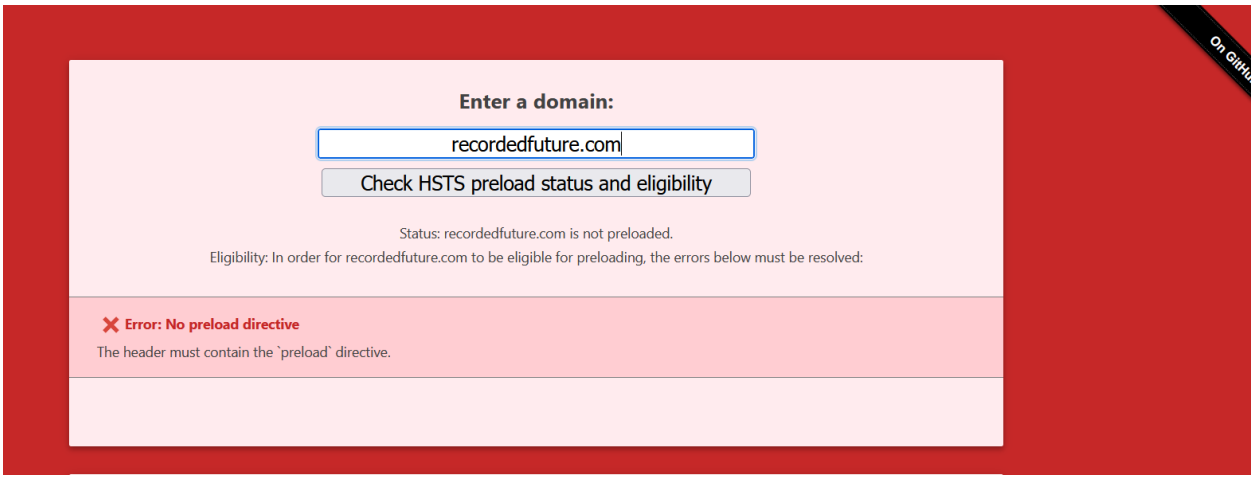
- To exploit this type of vulnerability, it is necessary to suitably position to intercept and change the victim's network traffic. these type of attacks usually happens when a client connects with a server through an unsecured connection such as public wifi or cooperate office network that is associated with a vulnerable computer. Even the ISP(internet service provider) also can perform this type of attack.

Issue remediation

- The server should strictly accept HTTPS requests rather than using HTTP.for that the HSTS header can do by adding a response header with the name 'Strict-Transport-Security' and the value 'max-age=expireTime,' where expiry time is the time in seconds that browsers should remember that the site should only be accessed using HTTPS.as well as we can add the 'includeSubDomains' flag and 'preload ' flag for more security.

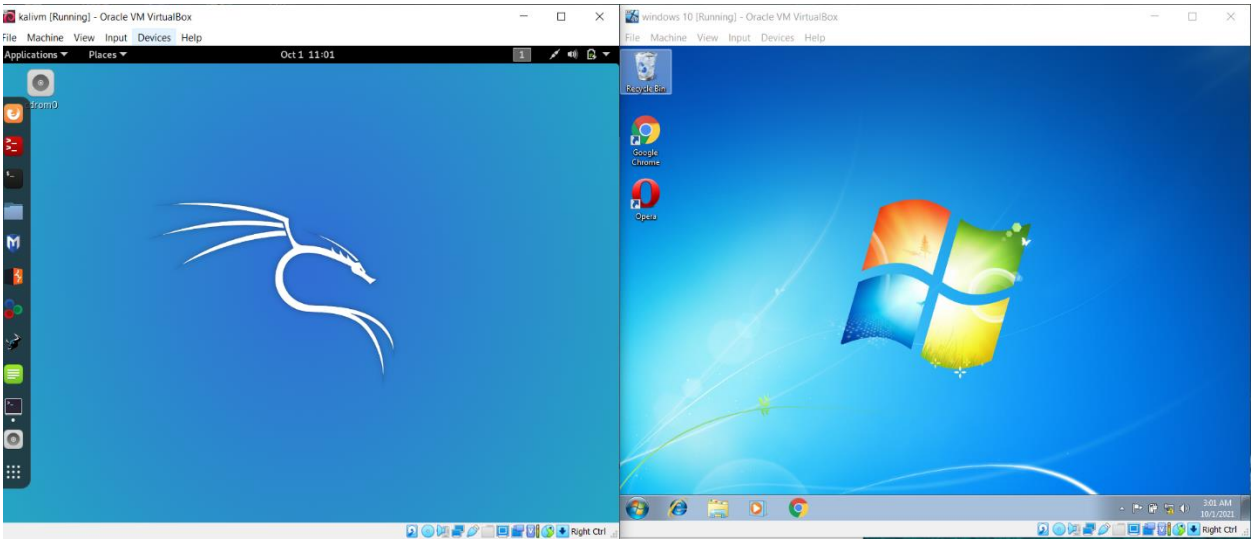
Before finding a bug, we need to know what is HSTS.HSTS simply means it says in the server-side server always strictly use HSTS.HSTS ensures the client must send the request as an HTTPS request, which means the client cannot send HTTP requests to the server. If a client unawarely sends an HTTP request, then the server says you need to send only HTTPS requests to me if you want to get my services.

To check our domain has configured HSTS, we can use the hstspreload.org website.

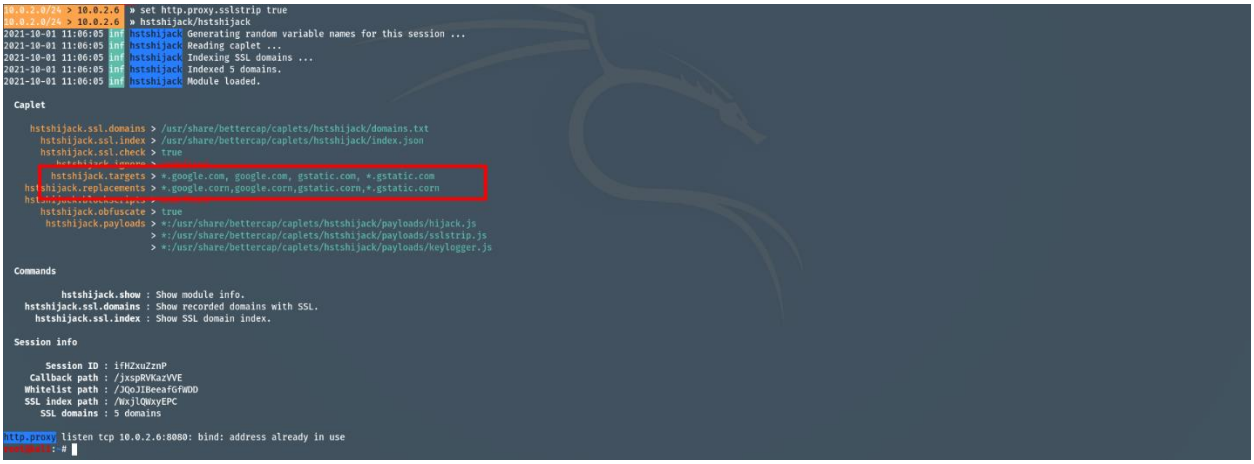


It says the reocordedfuture.com domain has no preload directives. We use preload directives because we know HSTS follows TOFU (Trust On First Use), but it has a problem. If An attacker can wait until a person makes his initial request, then the attacker can grab the data by intercepting his data traffic. that means we can try an SSL stripping attack and see if we are lucky to find a bug.

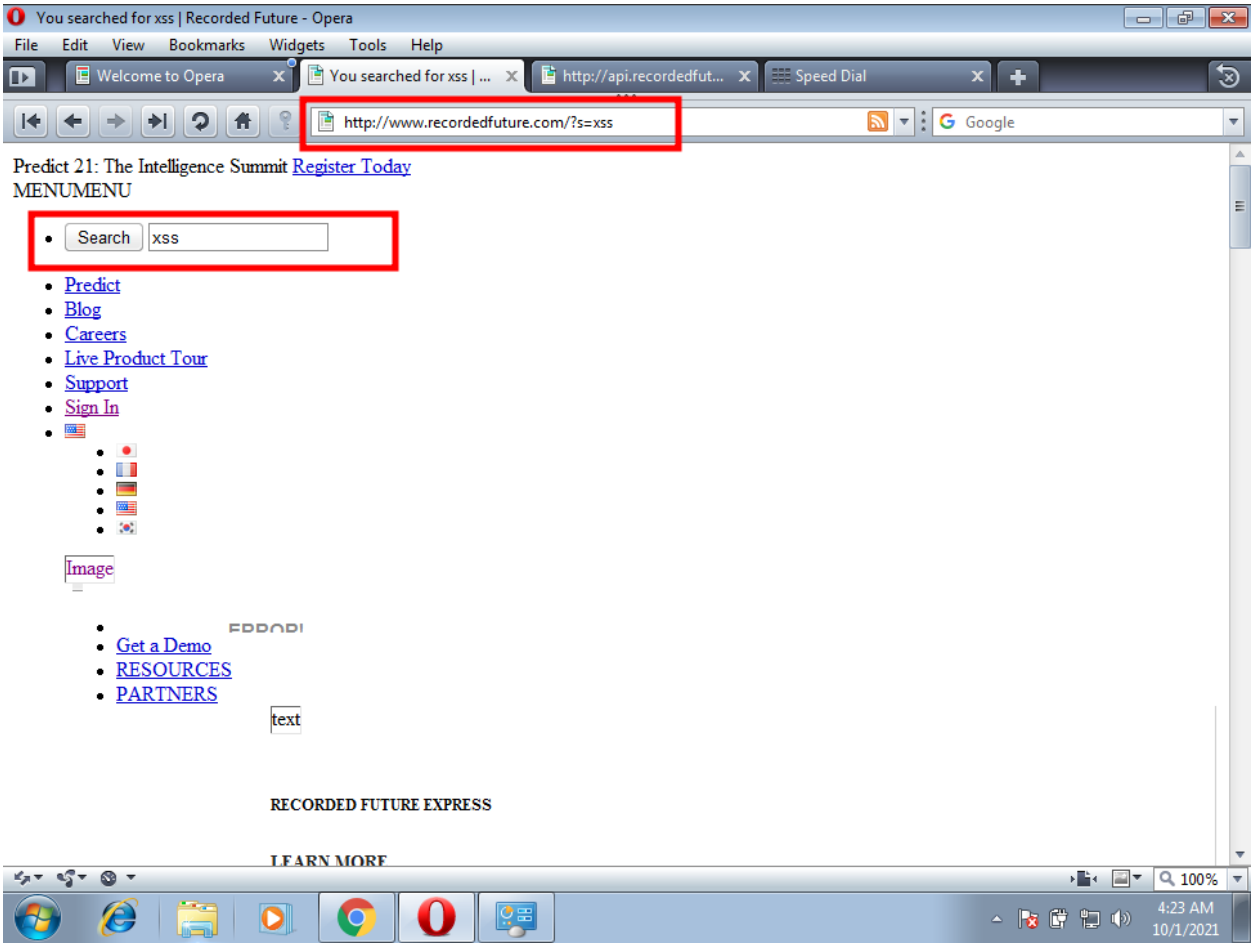
We need a tool called bettercap and two machines, one as the victim machine other for making the SSL stripping attack.



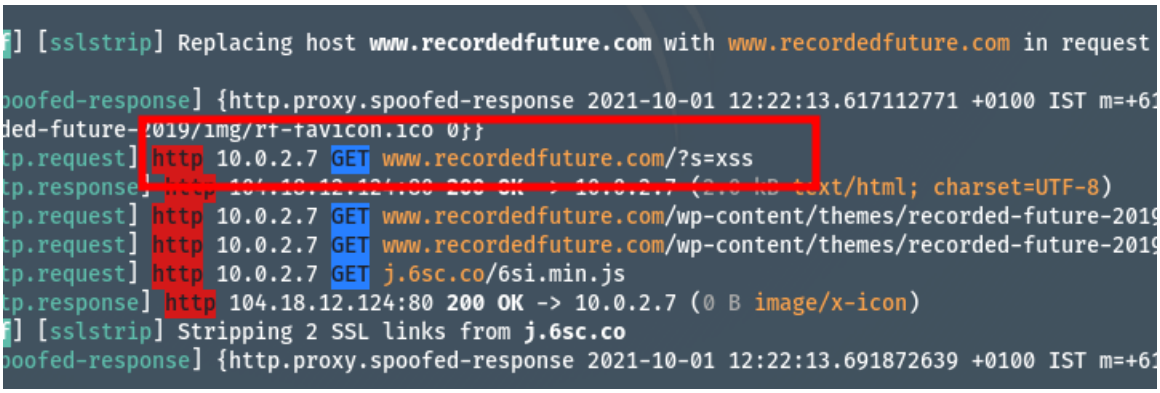
Both are virtual machines and running Kali Linux and Windows 7, and the right side machine as the victim and the left side machine as the attacker's machine. From an attacker's perspective, we can connect to the victim's network and do a network scan to identify the victim's IP address. But I know both machine's IP addresses, so I don't need to scan my network. Then we can run the bettercap by giving the target IP address and do other configurations.



You can see here if the target is google.com, it will replace with google.corn or stuff like that. It will take into consideration every scenario right here, as well as it will change from www to something else like wwww.



First, I open the domain with google chrome .google chrome supports the HSTS header, so when I insert the URL, it always redirects to HTTPS. Then I get a HSTS not supported browser. It is the opera 10.10 version .you can check what browsers support the HSTS header using caniuse.com.then, I put the XSS keyword to the search bar, and I see it captured by the bettercap.



As we can see, this is a get request forward through HTTP. It means if we can downgrade, the protocol domain is somewhat vulnerable to SSL stripping attacks. But when we use browsers like chrome, it will only allow requesting as HTTPS connection so that we cannot capture any data, .but we cannot load the login page with HTTP .so that it is not a critical security issue, but when the protocol is downgraded, we can capture a small amount of data using SSL stripping.

Conclusion

In the beginning, we looked at the background, such as what the company does and rules like that. We discussed some information. Then As the first step of bug finding, we gather some important information like IP address hosting company and the technology that domain uses etc. then we gather all the subdomains in the same server then we see that all the domains have the same IP .sometimes we have to use several tools to gather more information and confirm our gathered information is accurate. After that, we looked at if there are files and directives we can capture using tools like dirb, and we used maltego to view a diagrammatic view of our domain. It gave a better idea about the domain.

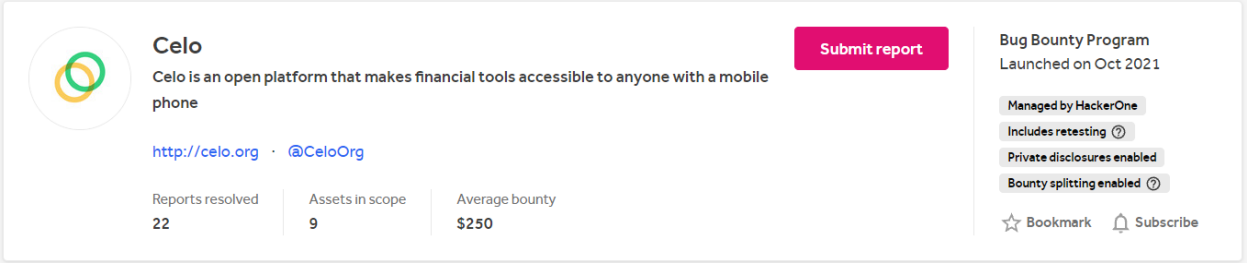
Then we move to the vulnerability assessment stage. At that point, we saw the vulnerabilities the domain has and how we could find them using some tools. Then we analyze the vulnerability using some websites and understand the real problem with this web application. After finding vulnerabilities, we tried to test a selected vulnerability and prove that it had a harmful bug .in that point, we have ensured that It was not a critical vulnerability, but we experienced a lot of interesting stuff.

REPORT 02

Searching Bugs Within Celo.com

Background

I selected this bug bounty program from hackerone.com, and let's see what the background of celo.com.CELO is is an international group of companies located in the UK. It is assigned to design manufacturing and distribution of high-quality technical screws and technical fixings.



Basically, celo is an open platform, and It makes financial tools accessible to anyone with a mobile phone. It looks like a mobile application. In the description, they are given the rewards and how they categorize them. We can see those as below.

Rewards			
Low (0.1-3.9)	Medium (4.0-6.9)	High (7.0-8.9)	Critical (9.0-10.0)
*.celo.org			
$50	$850	$1,200	$5,000
*.clabs.co			
$50	$850	$1,200	$5,000
Celo Protocol & Smart Contracts			
$1,000	$3,000	$10,000	$20,000

As you can see, they provide awards, and it will change according to the domain in which we are searching for bugs. And they said their rewards are based on the common vulnerability scoring standard. And they presented that as a small diagram to further clarifications. After that, they provided some examples of celo protocol vulnerabilities that we are eligible to get rewards for. They also gave the severity level as high, critical, and medium.

Examples for Celo Protocol

- Double spend by getting the clients to accept a different chain (CRITICAL)
- Double spend by validating malicious blocks (HIGH)
- Tamper/manipulate blockchain history to invalidate transactions (MEDIUM)
- Cause network to mint tokens to own account (CRITICAL)
- Undermine consensus mechanism to split chain (CRITICAL)
- Censorship (e.g. on votes) (CRITICAL)
- Steal tokens from node (HIGH)
- Get a phone number associated with you that you don't own (HIGH)
- Prevent node from accessing the network (MEDIUM)
- Abuse bugs in economic system to defraud other participants (e.g. avoid transaction fees to full nodes) (MEDIUM)
- DDOS attack on consensus (reliability cause consensus mechanism to stall indef) (CRITICAL)
- Shutdown network (CRITICAL)
- Get ⅓ of validators elected (CRITICAL)
- Get ⅔ of validators elected (HIGH)
- Get 1 validator elected (MEDIUM)
- Get elected by nefarious means (sneak into the kitchen door) (HIGH)
- Get more rewards than you should (hand in the tilt/cash register) (HIGH)
- Faking the uptime system / tricking the performance metric ("cooking" from the pub) (HIGH)
- VG (or V) Impersonation attacks (pretend you work at the restaurant) - social eng. attack (CRITICAL)
- DDOS on attestation service (MEDIUM)
- Manipulate account balances (HIGH)
- Steal Celo Gold from reserve (CRITICAL)

They give bonuses if we can prove exploitability and sell specific industry standards/compliance controls that the finding applies to. They also provide the program rules that we must follow during our work it is very important.

Program Rules

- Please provide detailed reports with reproducible steps. If the report is not detailed enough to reproduce the issue, the issue will not be eligible for a reward.
- **Reports out of scope will not be considered.** Please check before submitting.
- Note that Celo is an open source project.
- Submit one vulnerability per-report, unless you need to chain vulnerabilities to provide impact.
- When duplicates occur, we only award the first report that was received (provided that it can be fully reproduced).
- Multiple vulnerabilities caused by one underlying issue will be awarded one bounty.
- Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with the explicit permission of the account holder.
- Attacking any testnet other than the official Celo Baklava testnet ("Network") is prohibited.
- Any attacks that could cause physical damage or incur costs to other's property is prohibited.
- Any attacks against Network nodes that violate [Amazon Web Services Acceptable Use Policy] (https://aws.amazon.com/aup/) and Google Cloud Platform's Acceptable Use Policy and other specific services you use is prohibited.
- Follow the Celo Community Code of Conduct.
- Participation is subject to the Baklava testnet Terms & Conditions.

Next, they showed what vulnerabilities are not eligible for getting rewards, and they especially said that previously known vulnerabilities are not eligible. Finally, they put their in-scope domains, and there are no out-of-scope domains. The in-scope domains are given below.

- *.clabs.co
- *.celo.org
- https://github.com/celo-org/bls-zexe
- https://github.com/celo-org/celo-monorepo
- https://github.com/celo-org/celo-blockchain
- https://github.com/celo-org/zexe
- https://github.com/zviadm/celoterminal
- https://github.com/celo-org/celo-multisend

Setting The Scope

- *.clabs.co
- *.celo.org

So I selected these two domains, and from this point onwards, we are doing scanning analysis only for these two domains.

Gathering Information About Domain

In this step, we are trying to gather information about the selected domains that will help to further analysis. For that, we are using some tools in this stage. First, we use **whoislookup** to gather some general information.

So I got two results for our domains. Let's see what we can find there.

Whois Record for CIAbs.co

– Domain Profile

Registrant	REDACTED FOR PRIVACY
Registrant Org	c/o whoisproxy.com
Registrant Country	us
Registrar	Key-Systems GmbH IANA ID: 269 URL: https://key-systems.net Whois Server: — abuse@key-systems.net (p) 496894939685
Registrar Status	clientTransferProhibited
Dates	599 days old Created on 2020-02-11 Expires on 2026-02-11 Updated on 2021-03-09
Name Servers	NS-CLOUD-B1.GOOGLEDOMAINS.COM (has 7,403,824 domains) NS-CLOUD-B2.GOOGLEDOMAINS.COM (has 7,403,824 domains) NS-CLOUD-B3.GOOGLEDOMAINS.COM (has 7,403,824 domains) NS-CLOUD-B4.GOOGLEDOMAINS.COM (has 7,403,824 domains)
Tech Contact	REDACTED FOR PRIVACY REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY (p) x (f) x
IP Address	74.125.195.121 - 506,218 other sites hosted on this server
IP Location	- California - Mountain View - Google
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
Hosting History	3 changes on 3 unique name servers over 2 years

Whois Record for Celo.org

– Domain Profile

Registrant Org	Contact Privacy Inc. Customer 1242485918
Registrant Country	ca
Registrar	Google LLC IANA ID: 895 URL: https://domains.google.com Whois Server: whois.google.com registrar-abuse@google.com (p) 18772376466
Registrar Status	clientTransferProhibited
Dates	3,774 days old Created on 2011-06-03 Expires on 2030-06-03 Updated on 2021-09-27
Name Servers	BENEDICT.NS.CLOUDFLARE.COM (has 22,051,561 domains) PAT.NS.CLOUDFLARE.COM (has 22,051,561 domains)
Tech Contact	–
IP Address	104.18.3.246 is hosted on a dedicated server
IP Location	- California - San Francisco - Cloudflare Inc.
ASN	AS13335 CLOUDFLARENET, US (registered Jul 14, 2010)
Domain Status	Registered And Active Website
IP History	67 changes on 67 unique IP addresses over 16 years
Hosting History	24 changes on 12 unique name servers over 15 years

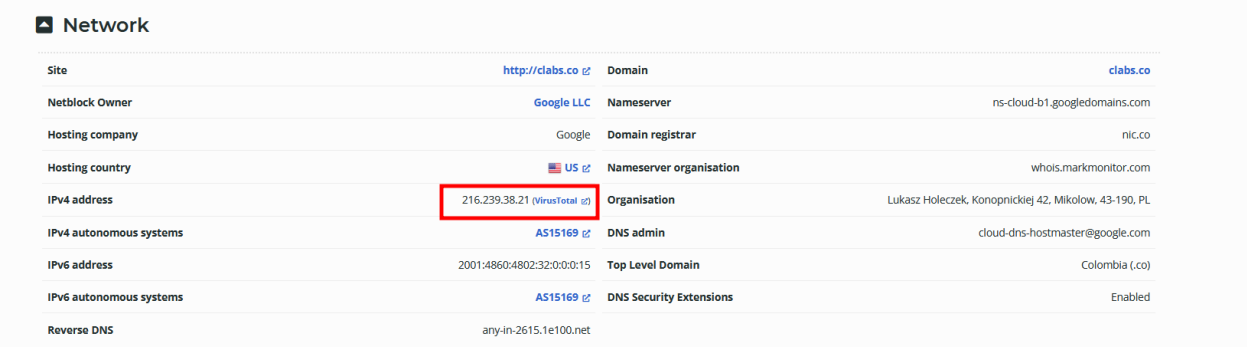
– Website

Website Title	None given.

We can see the domains are in two different servers, so we can see different IP addresses.celo.org domains name server is Cloudflare and clabs.co domains hosting company is googledomains. These are the main pieces of information we can get from this site. Then we need information about technologies used in these domains. For that, we can use Netcraft.

Technologies

The first thing we can see in the results is that we can see a different ipv4 address for clabs.co .these things we can ensure when we are scan for subdomains.



Network

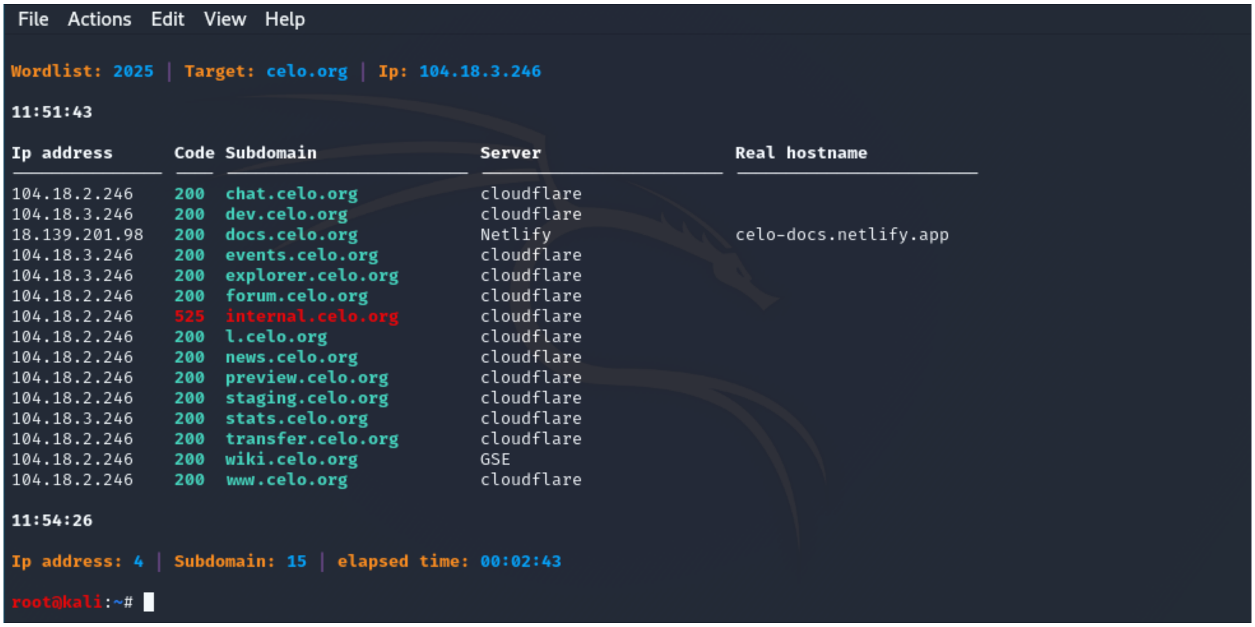
Site	http://clabs.co	**Domain**	clabs.co
Netblock Owner	Google LLC	**Nameserver**	ns-cloud-b1.googledomains.com
Hosting company	Google	**Domain registrar**	nic.co
Hosting country	US	**Nameserver organisation**	whois.markmonitor.com
IPv4 address	216.239.38.21 (VirusTotal)	**Organisation**	Lukasz Holeczek, Konopnickiej 42, Mikolow, 43-190, PL
IPv4 autonomous systems	AS15169	**DNS admin**	cloud-dns-hostmaster@google.com
IPv6 address	2001:4860:4802:32:0:0:0:15	**Top Level Domain**	Colombia (.co)
IPv6 autonomous systems	AS15169	**DNS Security Extensions**	Enabled
Reverse DNS	any-in-2615.1e100.net		

In the clabs.co domain, it says it uses SSL encryption, but it doesn't support SSL version 3. it only uses google manager service as third-party resources. And also, we can see some client-side technologies and encoding mechanisms as well.

Celo.org uses google CDN as a third-party resource, and it uses an HTTP accelerator to reduce the website access time. Then same as clabs.org, this domain also uses javascript as a client-side technology. It uses UTF8 as a character encoding mechanism and HTTP compression mechanism. These are the main things we can find out using this site.

Gathering subdomain information

In the previous stage, we saw some differences between the two servers' IP addresses, and we saw these two domains are in different servers. To find out what is really happened here, we have to perform a subdomain scanning using some tools. First, we use knockpy for both domains and see what we can see as the result.

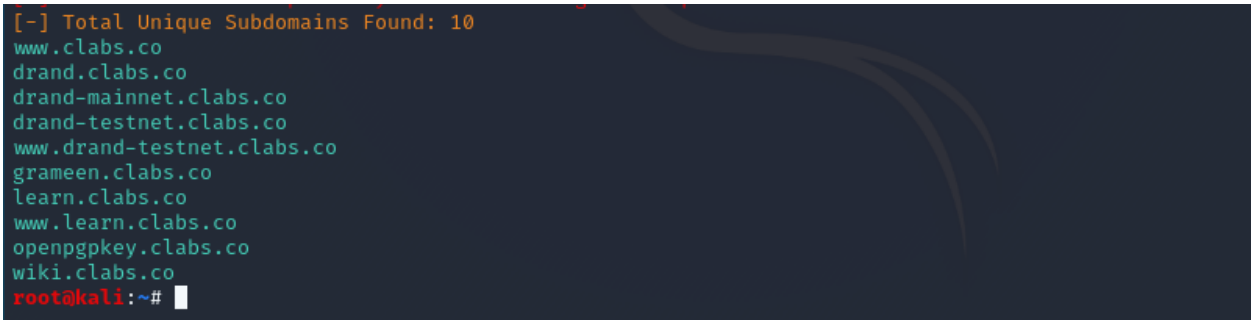

File Actions Edit View Help
Wordlist: 2025 | Target: celo.org | Ip: 104.18.3.246
11:51:43
Ip address Code Subdomain Server Real hostname
104.18.2.246 200 chat.celo.org cloudflare
104.18.3.246 200 dev.celo.org cloudflare
18.139.201.98 200 docs.celo.org Netlify celo-docs.netlify.app
104.18.3.246 200 events.celo.org cloudflare
104.18.3.246 200 explorer.celo.org cloudflare
104.18.2.246 200 forum.celo.org cloudflare
104.18.2.246 525 internal.celo.org cloudflare
104.18.2.246 200 l.celo.org cloudflare
104.18.2.246 200 news.celo.org cloudflare
104.18.2.246 200 preview.celo.org cloudflare
104.18.2.246 200 staging.celo.org cloudflare
104.18.3.246 200 stats.celo.org cloudflare
104.18.2.246 200 transfer.celo.org cloudflare
104.18.2.246 200 wiki.celo.org GSE
104.18.2.246 200 www.celo.org cloudflare
11:54:26
Ip address: 4 | Subdomain: 15 | elapsed time: 00:02:43
root@kali:~#

After subdomain enumeration, we can see celo.org's subdomains like this. We can see the subdomains of celo.org have the same IP address and save name server. We can see the actual hostname, and it is a mobile application. Let's see what we got by scan clabs.co's domain.

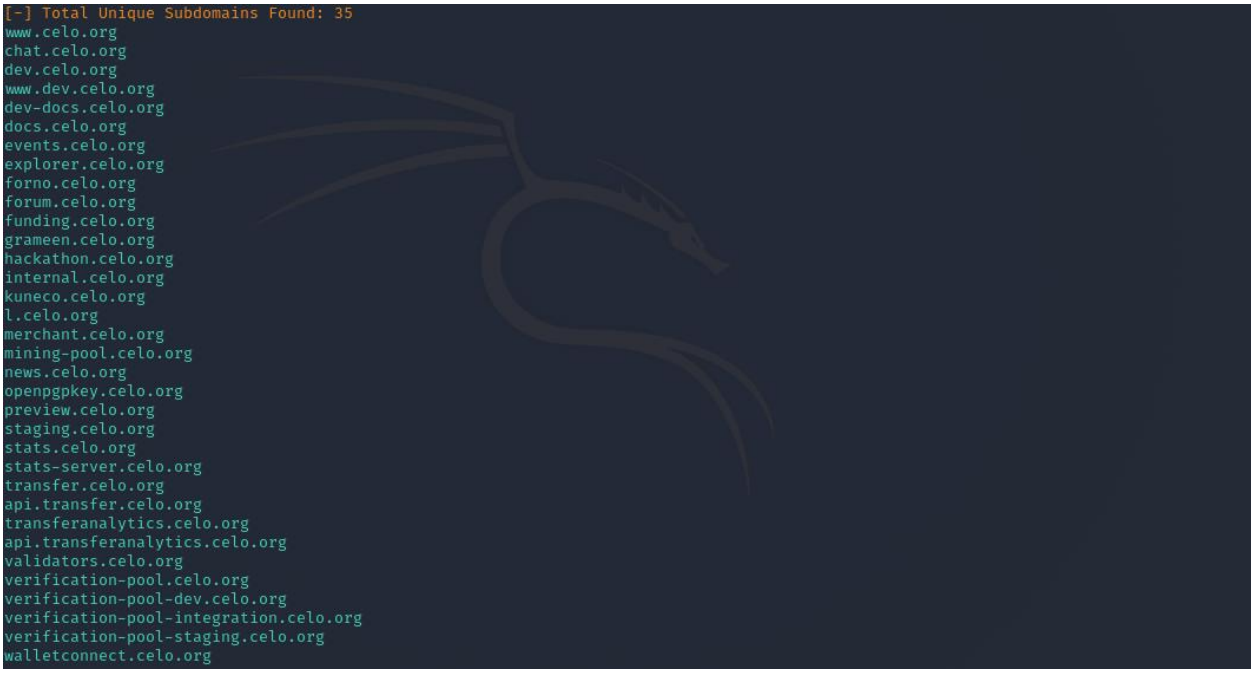

knockpy
v5.1.0
local: 2019 | google: 0 | duckduckgo: 2 | virustotal: 0
Wordlist: 2021 | Target: clabs.co | Ip: 216.239.32.21
11:53:03
Ip address Code Subdomain Server Real hostname
52.84.228.71 200 grameen.clabs.co AmazonS3 d2krwbuyknzcxd.cloudfront.net
209.15.63.8 200 learn.clabs.co
172.217.194.121 200 wiki.clabs.co GSE ghs.googlehosted.com
172.217.194.121 200 www.clabs.co Google Frontend ghs.googlehosted.com
11:56:07
Ip address: 6 | Subdomain: 4 | elapsed time: 00:03:03

We have only four subdomains by subdomain enumeration. Now we have the answer for the IP differences we saw earlier. The subdomain hosted by CloudFront has 52.84.228.71 IP address, and the subdomain hosted by google has 172.217.194.121 as the IP address. now, we can

eliminate the IP address we got earlier. But we know these enumeration tools work based on brute-force attacks, so there is a possibility to miss that domain. Anyway, now we got subdomains of our selected two domains. To make sure we can do another enumeration scan by using a different tool or different wordlist.

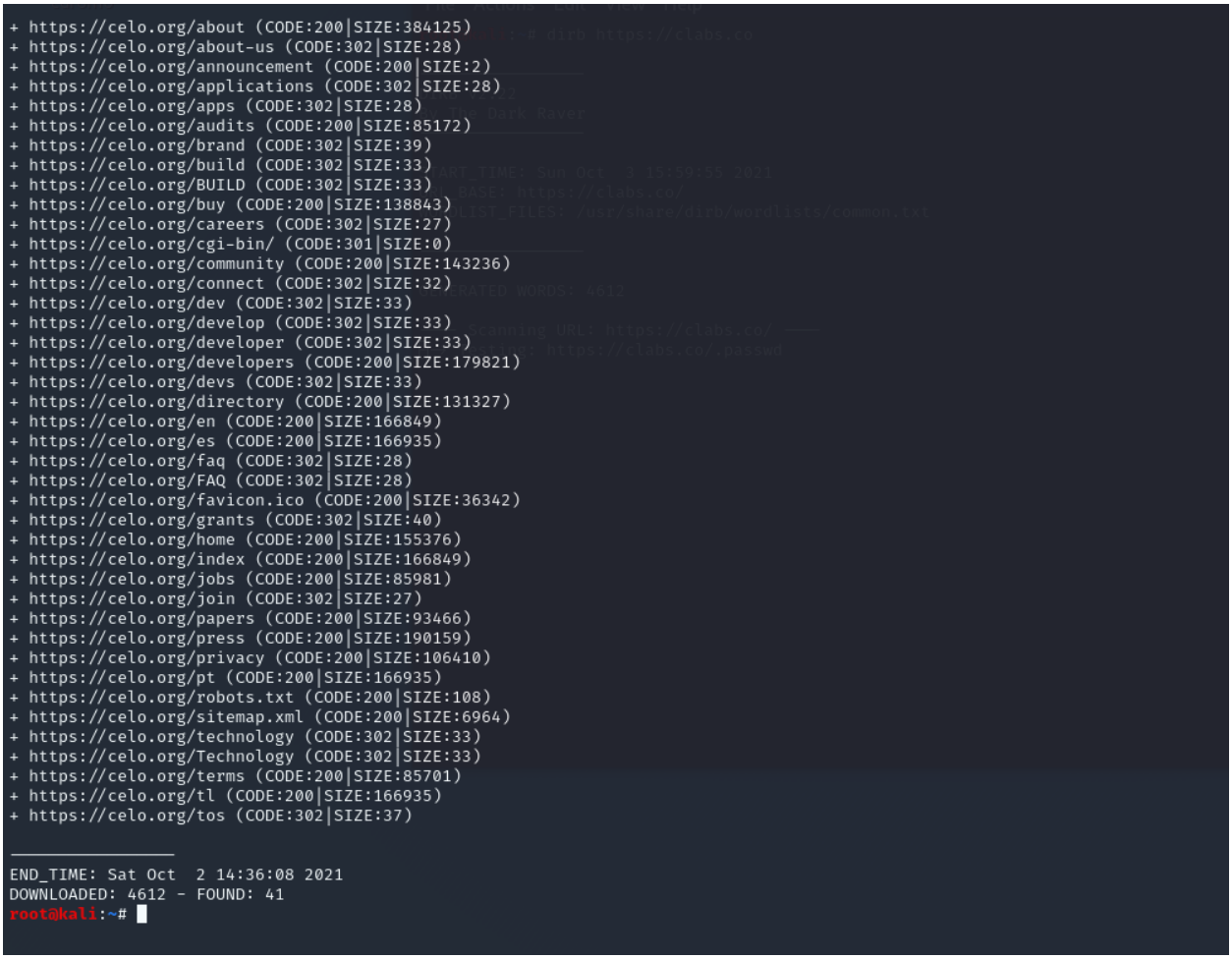


In this time, we got ten subdomains for clabs.co by using the sublist3r tool .previously, we got only four subdomains. Now we know clabs.co has some other subdomains as well.so I did another enumeration for celo.org, and it shows 35 subdomains.



Gather information about files and directories

In the previous stage, we gathered information about our domain. So now we have some information about the IP addresses and the name servers, then we found the other subdomains and technologies it uses. In this step, we try to find files and directories and find further information by analyzing them because sometimes files include some sensitive data. So we are going to use dirb to scan the web content of our selected domains.

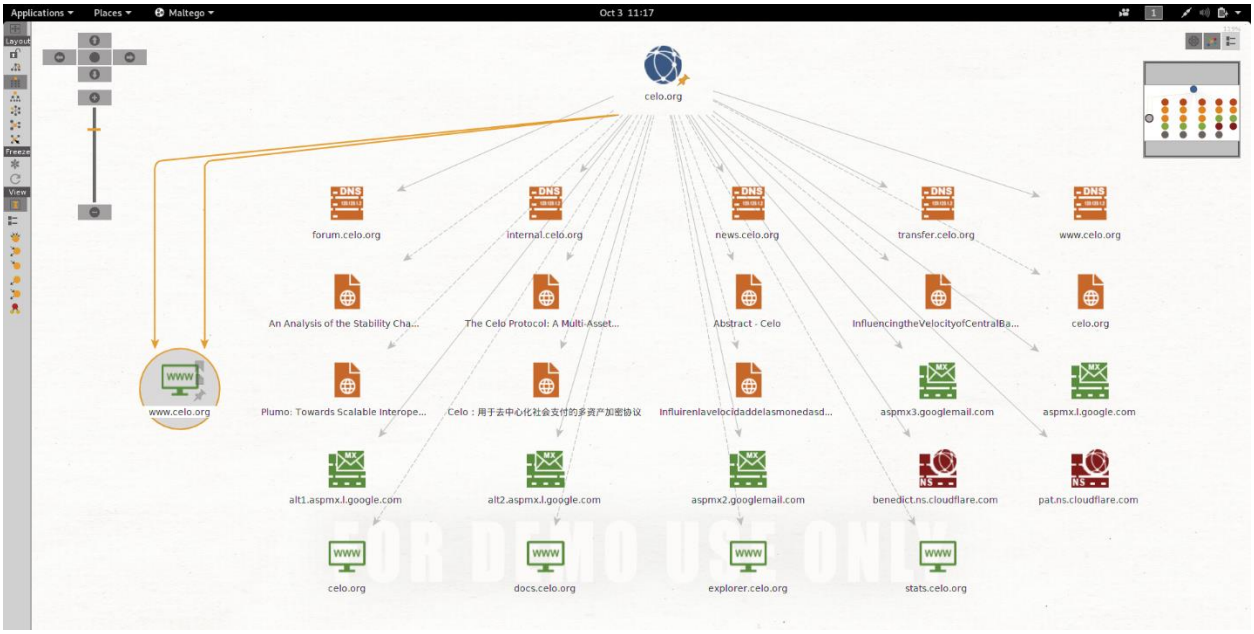


For celo.org, we can find 41 results with dirb web content scanner .most of the files are directed to the main web pages of this domain, and there are two files different from those files that are robots.txt file and sitemap.xml file, .but there is no information that is important to us.

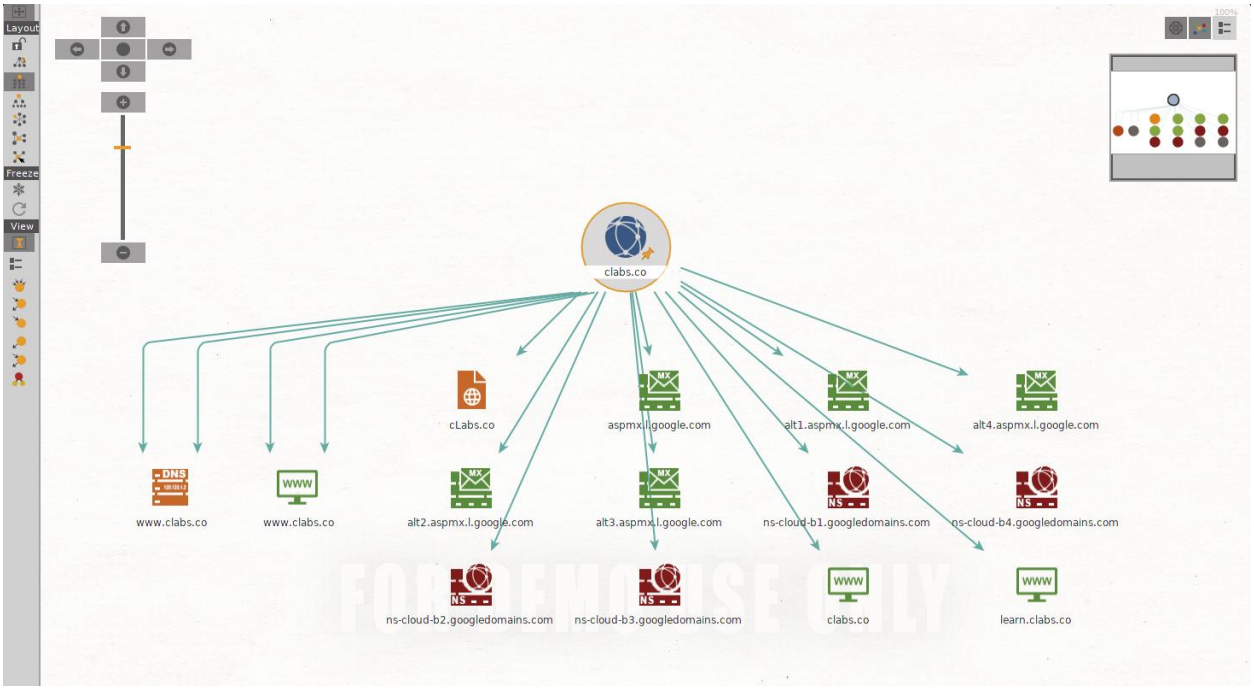
```
GENERATED WORDS: 4612

---- Scanning URL: https://clabs.co/ ----
+ https://clabs.co/careers (CODE:200|SIZE:231935)
+ https://clabs.co/cgi-bin/ (CODE:308|SIZE:8)
+ https://clabs.co/en (CODE:200|SIZE:70527)
+ https://clabs.co/jobs (CODE:308|SIZE:8)
+ https://clabs.co/privacy (CODE:200|SIZE:52315)
+ https://clabs.co/robots.txt (CODE:200|SIZE:108)
+ https://clabs.co/sitemap.xml (CODE:200|SIZE:966)
+ https://clabs.co/terms (CODE:200|SIZE:110428)

END_TIME: Sun Oct  3 16:36:02 2021
DOWNLOADED: 4612 - FOUND: 8
root@kali:~#
```

These are the results we get by scanning clabs.co's domain. From this scan, also we got the robots.txt file and sitemap.xml file. Other than those, we cannot find anything else.

In addition to this tool, we can use maltego to find directories and files, but it will now only show about files .it will show technologies that the domain uses, file systems, and more things.



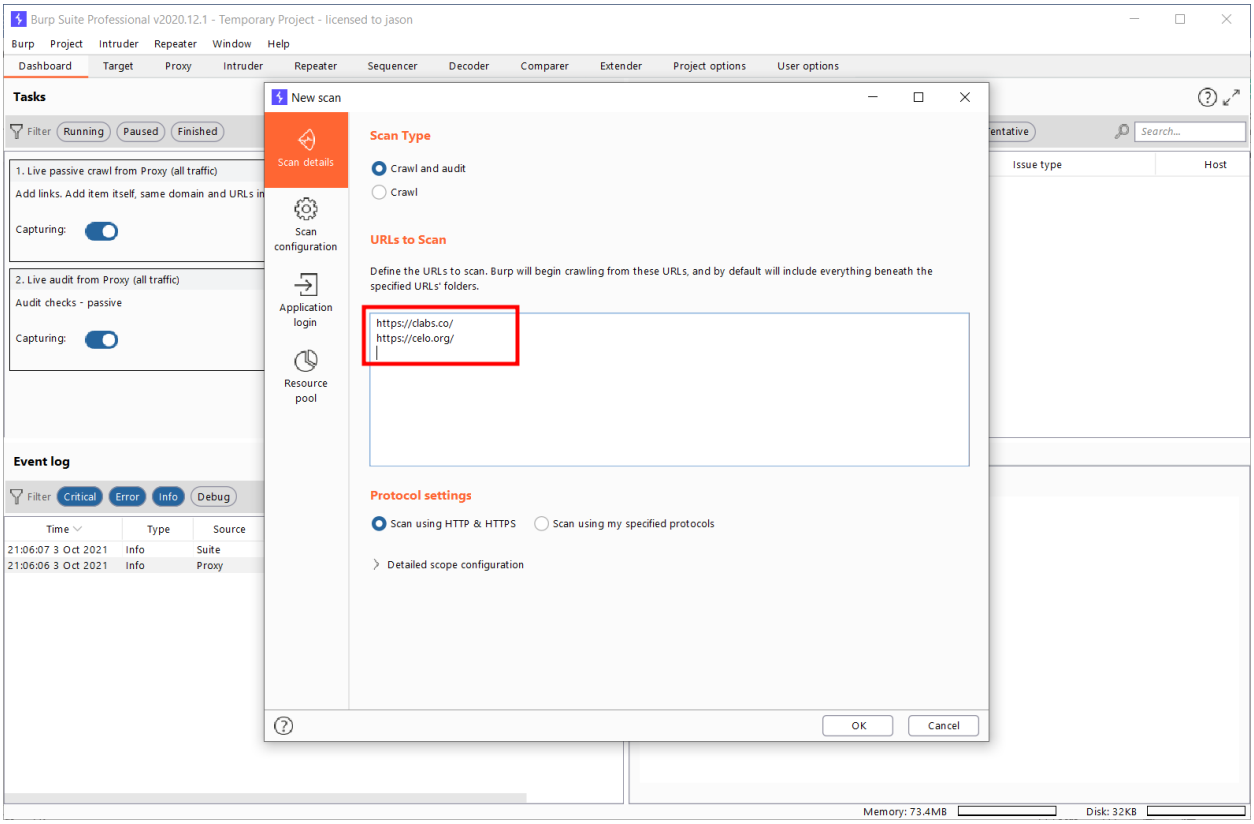
Here we can see some domains that we are found earlier step. We can see the Cloudflare name servers and google mail services. We got some files that we are not getting earlier using dirb. Still, I couldn't find any critical information by referring them. But we can get a graphical view of the domain. We can use this tool to find information using different methods. Let's see what we can get for clabs.co domain.



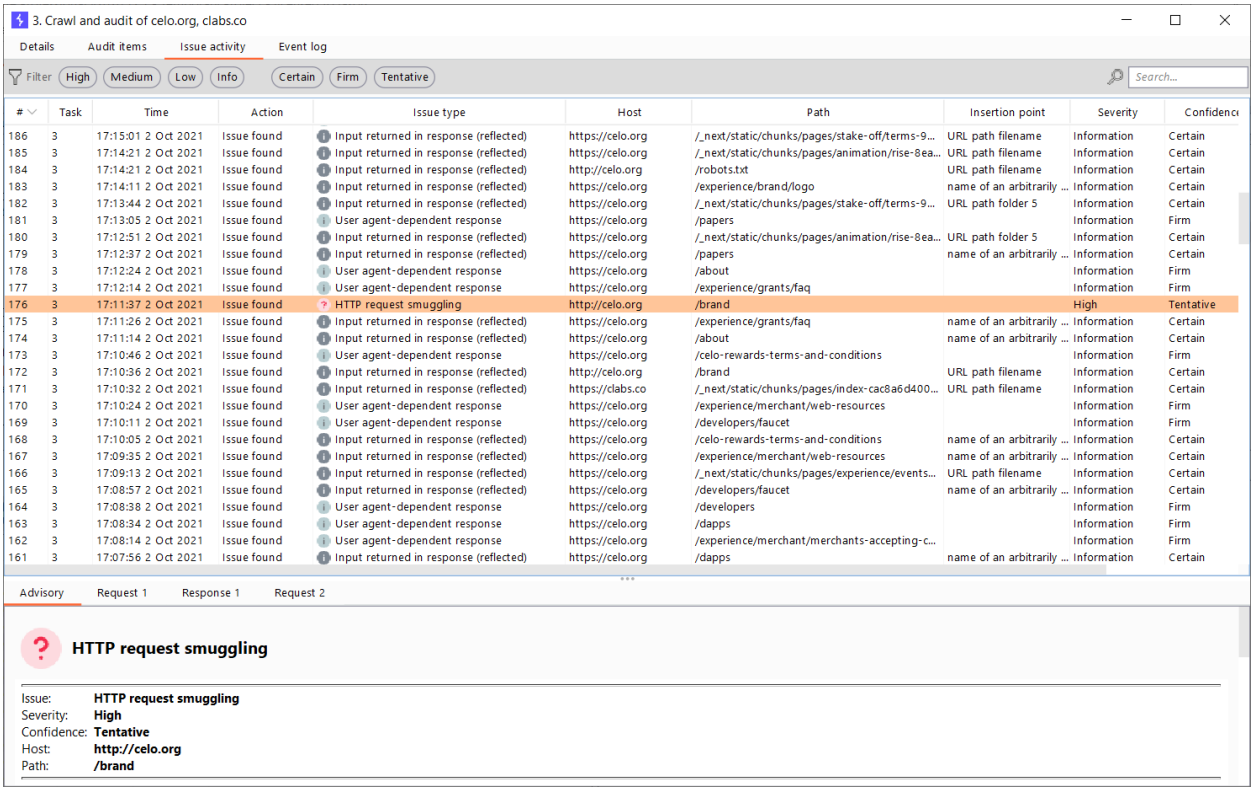
Using maltego, we could find only one file, and we can see some services provided by Google, and we can see the googledomains name server we saw earlier when we used Netcraft. We also got three subdomains as well.

Vulnerability Assessment

Now we gathered information about the selected two domains, and now we are going to prepare for the vulnerability finding part. So we can use several tools for a vulnerability scan, but I chose burp suite for vulnerability scanning this time. Because we have to scan for two different domains, the burp suite is beneficial in situations like this. But the vulnerability scanning feature is only available in the professional version of the burp suite.



First, we need to click on the new scan and give the domains that we want to find vulnerabilities. We can use the crawl and audit option or only the crawl option according to the situation. Then we can run a scan and see what we got.



At this time, we got a high severity alert, and it shows there is some critical problem related to HTTP request smuggling. Other than this vulnerability, we got some header-related low severity alerts, but we are only considering the high severity one at this point.

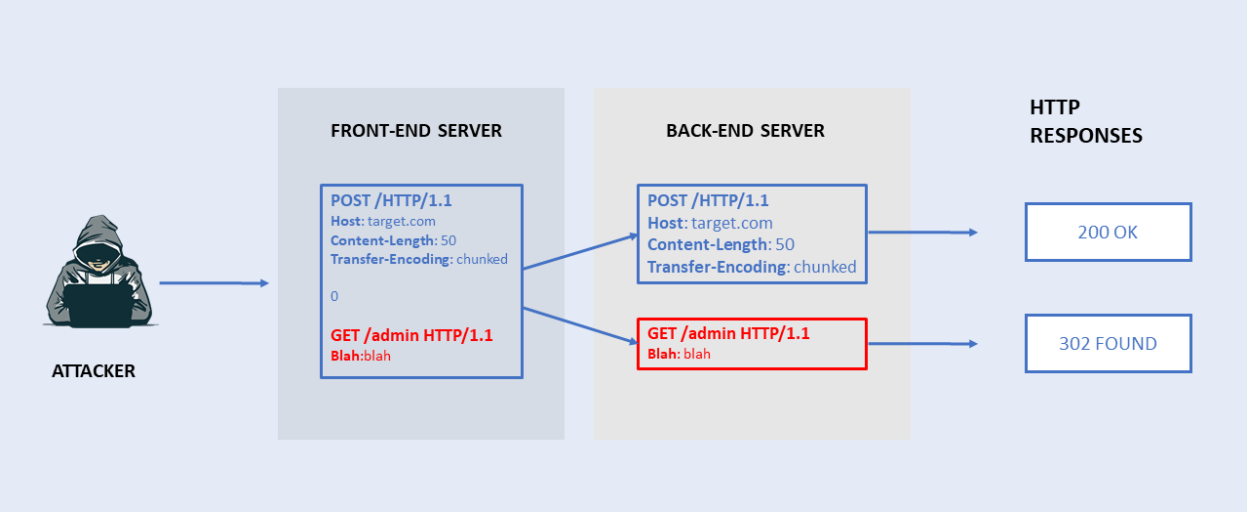
Vulnerabilities we found

HTTP request smuggling

Then take a look at what is HTTP request smuggling and how we can prevent that vulnerability.

This vulnerability is generally an attack technique, and it will interfere with the processing of requests between the server's back end and the front end. The threat actor will modify the request and include another different request in the

first request's body. That is how the attacker exploits the vulnerability. The attacker abuses the content-length and transfer-encoding headers, and if the attack is successful, the modified request in the first request's body will be processed.



Usually, two types of HTTP headers are uses during an attack.

- Content-length header - request body size in bytes.
- Transfer-encoding header – the request body will be sent as separate parts and separated by newline.0 is used to end apart.

The attack needs to meet some conditions to proceed.

- The front-end servers need to forward several requests to the backend server through the same network connection.
- The back end does not agree with the front end about where each message should end.
- The request modified by the attacker gets interpreted as two separate HTTP requests by the backend server.
- The attacker creates a second request to do a malicious action that the first request cannot do.

```
POST / HTTP/1.1
Host: vulnerable-host.com
Content-Type:
application/x-www-form-urlencoded
Content-length: 4
Transfer-Encoding: chunked

0

GET /confidential HTTP/1.1
Foo: foo
```

As you can see, the request will be interpreted as two separate requests in the backend server.

`GET /confidential HTTP/1.1` `Foo: foo`	`POST / HTTP/1.1` `Host: vulnerable-host.com` `Content-Type:` `application/x-www-form-urlencoded` `Content-length: 4` `Transfer-Encoding: chunked` `0`

Suppose someone needs to do this type of exploitation. In that case, that person must have special knowledge of the attack methods. This vulnerability does not cause the exploitation of other vulnerabilities in the target web application.

Impact of the vulnerability

- Execute Unauthorized Commands
- Gain Privileges
- Bypassing security controls
- Access/Modify Data
- Session Hijacking
- Cache poisoning

Prevention mechanisms

- Configure the front-end server to detect ambiguous requests coming into it.
- Configure the backend server to not proceed with those kinds of ambiguous requests and terminate the network connection.

Solutions based on the above mechanisms

- Disable reuse of back end connections
- Use http/2 for back end connections
- Prevent from using different web server software to font-end, and the back end servers .always use the same web server software.
- Use a WAF (web application firewall) to detect ambiguous requests.

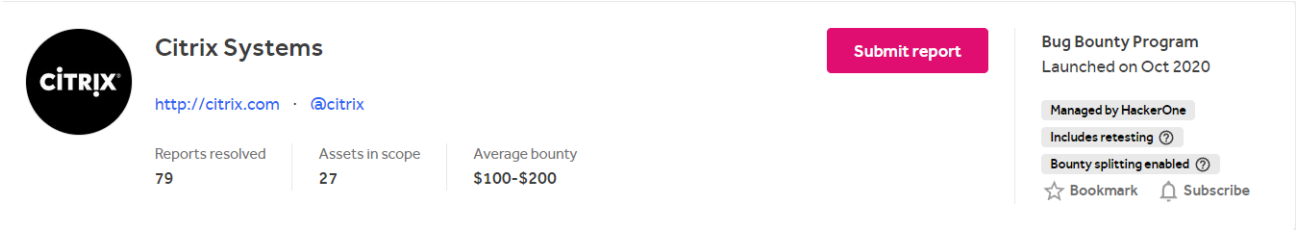
Conclusion

In the beginning, we talked about the domain we selected, and then we selected celo.org and clabs.co domains to further analysis. Then we found some information about the domain and its technologies. Next, we looked for the subdomains and saw the domains have different IP addresses. After finding some information, we moved to vulnerability scanning in that step. We saw the celo.org has a critical vulnerability, which is HTTP request smuggling. After finding those things, we discussed what http request smuggling is and the solutions in this report.

REPORT 03

INTRODUCTION

In this report, I selected Citrix Systems company as the bug bounty program from hackerone.com.lets to start the analysis with this program. Citrix Systems is a cloud computing and virtualization technology company, and it provides services such as servers, cloud computing technologies, application and desktop virtualization, etc. Citrix software is the main service provided by the Citrix systems, and simply after it is installed on two endpoint devices such as personal computers, then Citrix software provides the users a fast, secure document sharing facilities .in the Citrix service's bug bounty program page, we can't find any detail about what the Citrix systems do.



In the description, first given the rewards according to the severity level of the bug and they say for low severity bug they give $100, medium severity $500, high severity $4000 and for critical level severity $10 000 .after that, they show how the vulnerabilities are categorized into each severity levels.

Rewards

Low	Medium	High	Critical
$100	$500	$4,000	$10,000

Critical

- Remote code execution, e.g., code execution on CC production, remote code execution with root level access on host machine or multi-tenant key compromise
- Service key compromise, e.g., taking over a multi-tenant key

High

- Arbitrary account takeover of a user's cloud account
- Service key compromise, e.g., taking over a single tenant key
- SQL injection, e.g., cross-tenant data exfiltration
- IDOR/missing authorization checks leading to key compromise or customer data leakage
- Unrestricted XXE/file system access, e.g., cross-tenant data leak
- Directory traversal/arbitrary file read - depending on types of files that can be read, e.g., system file read issues

Medium

- CSRF - excluding on logout and on publicly available forums
- XSS - depending on impact and type of XSS
- Server misconfiguration leading to compromise or data leak
- Misconfigured S3 buckets - only when the attacker can weaponize the buckets/instance

Low

- All subdomain takeovers on subdomains of *.cloud.com and *.citrixworkspacesapi.net
- Other vulnerabilities with proven impact which are not listed as out of scope

Next, we can see the policy of this bug bounty program and some other instructions to create Citrix accounts, as well as shows the program rules .in this description, we cant see eligible vulnerabilities, but they provide out scope vulnerabilities so we can avoid trying to find these kinds of vulnerabilities from the given domains. The out scope vulnerabilities are given below.

- Subdomain takeovers on ShareFile domains
- **Vulnerabilities found on subdomains of cloud.com which are not explicitly listed in scope**
- Clickjacking and issues only exploitable through clickjacking
- Descriptive error messages (e.g., Stack Traces, application, or server errors) without proof of vulnerability or risk
- HTTP 404 codes/pages or other HTTP non-200 codes/pages
- Fingerprinting/banner disclosure on common/public services
- Disclosure of known public files or directories, e.g., robots.txt
- Scripting or other automation and brute forcing of intended functionality
- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Lack of Secure and HTTPOnly cookie flags
- Content spoofing (text injection) or IDN homograph attacks or reflected file download attacks
- Tabnabbing
- Email configuration issues (SPF, DKIM, DMARC)
- Weak captcha or captcha bypass
- Forced login/logout CSRF
- Account lockout, login, or forgot password page brute force
- Password complexity or account recovery policies
- HTTPS Mixed Content
- Missing HTTP security headers
- Known SSL issues
- SSL Forward Secrecy or HSTS not enabled
- Weak SSL/TLS cipher suites
- Issues related to networking protocols or industry standards not controlled by Citrix
- Sending vulnerability reports using automated tools without validation
- Use of a known-vulnerable library without evidence of exploitability
- Problems related to widely publicized CVE's
- Attacks requiring physical access to a user's unlocked device
- Reports of spam, phishing, or security best practices
- Username/email enumeration
- Bugs in content/services that are not owned/operated by Citrix
- Vulnerabilities affecting users of outdated or unsupported browsers or platforms
- Any activity that could lead to the disruption of our service (DoS)
- Comma Separated Values (CSV) injection without demonstrating a vulnerability
- Content spoofing and HTML injection issues without showing an attack vector/without being able to execute JavaScript
- HTTP OPTIONS/TRACE/PUT methods enabled
- Disclosure of private IP addresses in HTTP responses
- 3rd party feature abuse (data: URL schema)
- Partner sites/services

After that, we can see the in-scope domains, and we are going to select a few for the analysis.

In Scope

Domain	citrix.cloud.com	Critical	Eligible
Domain	www.cloud.com	Critical	Eligible
Domain	ap-s.cloud.com	Critical	Eligible
Domain	eu.cloud.com	Critical	Eligible
Domain	us.cloud.com	Critical	Eligible
Domain	*.citrixworkspacesapi.net	Critical	Eligible
Domain	onboarding.cloud.com	Critical	Eligible

Setting The Scope

- www.cloud.com
- citrix.cloud.com

We can see a long list of domains in the in-scope domains section, but we will only analyze a few of them. Then we can see the out-of-scope domains, so in the next steps, we can reject them if we get some vulnerabilities from these domains.

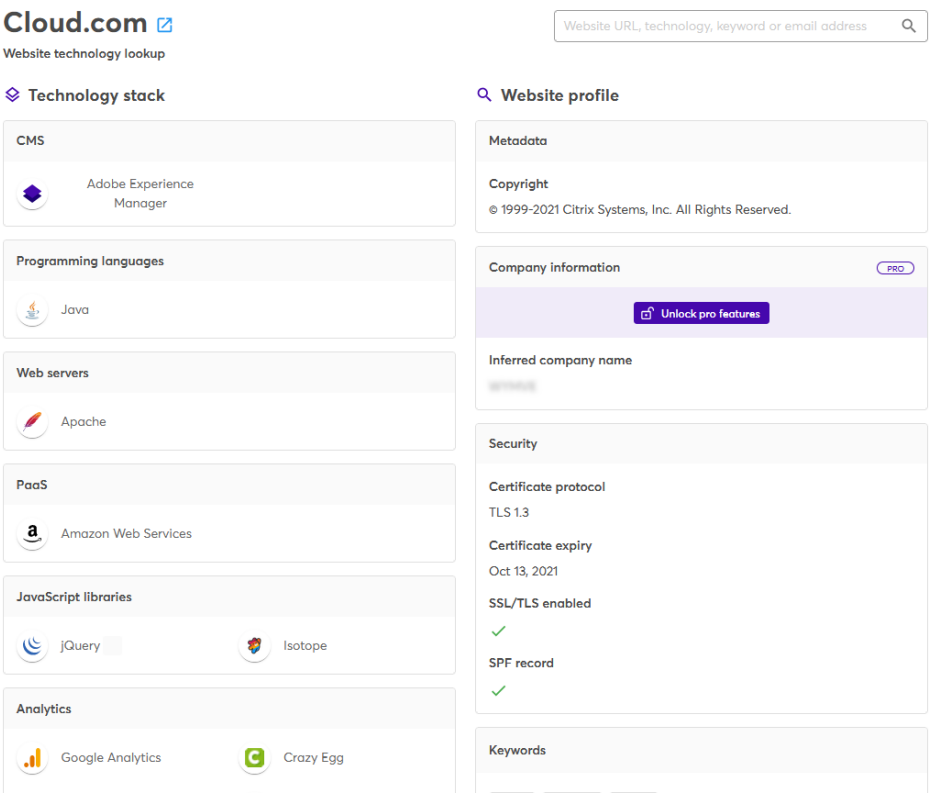
Out of Scope

Domain	*.citrix*.com
Domain	*.cloudburrito.com
Domain	*.sharefile.com
Domain	*.sharefile.eu
Domain	*.securevdr.com
Domain	*.podio.com
Domain	*.sharefile*.com
Domain	*.sharefile*.eu

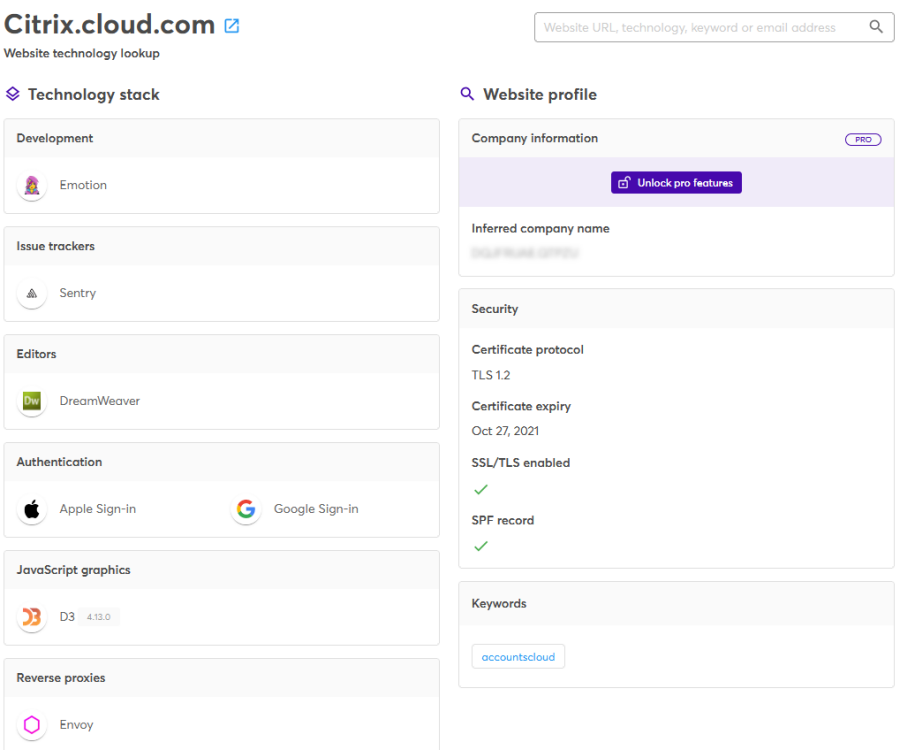
From this point onwards, we are going to analyze the domains we selected from the in-scope domains.

Gathering Information About Domains

Now we have two domains to analyze, so we will gather information for both domains and see what we can learn about these two domains. Now we need some tools to gather information about domains. First, I am going to use wappalyzer to see about the domains.



These are the information I got by giving www.cloud.com as the domain. Using wappalyzer, we can see a small number of details, but we can see details like what services are running and what technologies it uses in the given domain. We can uses java as a programming language. The webserver is an apache server.in the security section, we can see the certificate details and other security mechanisms like ssl .to see the company information we have to log in to get the pro features.



The citrix.cloud.com uses a different set of services. It uses emotion libraries and some different sets of services. This domain is also using SSL, and we can see the certificate protocols are different. It uses some authentication mechanisms like apple signing and Google sign-in. Next, we are going to use whoisllokup to gather information like IP and other server-related information.

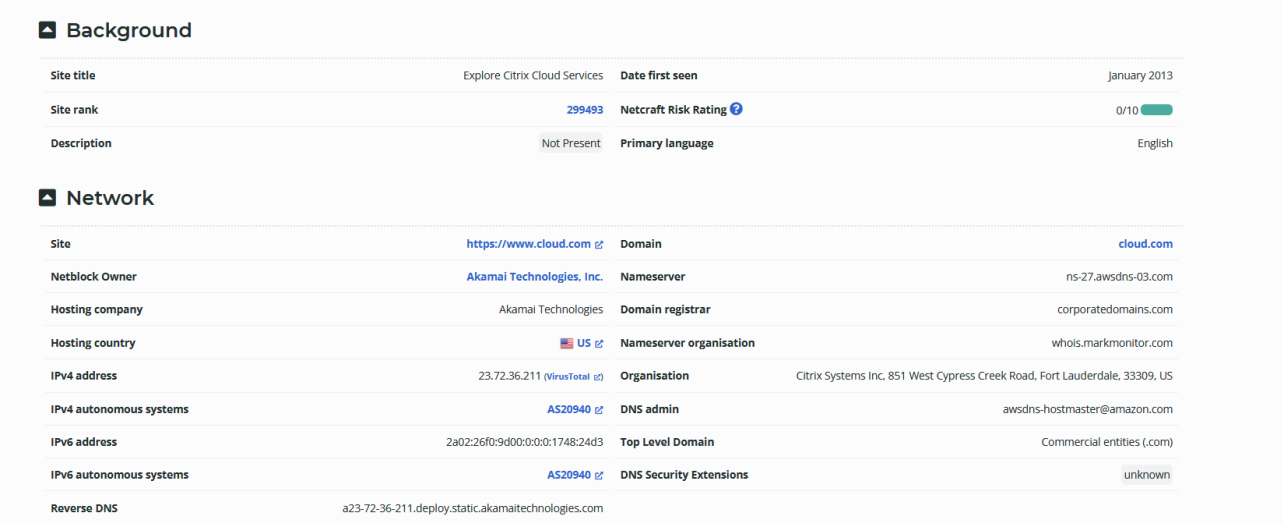
– Domain Profile

Registrant	Abuse Management
Registrant Org	Citrix Systems Inc
Registrant Country	us
Registrar	CSC CORPORATE DOMAINS, INC. CSC Corporate Domains, Inc. IANA ID: 299 URL: www.cscprotectsbrands.com,http://cscdbs.com Whois Server: whois.corporatedomains.com domainabuse@cscglobal.com (p) 18887802723
Registrar Status	clientTransferProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	7,601 days old Created on 2000-12-13 Expires on 2021-12-13 Updated on 2020-10-21
Name Servers	NS-1310.AWSDNS-35.ORG (has 47,489 domains) NS-1736.AWSDNS-25.CO.UK (has 377 domains) NS-27.AWSDNS-03.COM (has 6,924 domains) NS-977.AWSDNS-58.NET (has 162 domains)
Tech Contact	Abuse Management Citrix Systems Inc 851 West Cypress Creek Road, Fort Lauderdale, FL, 33309, us abuse@citrix.com (p) 19542673000 (f) 19542673000
IP Address	23.53.34.34 - 973 other sites hosted on this server
IP Location	- Washington - Seattle - Akamai Technologies Inc.
ASN	AS20940 AKAMAI-ASN1, NL (registered Jul 10, 2001)
Domain Status	Registered And Active Website
IP History	62 changes on 62 unique IP addresses over 16 years
Registrar History	3 registrars
Hosting History	13 changes on 12 unique name servers over 19 years

These results I got for the www.cloud.com domain. But when I tried to get citrix.cloud.com information, I got the exact same results. This domain may be a service of the cloud.com like account login or another service. Because of that, we can see the same IP and other details for both. We can see the IP location is Washington, and the ipv4 address is given as 23.53.34.34 .and we can see the name servers and some contact information, and the records of the domain created day and expiration date as well.

Technologies

We already found some technology uses in the target domains, but we need to further information about the technologies using another few tools then we can ensure that information and find new things we didn't find earlier.



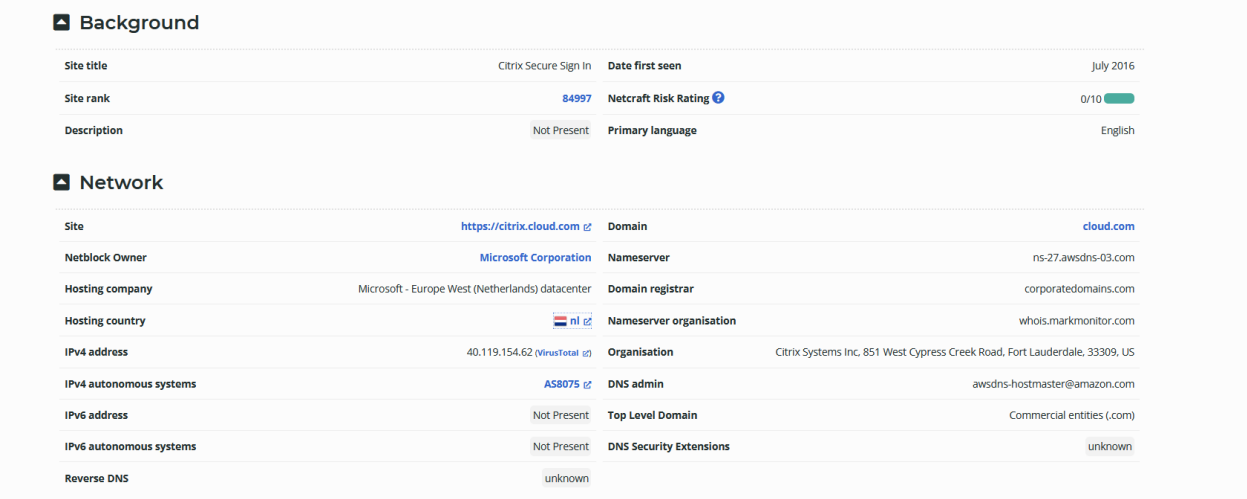
Background

Site title	Explore Citrix Cloud Services	**Date first seen**	January 2013
Site rank	299493	**Netcraft Risk Rating**	0/10
Description	Not Present	**Primary language**	English

Network

Site	https://www.cloud.com	**Domain**	cloud.com
Netblock Owner	Akamai Technologies, Inc.	**Nameserver**	ns-27.awsdns-03.com
Hosting company	Akamai Technologies	**Domain registrar**	corporatedomains.com
Hosting country	US	**Nameserver organisation**	whois.markmonitor.com
IPv4 address	23.72.36.211 (VirusTotal)	**Organisation**	Citrix Systems Inc, 851 West Cypress Creek Road, Fort Lauderdale, 33309, US
IPv4 autonomous systems	AS20940	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	2a02:26f0:9d00:0:0:0:1748:24d3	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	AS20940	**DNS Security Extensions**	unknown
Reverse DNS	a23-72-36-211.deploy.static.akamaitechnologies.com		

In the result, we can see a different IP address in the result page .before we get both domains ipv4 address as 23.53.34.34, but here we get the IP address as 23.72.36.211.in the earlier step we see in the whoislookup result there was a message with the IP address, and it said that 973 other sites hosted in the same server so this can be the reason for that IP difference. Let's see the other domain's result.



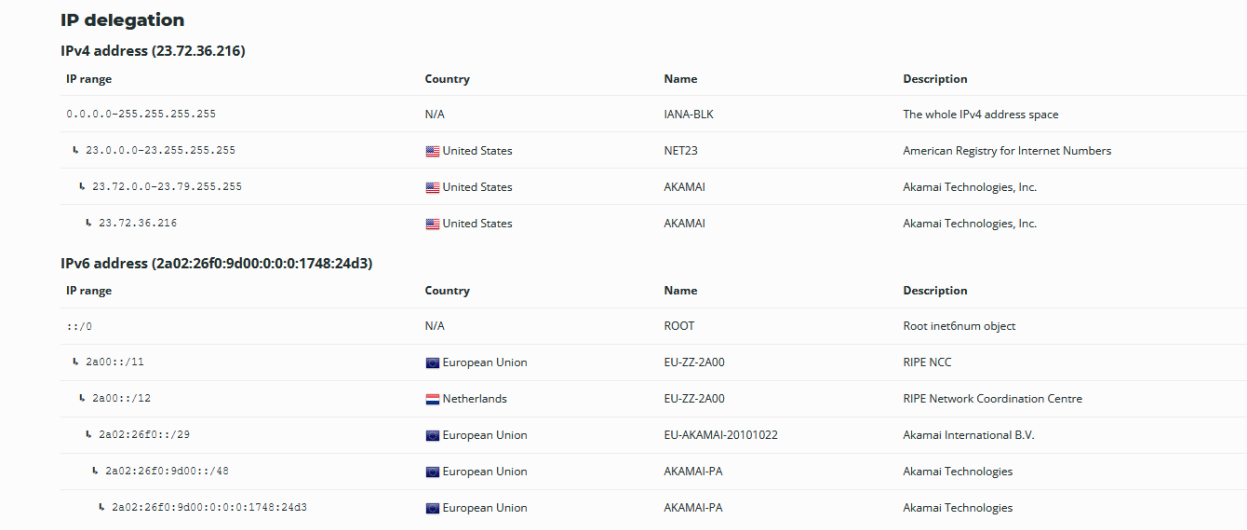
Background

Site title	Citrix Secure Sign In	**Date first seen**	July 2016
Site rank	84997	**Netcraft Risk Rating**	0/10
Description	Not Present	**Primary language**	English

Network

Site	https://citrix.cloud.com	**Domain**	cloud.com
Netblock Owner	Microsoft Corporation	**Nameserver**	ns-27.awsdns-03.com
Hosting company	Microsoft - Europe West (Netherlands) datacenter	**Domain registrar**	corporatedomains.com
Hosting country	nl	**Nameserver organisation**	whois.markmonitor.com
IPv4 address	40.119.154.62 (VirusTotal)	**Organisation**	Citrix Systems Inc, 851 West Cypress Creek Road, Fort Lauderdale, 33309, US
IPv4 autonomous systems	AS8075	**DNS admin**	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	**Top Level Domain**	Commercial entities (.com)
IPv6 autonomous systems	Not Present	**DNS Security Extensions**	unknown
Reverse DNS	unknown		

In this result, we can see it is another different IP as well as a different IP location. And it mentions that this is also a subdomain of cloud.com.so we can think even this is a subdomain of cloud.com, but this server location is different. To confirm that, you can investigate the IP delegation section.



IP delegation

IPv4 address (23.72.36.216)

IP range	Country	Name	Description
0.0.0.0-255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 23.0.0.0-23.255.255.255	United States	NET23	American Registry for Internet Numbers
↳ 23.72.0.0-23.79.255.255	United States	AKAMAI	Akamai Technologies, Inc.
↳ 23.72.36.216	United States	AKAMAI	Akamai Technologies, Inc.

IPv6 address (2a02:26f0:9d00:0:0:0:1748:24d3)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
↳ 2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
↳ 2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
↳ 2a02:26f0::/29	European Union	EU-AKAMAI-20101022	Akamai International B.V.
↳ 2a02:26f0:9d00::/48	European Union	AKAMAI-PA	Akamai Technologies
↳ 2a02:26f0:9d00:0:0:0:1748:24d3	European Union	AKAMAI-PA	Akamai Technologies

Now we know this is exactly another server in a different location. If you want to confirm that further, you can use the IP Geolocation area to see visualization on the world map. now we know citrix.cloud.com is a subdomain, but in the beginning,

we saw this domain given under the in-scope domains. So now we can reject this domain and gather information only for the cloud.com domain.

In the description, it says the server does not support ssl version 3 and uses DMARC(domain-based message authentication).this domain uses adobe analytics as third-party resources. This result also says it uses javascript as a client-side technology, and it uses UTF8 encoding and Google webmaster tools. And for security, its implemented some technologies are given below.

- Document Compatibility Mode
- X-Content-Type-Options
- Strict Transport Security
- X-Frame-Options Same Origin
- Referrer-Policy
- X-XSS-Protection Block
- Content Security Policy

Gathering subdomain information

Now we know the second domain we selected is also a subdomain of cloud.com, and in this step, we only gather its subdomain information. We can use a tool like sublis3r, but it only gives subdomains. If we use knockpy for subdomain enumeration, we can see the subdomain and the corresponding IP address. We use both tools to subdomain enumerate, and after, we will analyze them.

```
13:51:19

Ip address      Code Subdomain                 Server                    Real hostname
--------------- ---- ------------------------- ------------------------- -------------------------
51.138.2.249    200  academy.cloud.com                                   sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
40.115.64.138   404  accounts.cloud.com                                  ctxathpause06-identity4-nt1.australiasoutheast.cloudapp.azure.com
20.69.200.148   200  acme25.cloud.com                                    sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  admin65.cloud.com                                   sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  af.cloud.com                                        sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.197.100.234  200  aiacvad.cloud.com                                   sfaas-prod-seas-waf-b-appgw.southeastasia.cloudapp.azure.com
20.197.100.234  200  alibaba.cloud.com                                   sfaas-prod-seas-waf-b-appgw.southeastasia.cloudapp.azure.com
20.69.200.148   200  allergan.cloud.com                                  sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  altareturn.cloud.com                                sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  amerigas.cloud.com                                  sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
13.107.246.59   200  analytics.cloud.com                                 part-0031.t-0009.t-msedge.net
13.107.246.59   200  analytics-staging.cloud.com                         part-0031.t-0009.t-msedge.net
13.107.246.59   200  api.cloud.com                                       part-0031.t-0009.t-msedge.net
40.88.49.69     410  apollo.cloud.com                                    ctxwsp-eastus-release-b-nt-releasescloudproxy.eastus.cloudapp.azure.com
40.88.49.69     410  applications.cloud.com                              ctxwsp-eastus-release-b-nt-releasescloudproxy.eastus.cloudapp.azure.com
20.69.200.148   200  arizona.cloud.com                                   sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
51.138.2.249    200  ascogroup.cloud.com                                 sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
51.138.2.249    200  asosremote.cloud.com                                sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
51.138.2.249    200  atlas.cloud.com                                     sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
40.88.49.69     410  au.cloud.com                                        ctxwsp-eastus-release-b-nt-releasescloudproxy.eastus.cloudapp.azure.com
20.69.200.148   200  austin.cloud.com                                    sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  badnauheim.cloud.com                                sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  bobweb.cloud.com                                    sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  bsd.cloud.com                                       sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
51.138.2.249    200  cargolux.cloud.com                                  sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
104.75.166.84   403  cdn.cloud.com             AkamaiGHost               e8793.dscd.akamaiedge.net
```

We get 128 subdomains, and there are several Ip addresses with different servers and different hostnames. Now we know why the domain has several servers spread around the world, so that's why it shows different IP addresses and servers.

```
51.138.2.249    200  cargolux.cloud.com                                  sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
104.75.166.84   403  cdn.cloud.com             AkamaiGHost               e8793.dscd.akamaiedge.net
20.69.200.148   200  channel.cloud.com                                   sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
40.88.49.69     410  charlie.cloud.com                                   ctxwsp-eastus-release-b-nt-releasescloudproxy.eastus.cloudapp.azure.com
20.69.200.148   200  chevron.cloud.com                                   sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  chevrondev.cloud.com                                sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
40.88.49.69     200  citrix.cloud.com                                    ctxwsp-eastus-release-b-nt-releasescloudproxy.eastus.cloudapp.azure.com
40.88.49.69     410  clientes.cloud.com                                  ctxwsp-eastus-release-b-nt-releasescloudproxy.eastus.cloudapp.azure.com
51.138.2.249    200  compusoft1.cloud.com                                sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
20.69.200.148   200  connect.cloud.com                                   sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
51.138.2.249    200  consulting.cloud.com                                sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
20.69.200.148   200  customer.cloud.com                                  sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
20.69.200.148   200  demo.cloud.com                                      sfaas-prod-eus2-waf-b-appgw.eastus2.cloudapp.azure.com
51.138.2.249    200  design.cloud.com                                    sfaas-prod-weu-waf-b-appgw.westeurope.cloudapp.azure.com
```

Now we can clearly see citrix.cloud.com is a subdomain in a different server .now clarify our problem, so we don't need to do a subdomain enumeration again.

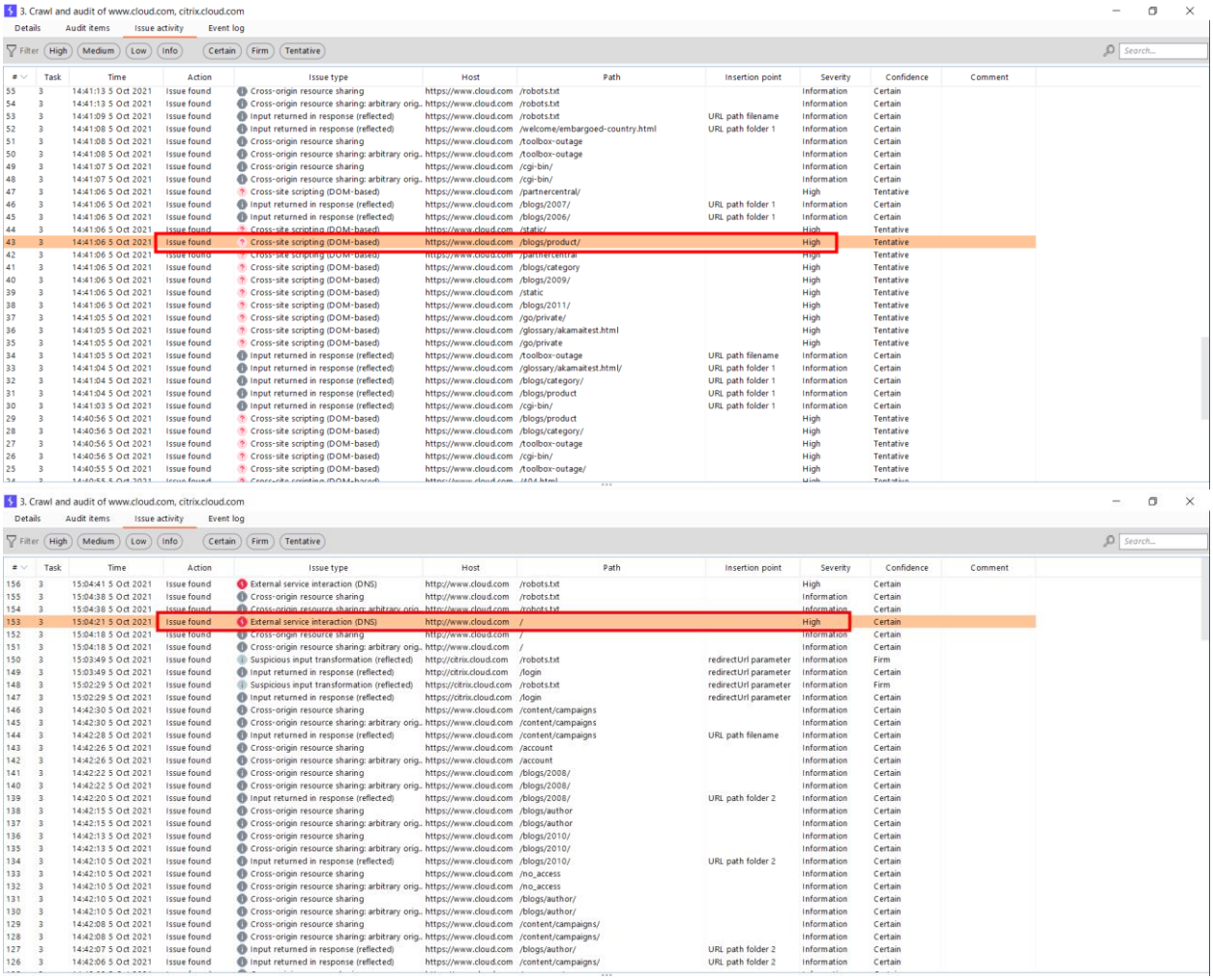
Gather Information About Files And Directories

We already got a lot of information about cloud.com, but performing a web content scanner is very important when looking for a bug in a particular domain. Because sometimes we can capture some sensitive data or clues using these files and directories .so we can do a web content scan using a tool called Dirb.

By using Dirb, we get only a few files and using these files, and we cannot get any helpful information.

Vulnerability Assessment

Now we are moving to the important part is vulnerability scanning .when we are talking about vulnerability scanning, if we are going to automate that process, we can use a lot of tools such as owasp zap, Nessus, Nmap, etc., but here I will use burp suite to vulnerability scanning because it is simple and very easy to understand.



Using the burp suite, we are getting two types of critical severity alerts. We get one alert, and it says there is a possibility to happen dom-based cross-site scripting .second alert we are getting from burp and it saying about External service interaction vulnerability. Cross-site scripting is a somewhat common attack, so we are going to talk about external service interaction and how we can mitigate it.

Vulnerabilities we found

External service interaction (DNS)

Request

```
GET / HTTP/1.1
Host: 9lvfpebj04e1zz41w9v82hu4gvmoag04s6gw3mrb.burpcollaborator.net
Pragma: no-cache
Cache-Control: no-cache, no-transform
Connection: close
```

Response

```
HTTP/1.0 400 Bad Request
Server: AkamaiGHost
Mime-Version: 1.0
Content-Type: text/html
Content-Length: 209
Expires: Tue, 05 Oct 2021 09:34:40 GMT
Date: Tue, 05 Oct 2021 09:34:40 GMT
Connection: close

<HTML><HEAD>
<TITLE>Invalid URL</TITLE>
</HEAD><BODY>
<H1>Invalid URL</H1>
The requested URL "&#91;no&#32;URL&#93;", is invalid.<p>
Reference&#32;&#35;9&#46;2c544b68&#46;1633426480&#46;37dc293f
</BODY></HTML>
```

Issue detail

- There is a possibility to persuade the web application to run a server-side DNS lookup with random domain names.

- The payload 1su7w6ib7wlt6rbt3120991wnntgh852zqpdf14.burpcollaborator.net was included in the HTTP host header.

- Then the web application ran a DNS lookup of the given domain.

Issue background

This type of vulnerability happens if there is a possibility to persuade a web application to interact with a given or random external services like a web server or a mail server. The possibility to enforce a random external service does not cause a vulnerability in its own right, but in some situations, it can be an intended behavior of the web application.

But most of the time, it will show a critical vulnerability that causes it to be very harmful when it is exploited. In situations where it can perform a DNS-based

interaction generally, it is possible to enforce interactions using other types of services, then these situations are reported as separate issues. Suppose there is an enforcement of a DNS-based interaction by causing a payload that includes a particular service type like URL. In that case, the web application is trying to connect using that other service, but this indicates that egress filters prevented attempts at the network layer.

If a web application has this vulnerability, it means it is able to send requests to other systems and services that will allow using that vulnerable server as an attack proxy. By injecting a suitable payload, a threat actor has the ability to attack other services and systems that the server can interact with. This attack will affect third-party systems within the same organization and services in the application server's loopback adapter. The vulnerability level depends on the network architecture, and sometimes it exposes other vulnerable services that external attackers cannot access.

Issue remediation

- The relevant application functionality should be reviewed, the purpose and the intended use, then analyzed and confirmed whether the ability to enforce arbitrary external interactions is are intended behavior or not.

- If it is not intended behavior, it needs to take suitable measures and be aware of the types of attacks that can be performed using this ability.

Possible measures

- Block the network access from the web application server to other systems inside the organization.

- Enable barriers to the application server to remove services that are available in the loopback adapter.

- Implement a whitelist of permitted services and hosts and block others.

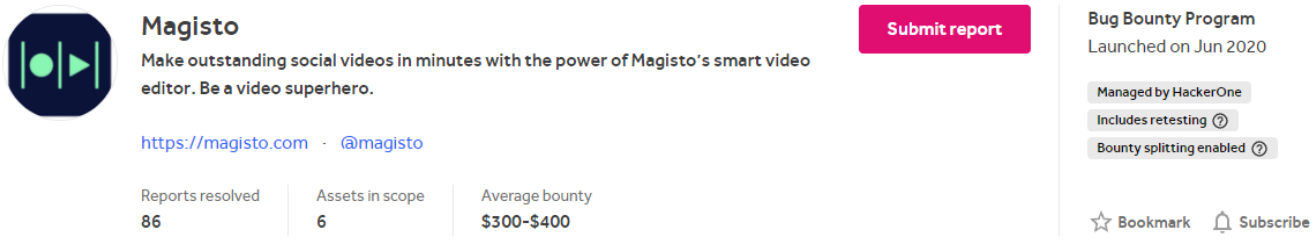
Conclusion

In this report, we selected the Citrix Systems bug bounty program to analyze and see whether we were able to find a bug. Then we tried to gather information about the technologies and the IP addresses, subdomains, and some other areas. Then we did some analysis about the IP address difference that occurs because it has many servers, so we clarified those things in that step. After doing a web content scan, we moved to vulnerability assessment and found there were two types of critical vulnerabilities. We chose external service interaction vulnerability to further analysis. Finally, we learned what this vulnerability means, what bad situations cause this vulnerability, and the solutions for that.

REPORT 04

INTRODUCTION

In this report, we will analyze the magisto.com domain with the intention of finding bugs, and this domain also I chose from HackerOne bug bounty programs. Magisto is a technology company, and its headquarters are situated in California. And its vision is to provide AI technology to create videos more easily and quickly. Magisto has an online video creating platform as well as applications for mobile phones with excellent video creating facilities.



In the description, we cannot find out further details about the company. Next, they have given the rewards they gave according to the severity level of the bug we are going to submit, and they have also given the scoring method to score the submission. According to the score we have, we are getting the corresponding rewards.

Rewards

Low	Medium	High	Critical
$100	$200	$500	$1,000

Critical (9.0 - 10.0)	High (7.0 - 8.9)	Medium (4.0 - 6.9)	Low (0.1 - 3.9)
$1,000-2,000	$500-1,500	$200-500	$100-300

Then they gave some information about their bug disclosure policies. They show the rules and regulations that we need to follow in this bug-finding process. These are important when we are doing some testings and analysis with this domain.

Rules

- To be considered the original reporter of a vulnerability :
  - You must be able to prove that there is a vulnerability using your own account(s) and your own data.
  - Submit one vulnerability per report, unless you need to chain vulnerabilities to provide impact.
  - Multiple vulnerabilities caused by one underlying issue will be awarded one bounty.
  - Please provide detailed reports with reproducible steps.
  - If the report is not detailed enough to reproduce the issue, the issue will not be eligible for a reward. Videos work best (No need to overlay music), Text with screenshots second, plain text last.
  - HackerOne and Magisto must be able to reproduce it
  - It must go to "TRIAGED" state and be paid the post triage acceptance bounty reward of $100 (Reporting first without meeting the rest of the requirements or just having a lower ticket number does not qualify as being the original reporter. Please note we have an active security team that does scans, contracts out for pentests, developers fixing issues on their own, etc. While not in HackerOne they will count as being "first reporter")
- **Don't** attempt to access other people's private data. **Basic Magisto accounts are free**, as well as the privacy features, so **setting up example cases with throwaway accounts should be easy**. Business accounts are available for a free trial. When you join, use the YEARLY Free trial during upgrade for one month of access (Monthly will only give 7 days). You are responsible for cancelling before it begins to bill.
- **Don't** use automated tools or scanners. Reports will be close as N/A.
- **Don't** DDoS or otherwise attack us in a way that would disrupt service for our customers

Next, they have said about vulnerabilities that they want to find with the help of us, so we have to read these things carefully. They are expecting a clear proof of concept. They need to clearly see how a particular vulnerability found by a bug

bounty hunter is exploiting. They say they are following the CVSS (the common vulnerability scoring standard)to rate the bug.

And they are especially saying that remote code execution, SQLi, get root access like vulnerabilities are considered critical vulnerabilities. So we can focus when we are analyzing to find out these vulnerabilities. They consider stored or reflected cross-site scripting and other novel bugs as medium-level vulnerabilities and CSRF and other security issues considered as low-level vulnerabilities.

Qualifying vulnerabilities

Please take the time to provide a clear proof of concept that shows how a particular vulnerability is exploitable. You must be able to reproduce the issue on request with your account(s). Use the following guidelines to categorize security issues. (These are guidelines, the CVSS score will determine its ultimate rating)

Critical: most impactful, Remote code execution, SQLi, root access to any systems

High: IDOR requiring simple brute force on incrementing identifier, stored xss that can be used against logged in users, account authentication issues (bypass etc)

Medium: stored or reflected cross site scripting, other novel bugs that have a security impact to many users

Low: CSRF missing from non excluded functions, other security issues that impact only a small subset of users

Practical, chained vulnerabilities where the resource identifier is obtainable by a reproducible vector, e.g. guessable, predicable, or via API calls will be eligible for reward at Magisto discretion.

Wont fix: information disclosure, see also other non qualifying vulnerabilities

We do appreciate reports containing CVSSv3 formatted scores (https://www.first.org/cvss/calculator/3.0)

Then they have given a non-qualifying vulnerabilities list, and it is a somewhat extensive list. At the bottom of the description, we can see the in-scope vulnerabilities, and we have to select one a few to further analyze from the set of given domains.

In Scope

Domain	**magisto.com,www.magisto.com**	Critical	Eligible
Domain	***.magisto.com** EXCEPTION - Subdomains owned/controlled/managed/etc by a 3rd party.	Critical	Eligible
Domain	**staging.magisto.com**	Critical	Eligible
Domain	**applause1.magisto.com**	Critical	Eligible
Android: Play Store	**com.magisto**	Critical	Eligible
iOS: App Store	**486781045**	Critical	Eligible

SETTING THE SCOPE

- magisto.com

We can see five domains in the in-scope section, but we are select only one domain because others seem like subdomains of the magisto.com domain. We are doing information gathering, analysis, and vulnerability assessment using this domain from this point onwards.

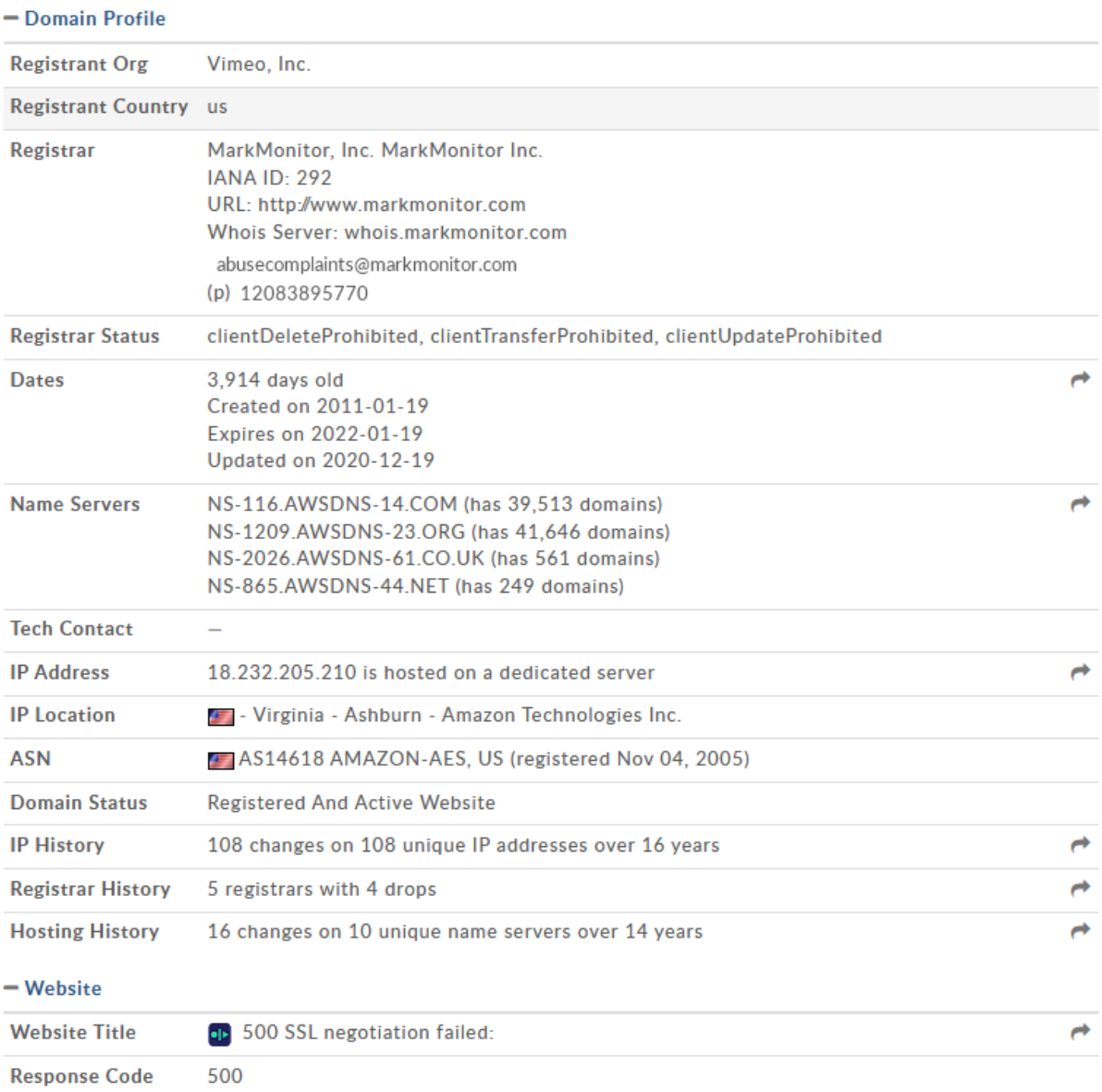
Out of Scope

Domain	*.test.magisto.com
Domain	*.dev.magisto.com
Domain	applause2.magisto.com
Domain	Gamma.magisto.com
Domain	delta.magisto.com
Domain	int001.vimeo.magisto.com
Domain	int002.vimeo.magisto.com
Domain	int003.vimeo.magisto.com

At last, they are given the out-of-scope domains, and when we are doing subdomain enumeration, we can reject them because the bugs we find by analyzing them are not eligible to get rewards.

INFORMATION GATHERING

Now we have select one domain that is magisto.com. In this step, we will gather some information using some tools, websites, etc., and learn what the technologies mechanism the web application is using, and more other things. At the very first, we are going to use whoislookup to gather information.



Domain Profile

Registrant Org	Vimeo, Inc.
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	3,914 days old Created on 2011-01-19 Expires on 2022-01-19 Updated on 2020-12-19
Name Servers	NS-116.AWSDNS-14.COM (has 39,513 domains) NS-1209.AWSDNS-23.ORG (has 41,646 domains) NS-2026.AWSDNS-61.CO.UK (has 561 domains) NS-865.AWSDNS-44.NET (has 249 domains)
Tech Contact	–
IP Address	18.232.205.210 is hosted on a dedicated server
IP Location	- Virginia - Ashburn - Amazon Technologies Inc.
ASN	AS14618 AMAZON-AES, US (registered Nov 04, 2005)
Domain Status	Registered And Active Website
IP History	108 changes on 108 unique IP addresses over 16 years
Registrar History	5 registrars with 4 drops
Hosting History	16 changes on 10 unique name servers over 14 years

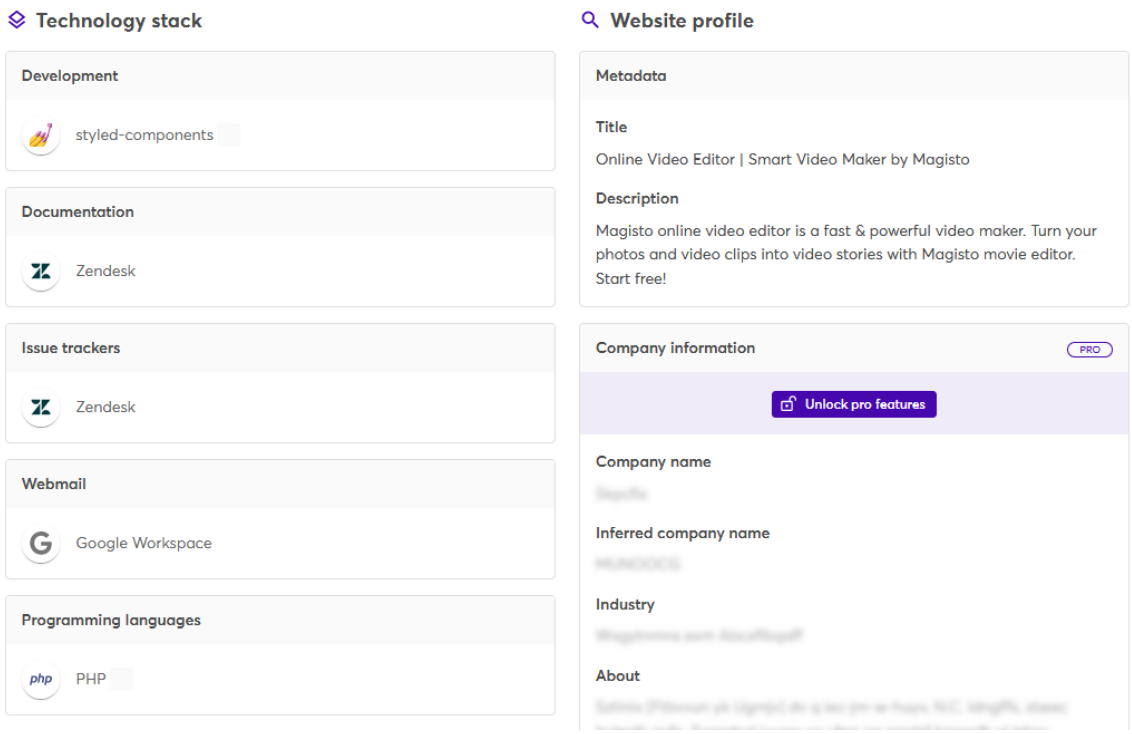
Website

Website Title	500 SSL negotiation failed:
Response Code	500

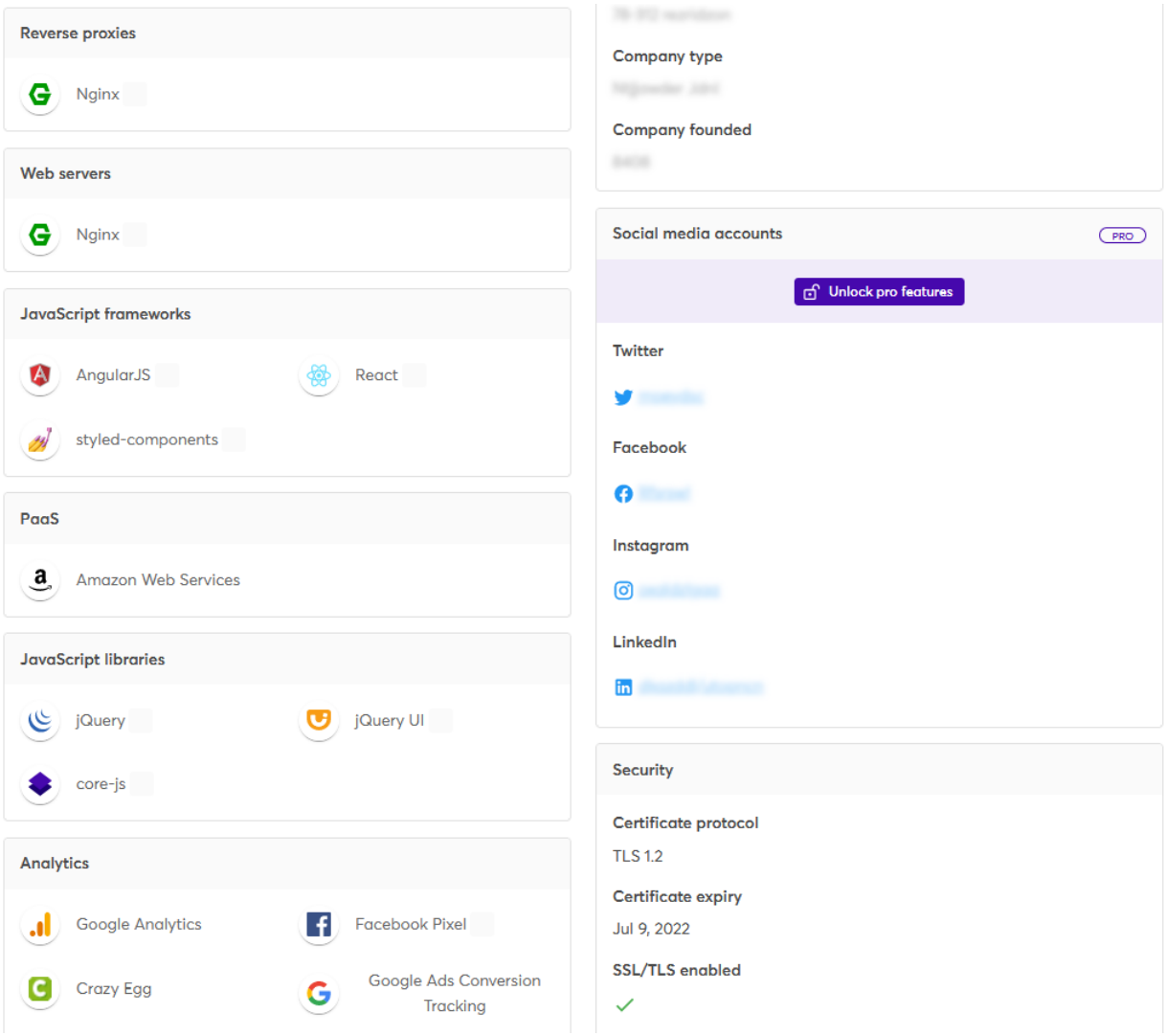
Using whoislookup, we got a lot of information about the domain we chose. the registrant organization of the magisto.com domain is 'Vimeo.inc', and its location in the united states. Then it shows some contact details and website created date and the expiration date, and also it shows when the web application updated.thereafter, we can see the name server is AWSDNS, and the domain's IP address is 18.232.205.210, and it says it is hosted on a dedicated server. There are some other details like Ip location, domain status, and response code.

TECHNOLOGIES

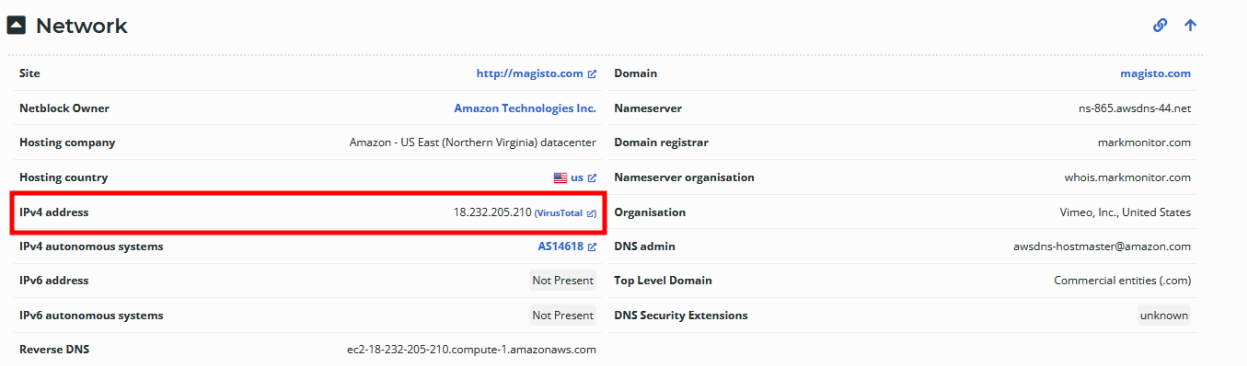
To gather information about the target domain, we are using several tools. Now we already have some information. In this step, we can confirm those information we found. We need to find more information about the domain.as the first tool, we will use the wappalyzer to find some information.



First we can see in the metadata it is given a small description about the company and what it does.to the development it uses styled-components and this means the application uses css and javascript for the development of the web application.then the uses Zendesk for the documentation and issue tracking purposes . Zendesk is a cloud-primarily based totally assist table control solution and it is offering customizable tools that we can use for web application development.and also we can see this web application uses google webmail services and it use PHP as a programming language.



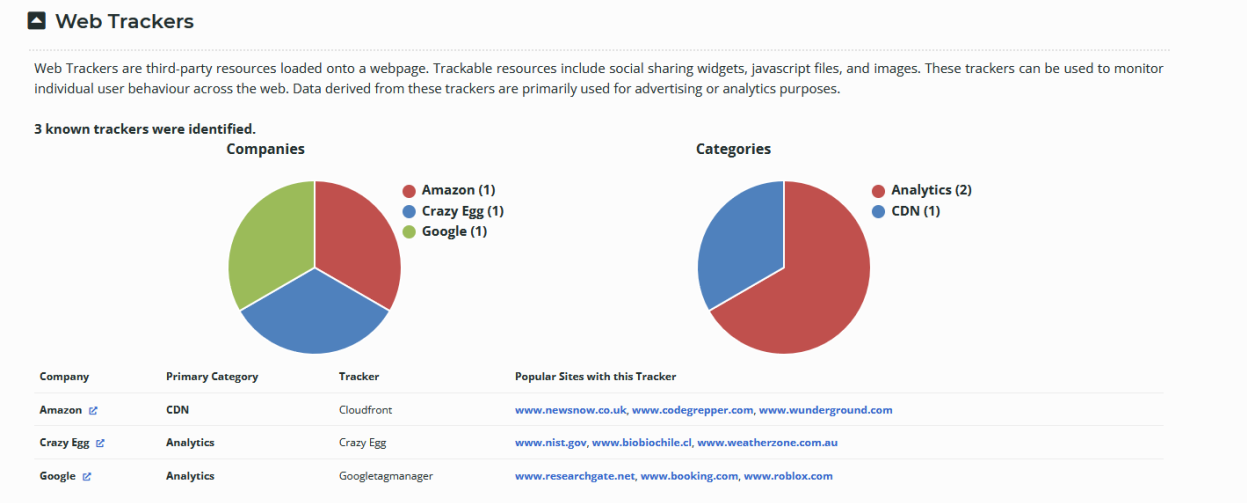
Next it says Nginx is the sever of the web application and it provides reverse proxies facilities to the application.the web application uses some javascript frameworks like angular js ,react and it uses some javascript libraries as well.also it is get help of analytics serverces like google analytics,facebook pixel etc.at the security section it is given the certificate protocol as TLS 1.2 and the certificate expiry date and SSL/TSL is enabled for this application.for get more informations we uses netcraft site.



Network

Site	http://magisto.com	Domain	magisto.com
Netblock Owner	Amazon Technologies Inc.	Nameserver	ns-865.awsdns-44.net
Hosting company	Amazon - US East (Northern Virginia) datacenter	Domain registrar	markmonitor.com
Hosting country	us	Nameserver organisation	whois.markmonitor.com
IPv4 address	18.232.205.210 (VirusTotal)	Organisation	Vimeo, Inc., United States
IPv4 autonomous systems	AS14618	DNS admin	awsdns-hostmaster@amazon.com
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	ec2-18-232-205-210.compute-1.amazonaws.com		

In the network section we can see some details we already have .the netblock owner of the domain is amazon technologies and the hosting company is also the amazon.then we can see the ip address and it is the exact same one we got earlier so now we know the information we got is correct.and the result shows is this is not a HTTPS site.that means the site is somewhat not secure.we see those things in further steps.



Web Trackers

Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

3 known trackers were identified.

Companies

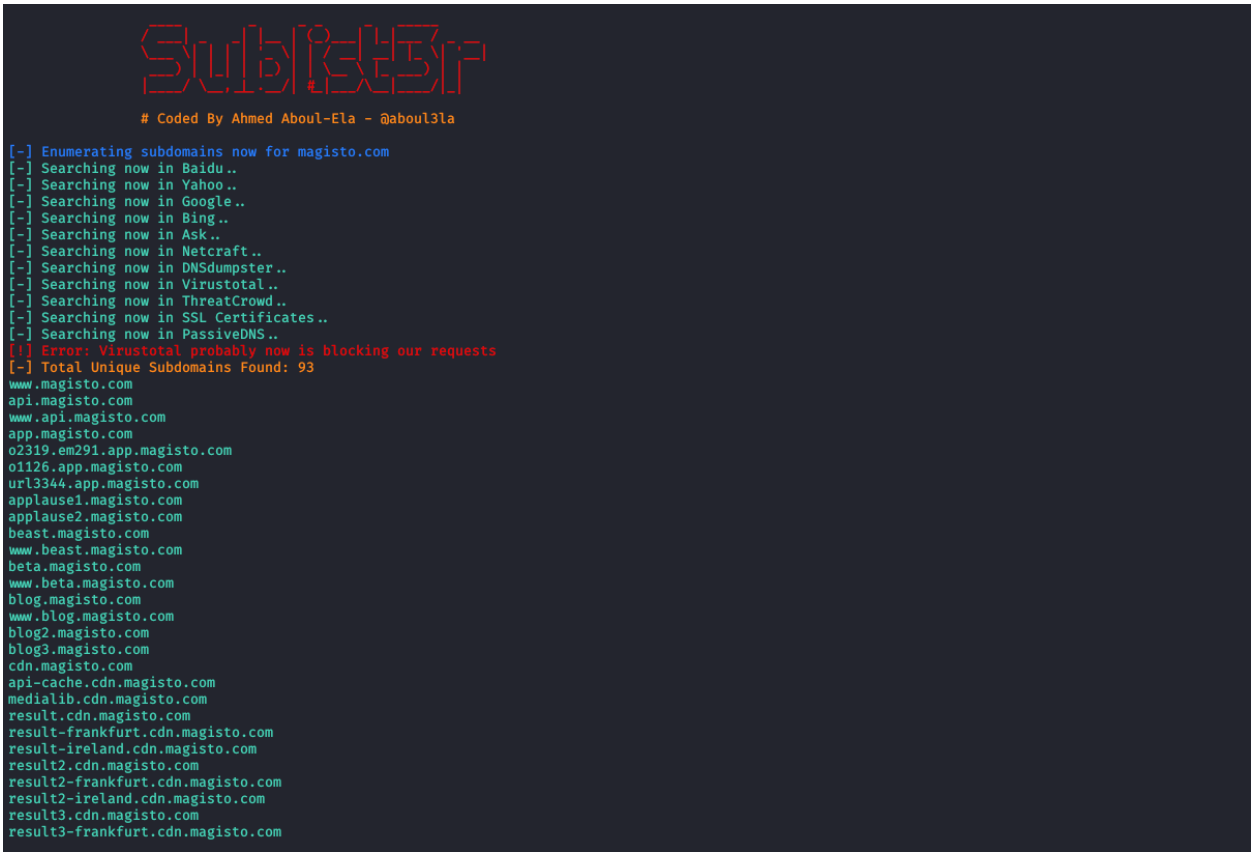
Categories

Company	Primary Category	Tracker	Popular Sites with this Tracker
Amazon	CDN	Cloudfront	www.newsnow.co.uk, www.codegrepper.com, www.wunderground.com
Crazy Egg	Analytics	Crazy Egg	www.nist.gov, www.biobiochile.cl, www.weatherzone.com.au
Google	Analytics	Googletagmanager	www.researchgate.net, www.booking.com, www.roblox.com

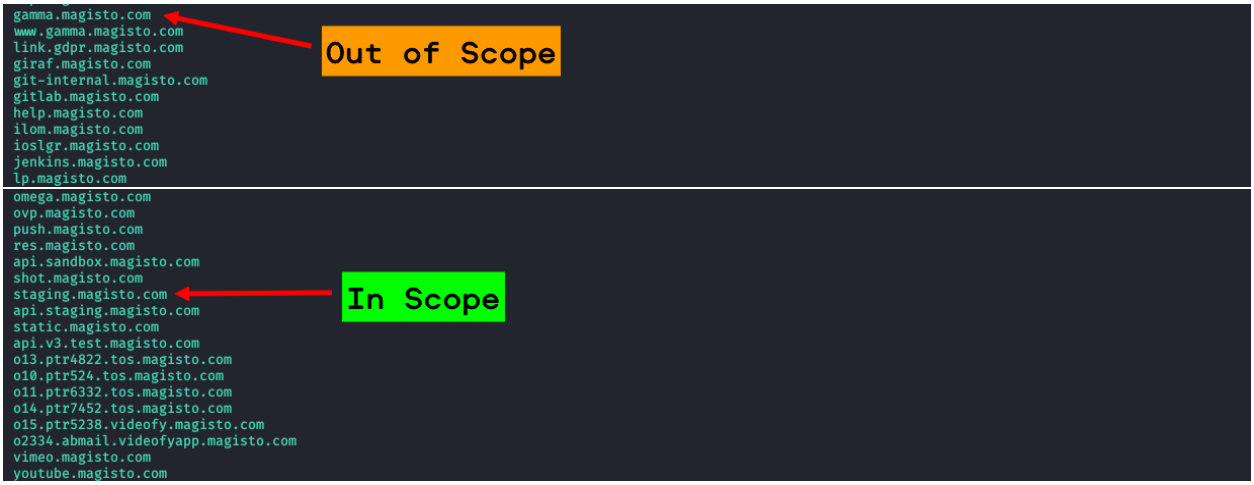
In the web trackers section it says the web application uses amazon CDN,Crazy Egg analytics and google analytics as third party resources .we saw some of them at the previous step.and most of the other details in the result page we gathered earlier.

Gather Subdomain Information

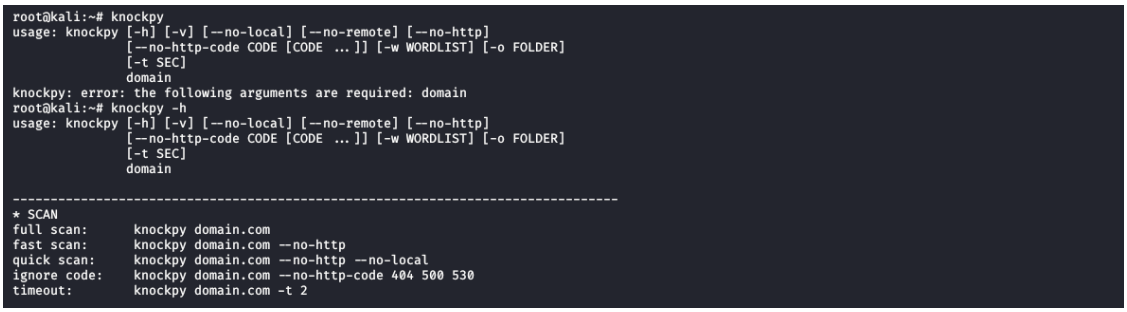
So far we found information about the network ,security and technologies of the our target domain that is magisto.com.as those information subdomain informaations are also important so we are now going to see how we can find subdomains and their information.for that we need some tools for subdomain enumeration .

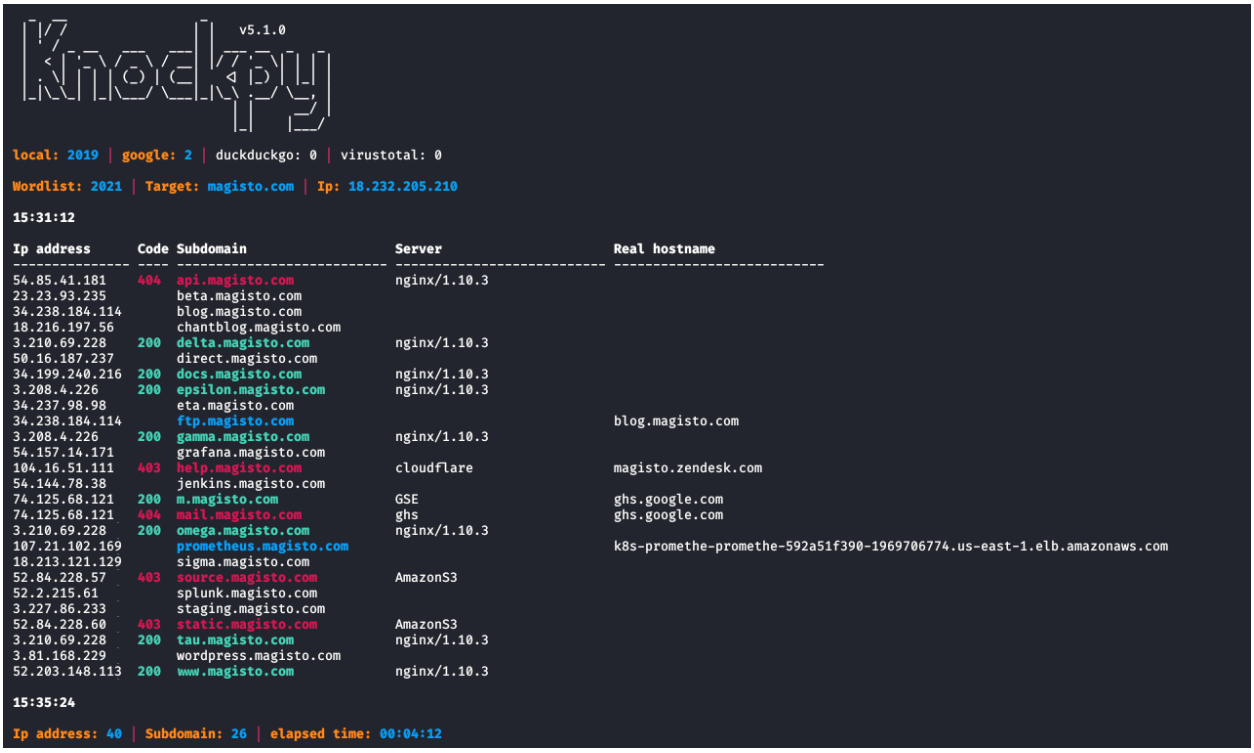


For the first information gathering I used sublist3r tool for subdomain enumeration and it gives 93 results by perform a brute force attack using the default word list.if you want to use sublist3r for find subdomain what you need to do is first give the word as sublist3r and give the domain which you want to find subdaomins .if you want to get help type sublist3r -h in the terminal.but the disadvantage of this tool is we can only get the subdomain and we cannot get other information like ip address ,server etc.



We can see in the subdomain list we can find the in scope and out of scope domains as well so we can keep trust on these tools because we can prove the result is correct.to get some additional data that not given by the sublist3r we can use another tool called knockpy.knockpy is written In python so if you want to use this tool first you have to install python to your machine. Then we can simply install the tool and give the command knockpy < domain > in terminal and press enter.if you want more details and help type knockpy -h in the terminal.

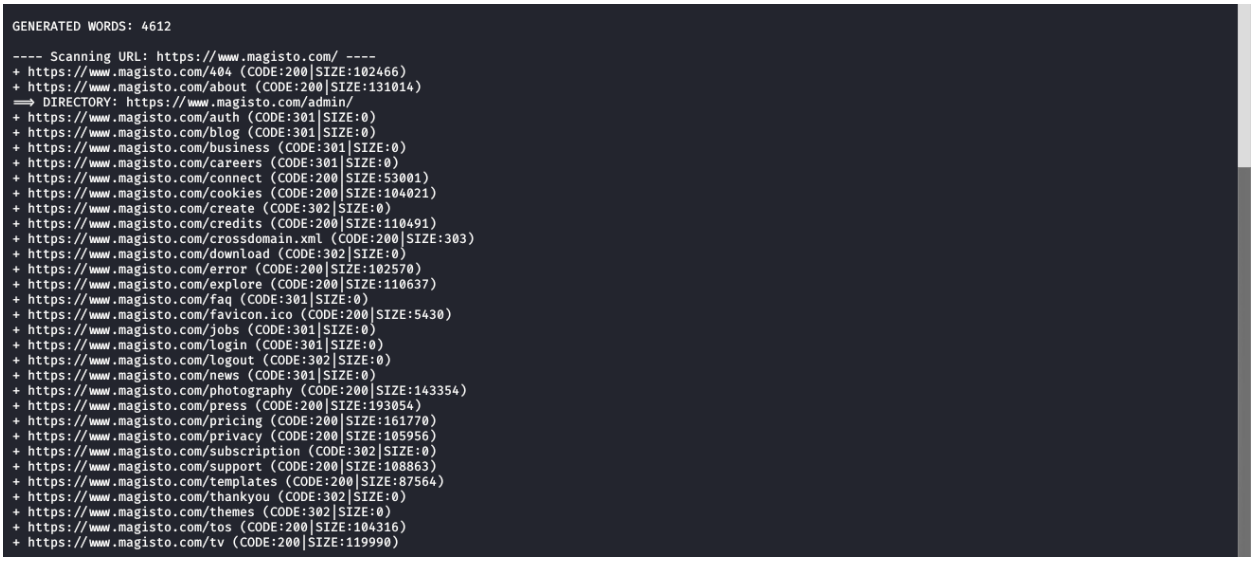




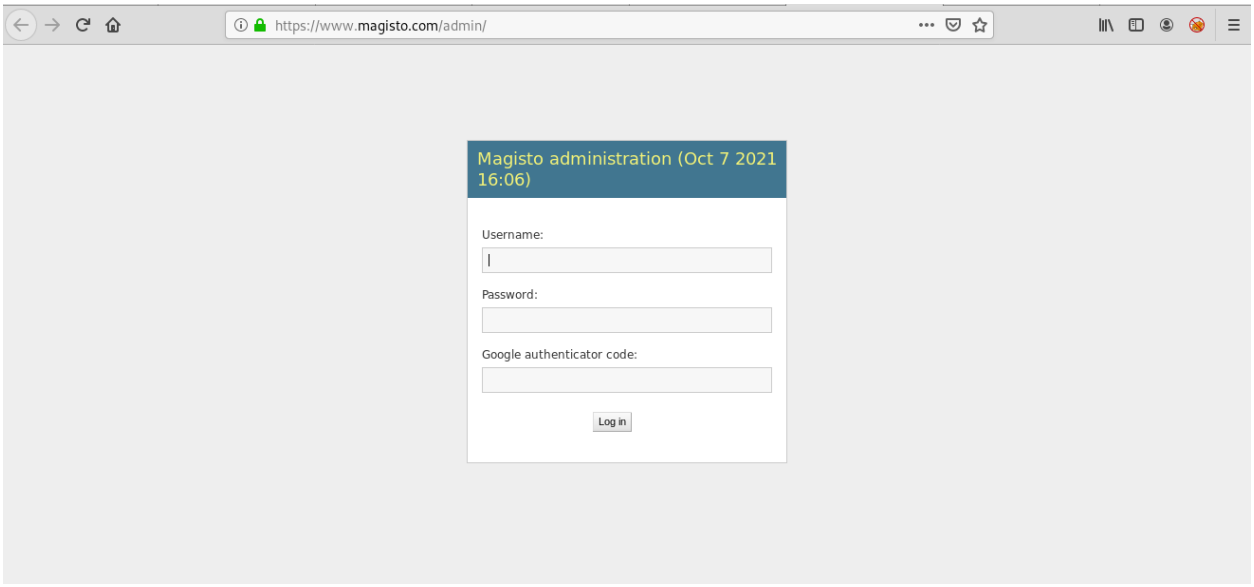
Now we have the subdomains and we gather these subdomains by using the knockpy tool.in the result we can see only 26 subdomains but this time we have the corresponding ip addresses and servers. In the result there are several ip addresses and different servers.that means some of subdomains are located in separate servers .some of servers we saw when we are doing the information gathering about technology.

GATHER INFORMATION ABOUT FILES AND DIRECTORIES

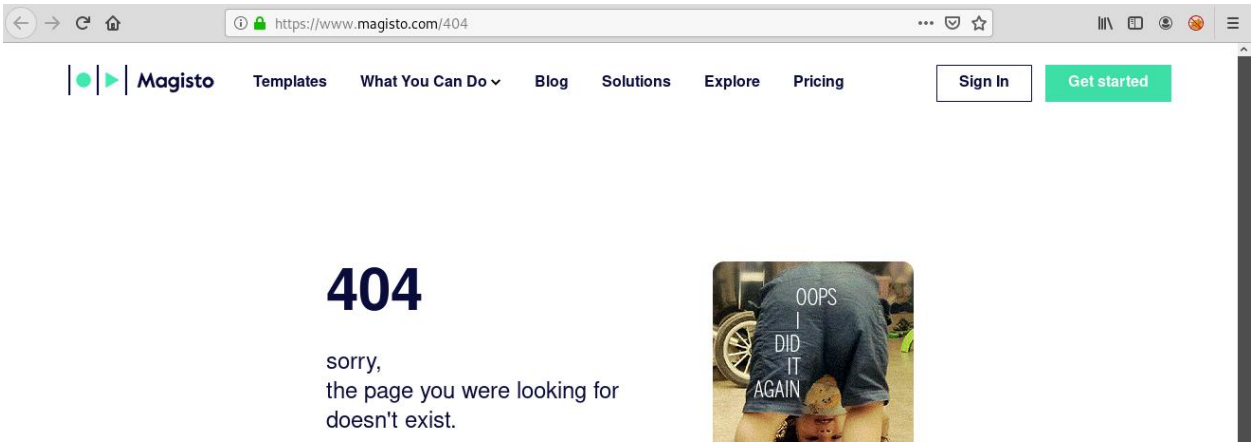
Now we have lot of details about the domain and now we are going to look for the files and directories stored in the web application and go into them and find some informations.we call that process as web content scanning and we can do in manually or using some tools.when you are doing manually you have to go to the directory by directory and search.if you are using a tool for that then the tool uses brute force attack with a world list and search for files.there are few tools that can do a web content scanning among them I select DIRB tool.



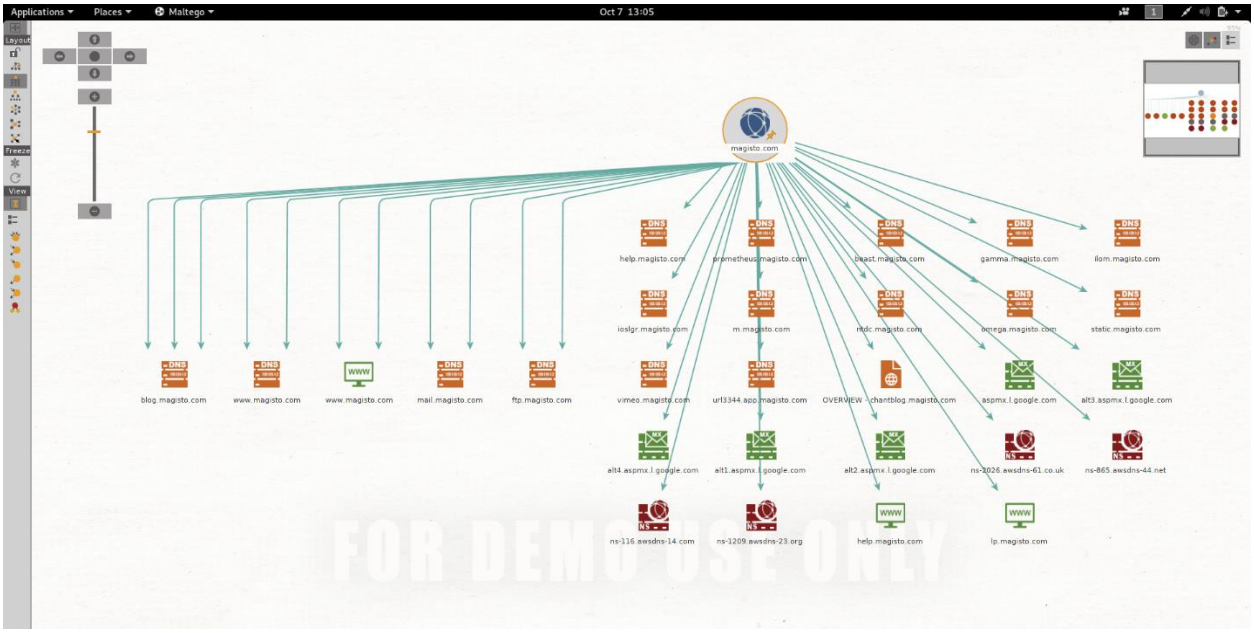
These are the files we found using DIRB and as you can see some of files are we can browse when we are working this site but some of them are not revealed to the normal user .as a example there is a file called crossdomain.xml and inside that we can see crossdomain policy is configured.as well as we can see the admin login page inside that we can see it is using some google authentication service to improve the security.



And we can see another thing they put separate pages for show to the client when occurs an error.for example they created separate page for page not found error (404).



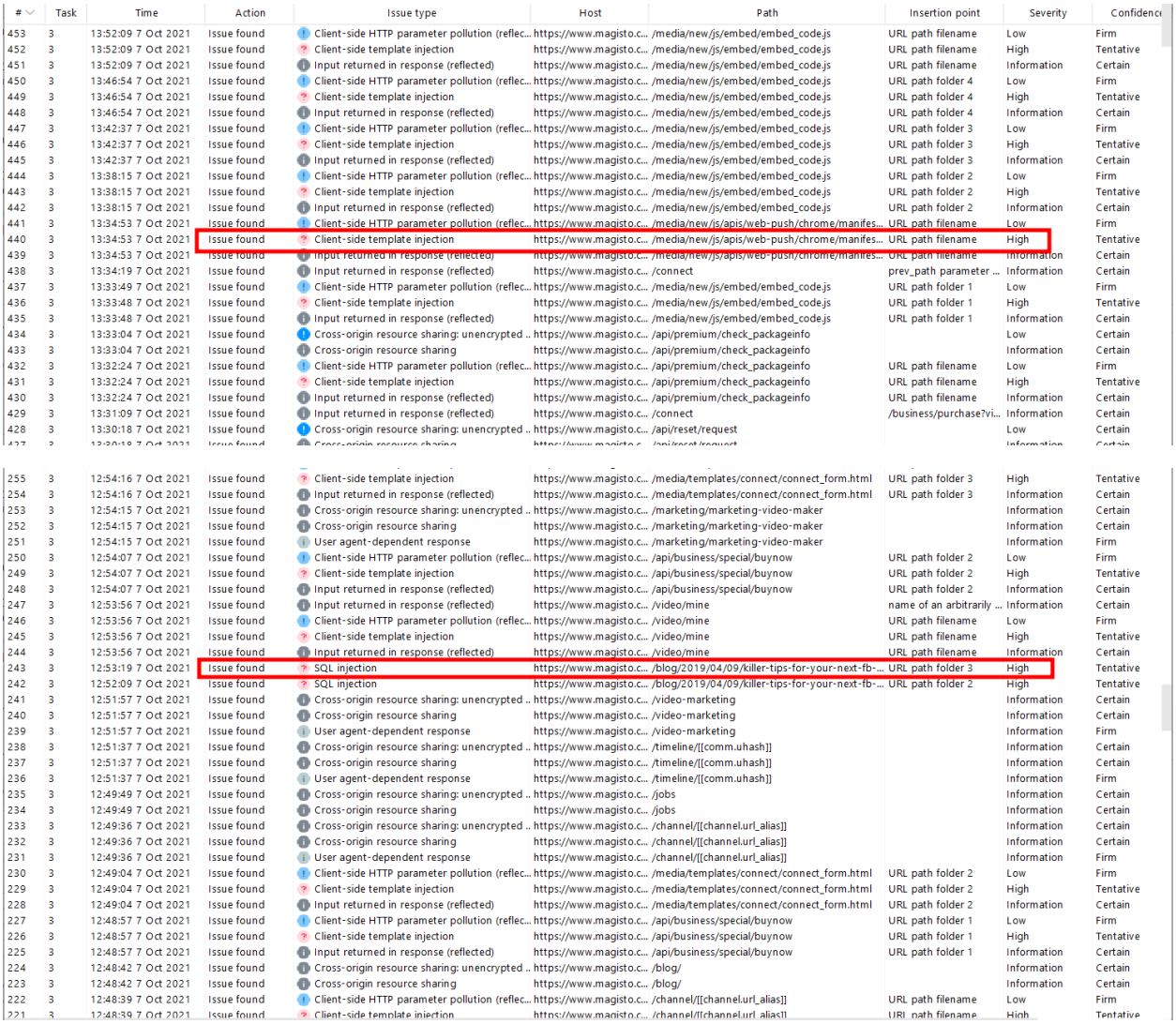
In addition the informations we found so far we can use maltego to see whether we can get more details if not we can see a graphical representation to get clear idea about the domain.



We are getting same results from the maltego but we can see a graphical view of the information we gathered so far.

Vulnerability Assessment

In this area we are mainly focus on vulnerabilities and trying to find security weaknesses in the target domain that can be way a attacker can hack into the system.to find that kind of vulnerability we can use vulnerability scanning tools .there are some tools we can get into use but here we are only using the burp suit vulnerability scnner. For that we need the professional version of burp suite and you have to pay for get that version.to do a scanning we need to click on new scan and give the URLs that you want to scan.lets see what we can get after scanning the domain.



#	Task	Time	Action	Issue type	Host	Path	Insertion point	Severity	Confidence
453	3	13:52:09 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path filename	Low	Firm
452	3	13:52:09 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path filename	High	Tentative
451	3	13:52:09 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path filename	Information	Certain
450	3	13:46:54 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 4	Low	Firm
449	3	13:46:54 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 4	High	Tentative
448	3	13:46:54 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 4	Information	Certain
447	3	13:42:37 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 3	Low	Firm
446	3	13:42:37 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 3	High	Tentative
445	3	13:42:37 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 3	Information	Certain
444	3	13:38:15 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 2	Low	Firm
443	3	13:38:15 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 2	High	Tentative
442	3	13:38:15 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 2	Information	Certain
441	3	13:34:53 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/media/new/js/apis/web-push/chrome/manifes...	URL path filename	Low	Firm
440	3	13:34:53 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/new/js/apis/web-push/chrome/manifes...	URL path filename	High	Tentative
439	3	13:34:53 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/new/js/apis/web-push/chrome/manifes...	URL path filename	Information	Certain
438	3	13:34:19 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/connect	prev_path parameter ...	Information	Certain
437	3	13:33:49 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 1	Low	Firm
436	3	13:33:48 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 1	High	Tentative
435	3	13:33:48 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/new/js/embed/embed_code.js	URL path folder 1	Information	Certain
434	3	13:33:04 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/api/premium/check_packageinfo		Low	Certain
433	3	13:33:04 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/api/premium/check_packageinfo		Information	Certain
432	3	13:32:24 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/api/premium/check_packageinfo	URL path filename	Low	Firm
431	3	13:32:24 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/api/premium/check_packageinfo	URL path filename	High	Tentative
430	3	13:32:24 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/api/premium/check_packageinfo	URL path filename	Information	Certain
429	3	13:31:09 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/connect	/business/purchase?vi...	Information	Certain
428	3	13:30:18 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/api/reset/request		Low	Certain
427	3	13:30:18 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/api/reset/request		Information	Certain
255	3	12:54:16 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/templates/connect/connect_form.html	URL path folder 3	High	Tentative
254	3	12:54:16 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/templates/connect/connect_form.html	URL path folder 3	Information	Certain
253	3	12:54:15 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/marketing/marketing-video-maker		Information	Certain
252	3	12:54:15 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/marketing/marketing-video-maker		Information	Certain
251	3	12:54:15 7 Oct 2021	Issue found	User agent-dependent response	https://www.magisto.c...	/marketing/marketing-video-maker		Information	Firm
250	3	12:54:07 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/api/business/special/buynow	URL path folder 2	Low	Firm
249	3	12:54:07 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/api/business/special/buynow	URL path folder 2	High	Tentative
248	3	12:54:07 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/api/business/special/buynow	URL path folder 2	Information	Certain
247	3	12:53:56 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/video/mine	name of an arbitrarily ...	Information	Certain
246	3	12:53:56 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/video/mine	URL path filename	Low	Firm
245	3	12:53:56 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/video/mine	URL path filename	High	Tentative
244	3	12:53:56 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/video/mine	URL path filename	Information	Certain
243	3	12:53:19 7 Oct 2021	Issue found	SQL injection	https://www.magisto.c...	/blog/2019/04/09/killer-tips-for-your-next-fb-...	URL path folder 3	High	Tentative
242	3	12:52:09 7 Oct 2021	Issue found	SQL injection	https://www.magisto.c...	/blog/2019/04/09/killer-tips-for-your-next-fb-...	URL path folder 2	High	Tentative
241	3	12:51:57 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/video-marketing		Information	Certain
240	3	12:51:57 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/video-marketing		Information	Certain
239	3	12:51:57 7 Oct 2021	Issue found	User agent-dependent response	https://www.magisto.c...	/video-marketing		Information	Firm
238	3	12:51:37 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/timeline/[[comm.uhash]]		Information	Certain
237	3	12:51:37 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/timeline/[[comm.uhash]]		Information	Certain
236	3	12:51:37 7 Oct 2021	Issue found	User agent-dependent response	https://www.magisto.c...	/timeline/[[comm.uhash]]		Information	Firm
235	3	12:49:49 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/jobs		Information	Certain
234	3	12:49:49 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/jobs		Information	Certain
233	3	12:49:36 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/channel/[[channel.url_alias]]		Information	Certain
232	3	12:49:36 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/channel/[[channel.url_alias]]		Information	Certain
231	3	12:49:36 7 Oct 2021	Issue found	User agent-dependent response	https://www.magisto.c...	/channel/[[channel.url_alias]]		Information	Firm
230	3	12:49:04 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/media/templates/connect/connect_form.html	URL path folder 2	Low	Firm
229	3	12:49:04 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/media/templates/connect/connect_form.html	URL path folder 2	High	Tentative
228	3	12:49:04 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/media/templates/connect/connect_form.html	URL path folder 2	Information	Certain
227	3	12:48:57 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/api/business/special/buynow	URL path folder 1	Low	Firm
226	3	12:48:57 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/api/business/special/buynow	URL path folder 1	High	Tentative
225	3	12:48:57 7 Oct 2021	Issue found	Input returned in response (reflected)	https://www.magisto.c...	/api/business/special/buynow	URL path folder 1	Information	Certain
224	3	12:48:42 7 Oct 2021	Issue found	Cross-origin resource sharing: unencrypted ...	https://www.magisto.c...	/blog/		Information	Certain
223	3	12:48:42 7 Oct 2021	Issue found	Cross-origin resource sharing	https://www.magisto.c...	/blog/		Information	Certain
222	3	12:48:39 7 Oct 2021	Issue found	Client-side HTTP parameter pollution (reflec...	https://www.magisto.c...	/channel/[[channel.url_alias]]	URL path filename	Low	Firm
221	3	12:48:39 7 Oct 2021	Issue found	Client-side template injection	https://www.magisto.c...	/channel/[[channel.url_alias]]	URL path filename	High	Tentative

We are getting two types of critical severity alerts by using burp suite and one of them is saying about client side template injection vulnerability and the second one is saying about SQL injection vulnerability.here onwards we are talking about SQLi vylnerability and how it is occurs and what are the solutions.

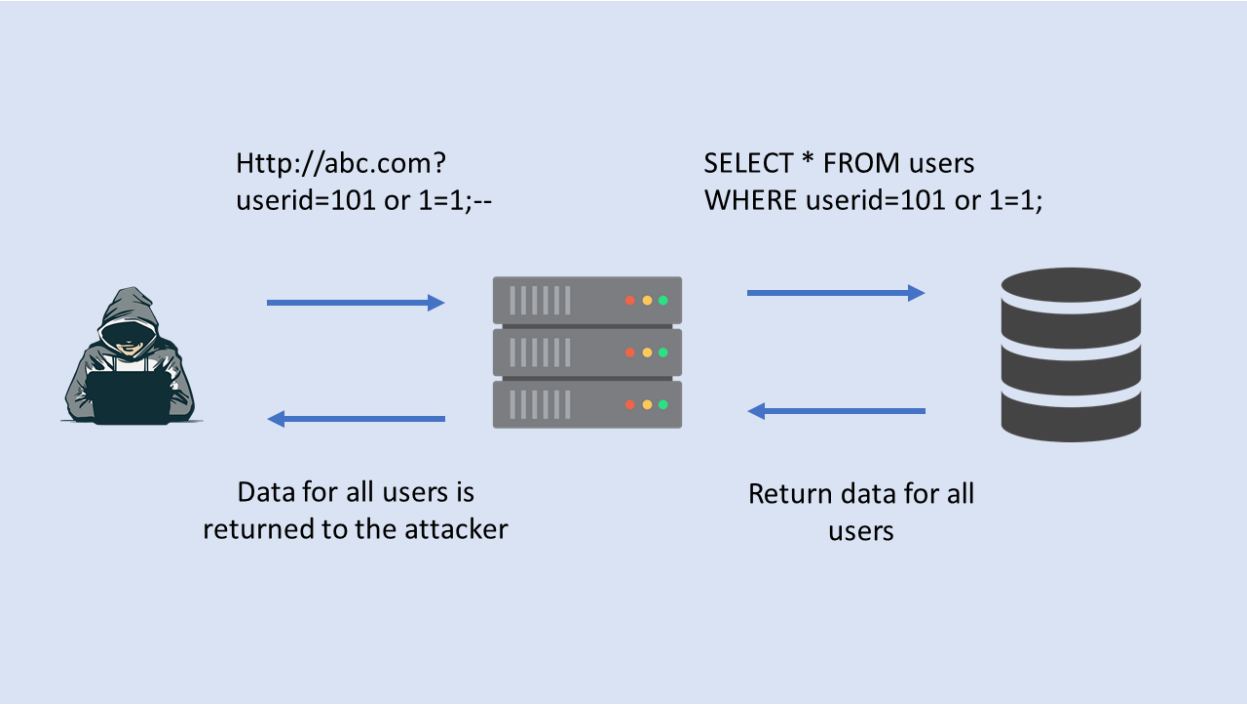
Vulnerabilities We Found

SQLi

Issue detail

The url path folder 3 is identified as vulnerable to SQLi attacks.it is tested by inserting a single quote to the url path folder 3 and then it returned a general error message.after that two single quotes were submitted and tested then it was not show the previous error message. to confirm whether there is a vulnerability we have to analyse the content of the erroer meassage and application's input handling .

Issue background



SQL injection or we can say SQLI is a type of injection attack but common attack vector than other injection attacks.it uses malicious sql quaries to manipulate the backend database and gain access to the information that was protected or not intended to be displayed.this disclosing information may include huge number of records including sensitive data that own a combany or a bank and if they stored their customers sensitive data those are also reavealed to the outside.

If someone able to do a successful SQLI attack the results may delete data records or entire tables ,viewing table data and sometimes the attacker gaining the administrative access rights like wise he can do a huge damage to the organization.

This type of attack vector can use against any database that uses SQL and most of the time websites are getting attacked.

Issue remediation

There are many ways to prevent form SQL injection attacks but the most effective way is use parameterized quaries (prepared statements)for all database accessing and manipulations.

In this method there are two steps to insert data that can potentially tained into the sql quaries.First the application needs to specifies the structure of a given query and it put placeholders for each item of the user input.Then the application scpecifies the internal contents of each placeholder.the reason is the structure of the sql query is already analyzed in the first step then in the second step the malicious data is not possible to interfere with the query structure.to determine the suitable APIs for use to perform parameterized queries we have to review the documentation for the database as well as the application platform.It is strongly recommended to parameterize all variable data elements that are included in database queries, even if they are not obviously contaminated, in order to avoid oversights and to avoid that vulnerabilities are introduced by changes in other parts of the application code base.

You should remember that some ordinarily used and suggested mitigations for SQL injection vulnerabilities don't seem to be invariably effective:

there is a common defense method and that is replace the single quotation marks by two quotations showing at intervals user input before incorporating that input into a SQL query. This defense is intended to stop distorted data from terminating the string into which it's inserted. However, If the information going into the queries is numeric, the defense could fail , as a result of numeric data might not be enclosed in quotation marks, during which case solely an area is needed to interrupt out of the data context and interfere with the query. Further, in second-order SQL injection attacks, data that has been safely free once ab initio inserted into the info is afterwards scan from the informationbase then passed back to that again. Quotation marks that are doubled up ab initio can come to their original kind once the data is reused, permitting the defense to be bypassed.
Another usually cited defense is to use hold on procedures for database access. whereas stored procedures can give security benefits, they're not absolute to forestall SQL injection attacks. identical sorts of vulnerabilities that arise at intervals commonplace dynamic SQL queries can arise if any SQL is dynamically created within stored procedures. Although the procedure is robust, SQL injection also occurs if the procedure is called in an unsafe manner to exploit user-controllable data.

Request

```
GET /blog/2019/04'/09/killer-tips-for-your-next-fb-ad-campaign-from-10-industry-experts/ HTTP/1.1
Host: www.magisto.com
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en-US,en-GB;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36
Connection: close
Cache-Control: max-age=0
Referer: https://www.magisto.com/marketing/facebook-video-ads-maker?via=business_top_menu&prev_path=%2f
Cookie: buz_promo_popup=1-1633591231; vtid=569331633591231414; mg_abt=254:1; mgsk=n1z475hoc3z3gla14qe5
```

Response

```
HTTP/1.1 406 Not Acceptable
Date: Thu, 07 Oct 2021 07:22:23 GMT
Content-Type: text/html
Content-Length: 581
Connection: close
Server: nginx/1.10.3

<html>
<head><title>406  Not Acceptable</title></head>
<body bgcolor="white">
<center><h1>406  Not Acceptable</h1></center>
<hr><center>nginx/1.10.3</center>
</body>
</html>
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
<!-- a padding to disable MSIE and Chrome friendly error page -->
```

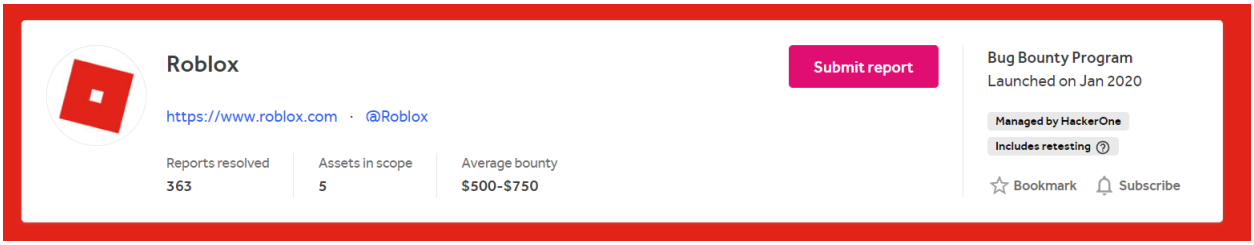
Conclusion

In this report we selected a domain from hackerone then we did some information gathering with several sections like subdomains ,file and directives and technologies like wise and when we were doing those things we analayse and we compared those information with earlier informations .then we moved to the vulnerability assessment step and we found two type of critical vulnerabilities and among them we select SQLI vulnerability for further discussion.then we learned what is SQLI and how it perform by an attacker then we discussed how the web application protect from this vulernability.

REPORT 05

INTRODUCTION

I chose a bug bounty program, and the company is Roblox corporations. It selected this one from HackerOne .roblox is a platform for online game creation, and this system was developed by Roblox cooperation. In addition to program games, it allows users to play games created by other users on this platform. It supports most kinds of platforms like Microsoft windows, android, ios, Xbox one, etc., and the headquarters is located in California, USA.



In the description, first, they said the program needs to enable two-factor authentication. We cannot find any other information about the company in the description. Next, they have given the rewards they are willing to give according to the severity level of the bug we will submit, and they also provide bonus rewards for well-developed reports. They do not clearly mention whether they are using the CVSS method to score vulnerabilities.

Low	Medium	High	Critical
$300	$1,000	$5,000	$10,000

Note: Reward amounts indicate the maximum amount payable for a qualifying report, not including bonuses (and Roblox will determine the final amount to be paid for a qualifying report).

Severity	Amount	Comment
Bonus for reports	Up to $200	Well documented reports that have clear and concise reproducible steps, with example exploit code.
Bonus for fix validation	Up to $500	Some bugs require complicated fixes. Help with validating those fixes can qualify you to earn you an extra reward.

Then they have given their policy details and some other areas .they also given the rules and regulations that the testers should follow in this bug-finding process. These rules are essential when we are analyzing the given domains, and they have given the rules covering a few areas that are given below.

Handling Data

- Your participation in the Roblox bug bounty program generally prohibits you from collecting, accessing, viewing, storing, altering or otherwise using data of Roblox users.
- While testing, take measures to avoid accessing user data or affecting other users' experiences. Please localize testing to your own test accounts wherever possible. If private user data is accessed during your security testing, please notify us immediately.
- If you have found an issue that may require touching other users' data to verify, please contact us first for guidance on how to safely test for such issues.
- In exceptional cases in which data of Roblox users is accessed and used for the security testing please restrict the data use to the extent that is crucially necessary to conduct proper security testing. This particularly means that you only use user data of very few Roblox users and that you limit the amount of the specific user data to the scope that is necessary for the specific testing measure.
- In case of accessing user data for testing purposes, please ensure to take measures to prevent unauthorized access, alteration or deletion of the user data. You may not use the user data for any purposes other than participating in the Roblox bug bounty program and conducting the security testing.
- You may not use the user data accessed during the security testing to contact Roblox users for any reason; including informing them about the security testing.
- After completing the testing, you must delete any user data from your systems irrevocably. We reserve the right to demand proof of proper deletion.
- You must refrain from sharing user data with others or publish user data.
- A violation of these data protection obligations may lead to exclusion from the bug bounty program. In the event of infringement, Roblox reserves the right to reclaim already awarded bounties. Infringing data protection laws, including the European General Data Protection Regulation (GDPR), can result in substantial fines and/or users may be entitled to damages.

Testing

- If you are aware that your attacks may harm the reliability or integrity of our services or data, stop immediately and contact us
- Vulnerabilities found through DDoS/spam attacks are not allowed
- Never attempt non-technical attacks such as social engineering (e.g. phishing, vishing, smishing) or physical attacks against our employees, users, or infrastructure
- Recently disclosed 0-day vulnerabilities are not eligible, unless you have a working poc exploit.
- Follow HackerOne's disclosure guidelines
- When testing, please include the string "hackeronetest-`<your-roblox-userid>`" at the end of your user agent so we can more easily identify traffic that is coming from the bug bounty program.
- For any report involving the Roblox Client or Roblox Studio, include the version
- In Studio, click File > About Roblox Studio
- For client, the version is shown in the properties of the exe file, normally located at %APPDATA%..\Local\Roblox\Versions`<version>`\RobloxPlayerBeta.exe. There are typically two folders, one for client, one for studio.
- Report the approximate date/time/timezone of the most recent test of the issue
- Please do NOT contact our customer support team or employees out of band to contest or escalate a report; all inquiries should happen on the report itself. Failure to follow this rule may result in a bounty not being paid out and repeat offenses can lead to removal from the bug bounty program

Next, they say about disclosure policy, and after that, they have given the out-of-scope vulnerabilities in the description. There are no signs of eligible vulnerabilities in the description, which means that, except for these vulnerabilities, other types of vulnerabilities are eligible .they are specialyy saying that when we report a bug, we have to show how easily or realistically exploitable the bug and the security impact of the bug.

The following vulnerabilities typically will not qualify for Roblox's program:

- Vulnerabilities previously disclosed through the program or otherwise known to Roblox or to the public
- User account hacks that require user interaction
- Chat filter bugs
- Missing autocomplete attributes
- Missing flags on cookies that don't house any sensitive information
- SSL/TLS scan reports (this means output from sites such as SSL Labs) and SSL/TLS version related vulnerabilities
- Missing security-related HTTP headers which do not lead directly to a vulnerability. Issues that only affect a smaller user base (e.g. users on outdated browsers or other outdated software).
- Vulnerabilities that are used for volumetric DDoS/DoS/Spam attacks are out of scope. But the vulnerabilities in the Roblox data model, which can be used by exploiters specifically for crashing the game servers, is strongly encouraged to be reported.
- Cross-site Request Forgery (CSRF) with minimal security implications (Login/logout/unauthenticated)
- Version information disclosure (without verifying the presence of an actual exploitable vulnerability)
- Password complexity related vulnerabilities
- Unverified or incomplete "Scanner output" or scanner-generated reports
- Vulnerabilities requiring physical access to the victim's unlocked device
- Bugs requiring exceedingly unlikely user interaction
- Disclosure of information already in public domain or information previously disclosed by Roblox
- Disclosure of public information and information that does not present significant risk
- Vulnerabilities that Roblox determines to be an accepted risk will not be eligible for a paid bounty
- Language used in emails and policy documents
- SPF, DKIM or DMARC issues on sub-domains of roblox.com
- HTML injection vulnerabilities with no direct risk
- Social engineering or following a link will not be considered for bounty
- Self XSS or similar vulnerabilities
- Vulnerabilities found on *.ra.roblox.com that do not affect release servers

As I mentioned, they only give the out-of-scope vulenrabilities. Then they have given the in-scope domains under the scope section at the bottom of the description. Now, we have to select one or a few domains to further analyze from these given sets of domains.

In Scope

Domain	***.roblox.com** App api's that are used within Roblox.	Critical	Eligible
Domain	***.rbx.com**	Critical	Eligible
Domain	***.ra.roblox.com**	Low	Eligible
Executable	**Roblox Client** Applies to Windows/Osx/Mobile Platform	Critical	Eligible
Executable	**Roblox Studio** Applies to Windows/Osx/Mobile Platform	Critical	Eligible

SETTING THE SCOPE

- Roblox.com

We can see there are few domains under the in scope, but we have to select one to analyze in this report .so I selected Roblox.com, and we are going to do some information gatherings, set of analysis, and vulnerability assessments for this selected domain from this point onwards.

INFORMATION GATHERING

Since in the beginning, we read all the things they are given as instruction, and now we have selected one domain that is roblox.com.in this step, we are going to gather information about this domain under a few sections like technology, subdomains, and files, and directories using a set of tools and learn about the domain. While doing these things, sometimes we have to do some analysis as well.

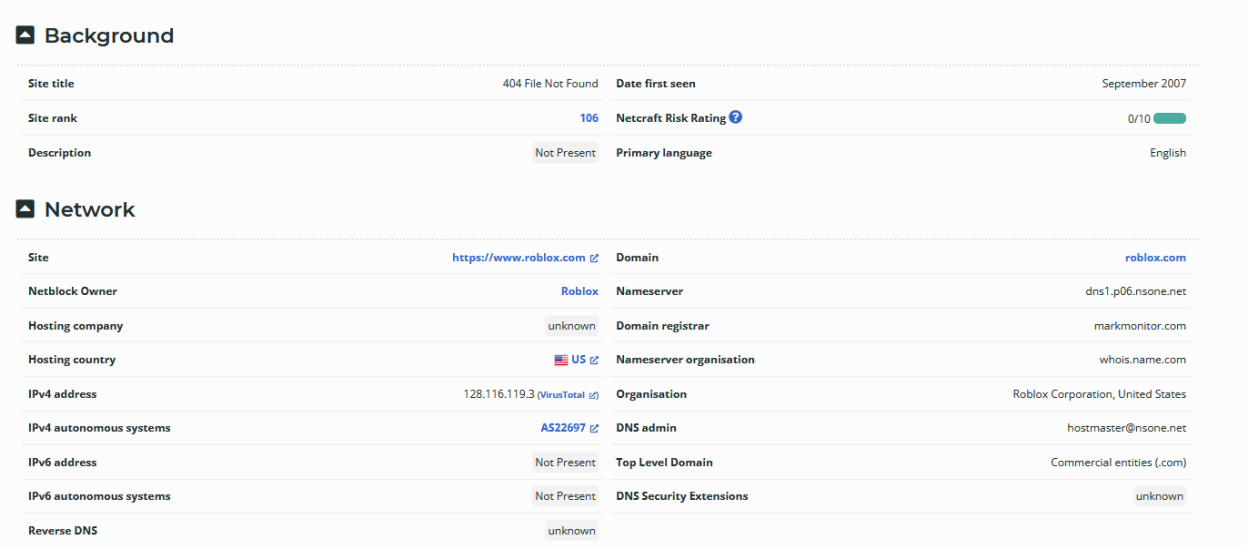
Registrant Org	Roblox Corporation
Registrant Country	us
Registrar	MarkMonitor, Inc. MarkMonitor Inc. IANA ID: 292 URL: http://www.markmonitor.com Whois Server: whois.markmonitor.com abusecomplaints@markmonitor.com (p) 12083895770
Registrar Status	clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited, serverDeleteProhibited, serverTransferProhibited, serverUpdateProhibited
Dates	6,463 days old Created on 2004-01-29 Expires on 2023-01-29 Updated on 2020-12-29
Name Servers	DNS1.P06.NSONE.NET (has 2,519,604 domains) DNS2.P06.NSONE.NET (has 2,519,604 domains) DNS3.P06.NSONE.NET (has 2,519,604 domains) DNS4.P06.NSONE.NET (has 2,519,604 domains) NS01.RBXINFRA.NET (has 0 domains) NS02.RBXINFRA.NET (has 0 domains) NS03.RBXINFRA.NET (has 0 domains) NS04.RBXINFRA.NET (has 0 domains)
Tech Contact	–
IP Address	128.116.100.3 - 4 other sites hosted on this server
IP Location	- California - San Mateo - Roblox
ASN	AS22697 ROBLOX-PRODUCTION, US (registered Dec 03, 2014)
Domain Status	Registered And Active Website
IP History	149 changes on 149 unique IP addresses over 17 years
Registrar History	4 registrars with 2 drops
Hosting History	9 changes on 8 unique name servers over 17 years

This is the result we were getting by using the whoislookup site, and we can see a lot of information there. The registrant organization of the roblox.com domain is Roblox corporation. We can see it is located in California .then it shows their contact details and the website created date and the expieration date as well as the date that happens the last update. After that, we can see the name servers of

this domain, and there are two nameservers in the result. The IP address is 128.116.100.3, and it says four other sites were hosted on that server. They also gave IP address location, domain status, response code, etc.

TECHNOLOGIES

To gather some information about the technologies this domain uses, we use several tools and collect more details about the technologies. We already have some information now we are going to find further information about our target domain. First, we are going to use the Netcraft site for doing some information gathering.



Background

Site title	404 File Not Found	Date first seen	September 2007
Site rank	106	Netcraft Risk Rating	0/10
Description	Not Present	Primary language	English

Network

Site	https://www.roblox.com	Domain	roblox.com
Netblock Owner	Roblox	Nameserver	dns1.p06.nsone.net
Hosting company	unknown	Domain registrar	markmonitor.com
Hosting country	US	Nameserver organisation	whois.name.com
IPv4 address	128.116.119.3 (VirusTotal)	Organisation	Roblox Corporation, United States
IPv4 autonomous systems	AS22697	DNS admin	hostmaster@nsone.net
IPv6 address	Not Present	Top Level Domain	Commercial entities (.com)
IPv6 autonomous systems	Not Present	DNS Security Extensions	unknown
Reverse DNS	unknown		

In the background section, we cannot find any important things, but in the networks section, we can see the site URL and its domains as roblox.com.then; it shows the netblock owner is Roblox and the hosting country is the USA these things we found earlier as well. But if we look at the ipv4 address this time, we are getting different IP addresses. But at an earlier point, we saw a message saying there are

four other sites on the same server. This can be the reason those problems we can clarify in the onward analysis.

IP delegation

IPv4 address (128.116.119.3)

IP range	Country	Name	Description
0.0.0.0–255.255.255.255	N/A	IANA-BLK	The whole IPv4 address space
↳ 128.0.0.0–128.255.255.255	United States	NET128	Various Registries (Maintained by ARIN)
↳ 128.116.0.0–128.116.127.255	United States	RC-376	Roblox
↳ 128.116.119.3	United States	RC-376	Roblox

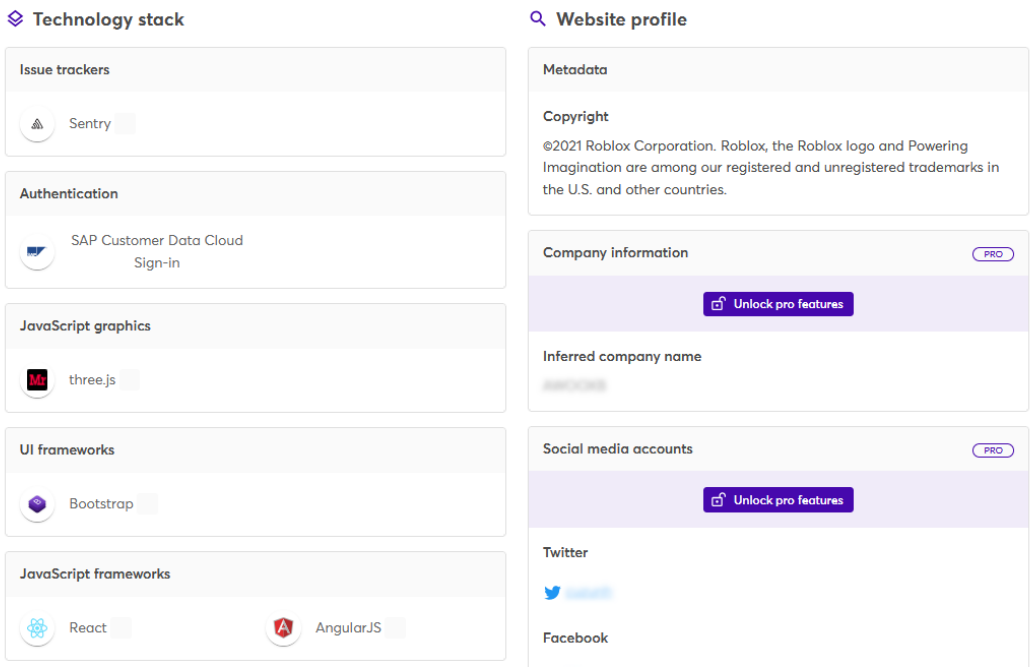
If we check the IP delegation section, it clearly shows us that other IP addresses are available in this given IP address range. First, we got 128.116.100.3 as the ipv4 address, and then we got 128.116.119.3.there is an IP range from 128.116.0.0 to 128.116.127.255 means both IP addresses we got should be in this range, and maybe they are separate servers.

SSL/TLS

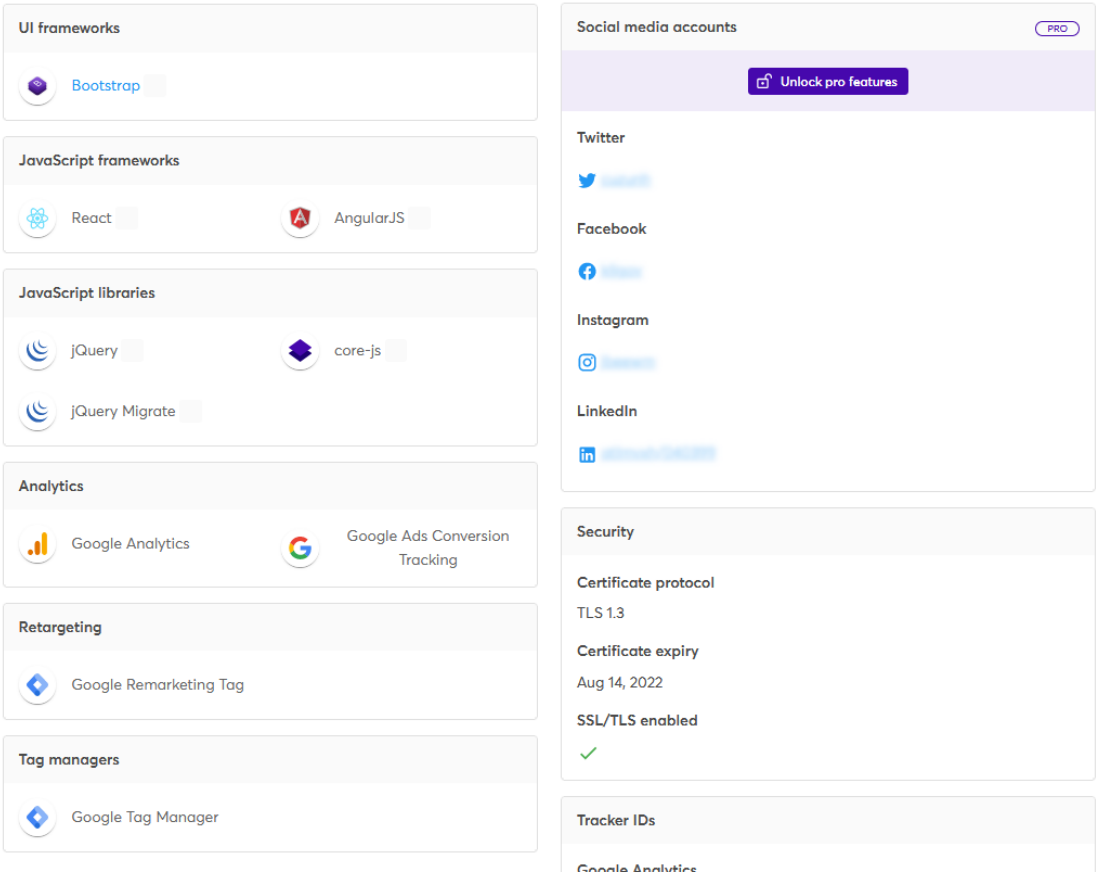
Assurance	Domain validation	**Perfect Forward Secrecy**	Yes
Common name	*.roblox.com	**Supported TLS Extensions**	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC7301 application-layer protocol negotiation
Organisation	Not Present	**Application-Layer Protocol Negotiation**	h2
State	Not Present	**Next Protocol Negotiation**	Not Present
Country	Not Present	**Issuing organisation**	GoDaddy.com, Inc.
Organisational unit	Not Present	**Issuer common name**	Go Daddy Secure Certificate Authority - G2
Subject Alternative Name	*.roblox.com, roblox.com	**Issuer unit**	http://certs.godaddy.com/repository/
Validity period	From Aug 13 2021 to Aug 13 2022 (12 months)	**Issuer location**	Scottsdale
Matches hostname	Yes	**Issuer country**	US
Server	Not Present	**Issuer state**	Arizona
Public key algorithm	rsaEncryption	**Certificate Revocation Lists**	http://crl.godaddy.com/gdig2s1-3208.crl
Protocol version	TLSv1.3	**Certificate Hash**	mtUiWlpL6P/BjZBvBYsHkKE/zBo
Public key length	2048	**Public Key Hash**	b47949b35f7241a41cc593b2d0b054aa04029425a5bcaec046dc51d39de20e74
Certificate check	ok	**OCSP servers**	http://ocsp.godaddy.com - *100% uptime in the past 24 hours*
Signature algorithm	sha256WithRSAEncryption	**OCSP stapling response**	No response received

Under the SSL/TLS section, we can see a lot of information related to the security of the domain. We can see the certificate details like certificate issuer and its

details, and then it gives its data encryption mechanisms and components. We cannot see the web tracker section in the result.



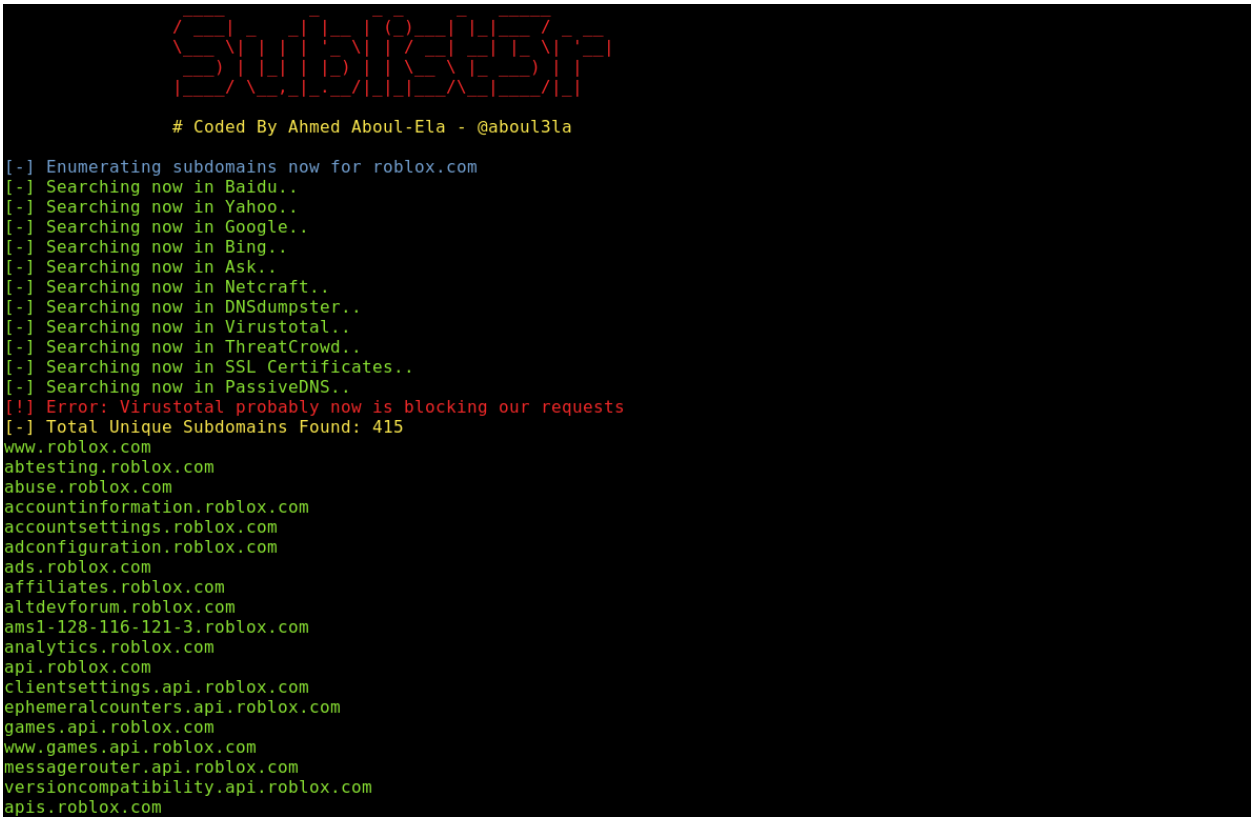
After that, we are using the wappalyzer to gather some information. First, we get metadata about the domain, and it says about the copyright they have. Then it says the domain uses sentry for issue tracking .sentry is a platform that we can use for workflow productivity, and it is open source. It uses SAP customer data cloud sign-in authentication for their domain, which means the users can save their progress in cloud storage. They use this authentication service to authenticate themselves for the security of their data. Then they are using javascript for graphics-related things, and they also use bootstrap as a UI framework, and there are using some other frameworks as well.



As you can see, they blur some information and say to get their paid version to see those if you want you can get this services by paying some money, then you can see some company information and social media account details. They are using some javascript libraries like jquery,core-js. They use some services from google for analytics. There are other services provided by google .then we can see they use TLS 1.3 as the certificate protocol and its alsoshowing the certificate expiery date.

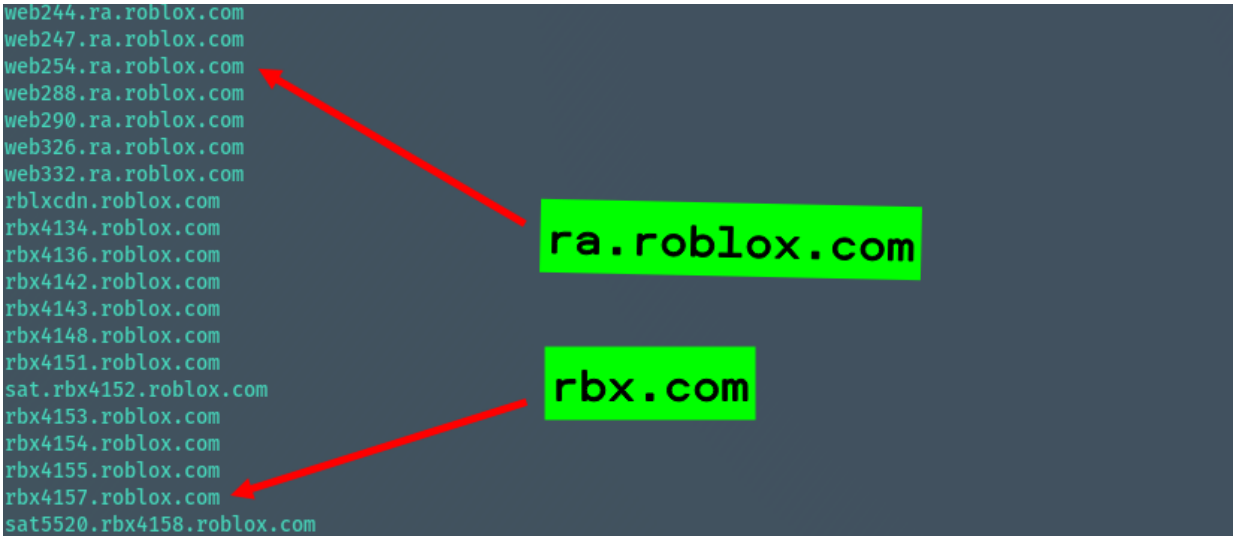
GATHER SUBDOMAIN INFORMATION

So far, we have found information about the network, technology, security, and some other areas of our target domain. Like those things we found, the subdomain information is also important when we are searching for a bug .now we are going to see how we can find subdomain information and analyze them according to the information we are getting .so that we need several tools for subdomain enumeration .first we are going to use a tool call sublist3r.



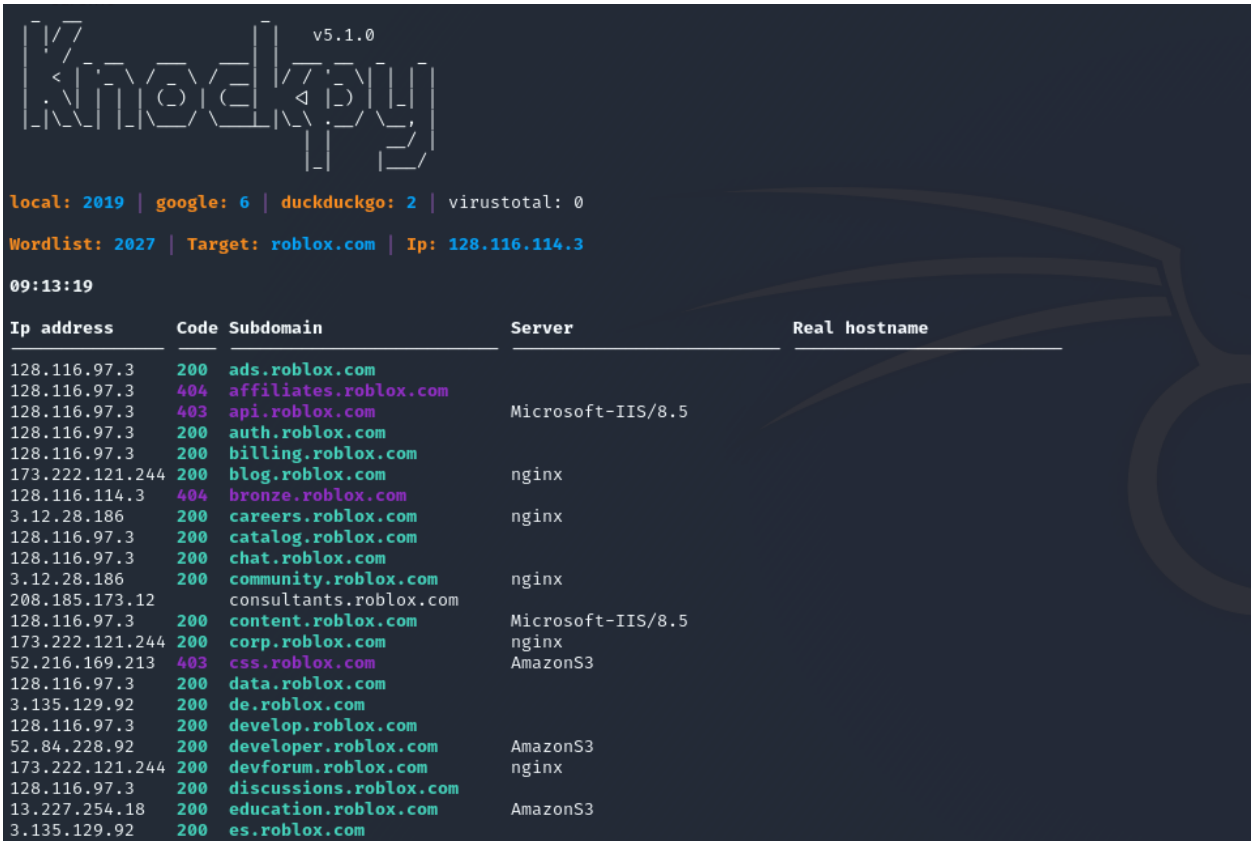
From the first scanning, we get 415 subdomains by using the sublsit3r tool. To use this tool, you only have to do is type sublist3r and give -d and the domain that you want to get subdomains. Suppose you want to see more type sublist3r -h to get

help. We are getting a massive number of subdomains, so that we have to check whether this result is valid. We can find the domains in the in-scope section in this result.



We can see there are in scope domains in the result we are getting by this tool, which means there are a large number of out-of-scope subdomains .that means we can trust these results by using these tools. But there is a disadvantage of this tool: we are only getting the subdomains, and we can't get any information about ip addresses and the servers, etc.

So that's why we are going to use another tool called knockpy. knockpy Is written in python, so if you want to use this tool, you have to install python into your machine, and then you can install knockpy and use it by giving the command knockpy <domain> in the terminal. If you want to get help, type knockpy -h end press enter.

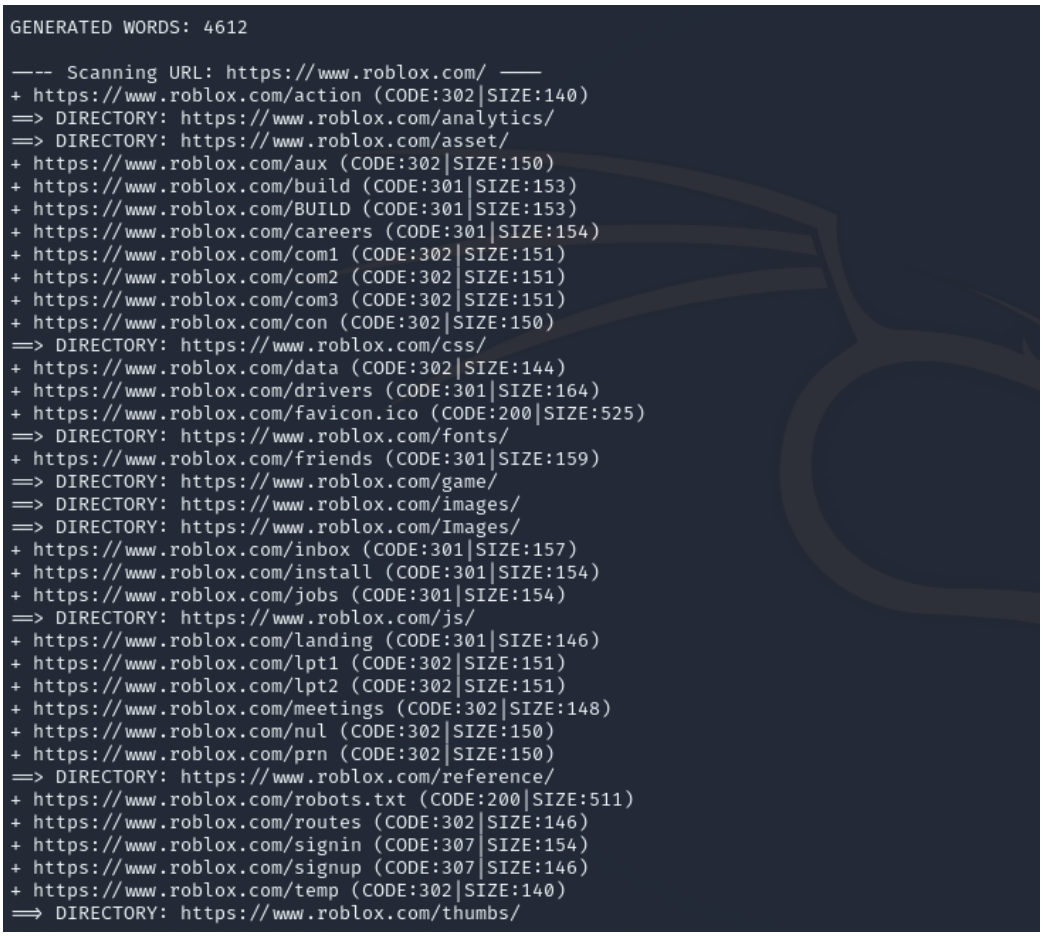


As you can see, this is the output of the knockpy tool given to us by subdomain enumerating. We are getting 59 domains, but this time we have the corresponding IP addresses and the servers. As a result, we can see a lot of IP addresses on different servers. This means these subdomains are located in separate servers, and this time, we are getting the ip address of roblox.com as 128.116.114.3, which means multiple servers should be there for the same domain.

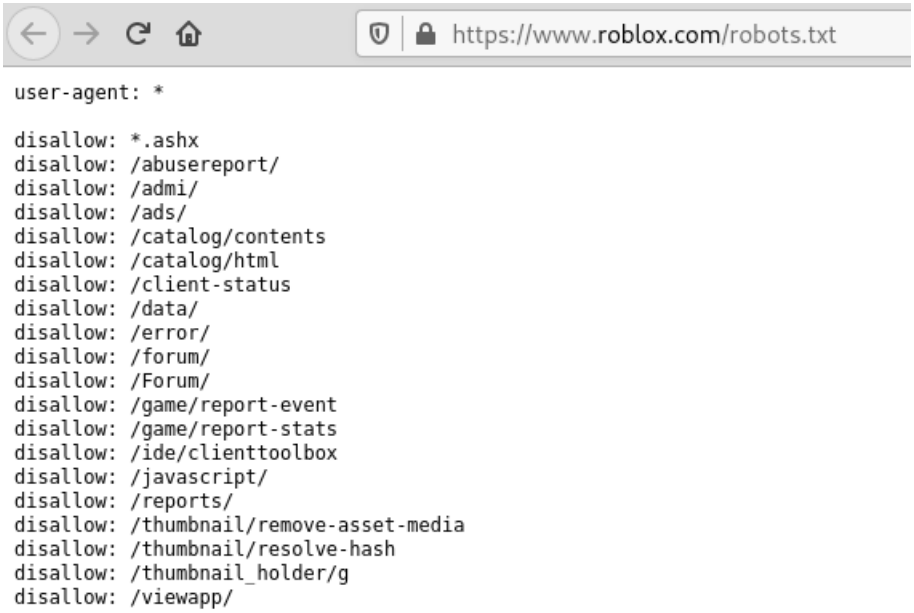
GATHERING INFORMATION ABOUT FILES AND DIRECTORIES

Now we have a lot of information about the domain. Now we are moving to gather information about files and directories stored in the web application. Then we can go into them and look for some clues or reveal some important things. We call this process web content scanning, and to do this, and we need some tools. Also, we can do it manually, but it takes a lot of time and effort, so we are using some tools. The tool we are going to use is DIRB, and let's see how we can use this tool.

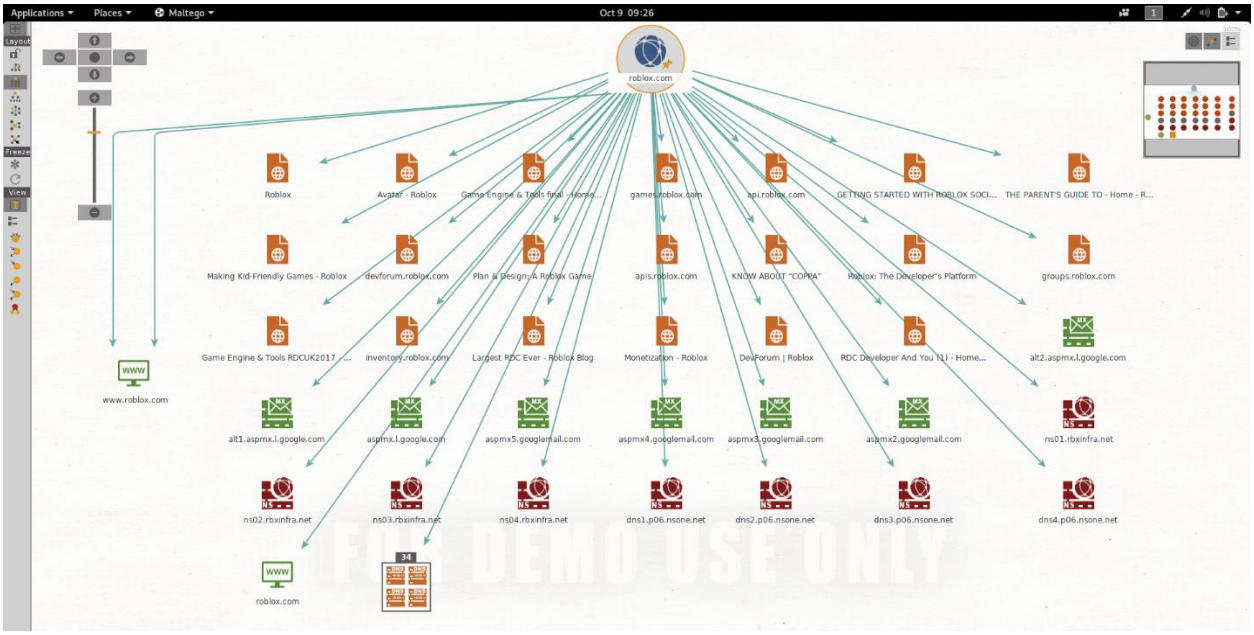
First, you need to install this tool on your machine, and in the terminal, you can run this tool by giving commands. You have to provide the word dirb, then the target url, and press enter. Then it will generate a word list and trying to brute force and get the files according to the word list.



As we can see, DIRB generates a word list. According to that, it captured all the files and directories .it is going directory by directry and capture all the files inside that directory.lot of files have 302 status code so we cannot get anything from those files.most of the files related to the pages of the web application. We can see the robots.txt in this file list .other than that, and It is diffuctult to find anything because we have no access to privilegaes to see the content of those pages.

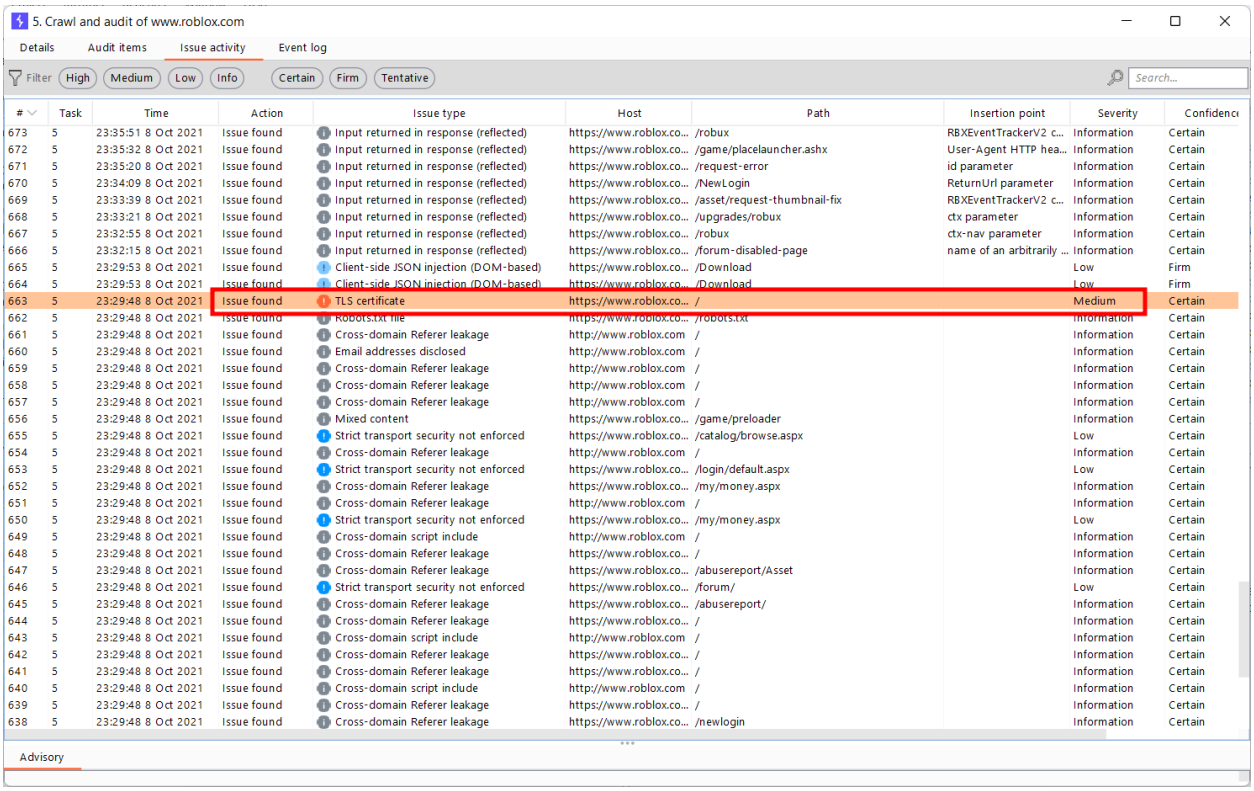


In addition, we can use maltego to gather more informations and see a graphical view of the information we collected so far and it will give a clear idea about the domain.



Vulnerability assessment

In this section, our primary purpose is to find a vulnerability that will allow an attacker to get into the web application. We need to find that kind of security weaknesses by analyzing the web application. After that, we can analyse what is the problem and what are solutions we can implement for preventing form that vulnerability. for that, we can use several tools like owasp zap ,zenmap etc.but here we are using burp suite to check the web application for vulnerabilities.but you cannot use the free version for vulenrabiltiy scanning. Hence, you have to purchase the professional version for that .then you can click on the new scan and give the URL that you want to do the scanning. Let's see what we can find by scanning the domain.



At this time, we are only getting one medium severity level vulnerability others are low-level severity alerts. It is saying that a vulnerability about there is a problem with the TLS certificate .so from this point onwards, we are going to talk about this vulnerability.

Vulnerabilities we found

TLS certificate has some issues.

Issue detail

It says that there is a problem with the server's TLS certificate, and it says that the certificate is not a trusted certificate.

The server presented the following certificates:

Server certificate

Issued to: *.roblox.com, roblox.com

Issued by: Go Daddy Secure Certificate Authority - G2

Valid from: Sat Aug 14 04:23:34 IST 2021

Valid to: Sun Aug 14 04:23:34 IST 2022

Certificate chain 1

Issued to: Go Daddy Root Certificate Authority - G2

Issued by: Go Daddy Root Certificate Authority - G2

Valid from: Tue Sep 01 05:30:00 IST 2009

Valid to: Fri Jan 01 05:29:59 IST 2038

Certificate chain 2

Issued to: Go Daddy Secure Certificate Authority - G2

Issued by: Go Daddy Root Certificate Authority - G2

Valid from: Tue May 03 12:30:00 IST 2011

Valid to: Sat May 03 12:30:00 IST 2031

Certificate chain 3

Issued to: Go Daddy Root Certificate Authority - G2

Issued by: Go Daddy Root Certificate Authority - G2

Valid from: Tue Sep 01 05:30:00 IST 2009

Valid to: Fri Jan 01 05:29:59 IST 2038

Issue background

TLS (or SSL) helps safeguard the confidentiality and integrity of knowledge in transit between the browser and server and supply authentication of the server's identity. To accomplish this purpose, the server must present a Nursing Associate TLS certificate that is valid for the server's hostname, issued by a trusted authority, And is legitimate for the current date. The server does not provide the complete protection that TLS was designed to provide. It has to be cited that numerous assaults exist towards TLS in general and inside the context of HTTPS net connections in particular. It may be attainable for a determined and suitably positioned assailant to compromise TLS connections without user detection even once a sound TLS certificate is used.

NOTE: Burp is based on Java truststore to determine whether the certificates can be trusted. The Java trust store does not contain all of the root CA certificates that are included in the browser trust stores. Burp may incorrectly report that a certificate is not trustworthy when using a valid Root CA certificate that is not in the Java truststore.

CONCLUSION

In this report, we selected a bug bounty program from HackerOne. At First, we talked about the bug bounty program and the given details, such as rules and policies. We chose one domain from that given list of in-scope domains, and we began to gather information about it. We did the information gathering under several sectors like technology, subdomains, and files and directories. Then we moved to the vulnerability assessment phase, and we found there is one medium severity alert we can get. Other than that, all other alerts are low severity, so that's why we selected that medium severity one. According to that, we talked about what vulnerability is what is the background of that vulnerability.

Experience

Before beginning to write this book, I first created a structure for this book. For, I have to read many books and research papers, and articles in a few weeks. While I was doing that, I did some practices using hack the box, OWASP juice shop, and I collected more hands-on experiences. Then I watch tutorials, guidance, and discussions related to cybersecurity and bug bounty hunting. These things I did for two or three weeks, then I started to write my reports. As a beginner, I needed motivation and guidance for doing these things so that I team up with my friends and we practice this stuff and share our knowledge . I think it is so helpful to cybersecurity leaner or bug bounty hunters. When I was writing my reports, sometimes I had to stop writing for a while and learn new things in situations like when I got a new vulnerability I had never heard before likewise.

In some points, I have to use several tools and methods to confirm whether my analysis is accurate. When I first used some tools, I installed them on my testing environment and tested those tools my own. In some points, I mentioned how these tools can be used and the advantages and disadvantages of those tools. When I am writing, I have to learn new things and after that I wrote those things.with my experiences, I suggest three ways to learn and start bug bounty hunting. First, you need to put a lot of time and effort into this if you want to be a bug bounty hunter. Then create a team with your colleagues and practice those things you have learned and make this enjoyable. The third thing is you have to keep learning throughout this journey.