Bug Bounty Reports

Written by: H.R.T Peiris
IT21163340

Sri Lanka Institute of Information Technology

BUG BOUNTY REPORTS

IE2062 - Web Security

Peiris H.R.T
IT21163340
Y2 S2 CS Weekend Group

Table of Contents

01.Acknowledgement

Well-known businesses all over the world launch bug bounty programs, and they require the assistance of white hat hackers to find defects in their online applications and who are capable of discovering a problem that that business will fix.
Reward the individual. Because of this, the number of bug reward programs is growing daily, and ethical hackers now have a lot of opportunities.
Simply defined, bug bounty seeking is covered in this text. Then, we'll talk about the tools we can use for bug bounties, and I'll present ten reports that cover topics like how I got started with bug bounties and how I studied web apps as a student.

02.Objective

The primary objective of this task is to determine whether or not a well-known website has any security flaws. These security holes might potentially lead to breaches in the website's protection. Students who are majoring in cyber security at the undergraduate level may extend their academic understanding in the practical aspects of cyber security by completing this assignment. It was suggested that we use both automatic testing as well as human testing for this website review. The automated method of checking for vulnerabilities was carried out with the assistance of testing. Dotdotpwn, uniscan, nkto, sublist3r,knockpy, wafw00f, nessus, Owas zap, Netsparker.

03.Introduction

There is an increasing amount of anxiety over the most effective strategy to prevent cybercrime, which is an issue that has to be dealt with by every business. Every day, cybercrime wreaks havoc on the data systems of the company, causing considerable financial loss as well as harm to the company's brand. Pride has no place in this setting.

Any moment might be the right time for a cyberattack on the data system of your organization. You most definitely do not want the information of your company to be compromised, since more than 43 percent of digital assaults target small enterprises. 64% of companies have reported experiencing web-based assaults. 62 percent of respondents reported being victims of attacks that used phishing and social engineering. Invasive codes and botnets were discovered in 59 percent of businesses, while 51 percent of businesses were attacked by unauthorized administration attempts. It is very necessary to have a robust data framework security in place in order to safeguard an organization's information system from being breached, misrepresented, or otherwise compromised by cybercrime. Each institution is accountable for ensuring that the information it maintains is trustworthy, protected from unauthorized access, and kept in strict confidence. The security of an association may be affected by a number of factors, including the client practices, the product, and the data taking care of cycles. In any case, how can a company assess what aspects of its operations need protection and the methods that should be used to provide that protection?
Where should we get started with the organization? Web security auditing is the point at which everything gets started. Misrepresentation and data penetration should be done on a regular basis, as an orderly assessment by a free master on adherence, to find a shortcoming in the organization's IT framework, even though some writing claims that web security auditing is a critical step in securing an organization's data framework against cybercrime. This is because some writing claims that web security auditing is a critical step in securing an organization's data framework against cybercrime.

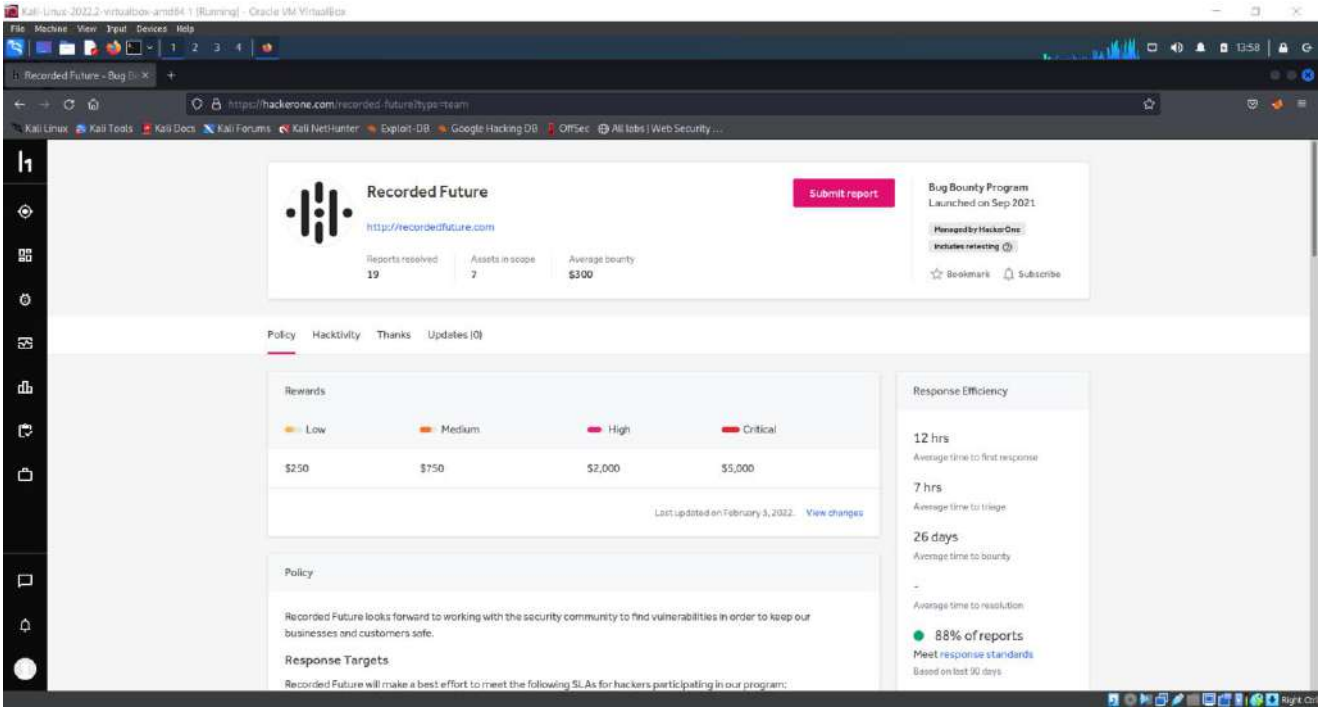
Is it true that an audit of an organization's information technology security may help enhance data security and reduce the likelihood of possible network security risks? This report on the examination will explain how and why an effective Web security audit is undertaken, in addition to addressing the question of whether or not the approach contributes to an increase in IT security. In order to accomplish this objective, I will investigate the manner in which numerous Linux frameworks are now inspected on the website www.semrush.com, which serves as the target market. After this phase, in line with the business norms and standards, an IT web audit program is executed for those frameworks, and an audit report is provided that contains the results and the subsequent measures that should be made to minimize any data security concerns. In point of fact, auditing information technology requires major resources like time and money. In any case, the costs associated with a data breach, deceit, or cybercrime are quite likely to be rather significant. Because of this, avoiding it is a wise decision. This investigation's primary objective is to investigate the advantages of IT security auditing as a valuable tool for increasing an organization's data security, as well as to analyze the relevance of online security auditing as a means of introducing the relevance of online security auditing. The inquiry also looks at how effectively the company uses global security standards and laws, how well they pay attention to cybercrime concerns, and how they execute periodic IT security audits. An example website known as Semrush is deployed here as a means of testing and verifying an online security assessment.

04.Bug Bounty Reports

i. Report 01

Target information: http://recordedfuture.com

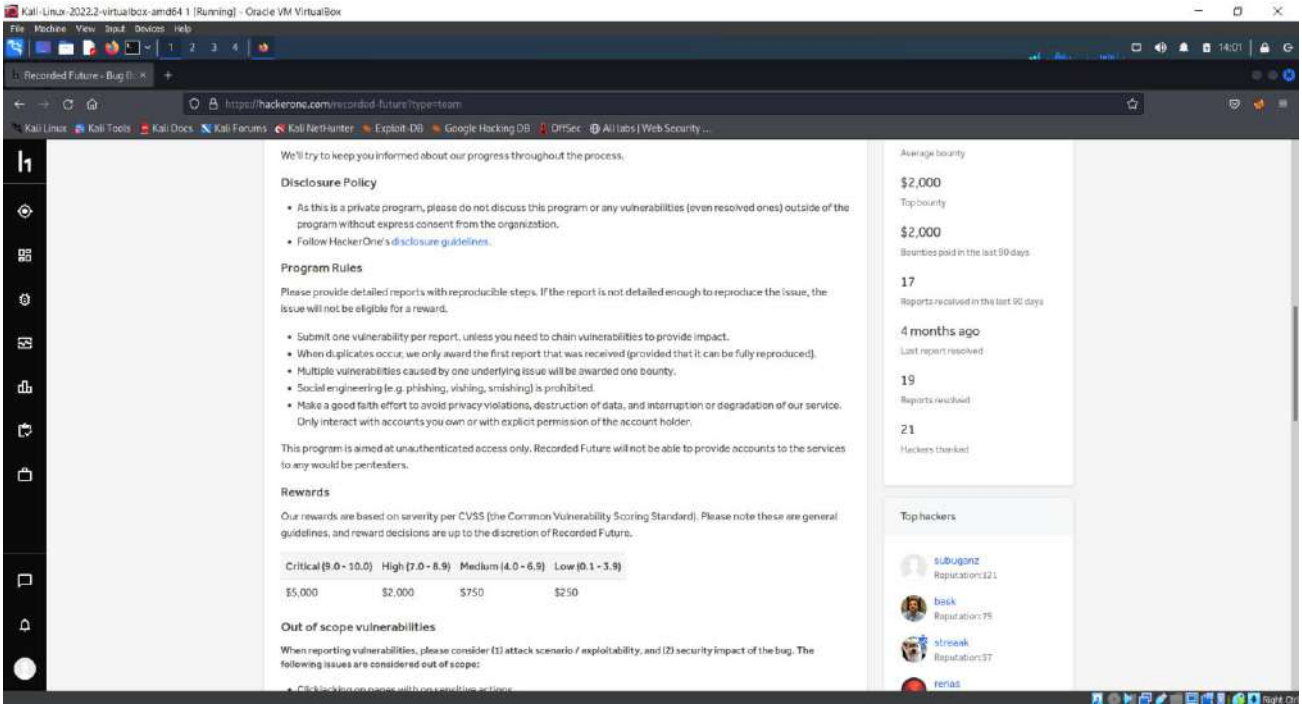
Finding vulnerabilities in the target domain (http://recordedfuture.com) and determining the risk level associated with such vulnerabilities is the purpose of this assessment. The aim of the assessment is to uncover vulnerabilities in the target domain.



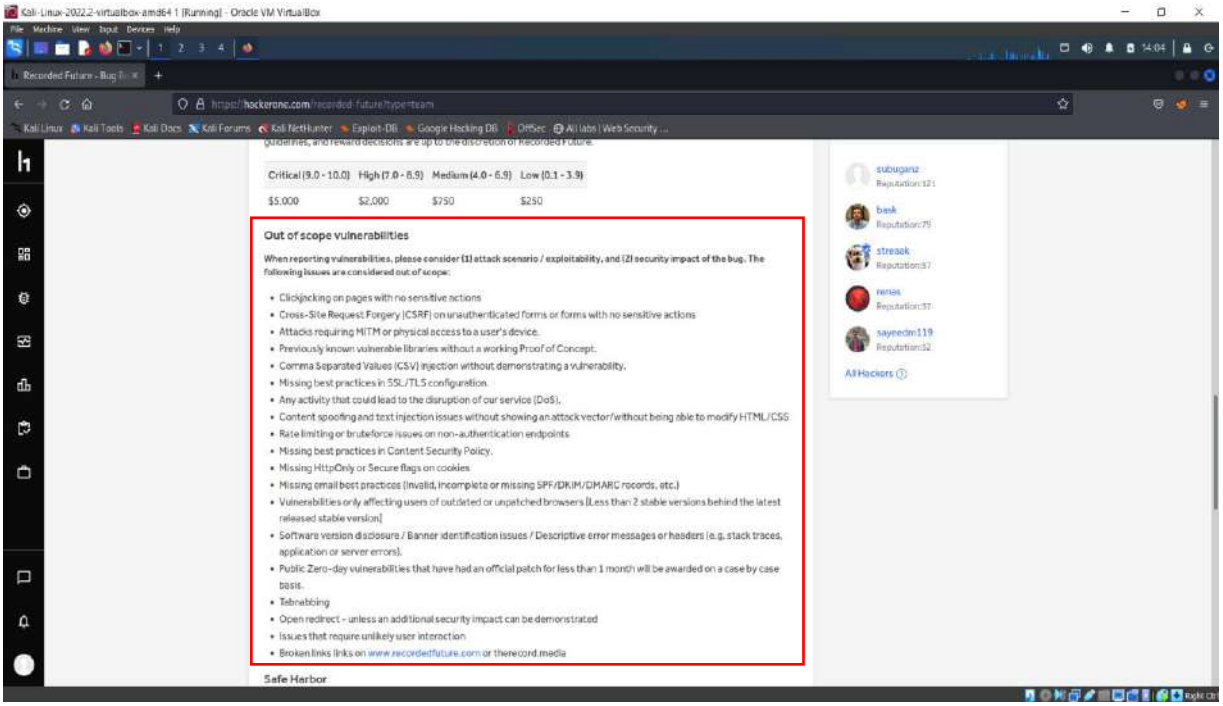
Recorded Future's insight Platform generates precise and actionable insight at scale, and it does it in real time. It brings together an unprecedented mix of open source, dark web, technical sources, and unique research by combining automated analytics with human experience.

To begin, we are required to read the policies and any other information that are

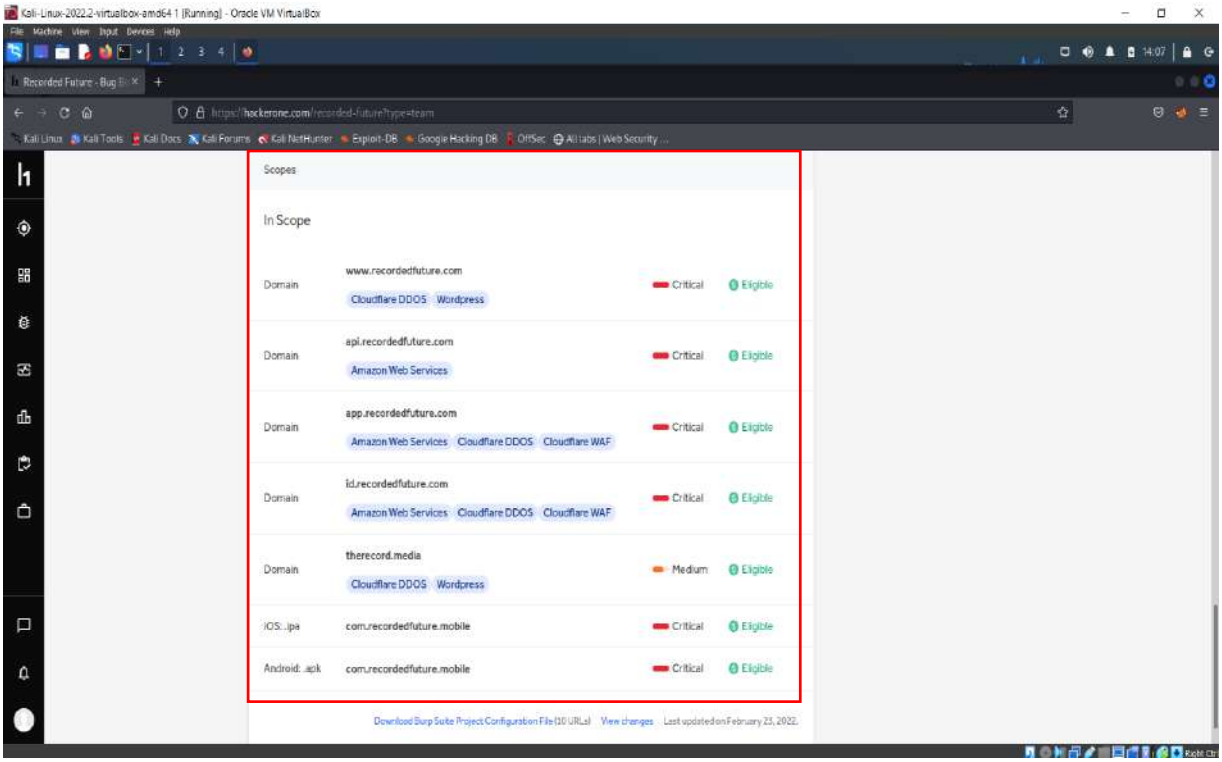
included in the description.Then, we will have a greater understanding of what goes on in this firm, as well as our scope and other related matters. They began by doling out the benefits in accordance with the danger level. As a reward, low-level bugs are worth $100, medium-level bugs are worth $300, high-level bugs are worth $750, and serious bugs are worth $2000. After then, they explain the regulations of their programme. Given that we will be analysing their online application, it is imperative that we conduct ourselves in accordance with the guidelines that have been provided to us.



After that, they will talk about any vulnerabilities that are beyond the purview of the project before moving on. Due to the nature of these security flaws, we are unable to make any attempts to locate a bug or include their findings into our report. The aforementioned list requires that we find a mistake that should not be there. It is important for us to do so.

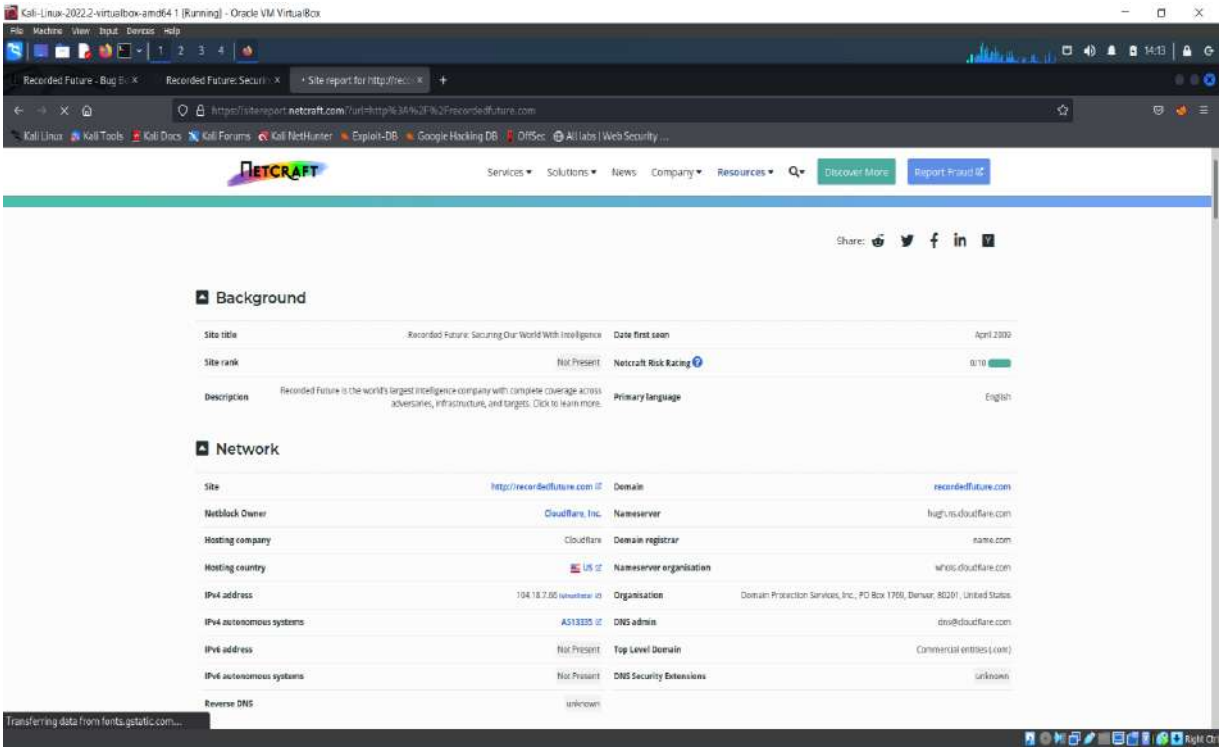


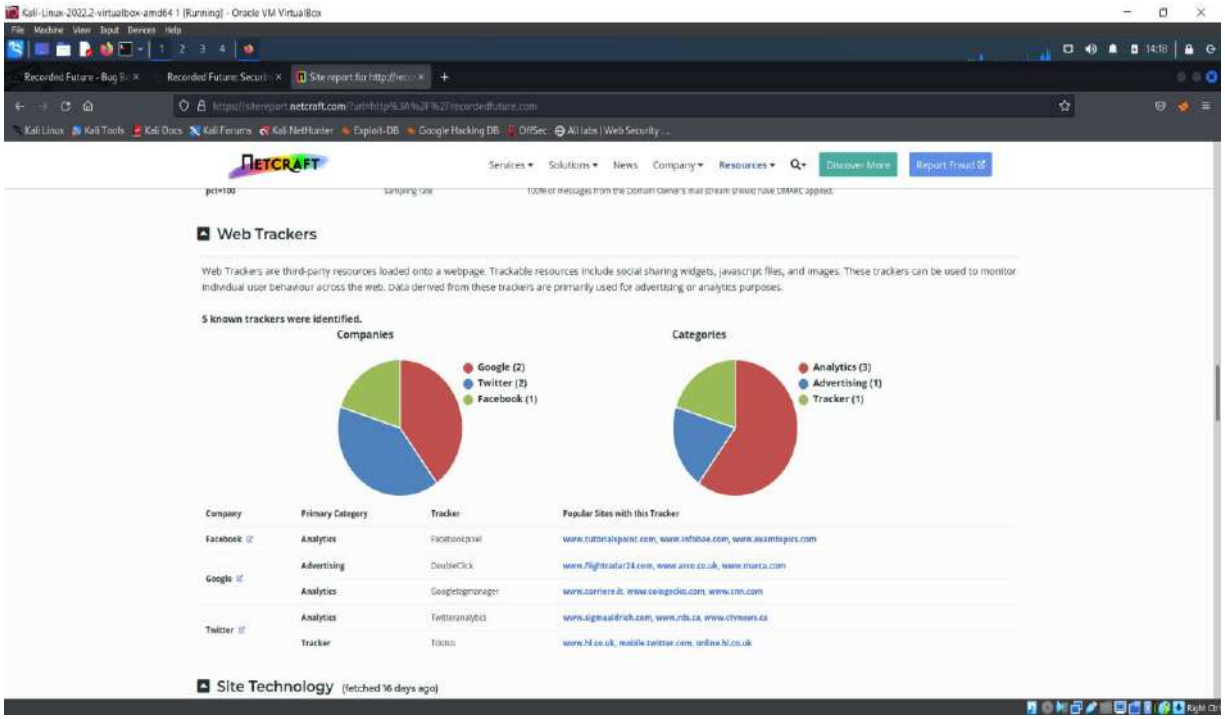
When it comes to searching for bugs that have been awarded bounties, the in-scope area is highly important to us since each scan that we do looks only for domains that are covered by the in-scope umbrella. In the event that things does not proceed as planned, we are going to face a number of challenges.

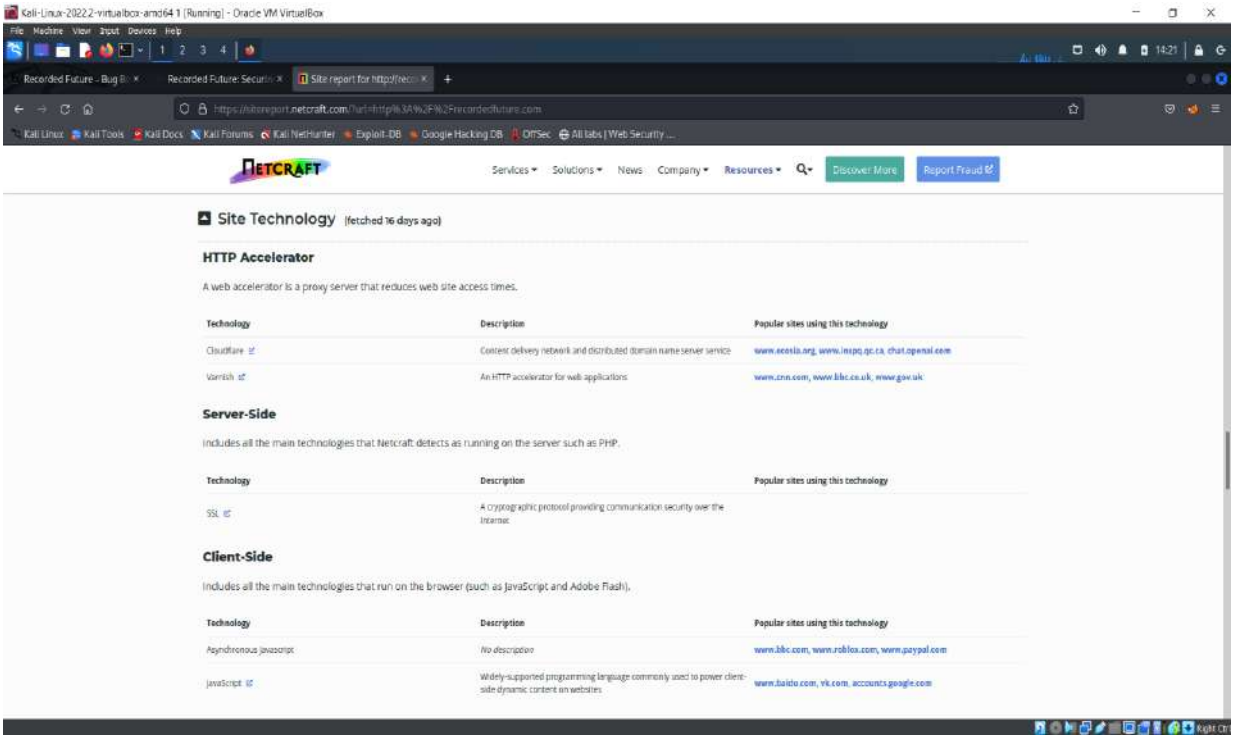


Information Gathering For Target Domain

Let's have a look at the many strategies that we may use in order to get information about recordedfuture.com technological capabilities as well as other useful information. There are a number of programmes and websites that are capable of doing this, but as we are just using Netcraft at the moment, let's type in our domain and investigate the information that can be gained by utilizing Netcraft.

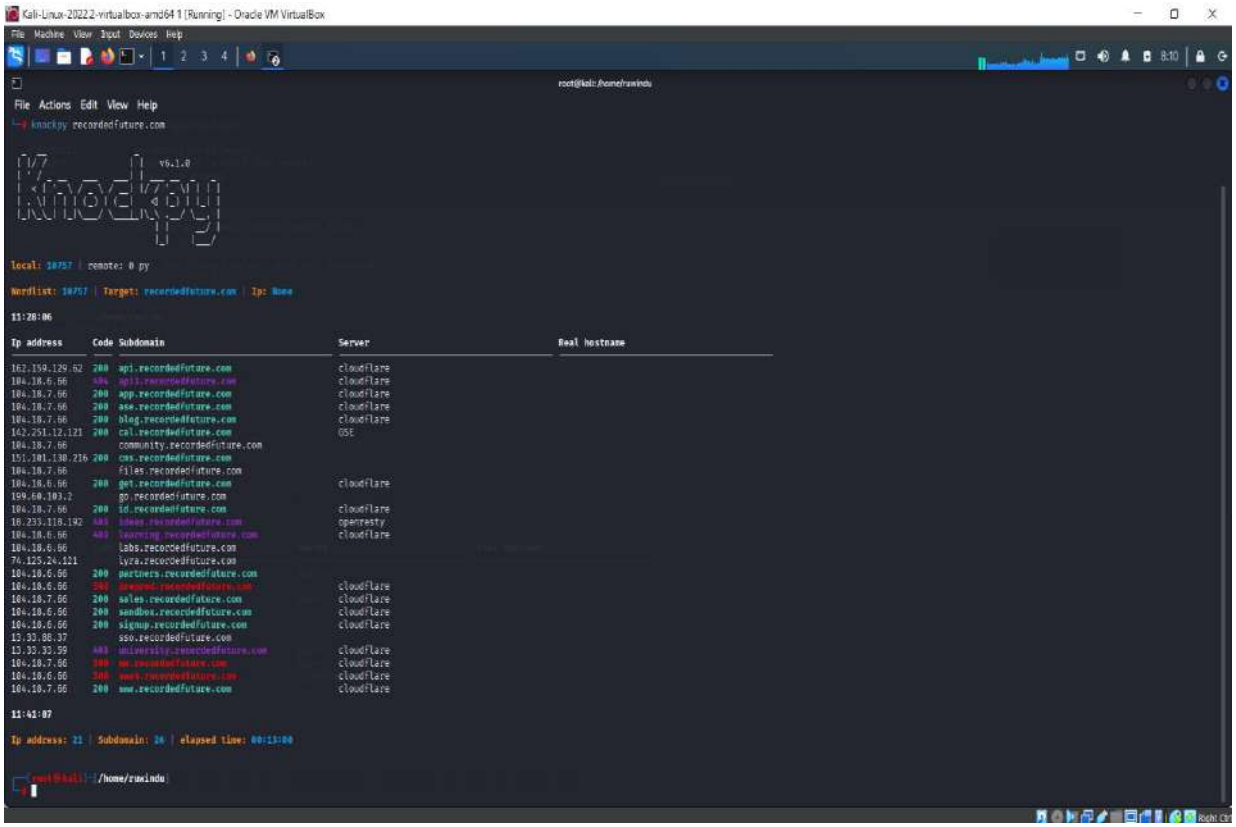



Web Trackers
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.
5 known trackers were identified.
Companies
Google (2)
Twitter (2)
Facebook (1)
Categories
Analytics (3)
Advertising (1)
Tracker (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Facebook
Analytics
Facebook Pixel
www.tutorialspoint.com, www.infobae.com, www.examtopics.com
Google
Advertising
DoubleClick
www.flightradar24.com, www.ansa.co.uk, www.marca.com
Analytics
Google Tag Manager
www.cornerx.it, www.coingecko.com, www.cnn.com
Twitter
Analytics
Twitter Analytics
www.sigmaaldrich.com, www.rds.ca, www.ctvnews.ca
Tracker
Tdotco
www.hl.co.uk, mobile.twitter.com, online.hl.co.uk
Site Technology (fetched 16 days ago)


Site Technology (fetched 16 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
www.ecosia.org, www.inspq.qc.ca, chat.openai.com
Varnish
An HTTP accelerator for web applications
www.cnn.com, www.bbc.co.uk, www.gov.uk
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
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.bbc.com, www.roblox.com, www.paypal.com
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites
www.baidu.com, vk.com, accounts.google.com

Using knockpy tool

In order for us to get to the bottom of what has really taken place here, we are going to need to do a subdomain scanning with the software that is designed for that specific purpose. In the first step of the process, we give knockpy a try on both domains and then watch the output to see what type of results we receive.

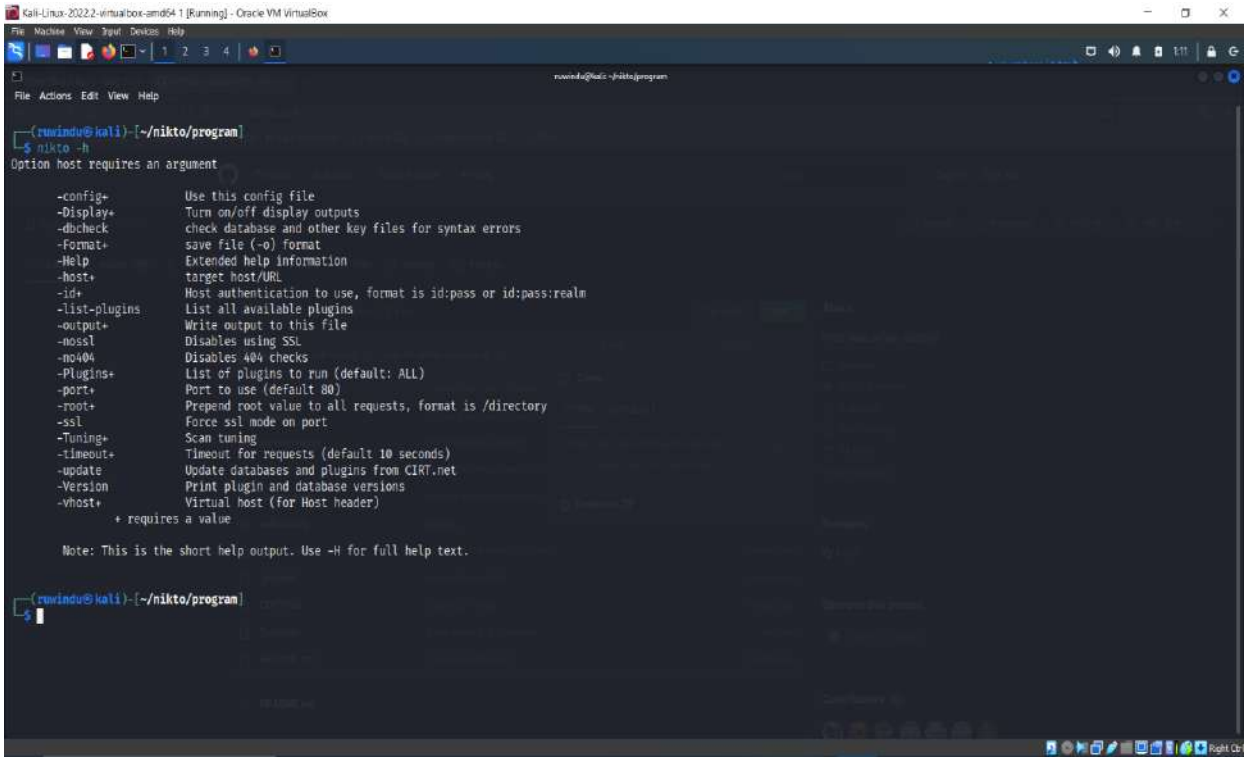


Following the enumeration of subdomains, we are able to see recordedfuture.com subdomains in this format. It is clear that the IP address and name server used by each subdomain of the recordedfuture.com domain are the same. We are able to determine that it is a mobile application from the real hostname that is shown. Let's have a look at the results of our scan of the clabs.co domain.

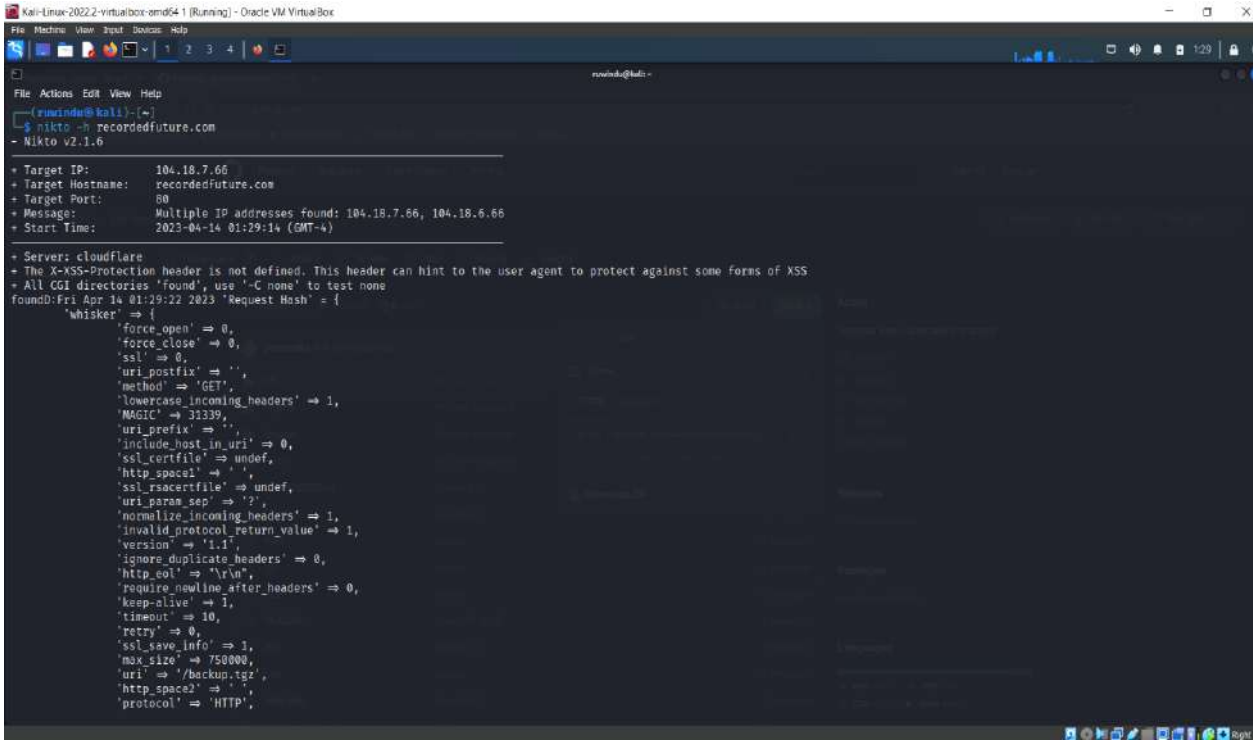
Using Nitko tool

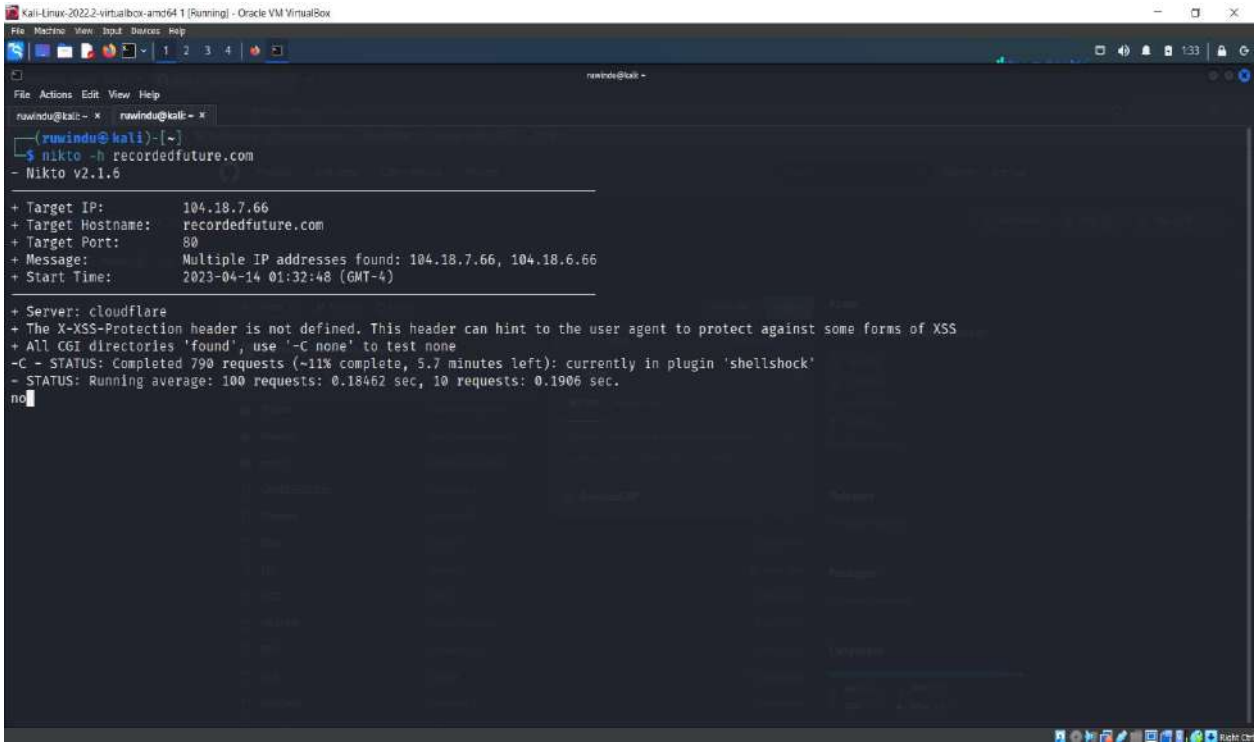
Nikto is a web worker scanner that is licenced under the GNU General Public Licence (GPL) and that performs thorough tests against web workers for a variety of different things. These tests involve scanning over 1250 servers for outmoded adaptations, searching for form explicit mistakes on over 270 servers, and examining over 1250 servers for possibly hazardous documents and programmes.

When we run the command with the –h switch, we are given access to a greater number of high-level options.



Scaned the target domain using nitko tool.

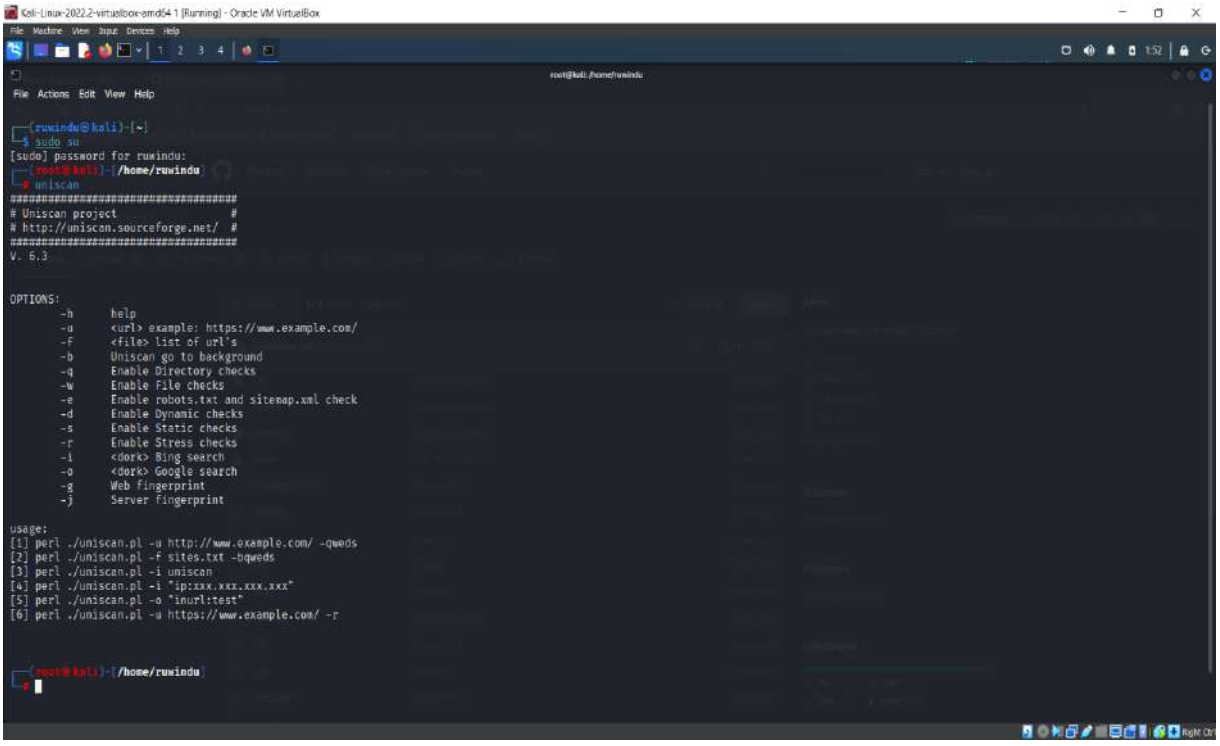




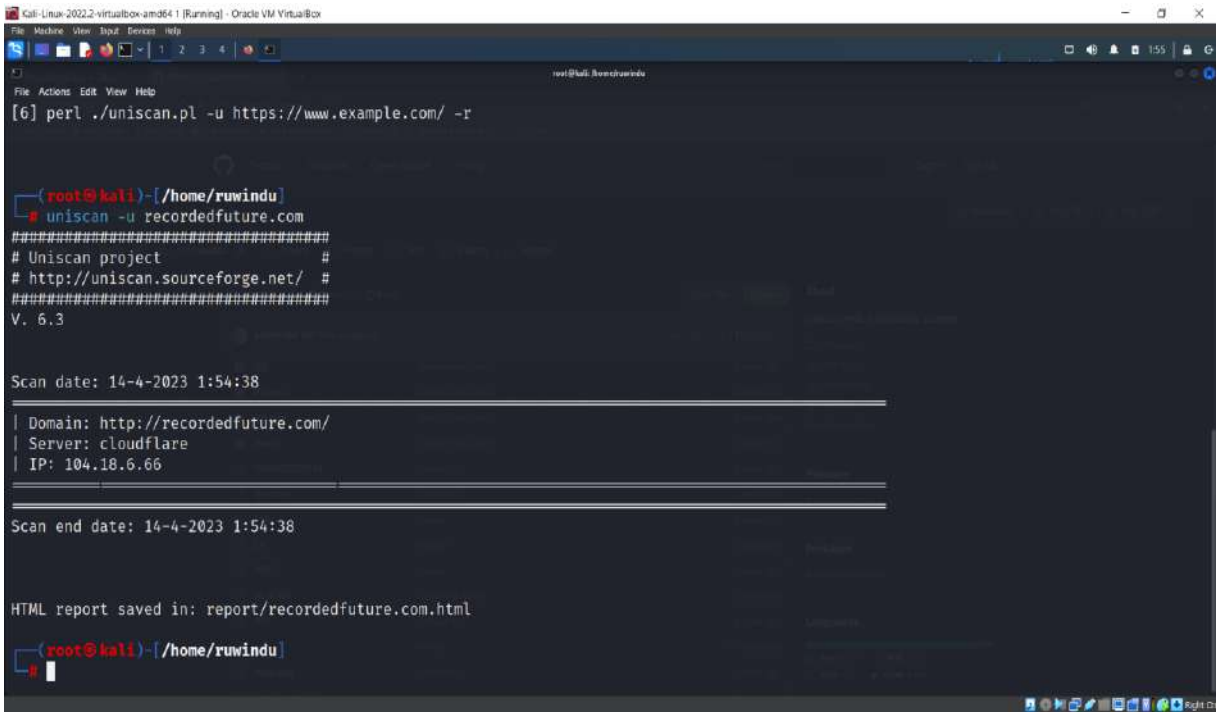
This scanner was not successful in identifying any vulnerabilities.

Using Uniscan tool

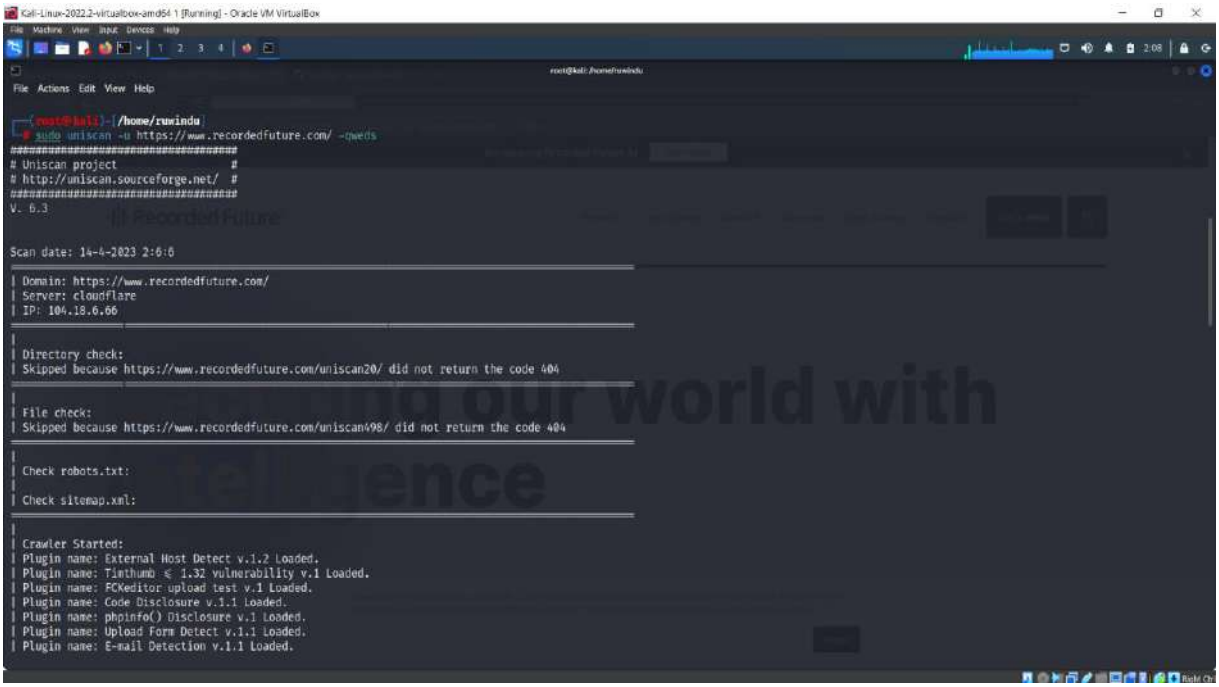
A straightforward online vulnerability scanner, Uniscan looks for issues such as remote command execution, remote file inclusion, and local file inclusion among other things. In addition, it may enumerate and fingerprint online services, in addition to relevant files and directories, as well as information on servers. This particular Perl programme has both a graphical user interface (GUI) and a command line tool option for users to choose from.

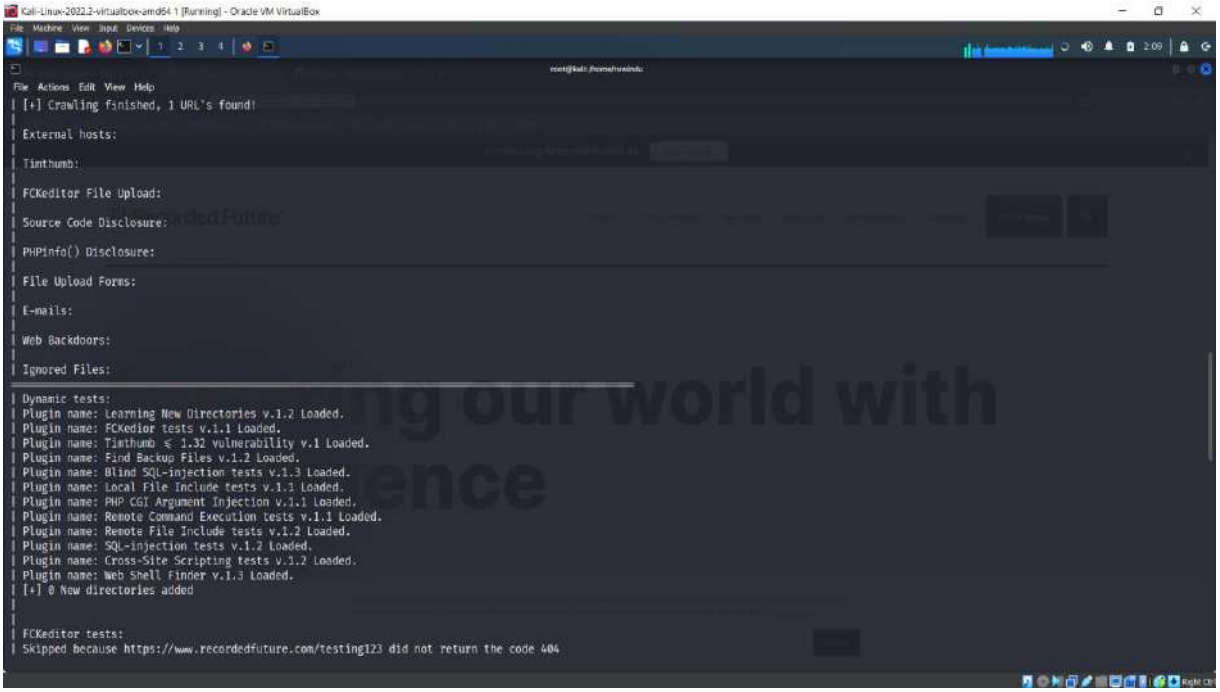


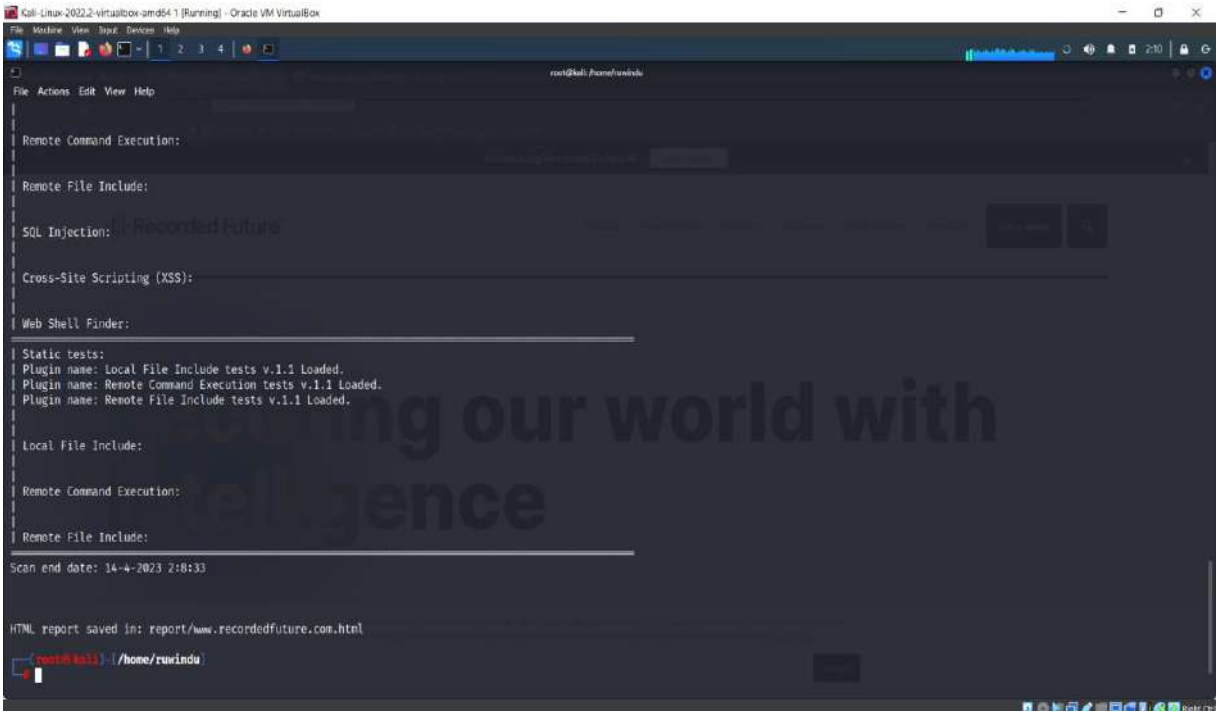
Quick scan by using the –u and enter the target domain.



And used the uniscan –u recordedfuture.com -qweds





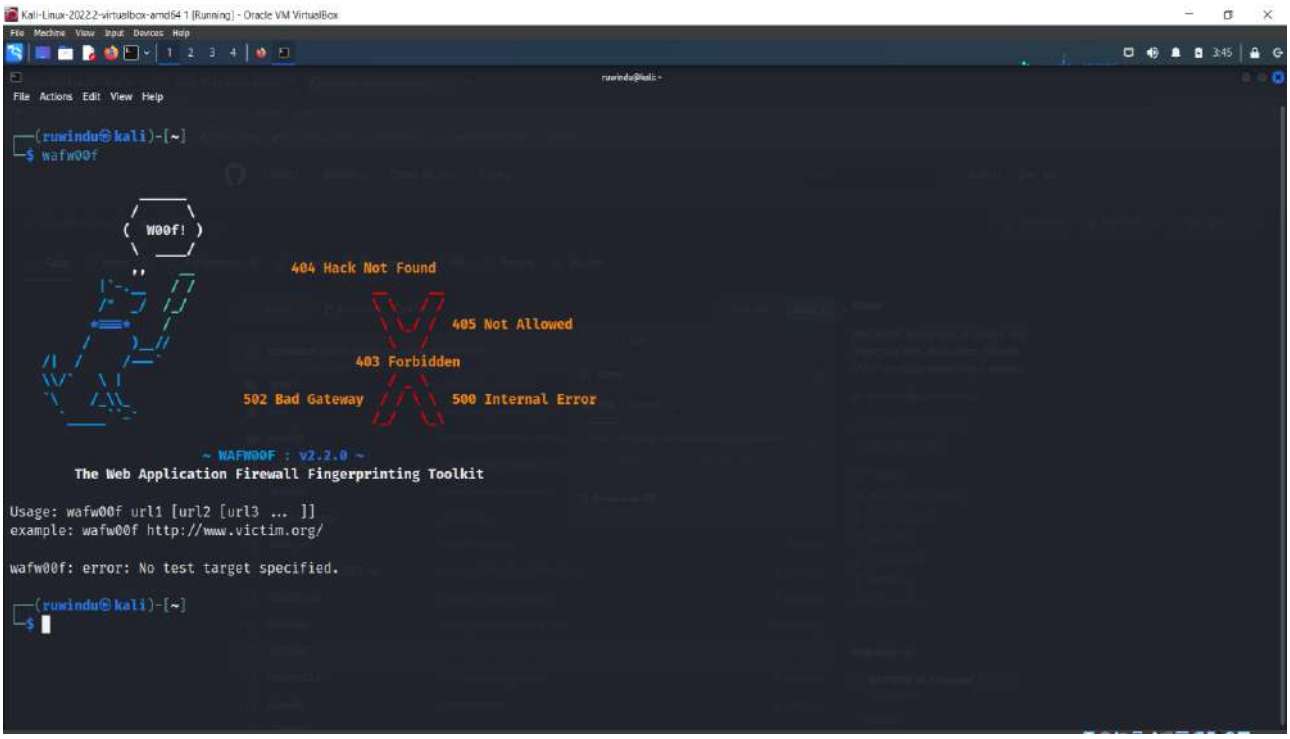


This is the section of the website where we were able to find some of the material that was hosted by other parties. In this specific case, web addresses, or URLs, were found.

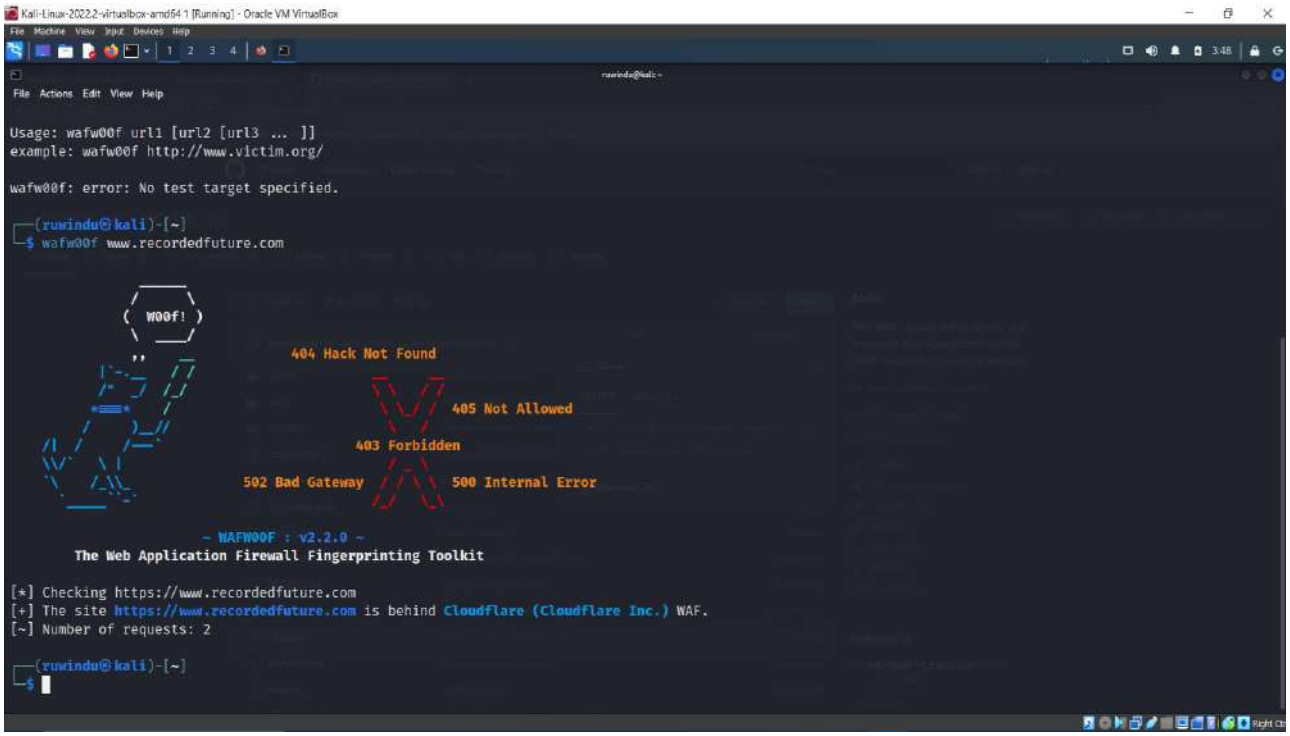
Using Wafw00f tool

In most cases, web application firewalls are application-layer firewalls that are assigned with the responsibility of monitoring and altering HTTP requests. The most significant distinction is in the fact that WAFs operate on the Application Layer of the OSI Model, which is referred to as Layer 7.

In general, every web application firewall (WAF) offers protection against a broad range of HTTP attacks and queries, such as SQL injection and cross-site scripting (XSS). The firewall is able to filter out requests in the same way that a traditional firewall would because it is able to identify the HTTP methods, SQL queries, and other scripts that are used as input to the various forms that are available on a website. This allows the firewall to function in the same manner as a traditional firewall. You may use a website to create a policy that outlines the categories of activities that are permitted and the categories of activities that are not permitted.

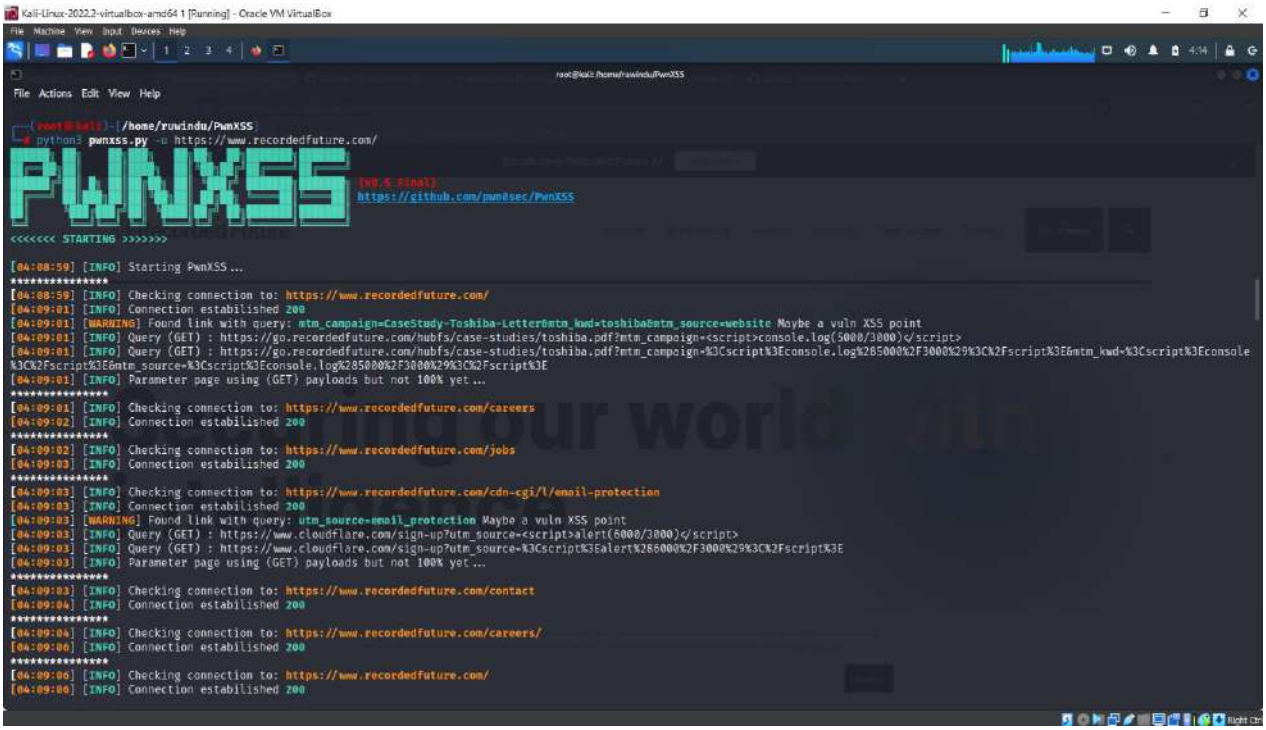


We are able to see that the website www.recordedfuture.com seems to be protected by a WAF or another form of security solution when we utilise the targeted URL in the wafw00f scan. This is something that we were able to determine when we ran the scan.

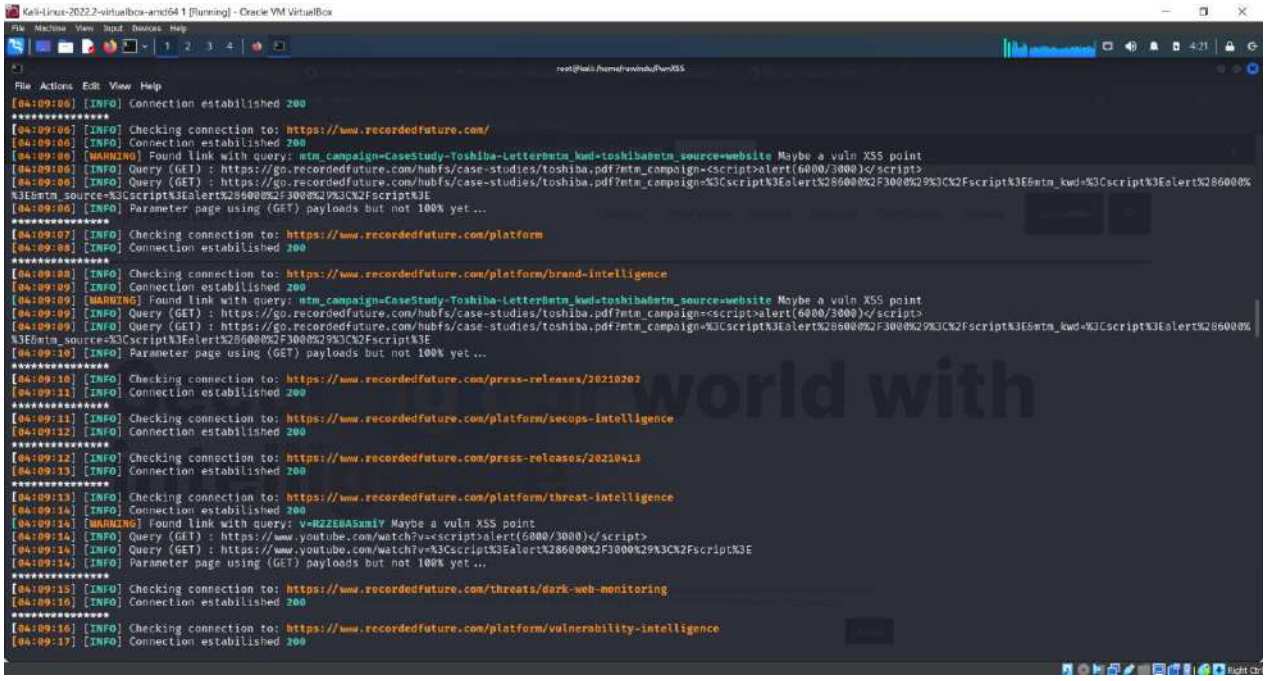


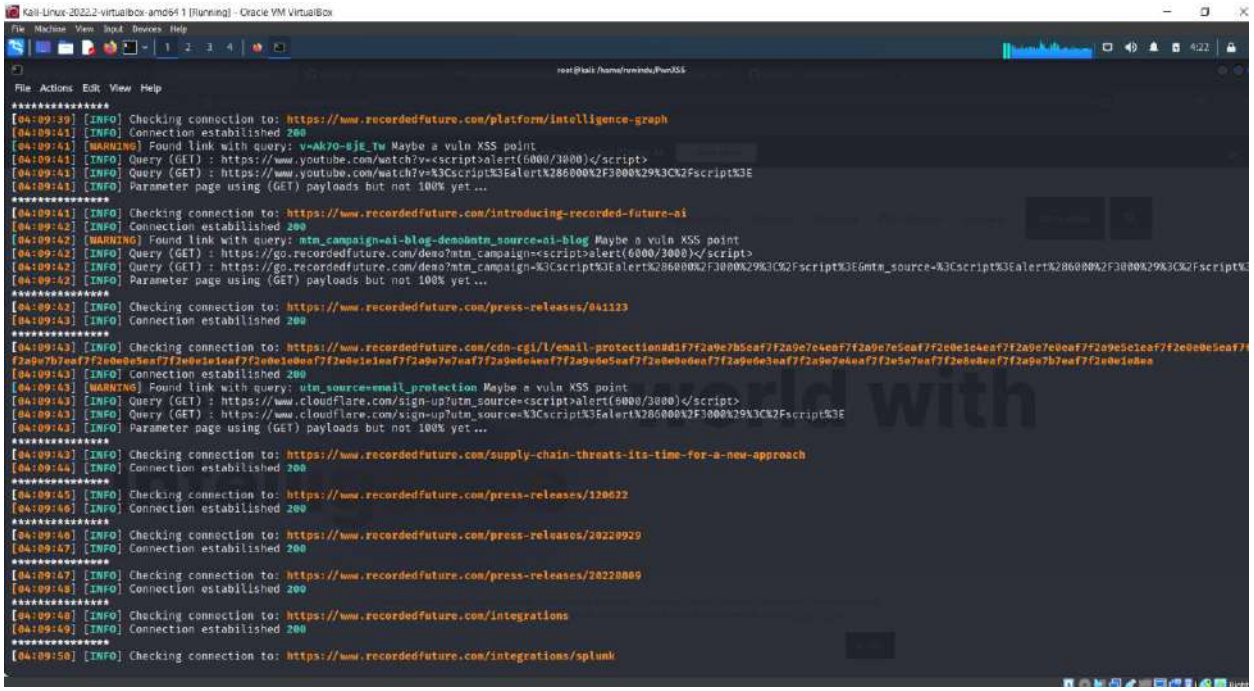
After the quick scan we found the powerful firewall in this domain.

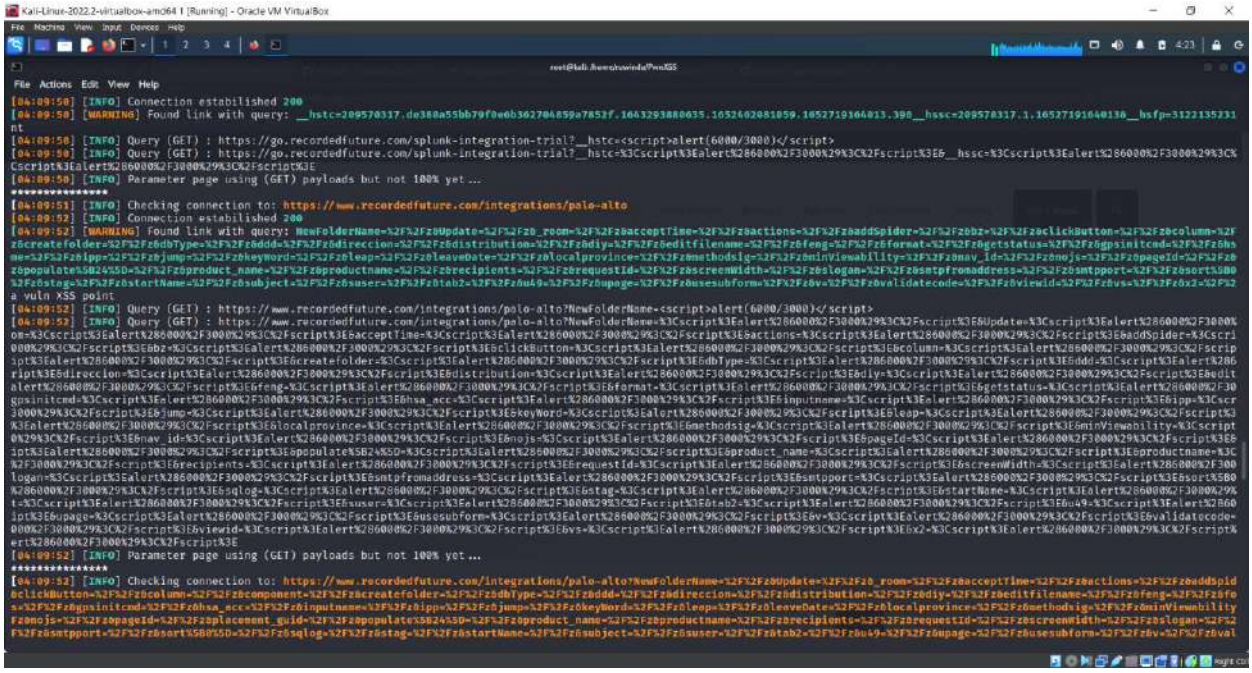
Using pwnXss tool

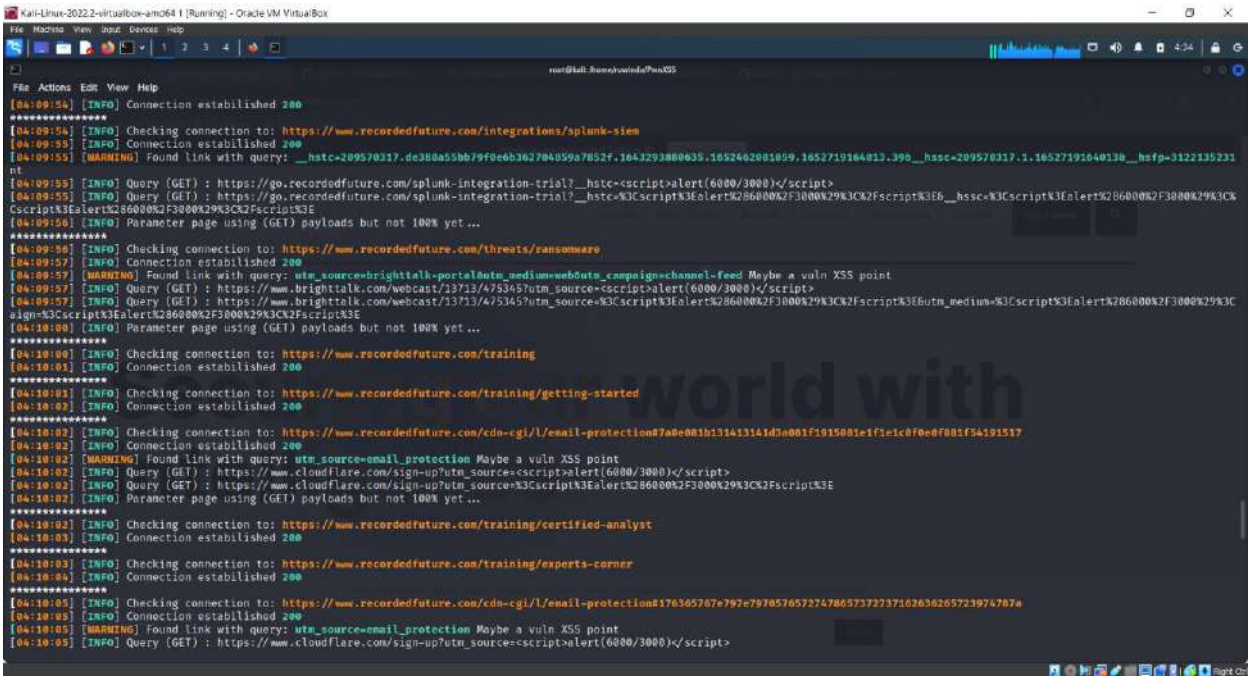


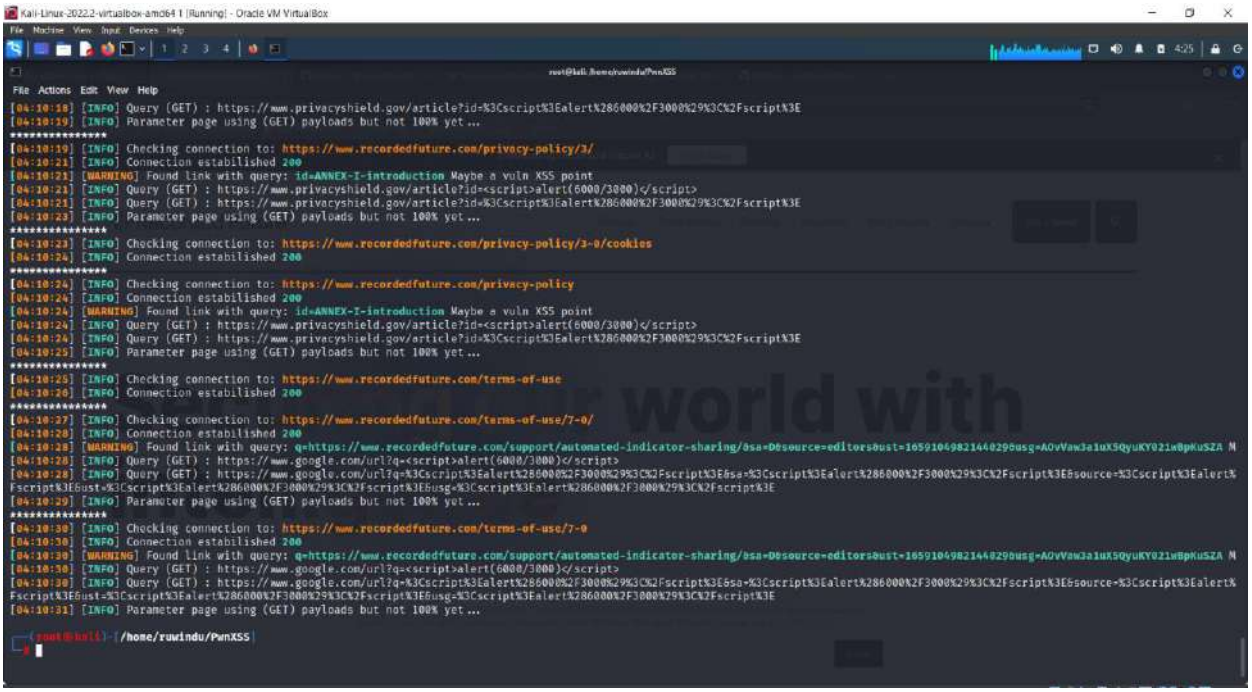
The PwnXss scanner was used to obtain the scan results that are displayed above and below. These results disclose the discoveries of several undefined XSS vulnerabilities that were detected on the domain https://www.recordedfuture.com/.




Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[04:09:39] [INFO] Checking connection to: https://www.recordedfuture.com/platform/intelligence-graph
[04:09:41] [INFO] Connection established 200
[04:09:41] [WARNING] Found link with query: v=Ak7O-8jE_Tw Maybe a vuln XSS point
[04:09:41] [INFO] Query (GET) : https://www.youtube.com/watch?v=<script>alert(6000/3000)</script>
[04:09:41] [INFO] Query (GET) : https://www.youtube.com/watch?v=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:09:41] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[04:09:41] [INFO] Checking connection to: https://www.recordedfuture.com/introducing-recorded-future-ai
[04:09:42] [INFO] Connection established 200
[04:09:42] [WARNING] Found link with query: mtm_campaign=ai-blog-demo&mtm_source=ai-blog Maybe a vuln XSS point
[04:09:42] [INFO] Query (GET) : https://go.recordedfuture.com/demo?mtm_campaign=<script>alert(6000/3000)</script>
[04:09:42] [INFO] Query (GET) : https://go.recordedfuture.com/demo?mtm_campaign=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&mtm_source=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%
[04:09:42] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[04:09:42] [INFO] Checking connection to: https://www.recordedfuture.com/press-releases/041123
[04:09:43] [INFO] Connection established 200
[04:09:43] [INFO] Checking connection to: https://www.recordedfuture.com/cdn-cgi/l/email-protection#d1f7f2a9e7b5eaf7f2a9e7e4eaf7f2a9e7e5eaf7f2e0e1c4eaf7f2a9e7e0eaf7f2a9e5e1eaf7f2e0e0e5eaf7
[04:09:43] [INFO] Connection established 200
[04:09:43] [WARNING] Found link with query: utm_source=email_protection Maybe a vuln XSS point
[04:09:43] [INFO] Query (GET) : https://www.cloudflare.com/sign-up?utm_source=<script>alert(6000/3000)</script>
[04:09:43] [INFO] Query (GET) : https://www.cloudflare.com/sign-up?utm_source=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:09:43] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[04:09:43] [INFO] Checking connection to: https://www.recordedfuture.com/supply-chain-threats-its-time-for-a-new-approach
[04:09:44] [INFO] Connection established 200
[04:09:45] [INFO] Checking connection to: https://www.recordedfuture.com/press-releases/120622
[04:09:46] [INFO] Connection established 200
[04:09:46] [INFO] Checking connection to: https://www.recordedfuture.com/press-releases/20220929
[04:09:47] [INFO] Connection established 200
[04:09:47] [INFO] Checking connection to: https://www.recordedfuture.com/press-releases/20220809
[04:09:48] [INFO] Connection established 200
[04:09:48] [INFO] Checking connection to: https://www.recordedfuture.com/integrations
[04:09:49] [INFO] Connection established 200
[04:09:50] [INFO] Checking connection to: https://www.recordedfuture.com/integrations/splunk


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
[04:09:50] [INFO] Connection established 200
[04:09:50] [WARNING] Found link with query: __hstc=209570317.de380a55bb79f0e6b362704859a7852f.1663293880635.1663602081859.1665719164013.390__hssc=209570317.1.1665719164013.390__hsfp=3122135231
nt
[04:09:50] [INFO] Query (GET) : https://go.recordedfuture.com/splunk-integration-trial?__hstc=<script>alert(6000/3000)</script>
[04:09:50] [INFO] Query (GET) : https://go.recordedfuture.com/splunk-integration-trial?__hstc=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&__hssc=%3Cscript%3Ealert%286000%2F3000%29%3C%
Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:09:50] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[04:09:51] [INFO] Checking connection to: https://www.recordedfuture.com/integrations/palo-alto
[04:09:52] [INFO] Connection established 200
[04:09:52] [WARNING] Found link with query: NewFolderName=%2F%2Fz0Update=%2F%2Fz0_room=%2F%2Fz0acceptTime=%2F%2Fz0actions=%2F%2Fz0addSpider=%2F%2Fz0bz=%2F%2Fz0clickButton=%2F%2Fz0column=%2F
z0createfolder=%2F%2Fz0dbType=%2F%2Fz0ddd=%2F%2Fz0direccion=%2F%2Fz0distribution=%2F%2Fz0diy=%2F%2Fz0editfilename=%2F%2Fz0feng=%2F%2Fz0format=%2F%2Fz0getstatus=%2F%2Fz0gpsinitcmd=%2F%2Fz0hs
me=%2F%2Fz0ipp=%2F%2Fz0jump=%2F%2Fz0keyWord=%2F%2Fz0leap=%2F%2Fz0leaveDate=%2F%2Fz0localprovince=%2F%2Fz0methodsig=%2F%2Fz0minViewability=%2F%2Fz0nav_id=%2F%2Fz0nojs=%2F%2Fz0pageId=%2F%2Fz0
z0population%5B24%5D=%2F%2Fz0product_name=%2F%2Fz0productname=%2F%2Fz0recipients=%2F%2Fz0requestId=%2F%2Fz0screenWidth=%2F%2Fz0slogan=%2F%2Fz0smtpFromaddress=%2F%2Fz0smtpport=%2F%2Fz0sort%5B0
%5D%2Fz0stag=%2F%2Fz0startName=%2F%2Fz0subject=%2F%2Fz0suser=%2F%2Fz0tab2=%2F%2Fz0u49=%2F%2Fz0upage=%2F%2Fz0usesubform=%2F%2Fz0v=%2F%2Fz0validatecode=%2F%2Fz0viewid=%2F%2Fz0vs=%2F%2Fz0x2=%2F%2
a vuln XSS point
[04:09:52] [INFO] Query (GET) : https://www.recordedfuture.com/integrations/palo-alto?NewFolderName=<script>alert(6000/3000)</script>
[04:09:52] [INFO] Query (GET) : https://www.recordedfuture.com/integrations/palo-alto?NewFolderName=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&Update=%3Cscript%3Ealert%286000%2F3000%
on=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&acceptTime=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&actions=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&addSpider=%3Cscri
000%29%3C%2Fscript%3E&bz=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&clickButton=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&column=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscrip
ipt%3Ealert%286000%2F3000%29%3C%2Fscript%3E&createfolder=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&dbType=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&ddd=%3Cscript%3Ealert%286
ript%3E&direccion=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&distribution=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&diy=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&edit
alert%286000%2F3000%29%3C%2Fscript%3E&feng=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&format=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&getstatus=%3Cscript%3Ealert%286000%2F30
gpsinitcmd=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&hsa_acc=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&inputname=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&ipp=%3Cscr
3000%29%3C%2Fscript%3E&jump=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&keyWord=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&leap=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3
%3Ealert%286000%2F3000%29%3C%2Fscript%3E&localprovince=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&methodsig=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&minViewability=%3Cscript
0%29%3C%2Fscript%3E&nav_id=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&nojs=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&pageId=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&
ipt%3Ealert%286000%2F3000%29%3C%2Fscript%3E&populate%5B24%5D=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&product_name=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&productname=%3C
%2F3000%29%3C%2Fscript%3E&recipients=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&requestId=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&screenWidth=%3Cscript%3Ealert%286000%2F300
logan=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&smtpFromaddress=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&smtpport=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&sort=%5B0
%286000%2F3000%29%3C%2Fscript%3E&sqlog=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&stag=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&startName=%3Cscript%3Ealert%286000%2F3000%29%
t=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&suser=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&tab2=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&u49=%3Cscript%3Ealert%2860
ipt%3E&upage=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&usesubform=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&v=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&validatecode=
000%2F3000%29%3C%2Fscript%3E&viewid=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&vs=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E&x2=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%
ert%286000%2F3000%29%3C%2Fscript%3E
[04:09:52] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[04:09:52] [INFO] Checking connection to: https://www.recordedfuture.com/integrations/palo-alto?NewFolderName=%2F%2Fz0Update=%2F%2Fz0_room=%2F%2Fz0acceptTime=%2F%2Fz0actions=%2F%2Fz0addSpid
erClickButton=%2F%2Fz0column=%2F%2Fz0component-%2F%2Fz0createfolder=%2F%2Fz0dbType=%2F%2Fz0ddd=%2F%2Fz0direccion=%2F%2Fz0distribution=%2F%2Fz0diy=%2F%2Fz0editfilename=%2F%2Fz0feng=%2F%2Fz0fo
s=%2F%2Fz0gpsinitcmd=%2F%2Fz0hsa_acc=%2F%2Fz0inputname=%2F%2Fz0ipp=%2F%2Fz0jump=%2F%2Fz0keyWord=%2F%2Fz0leap=%2F%2Fz0leaveDate=%2F%2Fz0localprovince=%2F%2Fz0methodsig=%2F%2Fz0minViewabilit
F2F0nojs=%2F%2Fz0pageId=%2F%2Fz0placement_guid=%2F%2Fz0populate%5B24%5D=%2F%2Fz0product_name=%2F%2Fz0productname=%2F%2Fz0recipients=%2F%2Fz0requestId=%2F%2Fz0screenWidth=%2F%2Fz0slogan=%2F%2
F%2Fz0smtpport=%2F%2Fz0sort%5B0%5D=%2F%2Fz0sqlog=%2F%2Fz0stag=%2F%2Fz0startName=%2F%2Fz0subject=%2F%2Fz0suser=%2F%2Fz0tab2=%2F%2Fz0u49=%2F%2Fz0upage=%2F%2Fz0usesubform=%2F%2Fz0v=%2F%2Fz0val



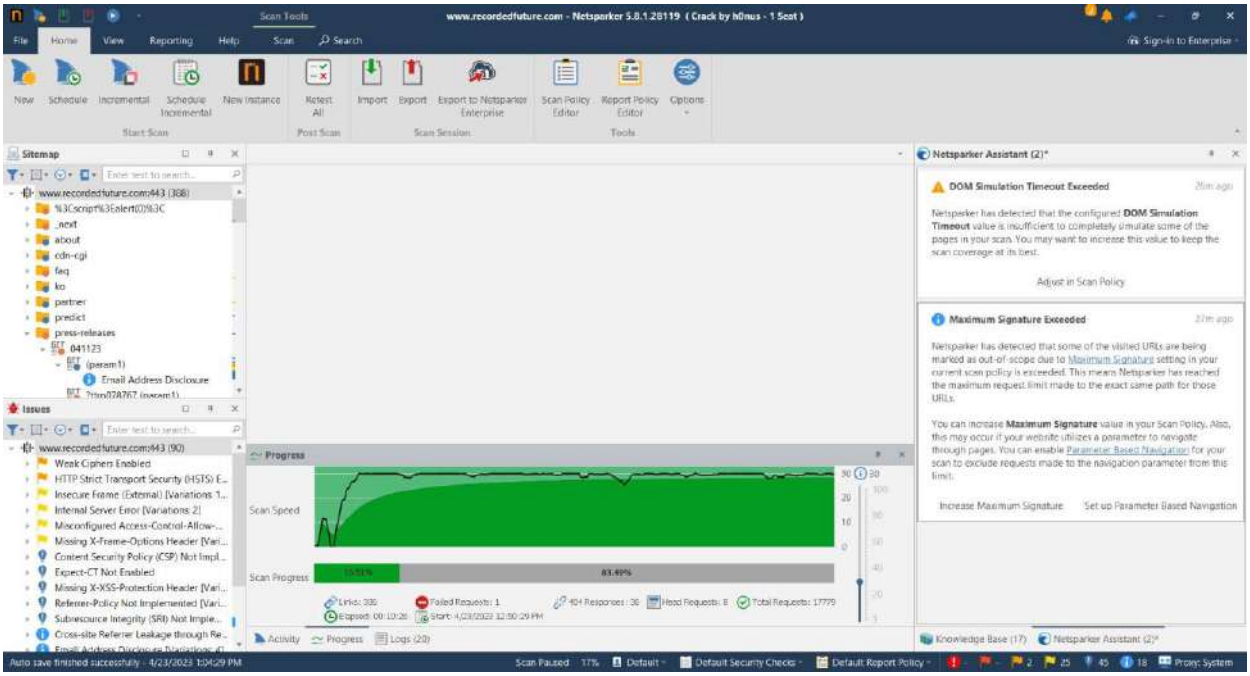


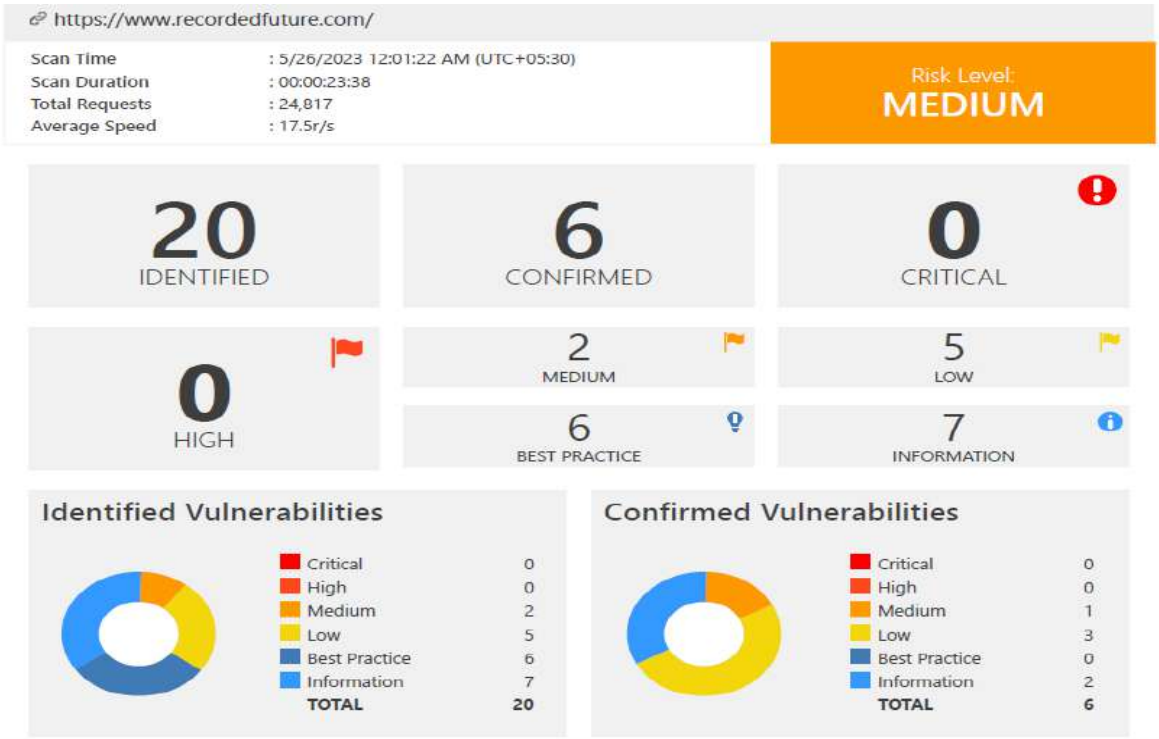
The list shown above contains 18 open XSS vulnerabilities that are not specified. I made an effort to take advantage of some of them. It was difficult to exploit these vulnerabilities due to the fact that the payloads are not 100% complete.

Using Netsparker

Examining websites, web applications, and web services is possible with the assistance of Netsparker (Invicti), an automated online application security scanner that provides a significant amount of configurability in addition to its scanning capabilities. You will be able to detect vulnerabilities in the security of your website, apps, and services by using this scanner. In spite of the fact that various platforms and programming languages were used throughout the construction of various sorts of online applications, Invicti is able to perform scans on all of these different kinds of web apps.

I'm doing a vulnerability scan of recordedfuture.com with the help of Netsparker professional Edition (V), which I'm using for my Audit.





After doing a scan of the domain, I was able to identify a total of 20 vulnerabilities related to the domain, including two vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.recordedfuture.com/	
	Weak Ciphers Enabled	GET	https://www.recordedfuture.com/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.recordedfuture.com/feed/	
	Missing X-Frame-Options Header	GET	https://www.recordedfuture.com/	
	Insecure Frame (External)	GET	https://www.recordedfuture.com/	
	Internal Server Error	GET	https://www.recordedfuture.com/%22%26%20ping%20-n%2025%20127.0.0.1%20%26?%2f%2fr87?com%2f%3f	
	Windows Short Filename	OPTIONS	https://www.recordedfuture.com/_next/static/*~1*%5ca.aspx?aspxerrorpath=/	

Content Security Policy (CSP) Not Implemented	GET	https://www.recordedfuture.com/	
Expect-CT Not Enabled	GET	https://www.recordedfuture.com/	
Missing X-XSS-Protection Header	GET	https://www.recordedfuture.com/	
Referrer-Policy Not Implemented	GET	https://www.recordedfuture.com/	
SameSite Cookie Not Implemented	GET	http://www.recordedfuture.com/	
Subresource Integrity (SRI) Not Implemented	GET	https://www.recordedfuture.com/	
[Possible] Internal Path Disclosure (*nix)	GET	https://www.recordedfuture.com/support/install-configure-getting-started	
Email Address Disclosure	GET	https://www.recordedfuture.com/faq/security	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Generic Email Address Disclosure	GET	https://www.recordedfuture.com/support/two-factor-authentication	
	Sitemap Detected	GET	https://www.recordedfuture.com/sitemap.xml	
	Web Application Firewall Detected	GET	https://www.recordedfuture.com/%3Cscript%3Ealert(0)%3C/script%3E	URI-BASED
	Forbidden Resource	GET	https://www.recordedfuture.com/.svn/wc.db	URI-BASED
	Robots.txt Detected	GET	https://www.recordedfuture.com/robots.txt	

Recordedfuture.com has been found to have the following identified vulnerabilities:

Identified vulnerabilities in Recordedfuture.com

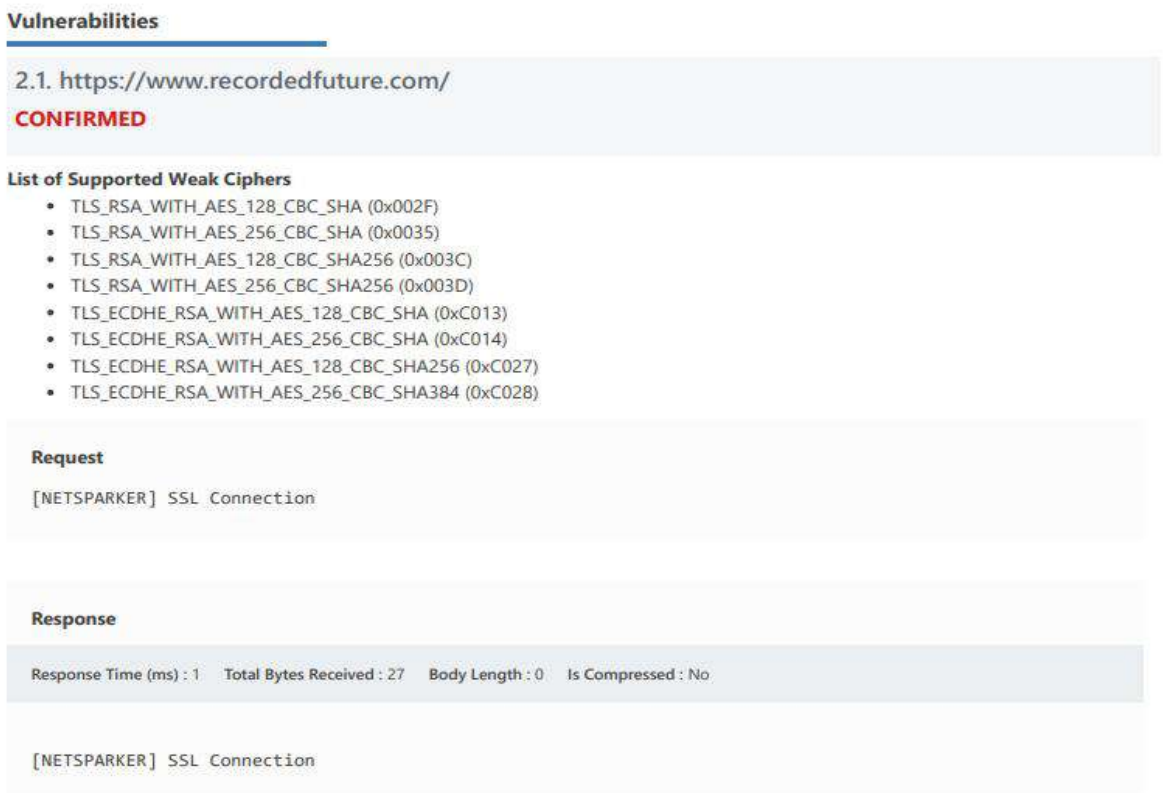
Vulnerability 01 - Weak Ciphers Enabled (Medium)

During a secure communication session (also known as SSL), Netsparker found that the ciphers being utilized were not very safe.

Your web server need to solely support powerful ciphers in order to guarantee the confidentiality and safety of any communication that takes place with visitors of your website.

Impact

An adversary may be able to understand the SSL connection that is taking place between your server and the individuals who are accessing your website. This might be a security risk.



Actions to Take

1. For Apache, you should modify the SSLCipherSuite directive in the `httpd.conf`.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

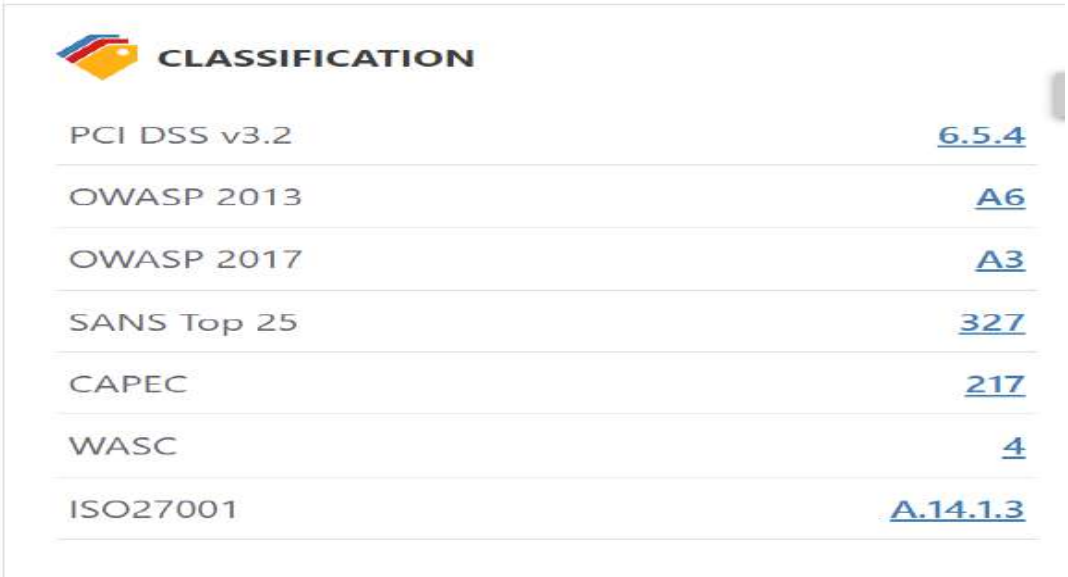
2. Lighttpd:

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

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

   a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
   b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
   c.Set "Enabled" DWORD to "0x0" for the following registry keys:

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



CLASSIFICATION

PCI DSS v3.2	6.5.4
OWASP 2013	A6
OWASP 2017	A3
SANS Top 25	327
CAPEC	217
WASC	4
ISO27001	A.14.1.3

Solution

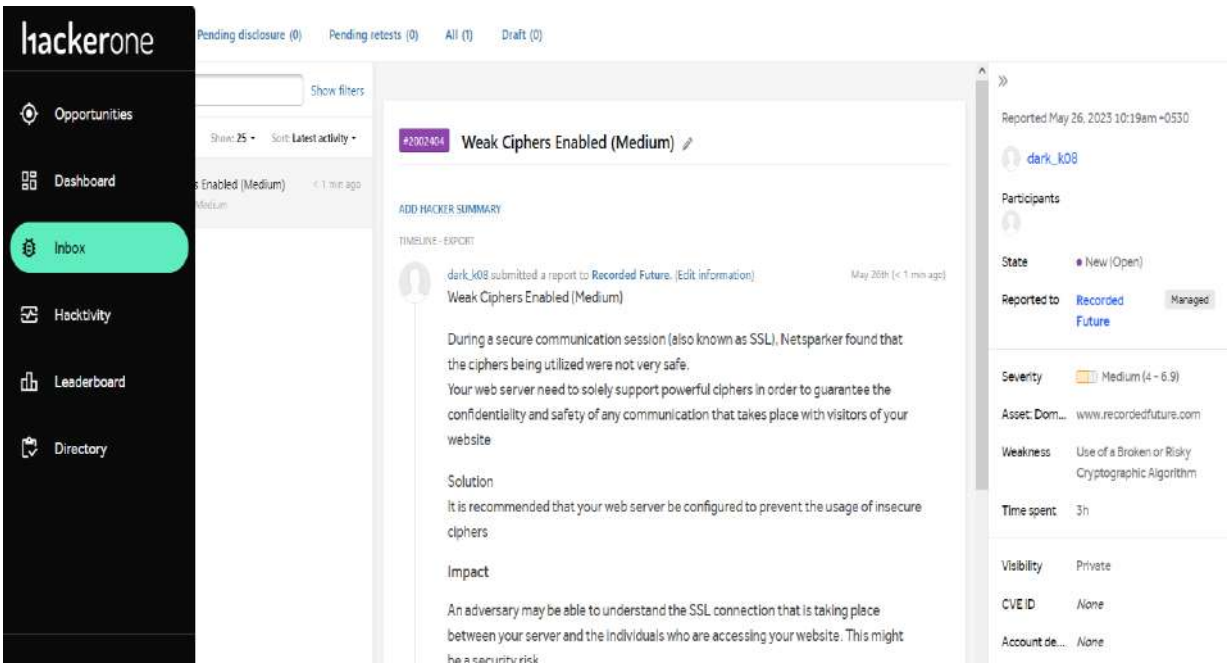
It is recommended that your web server be configured to prevent the usage of insecure ciphers.

Conclusion of the Report 01

Then The first thing that we do while looking for bugs is collect certain essential pieces of information, such as the IP address of the hosting business and the technology that the domain employs, among other things. There are instances when we need to utilise many tools in order to obtain more information and verify that the information we have gathered is true. After that, we investigated if there are any files and instructions that may be retrieved by using software such as pwnxss. It provided a clearer picture of the subject area.

After that, we go to the step of assessing the vulnerabilities. At that moment, we became aware of the vulnerabilities that the domain had and the methods by which we may use certain tools to locate them. After that, we do an analysis of the vulnerability by utilising a few other websites in order to better comprehend the nature of the issue with this web application. After discovering vulnerabilities, we attempted to put one of those vulnerabilities to the test and demonstrate that it included a malicious problem. At that time, we had established that the vulnerability was not a serious one; but, we were exposed to a great deal of fascinating information.

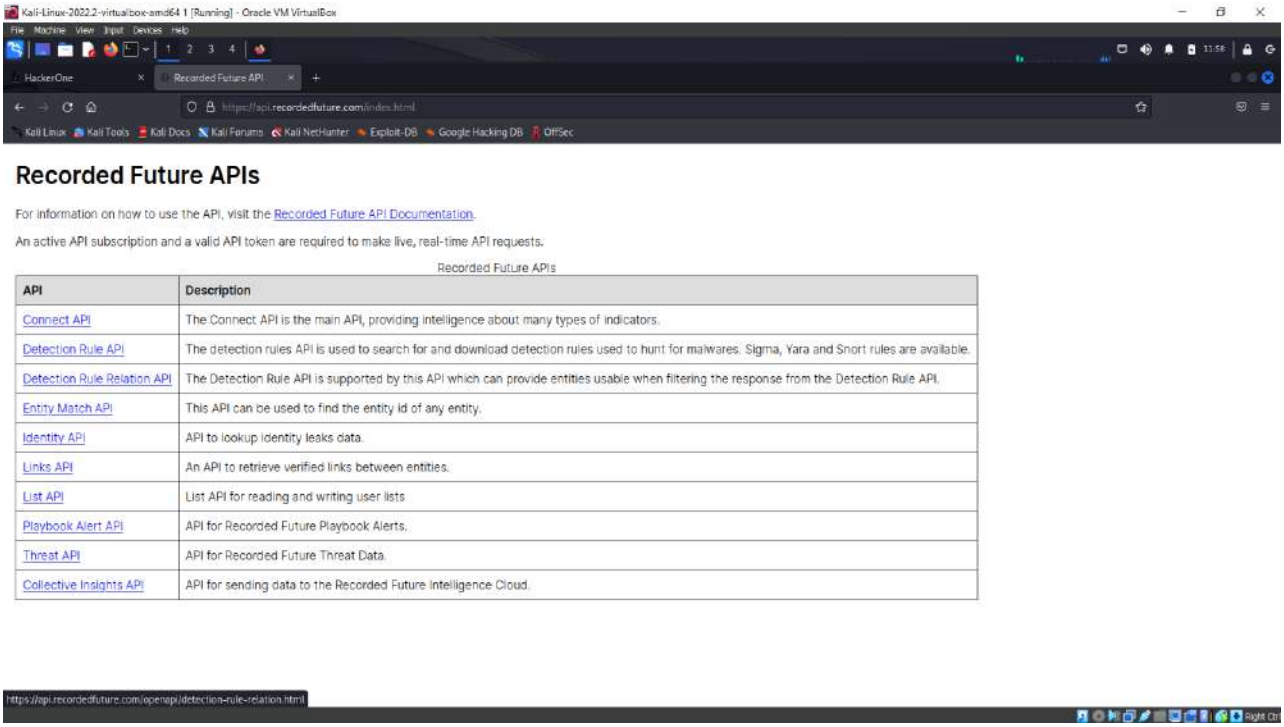
HackerOne Submitted Report Screenshot



ii. Report 02

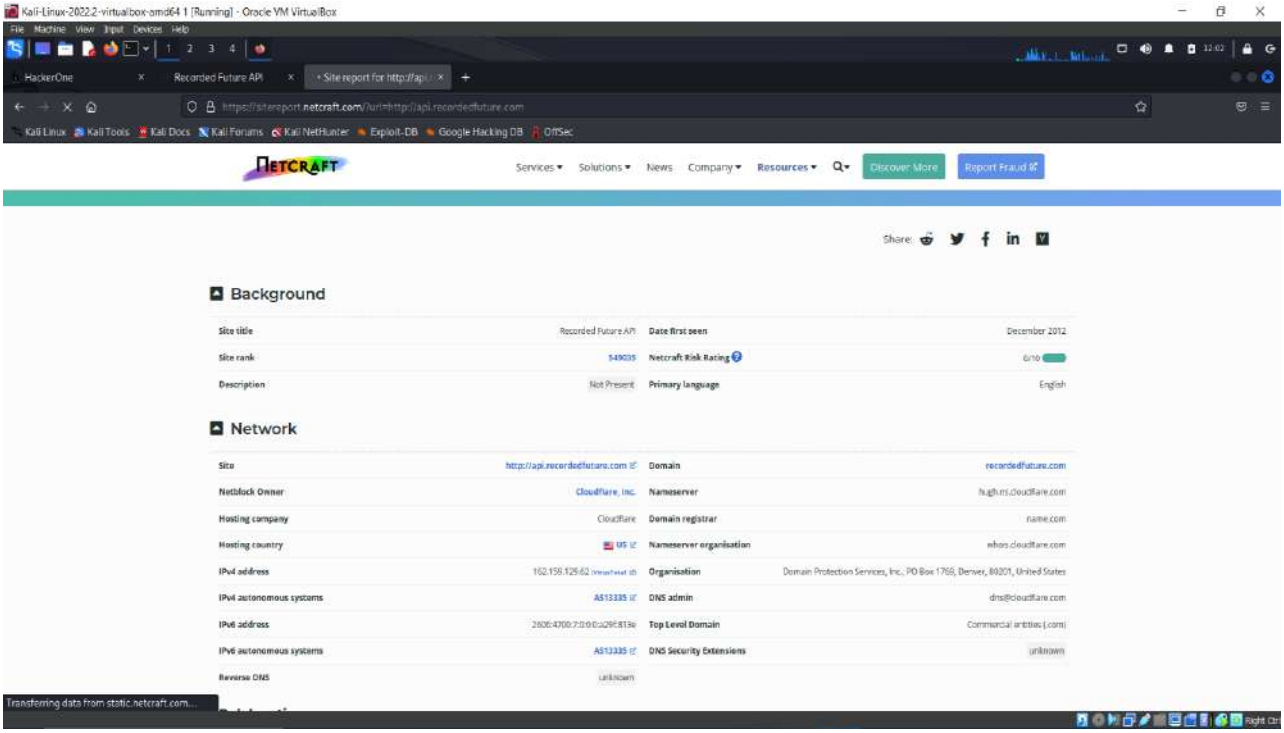
Target information: api.recordedfuture.com

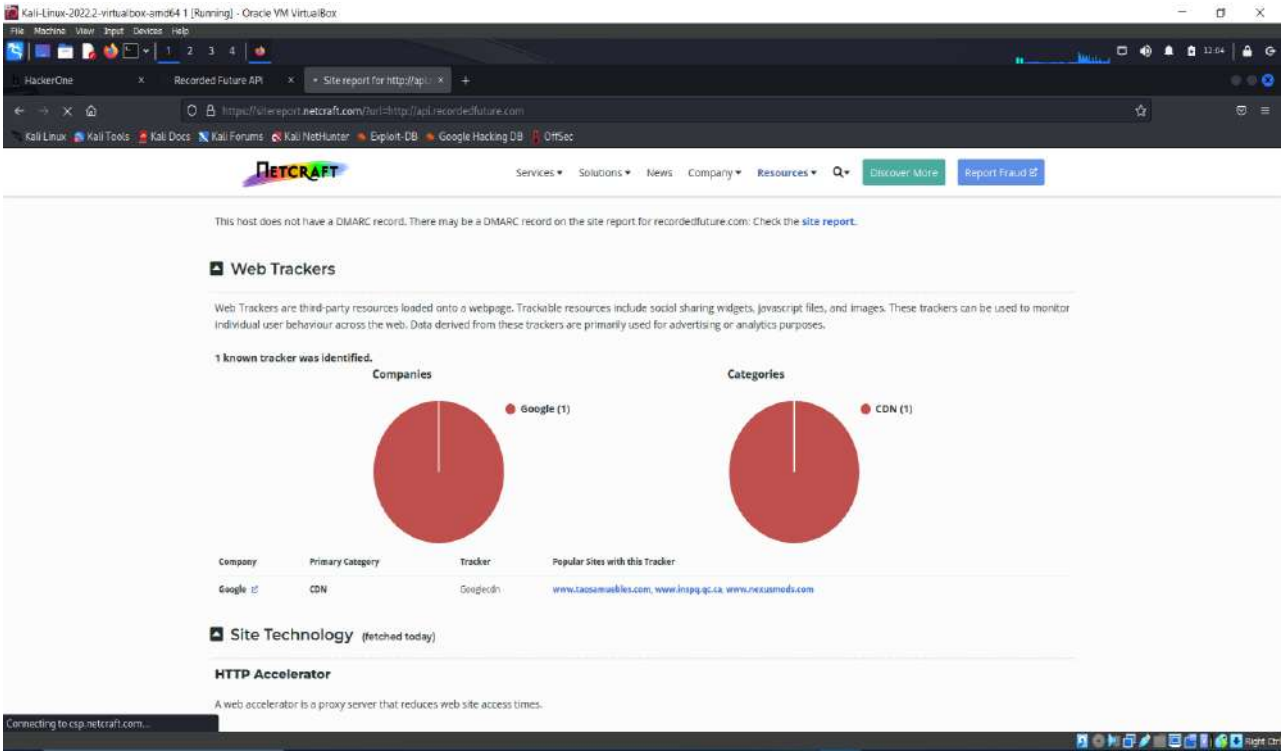
The purpose of this research is to determine whether or not there are vulnerabilities in the target domain (api.recordedfuture.com) and, if so, how much risk is associated with each of those vulnerabilities. If vulnerabilities are found, the study will also attempt to determine whether or not there are vulnerabilities in the target domain. The primary purpose of the investigation is to ascertain whether or not the target domain has any subdomains that are lacking in some manner through which they may be characterized.



Information Gathering For Target Domain

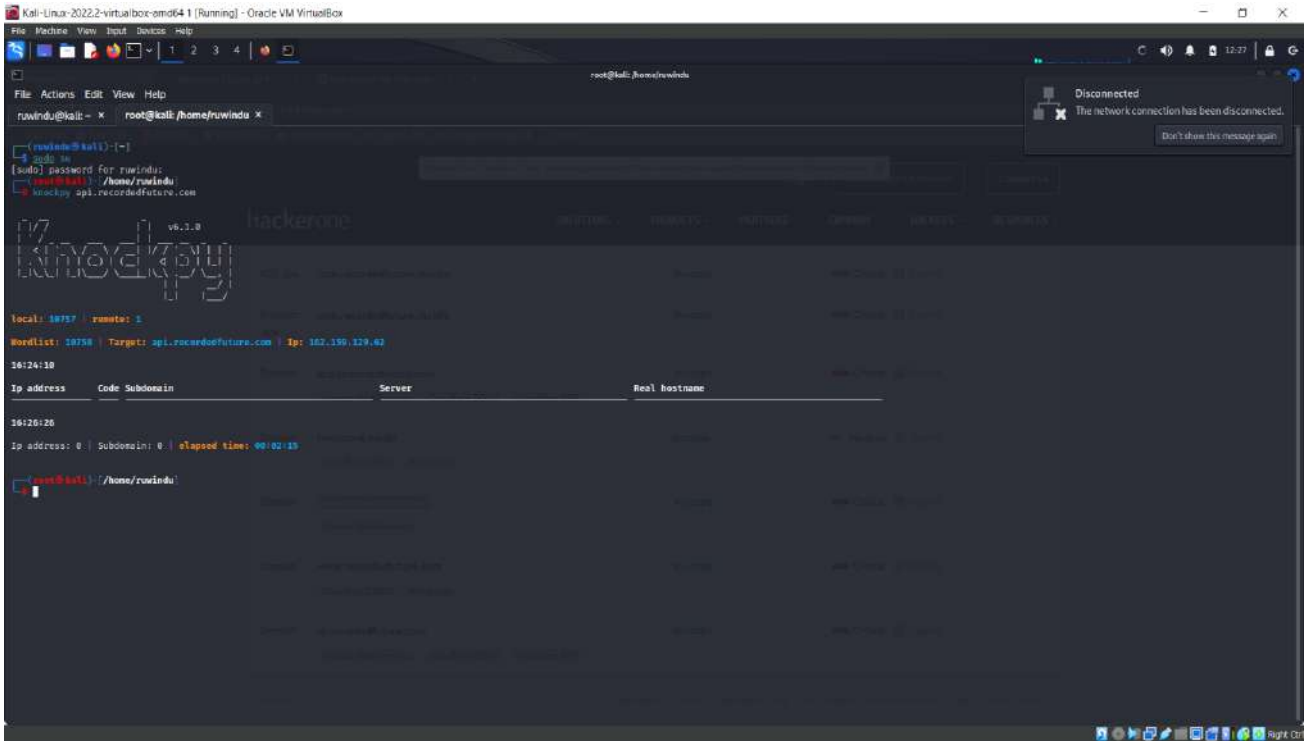
Let's look at the many options we have so we can find out not only what api.recordedfuture.com can do technologically but also other facts that are important to the case. Since Netcraft is the only tool we have right now, let's put in our name and do some research on the information we can get from it. We only have Netcraft right now, so let's type in our name and see what information we can get from it. There are a number of tools and sites that can do this, but since we're only using Netcraft right now, let's look at the information we can get from it.


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
HackerOne
Recorded Future API
Site report for http://api.recordedfuture.com
https://sitereport.netcraft.com/?url=http://api.recordedfuture.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Share:
Background
Site title
Recorded Future API
Date first seen
December 2012
Site rank
549035
Netcraft Risk Rating
Description
Not Present
Primary language
English
Network
Site
http://api.recordedfuture.com
Domain
recordedfuture.com
Netblock Owner
Cloudflare, Inc.
Nameserver
hugh.ns.cloudflare.com
Hosting company
Cloudflare
Domain registrar
name.com
Hosting country
US
Nameserver organisation
whois.cloudflare.com
IPv4 address
162.159.129.62
Organisation
Domain Protection Services, Inc., PO Box 1769, Denver, 80201, United States
IPv4 autonomous systems
AS13335
DNS admin
dns@cloudflare.com
IPv6 address
Top Level Domain
Commercial entities (.com)
IPv6 autonomous systems
AS13335
DNS Security Extensions
unknown
Reverse DNS
unknown
Transferring data from static.netcraft.com...


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
HackerOne
Recorded Future API
Site report for http://api.recordedfuture.com
https://sitereport.netcraft.com/?url=http://api.recordedfuture.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
This host does not have a DMARC record. There may be a DMARC record on the site report for recordedfuture.com: Check the site report.
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.
1 known tracker was identified.
Companies
Google (1)
Categories
CDN (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Google
CDN
Googlecdn
www.taosemueblles.com, www.inspq.qc.ca, www.nexusmods.com
Site Technology (fetched today)
HTTP Accelerator
A web accelerator is a proxy server that reduces web site access times.
Connecting to csp.netcraft.com...

Using knockpy tool

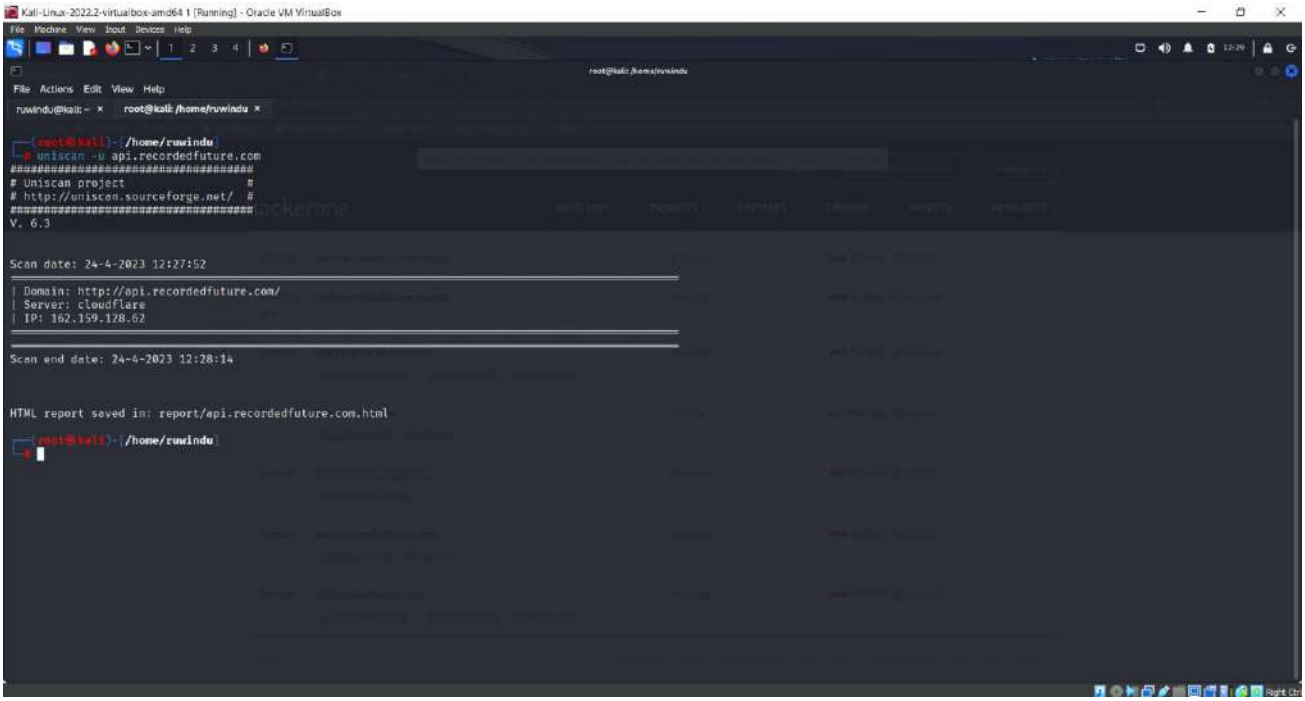
Using the knockpy tool, it is possible to collect subdomain names through scraping data sources, carrying out reverse DNS sweeping, and taking part in recursive brute forcing. All of these methods are described in the previous sentence. Using the instrument is one way to accomplish this goal. KALI Linux, which is the operating system that I'm using on the virtual machine that I have, was pre-installed on it when I acquired it, which means that I didn't have to do anything to get it set up when I first got it.



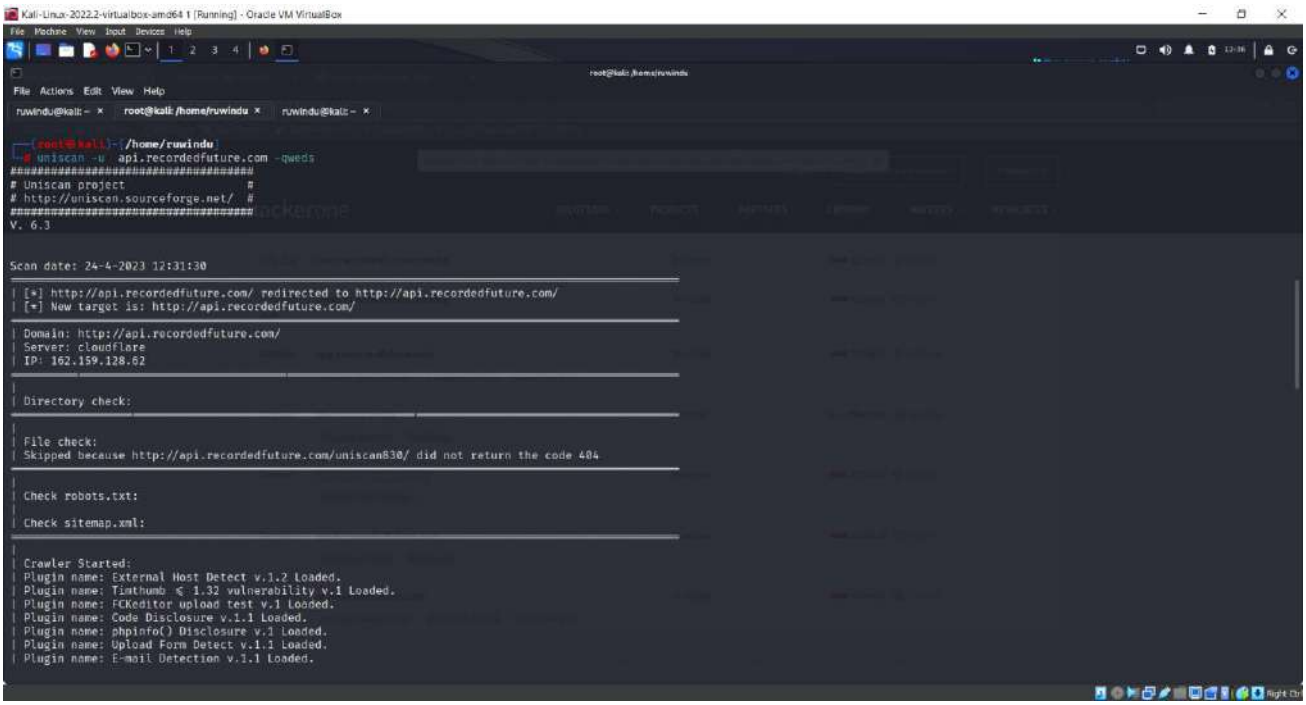
After the enumeration of the subdomains has been completed, we are allowed to see the api.recordedfuture.com subdomains in this manner since the subdomains have been recorded. It really shouldn't come as much of a surprise to anybody that the IP address and name server that are utilised by each and every one of the subdomains that are stored under the api.recordedfuture.com domain are the same ones that are used by the main domain itself. Because the real hostname for the application is shown, we are able to determine that this is a mobile application. Our conclusion is based on the fact that the real hostname is displayed. As a direct result of this, we are now in a position to make use of it. Let's have a look at the results of the inquiry that we conducted into the sphere and see what we found, shall we?

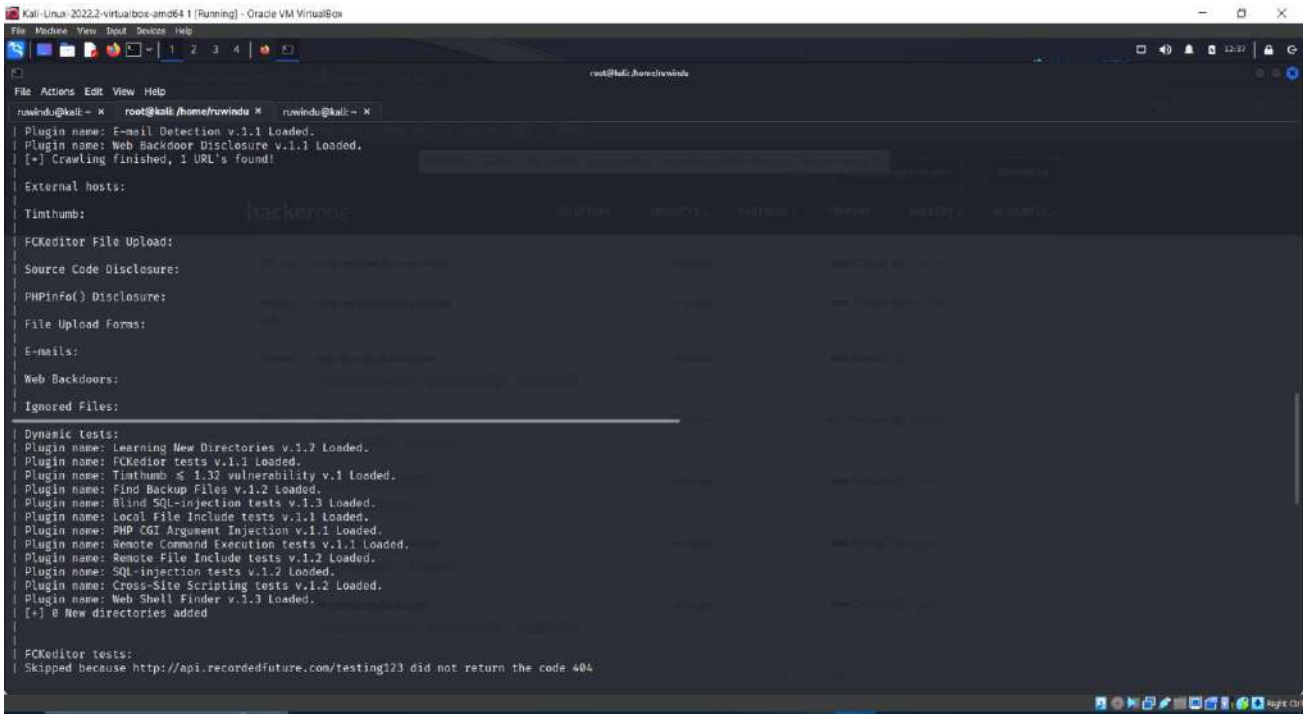
Using Uniscan tool

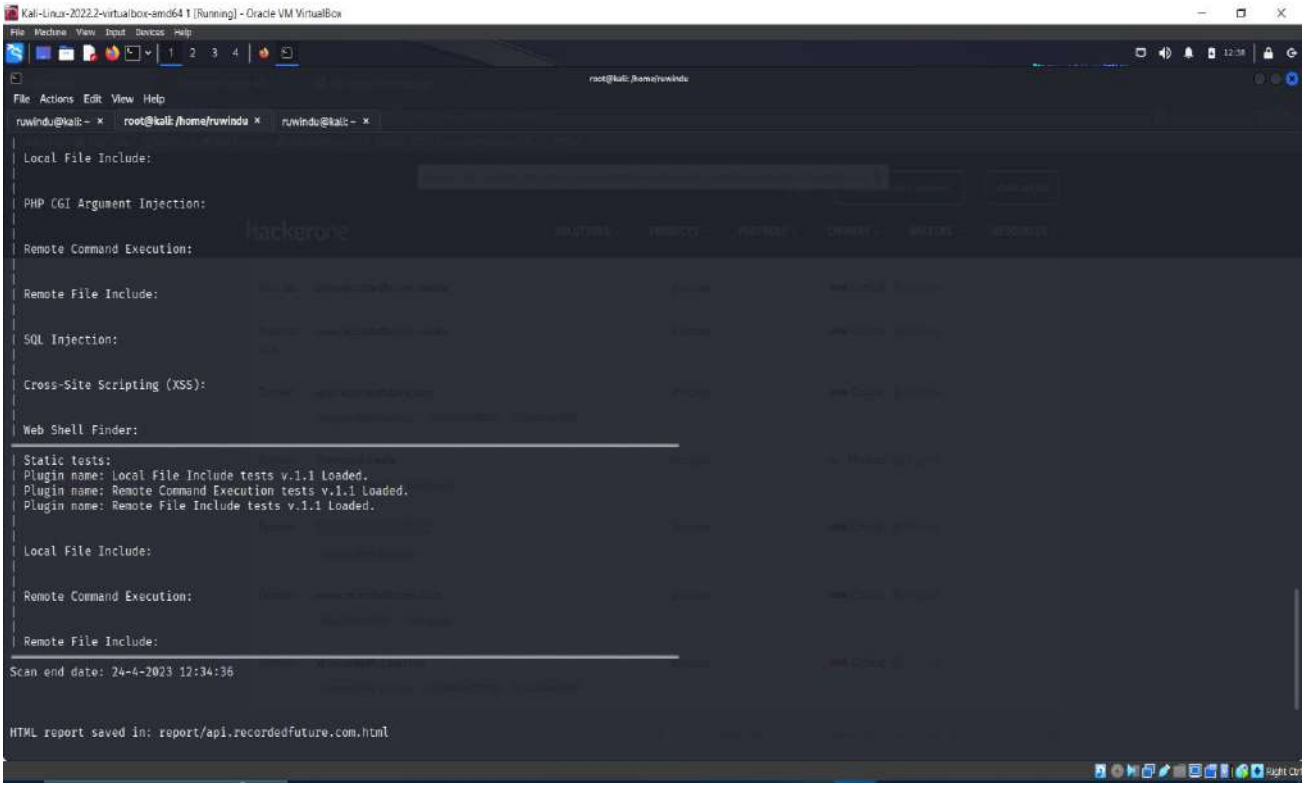
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u api.recordedfuture.com -qweds command:

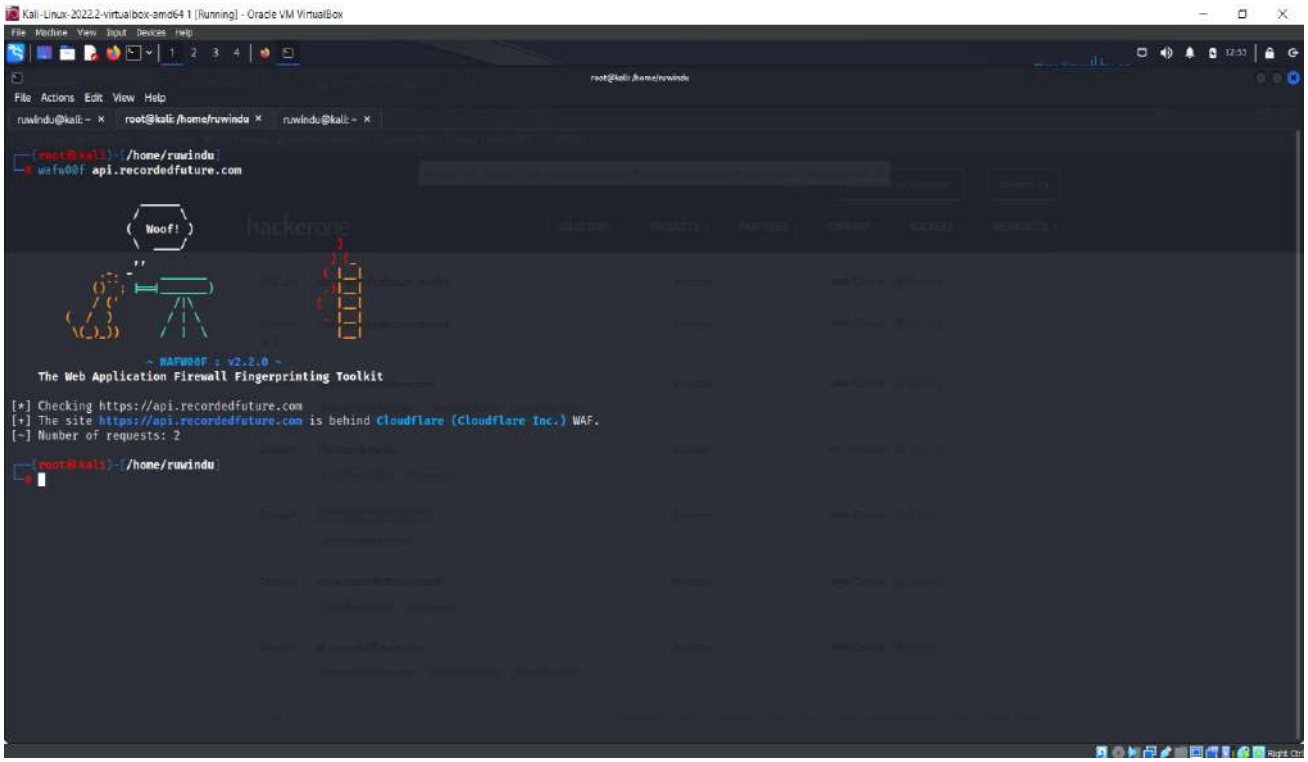



Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
ruwindu@kali: ~
root@kali: /home/ruwindu
ruwindu@kali: ~
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| [+] Crawling finished, 1 URL's found!
|
| External hosts:
|
| Timthumb:
|
| FCKeditor File Upload:
|
| Source Code Disclosure:
|
| PHPinfo() Disclosure:
|
| File Upload Forms:
|
| E-mails:
|
| Web Backdoors:
|
| Ignored Files:
|
| Dynamic tests:
| Plugin name: Learning New Directories v.1.2 Loaded.
| Plugin name: FCKedior tests v.1.1 Loaded.
| Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
| Plugin name: Find Backup Files v.1.2 Loaded.
| Plugin name: Blind SQL-injection tests v.1.3 Loaded.
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL-injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 Loaded.
| [+] 0 New directories added
|
|
| FCKeditor tests:
| Skipped because http://api.recordedfuture.com/testing123 did not return the code 404


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
ruwindu@kali: ~
root@kali: /home/ruwindu
ruwindu@kali: ~
|
| Local File Include:
|
|
| PHP CGI Argument Injection:
|
|
| Remote Command Execution:
|
|
| Remote File Include:
|
|
| SQL Injection:
|
|
| Cross-Site Scripting (XSS):
|
|
| Web Shell Finder:
|
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.
|
|
| Local File Include:
|
|
| Remote Command Execution:
|
|
| Remote File Include:
|
Scan end date: 24-4-2023 12:34:36
HTML report saved in: report/api.recordedfuture.com.html

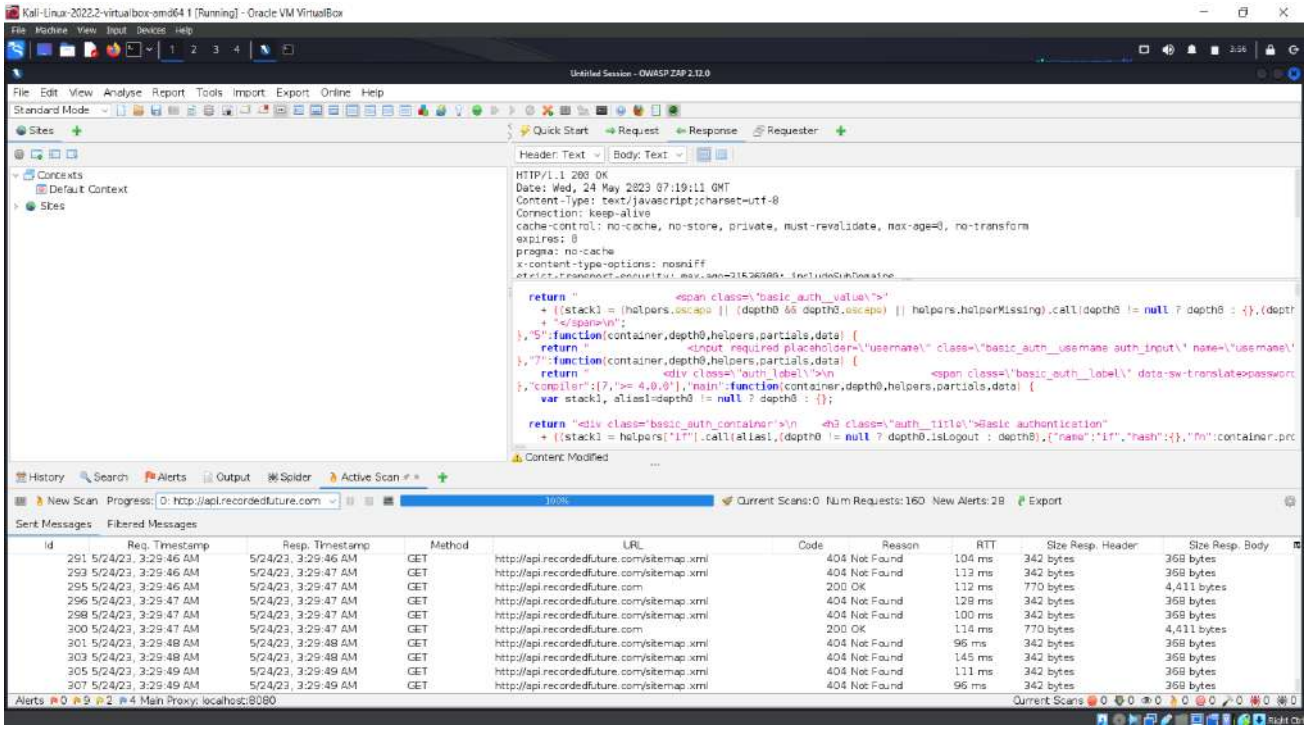
Using Wafw00f tool

When we run the wafw00f scan with the URL that we are targeting, we are able to see that the website api.recordedfuture.com seems to be protected by a web application firewall (WAF) or some other form of security solution. This is something that we are able to validate via our own direct experience. Because we had completed the scan, we were able to get this information and make the appropriate judgements.

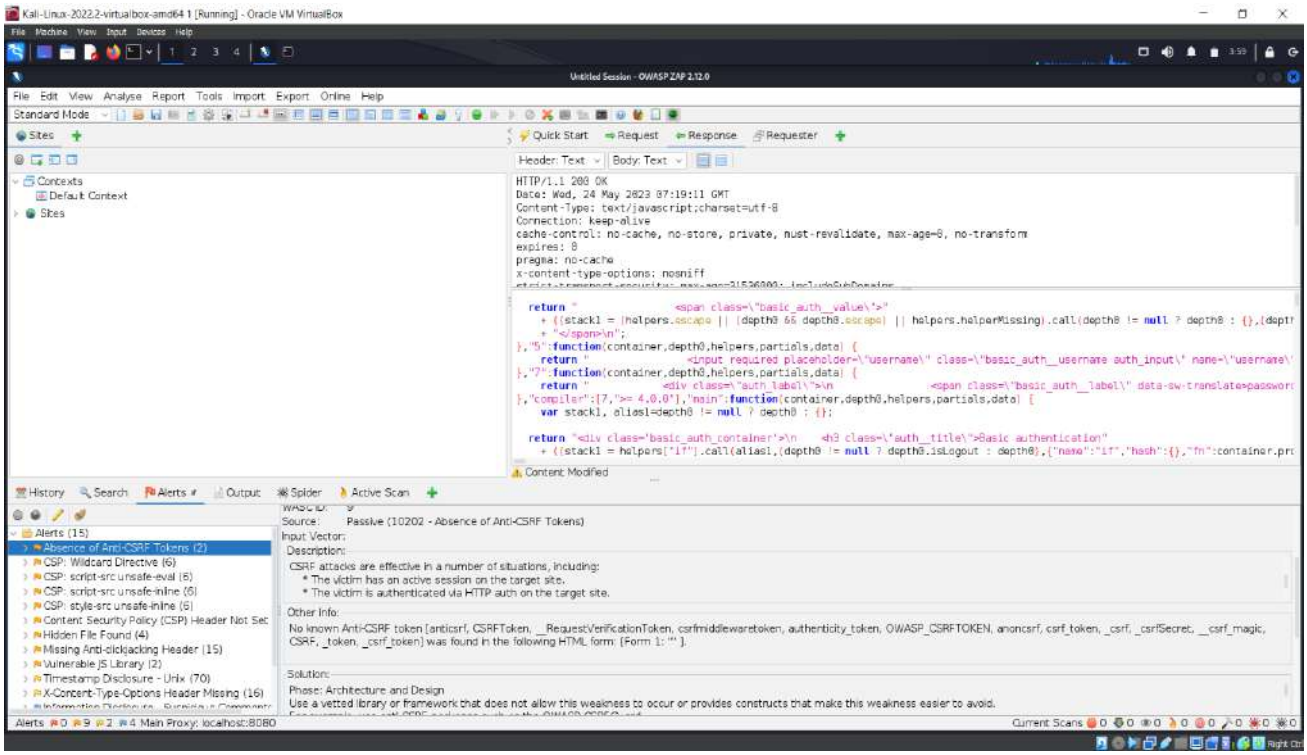


After the quick scan we found the powerful firewall in this domain.

Using OWASP-ZAP tool



Found 160 Requests.



Found 15 Alerts.

Vulnerabilities found

Absence of Anti-CSRF Tokens

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

Solution

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

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

Phase: Architecture and Design

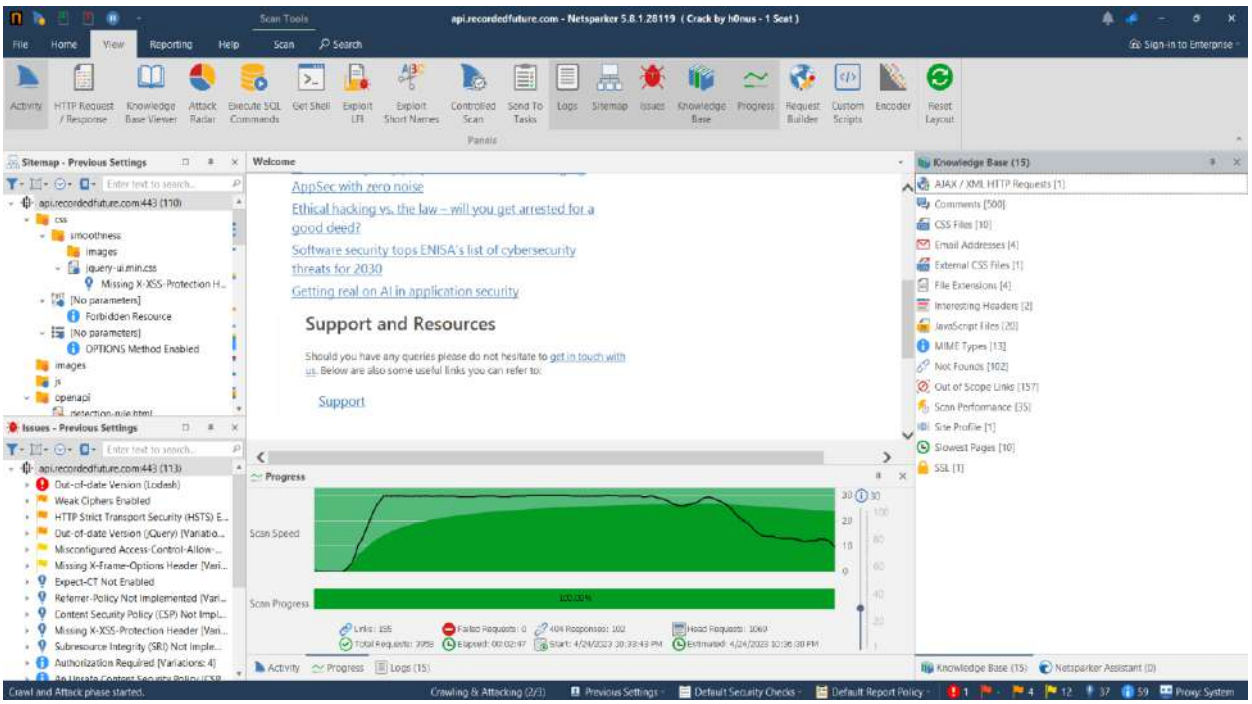
Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

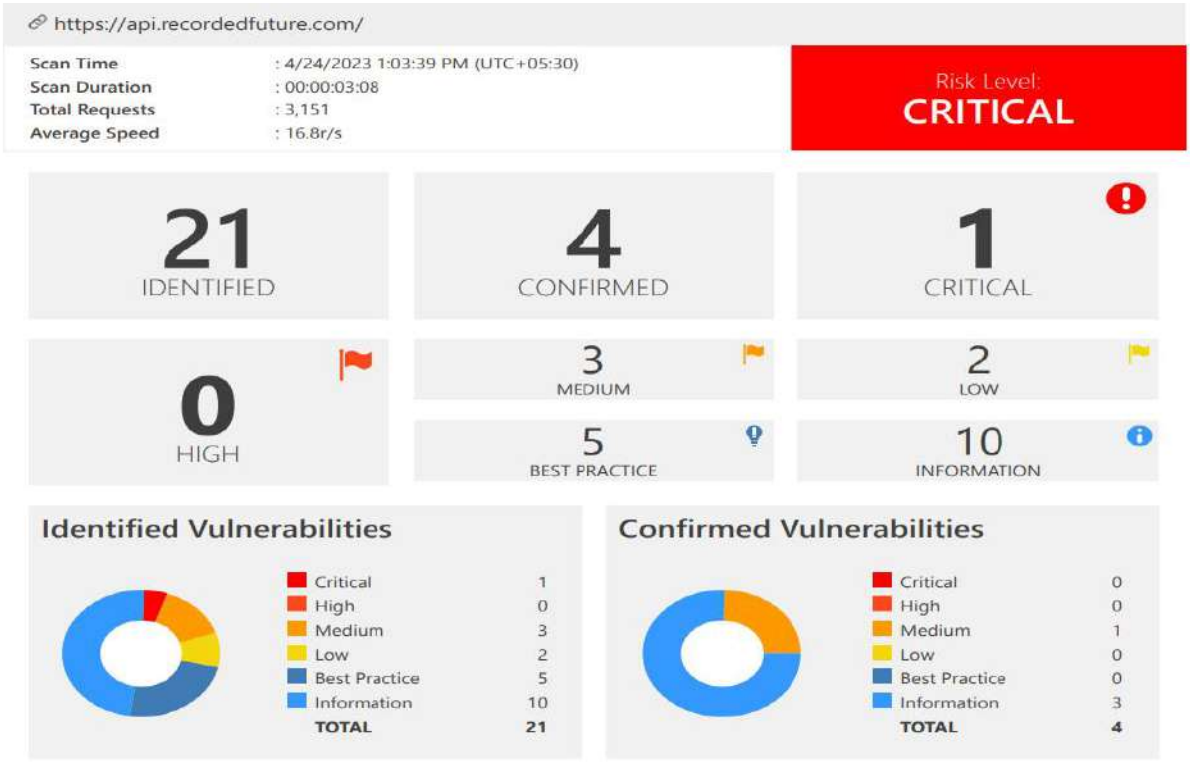
Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Using Netsparker

During the process of my Audit, I used Netsparker professional Edition (V) to aid me in doing a vulnerability check on api.recordedfuture.com. This check was carried out on the website.





After doing a scan of the domain, I was able to identify a total of 21 vulnerabilities related to the domain, including 3 vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (Lodash)	GET	https://api.recordedfuture.com/v2/	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://api.recordedfuture.com/	
	Out-of-date Version (jQuery)	GET	https://api.recordedfuture.com/v2/lib/jquery-1.8.0.min.js	
	Weak Ciphers Enabled	GET	https://api.recordedfuture.com/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://api.recordedfuture.com/v2/api-docs/swagger.json	URI-BASED
	Missing X-Frame-Options Header	GET	https://api.recordedfuture.com/v2/lib/	
	Content Security Policy (CSP) Not Implemented	GET	https://api.recordedfuture.com/links	
	Expect-CT Not Enabled	GET	https://api.recordedfuture.com/	
	Missing X-XSS-Protection Header	GET	https://api.recordedfuture.com/css/smoothness/jquery-ui.min.css	
	Referrer-Policy Not Implemented	GET	https://api.recordedfuture.com/v2/lib/	
	Subresource Integrity (SRI) Not Implemented	GET	https://api.recordedfuture.com/index.html?nsextt=%0d%0ans%3anetsparker056650%3dvuln	nsextt
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://api.recordedfuture.com/v2/lib/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://api.recordedfuture.com/v2/lib/	
	default-src Used in Content Security Policy (CSP)	GET	https://api.recordedfuture.com/v2/lib/	

api.recordedfuture.com has been found to have the following identified vulnerabilities:

Identified vulnerabilities in api.recordedfuture.com

<u>Vulnerability 02</u> - Out-of-date Version (Lodash) - Critical Vulnerability

It was established that the target website was making use of Lodash, but the creator is no longer providing maintenance for it, according to the findings of Netsparker.

Impact

Because this particular application is an older version of the program, it is possible for it to be susceptible to attacks because it is an older version of the program.
Lodash Improperly Controlled Modification of Object **Prototype Attributes (**Prototype Pollution') Vulnerability
Prototype pollution attack when using _.zipObjectDeep in lodash before 4.17.20.
Affected Versions
0.1.0 to 4.17.19

Request

```
GET /v2/ HTTP/1.1
Host: api.recordedfuture.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Referer: https://api.recordedfuture.com/index.html
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 385.3764 Total Bytes Received : 8868 Body Length : 8098 Is Compressed : No

```
HTTP/1.1 200 OK
expires: 0
x-content-type-options: nosniff
Server: cloudflare
CF-Cache-Status: DYNAMIC
Connection: keep-alive
content-security-policy: default-src 'self' data:; img-src 'self' https: data:; script-src 'self' 'unsa
fe-inline' 'unsafe-eval' cdn.jsdelivr.net; style-src 'self' 'unsafe-inline' fonts.googleapis.com cdn.js
delivr.net; font-src 'self' fonts.gstatic.com; worker-src blob:;
Content-Length: 8098
last-modified: Thu, 20 Apr 2023 06:37:42 GMT
strict-transport-security: max-age=31536000; includeSubDomains
accept-ranges: bytes
pragma: no-cache
CF-RAY: 7bcca91e8bfa7f11-CMB
Content-Type: text/html;charset=utf-8
Date: Mon, 24 Apr 2023 07:33:53 GMT
cache-control: no-cache, no-store, private, must-revalidate, max-age=0, no-transform

<!DOCTYPE html>
<html>
<head>
<title>Recorded Future Connect API</title>
<link rel="icon" sizes="16x16" href="images/favicon-16.png" type="image/png">
<link rel="icon" sizes="32x32" href="images/favicon-32.png" type="image/png">
<link rel="icon" sizes="96x96" href="images/favicon-96.png" type="image/png">

<link href="css/fonts.css" rel="stylesheet">
<link href='css/typography.css' media='screen' rel='stylesheet' type='text/css'/>
<link href="css/hightlight.default.css" media="screen,print" rel="stylesheet" type="text/css"/>
<link href="css/reset.css" media="screen,print" rel="stylesheet" type="text/css"/>
<link href="css/screen.css" media="screen,print" rel="stylesheet" type="text/css"/>
<link href="css/rf.css" media="screen,print" rel="stylesheet" type="text/css"/>
<link href="css/selectize.css" rel="stylesheet" type="text/css"/>

<script src='lib/object-assign-pollyfill.js' type='text/javascript'></script>
<script src='lib/jquery-1.8.0.min.js' type='text/javascript'></script>
<script src='lib/jquery.slideto.min.js' type='text/javascript'></script>
<script src='lib/jquery.wiggle.min.js' type='text/javascript'></script>
<script src='lib/jquery.ba-bbq.min.js' type='text/javascrip
_
```

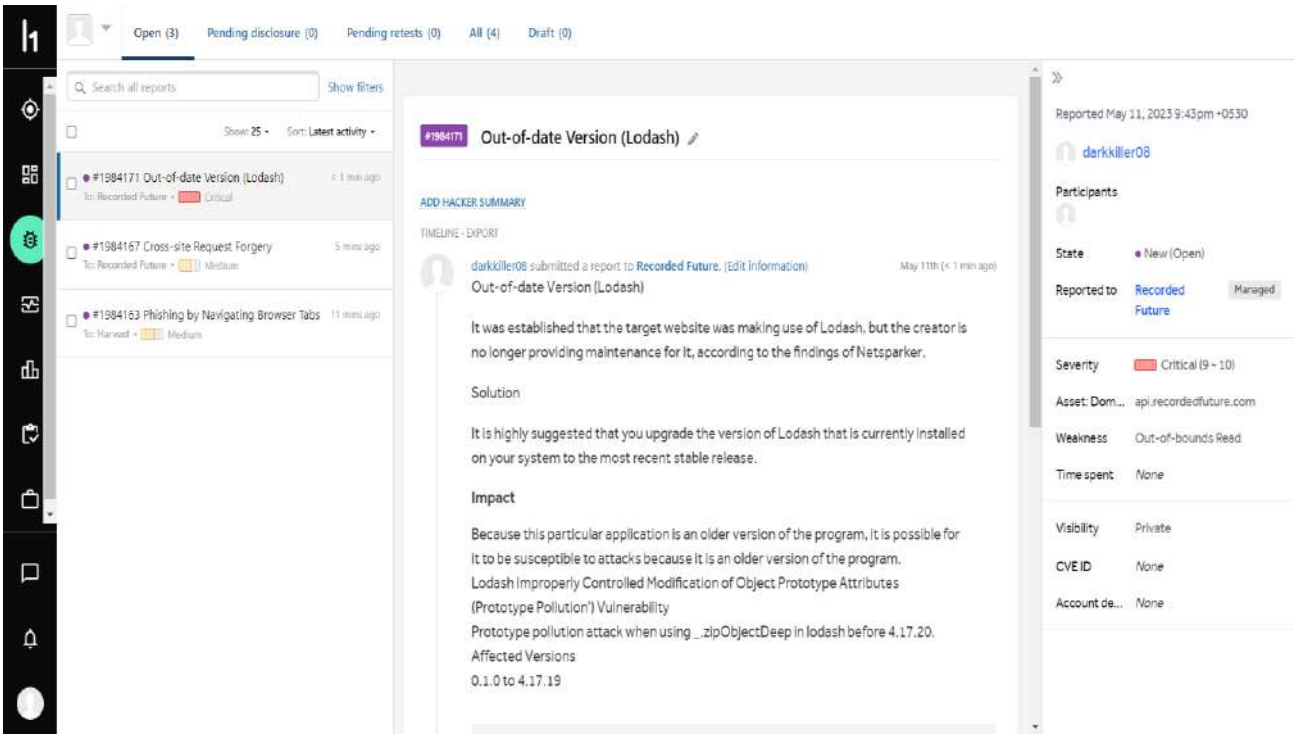
Solution

It is highly suggested that you upgrade the version of Lodash that is currently installed on your system to the most recent stable release.

Conclusion of the Report 02

For the purpose of to ensure the accuracy of this report, we choose to investigate and validate the recorded future bug bounty plan. In order to assess whether or not we were effective in discovering an issue in the programme, our primary objective was to determine whether or not we did so. Following that, we made an effort to compile information not only about the technologies, but also regarding the IP addresses, the subdomains, and a few other locations. Following the completion of the site content scan, we moved on to the vulnerability analysis. We were able to determine 21 distinct categories of critical flaws in the system by using a tool called a netsparker. We came to the conclusion that the possible risk created by collaborations with third-party organisations should be the primary focus of our investigation. In the end, we were able to get an understanding of precisely what this susceptibility entails, as well as the unfavourable circumstances that may contribute to it as well as the potential remedies to this problem.

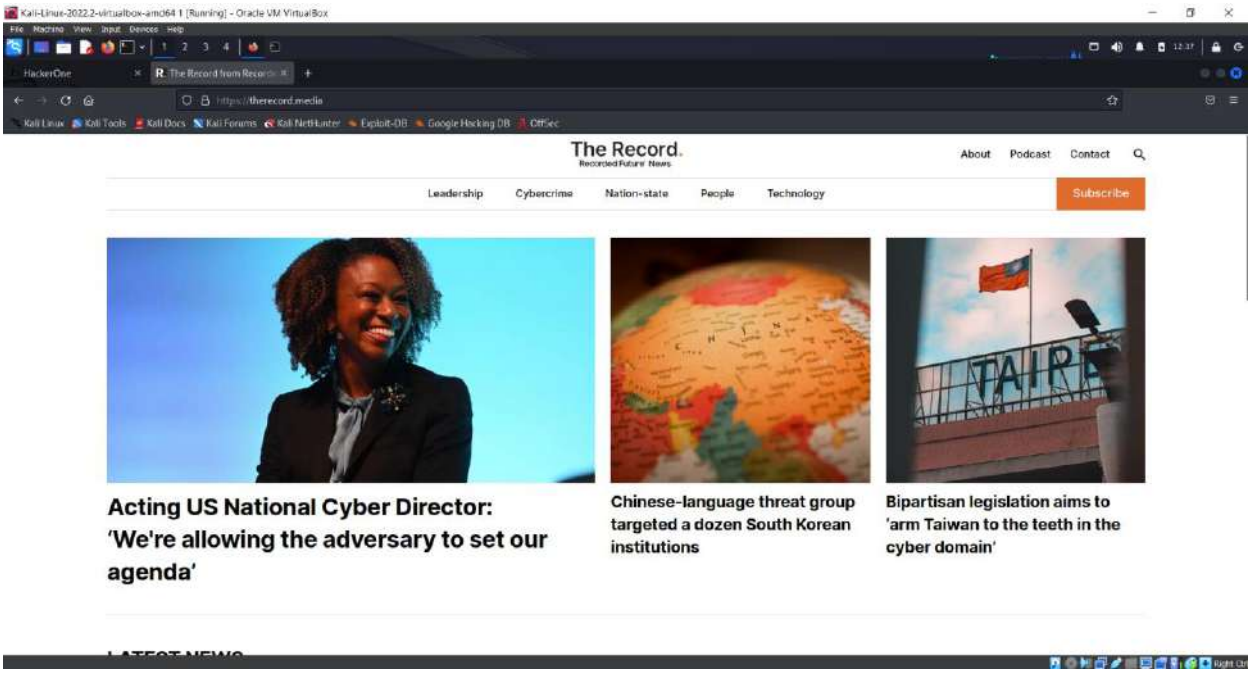
HackerOne Submitted Report Screenshot

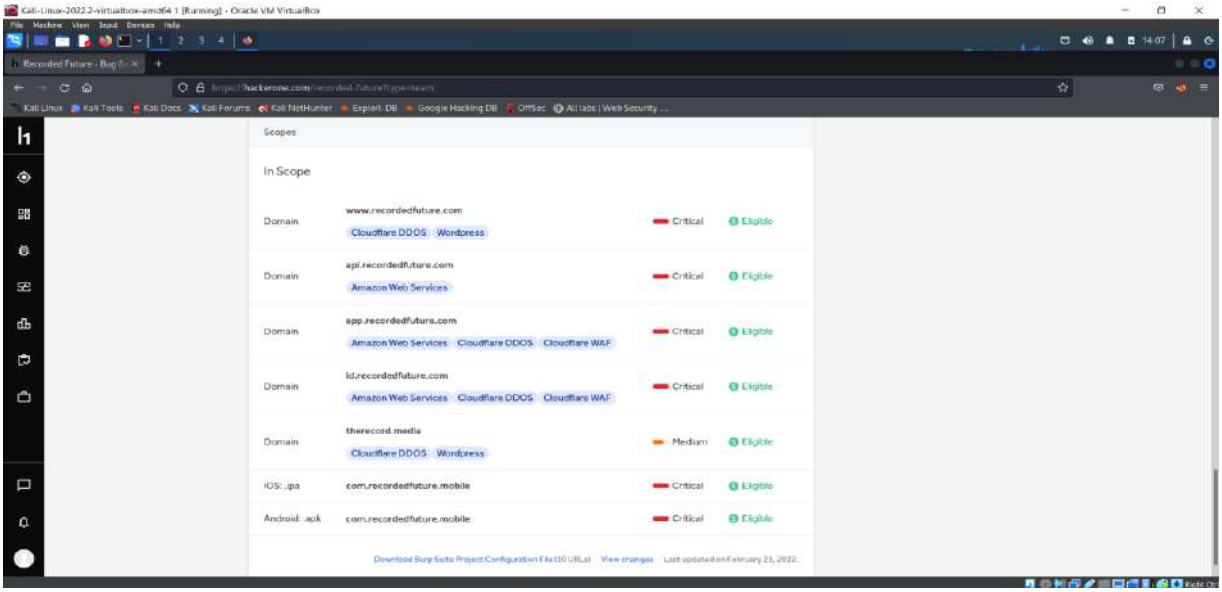


iii. Report 03

Target information: therecord.media

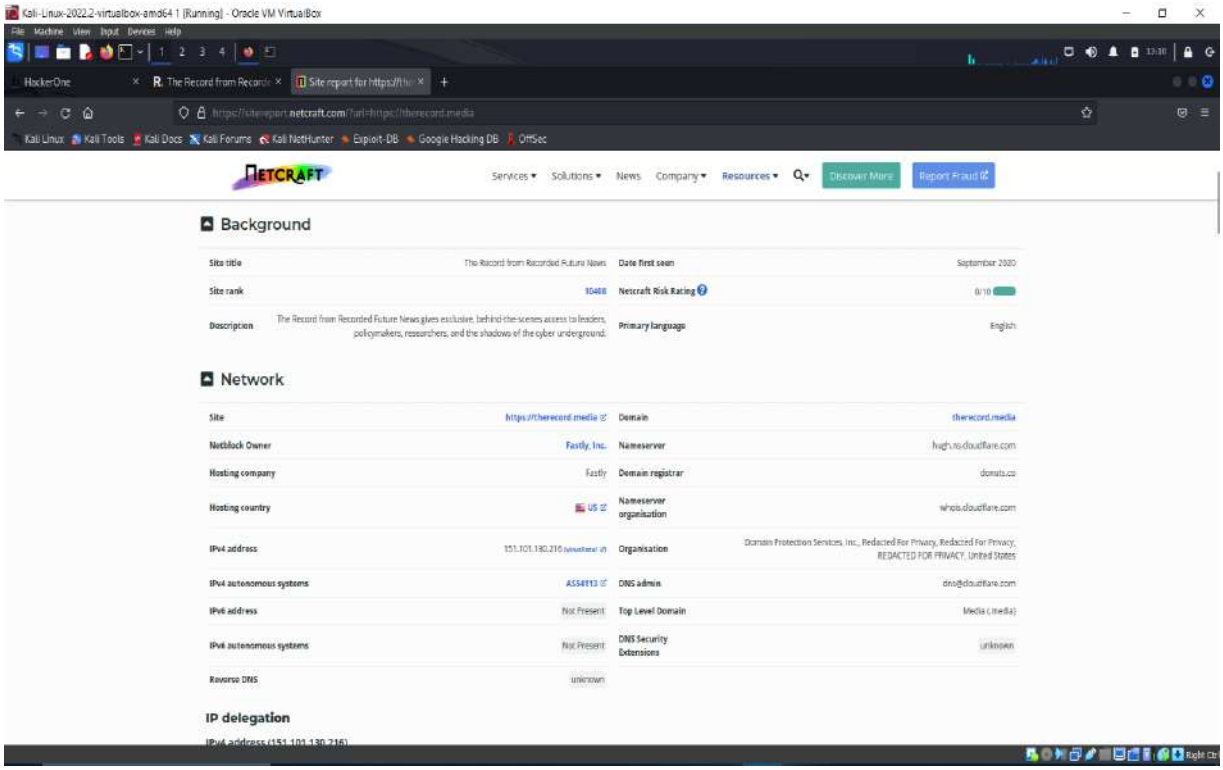
The purpose of this study is to determine whether vulnerabilities exist in the target domain (therecord.media) and the amount of risk that is associated with each of those vulnerabilities. The primary purpose of the evaluation is to identify any areas of the target domain that need improvement.

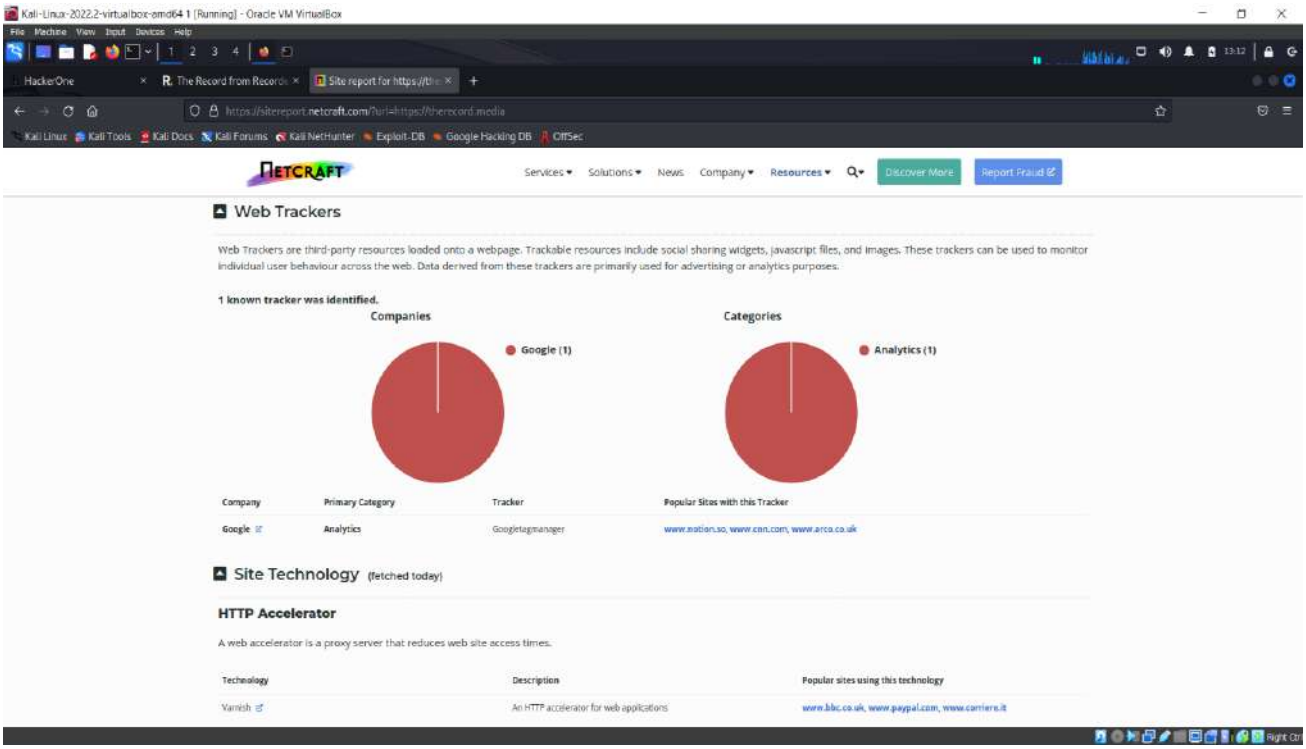


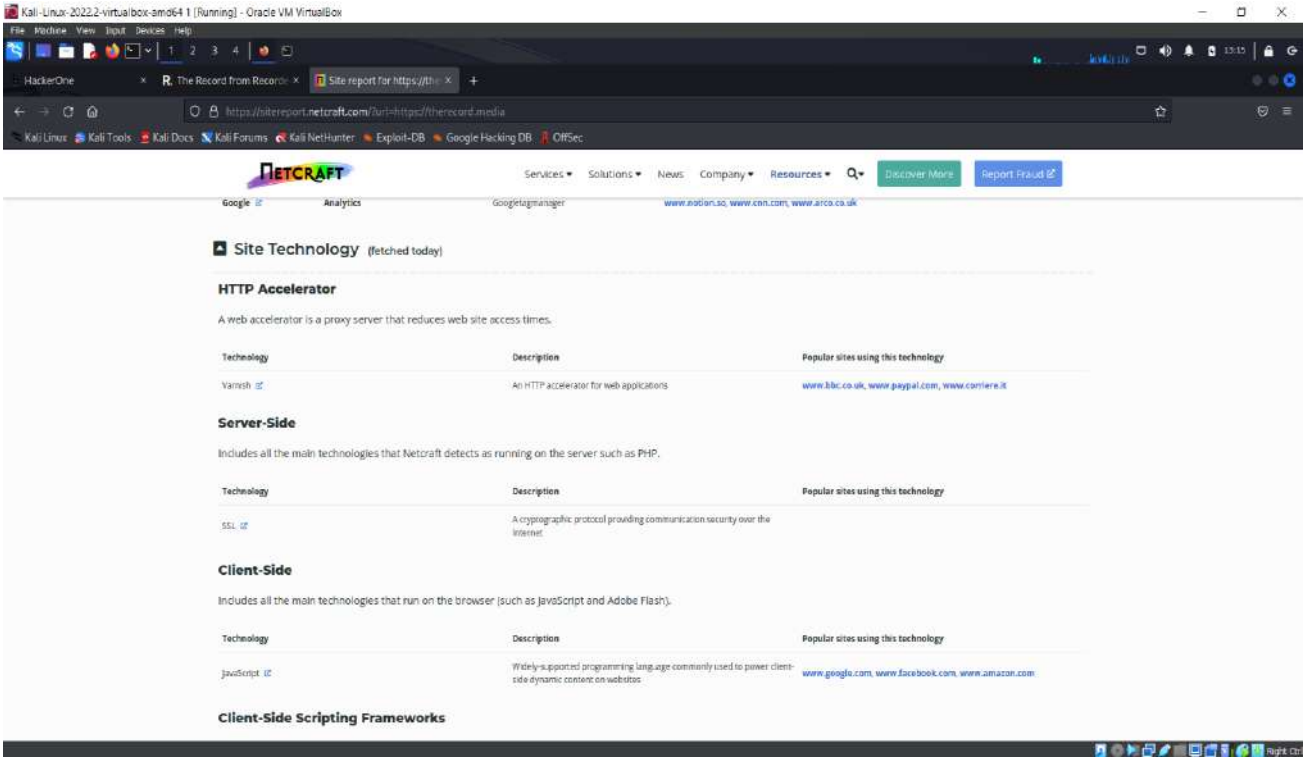


Information Gathering For Target Domain

Let's have a look at the many different options that are available to us so that we can get information not only about the technological capabilities of therecord.media but also about other facts that are pertinent to the situation. Let's put in our domain and perform some research on the information that can be gained by solely utilizing Netcraft for the time being since it is the only tool we have access to right now. Since we are only using Netcraft at the moment, let's type in our domain and examine the information that can be gained by using Netcraft. There are a number of programs and websites that are capable of performing this, but since we are only using Netcraft at the moment, let's study the information that can be obtained by using Netcraft.

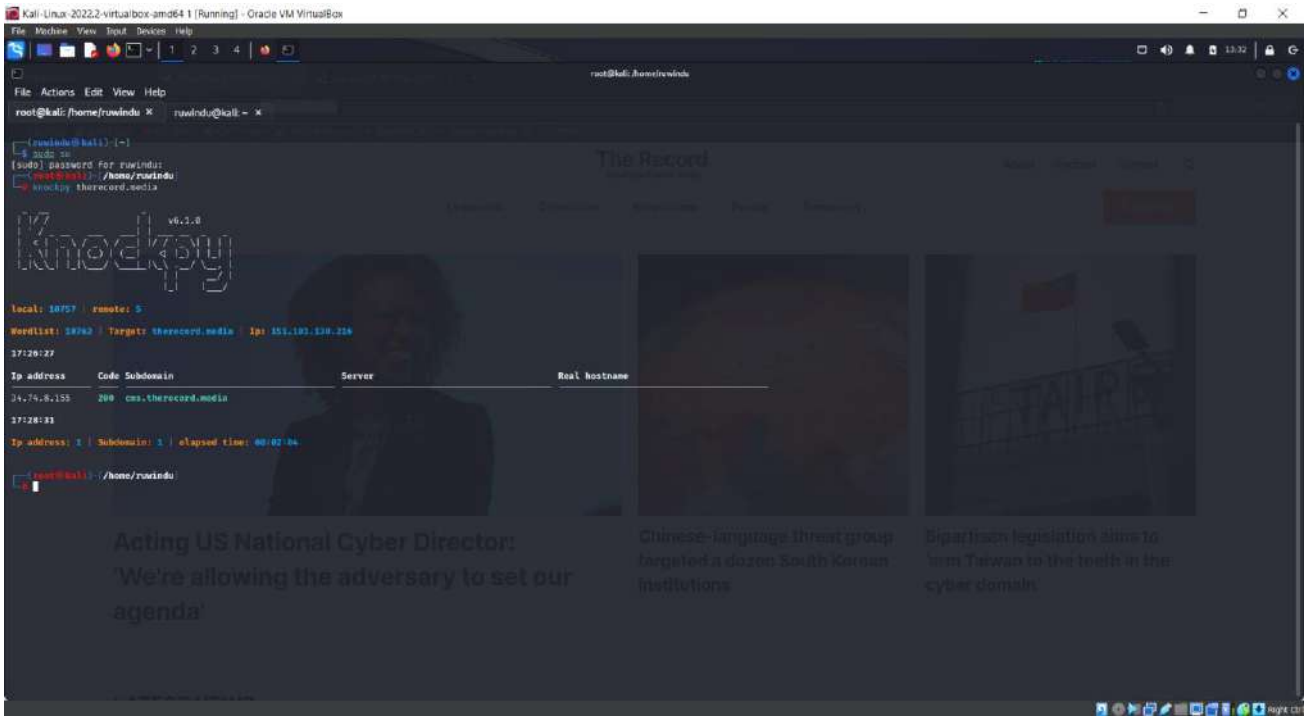



Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
Web Trackers
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.
1 known tracker was identified.
Companies
Google (1)
Categories
Analytics (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Google
Analytics
Googletagmanager
www.notion.so, www.cnn.com, www.arco.co.uk
Site Technology (fetched today)
HTTP Accelerator
A web accelerator is a proxy server that reduces web site access times.
Technology
Description
Popular sites using this technology
Varnish
An HTTP accelerator for web applications
www.bbc.co.uk, www.paypal.com, www.corriere.it


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
Site Technology (fetched today)
HTTP Accelerator
A web accelerator is a proxy server that reduces web site access times.
Technology
Description
Popular sites using this technology
Varnish
An HTTP accelerator for web applications
www.bbc.co.uk, www.paypal.com, www.corriere.it
Server-Side
Includes all the main technologies that Netcraft detects as running on the server such as PHP.
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).
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites
www.google.com, www.facebook.com, www.amazon.com
Client-Side Scripting Frameworks

Using knockpy tool

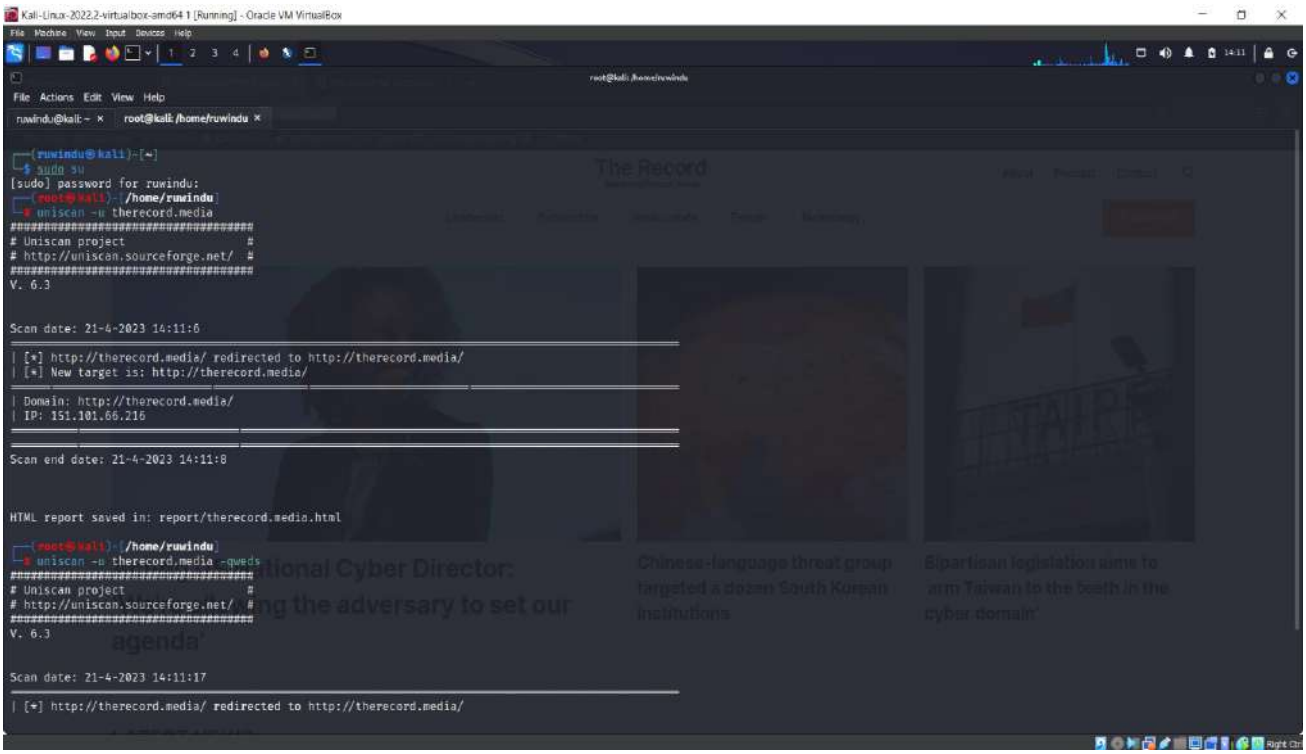
In order for us to get to the bottom of what has really taken place here, we are going to need to do a subdomain scanning using software that has been developed specifically for the purpose of carrying out a work such as this one. Only then will we be able to find out the truth about what has happened. After then, and only then, will we be able to get to the bottom of what really took place. After that — and only after that — will we be able to get answers to each and every one of the questions that we now have. The first thing that we do is run knockpy on a few different domains, and after that is complete, we examine the output to determine the various kinds of findings that it provides. Next that, we will proceed to the next stage. After we have completed this level, we will go to the next one. Going ahead, we will now go on to the subsequent stage of the treatment that has been planned.



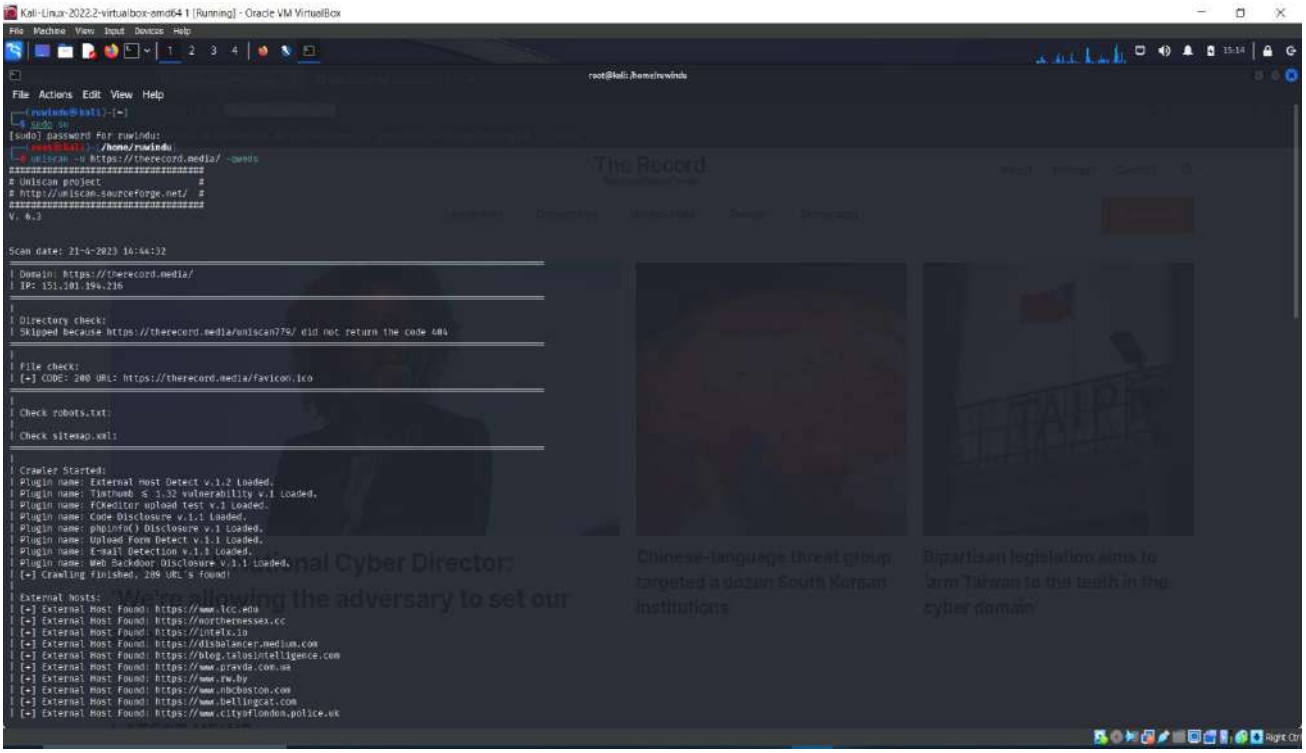
After the enumeration of the subdomains has been completed, we are able to see therecord.media's subdomains in this manner thanks to the recording of the subdomains. It should come as no surprise that all of the subdomains that are included under the therecord.media domain make use of the same IP address and name server. Because of the real hostname that is shown, we are able to determine that this is a mobile application. Consequently, we are able to utilize it. Let's have a look at the results of the inquiry that we conducted into the domain, shall we?

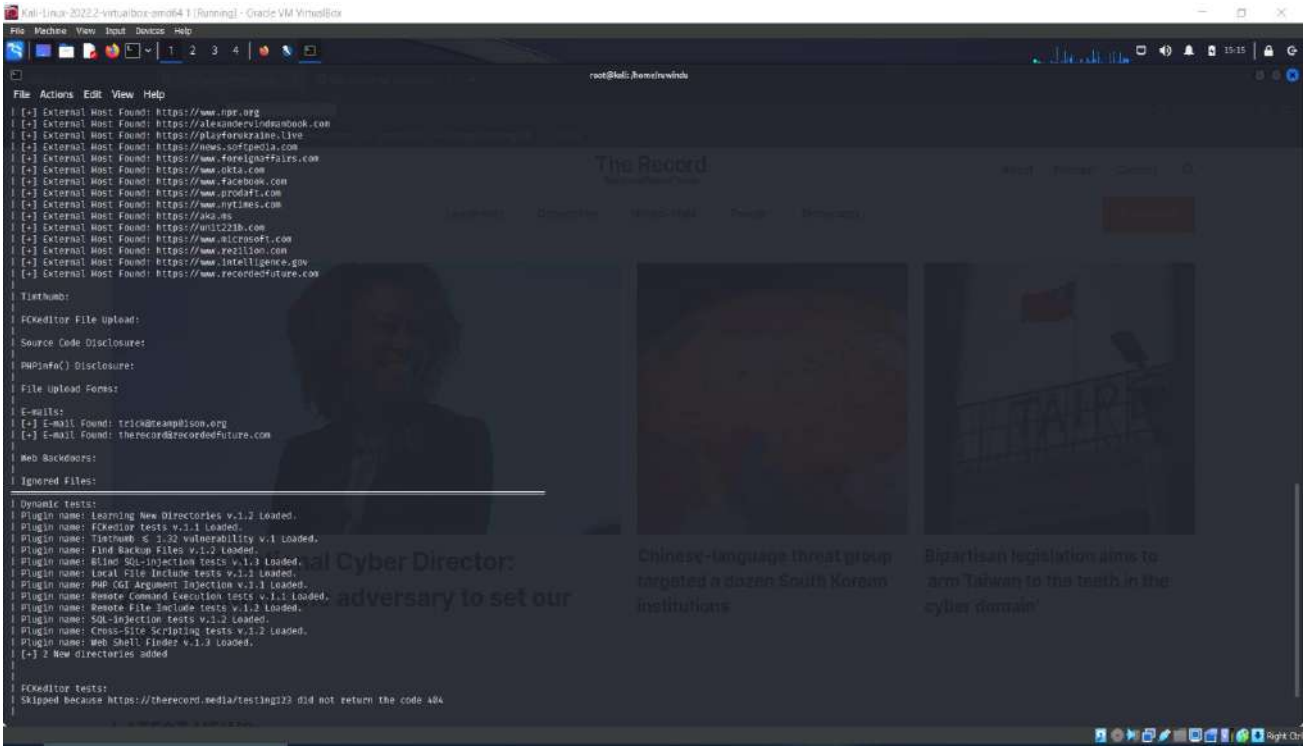
Using Uniscan tool

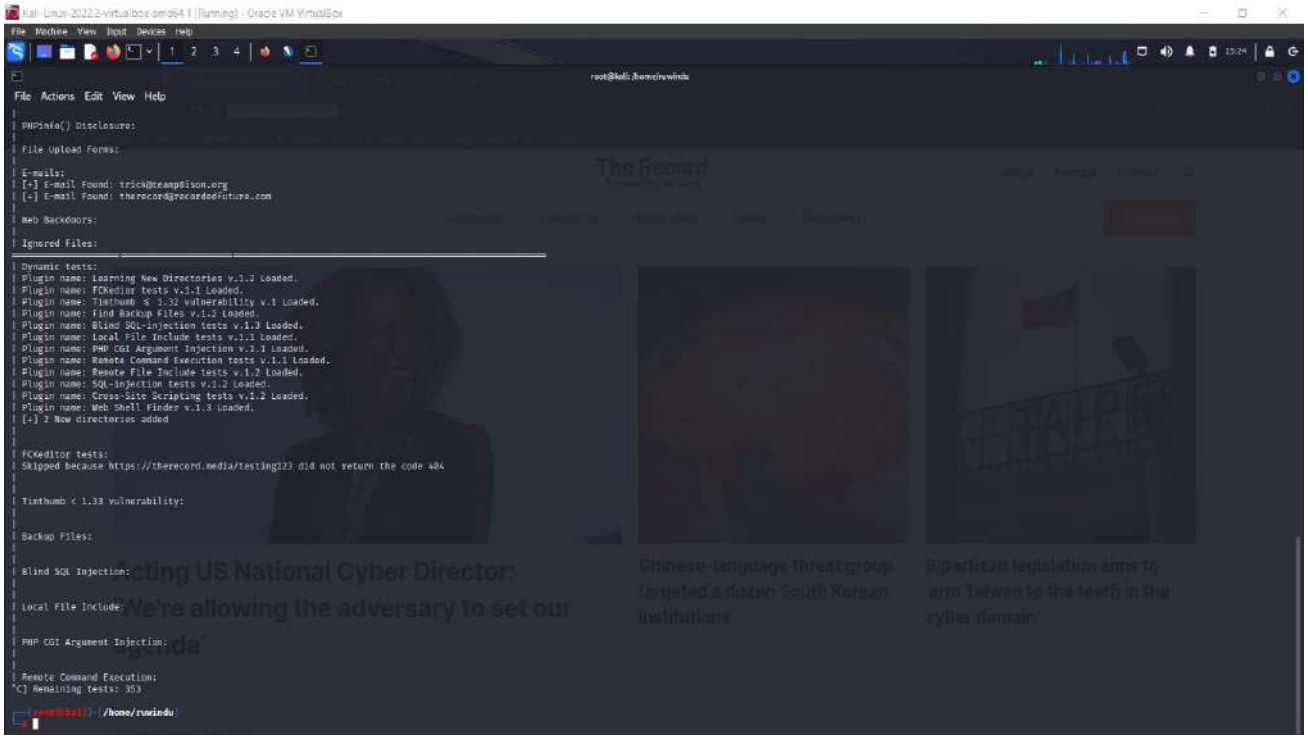
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u www.semrush.com -qweds command:

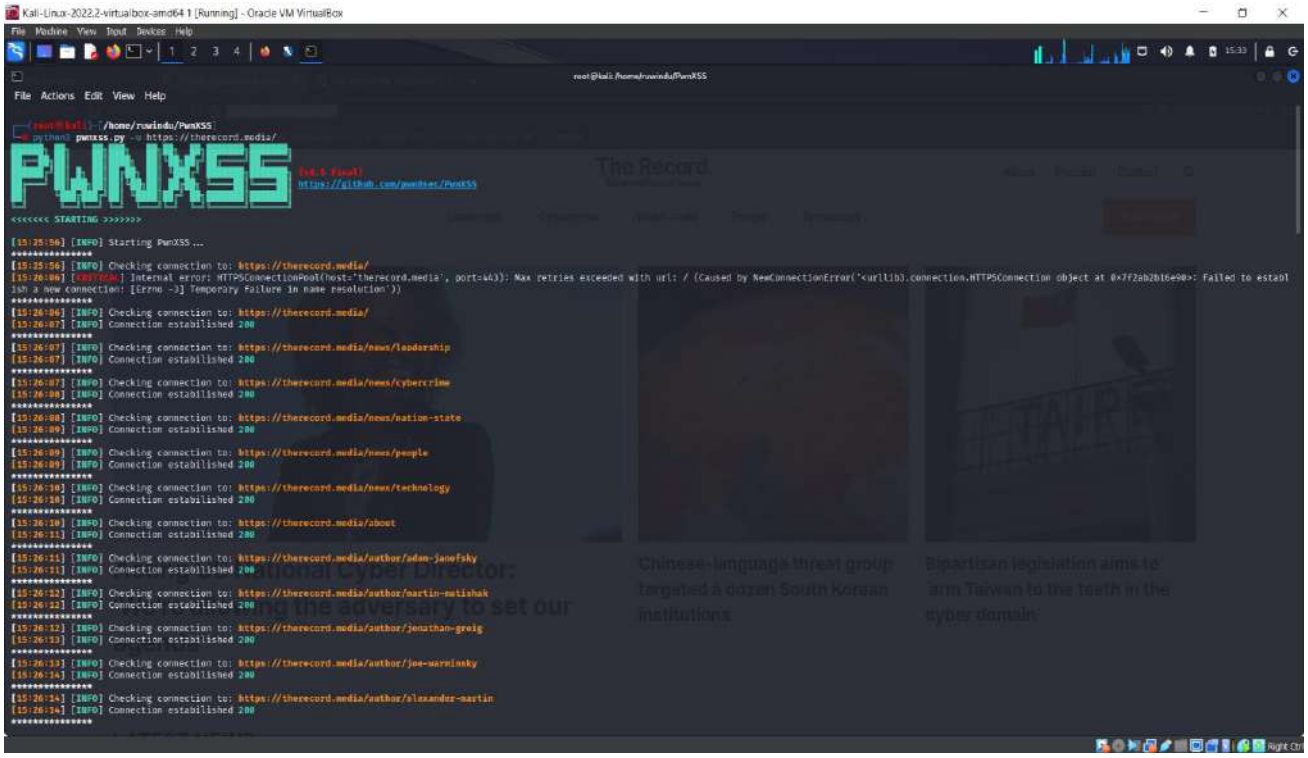


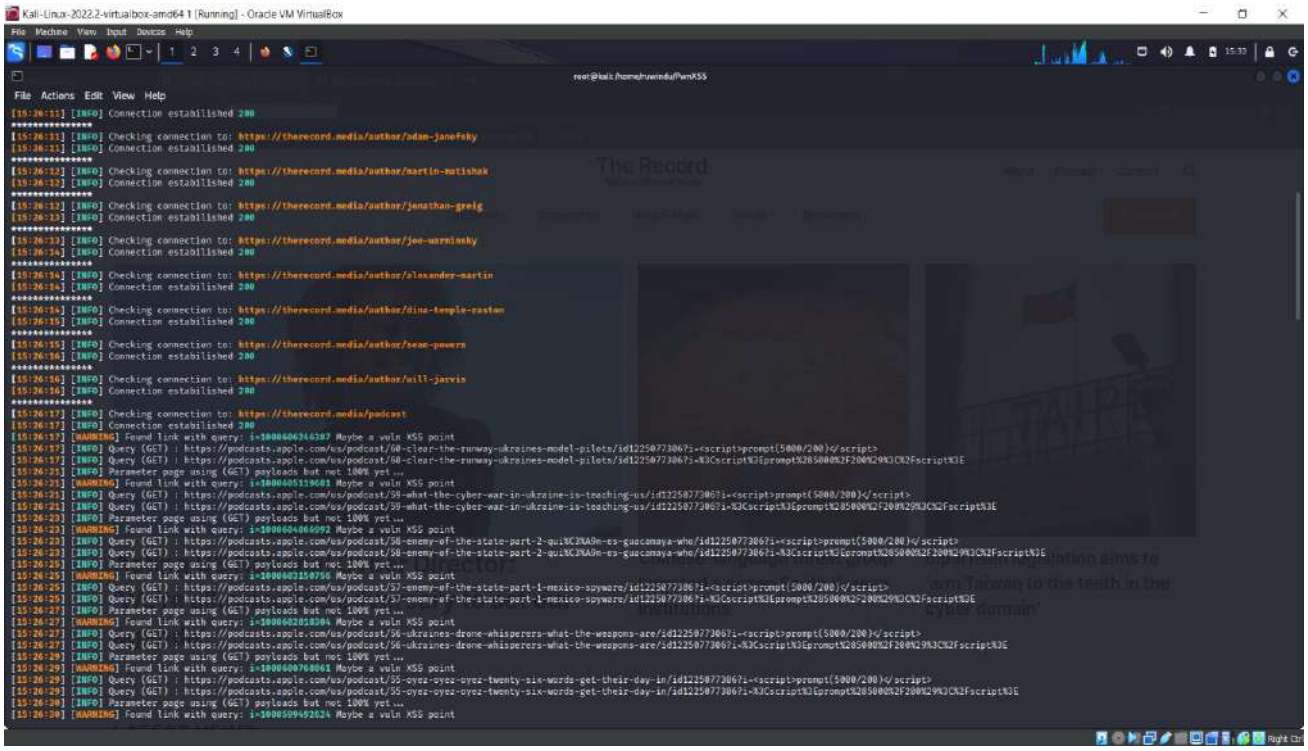


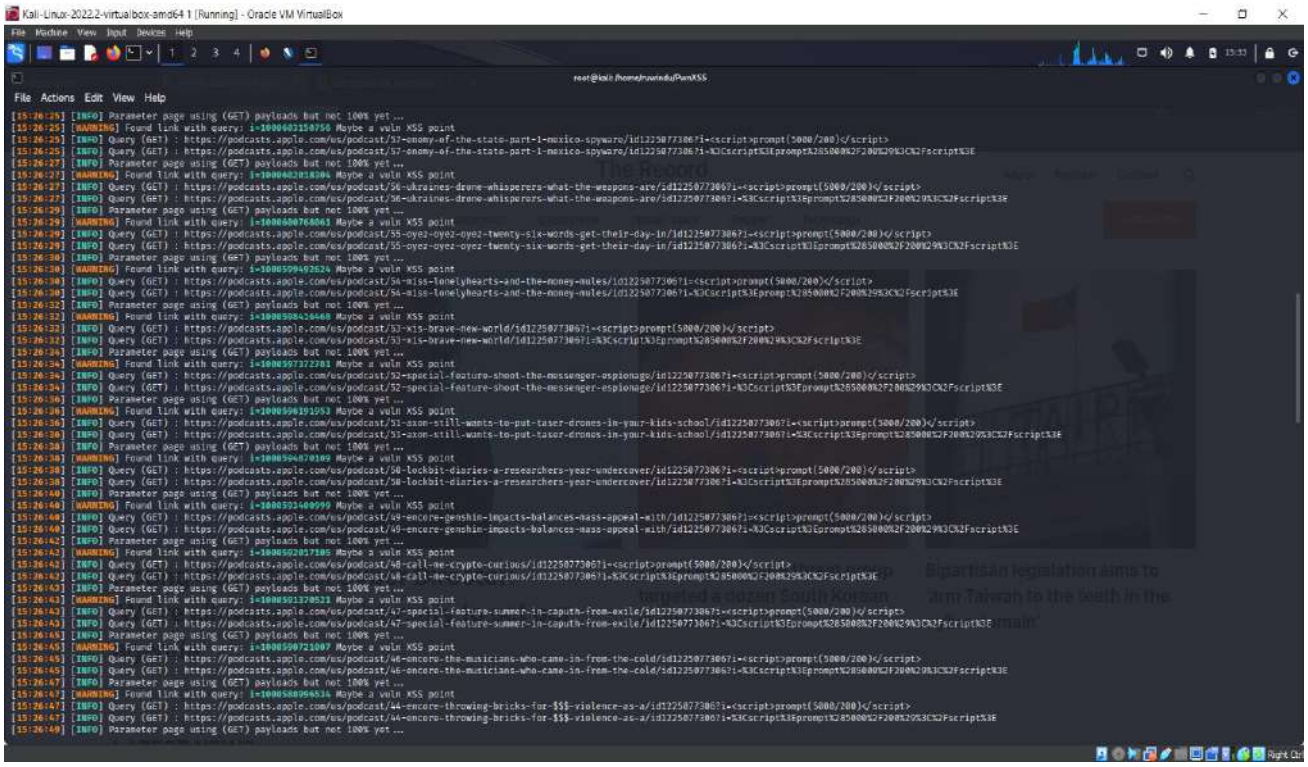


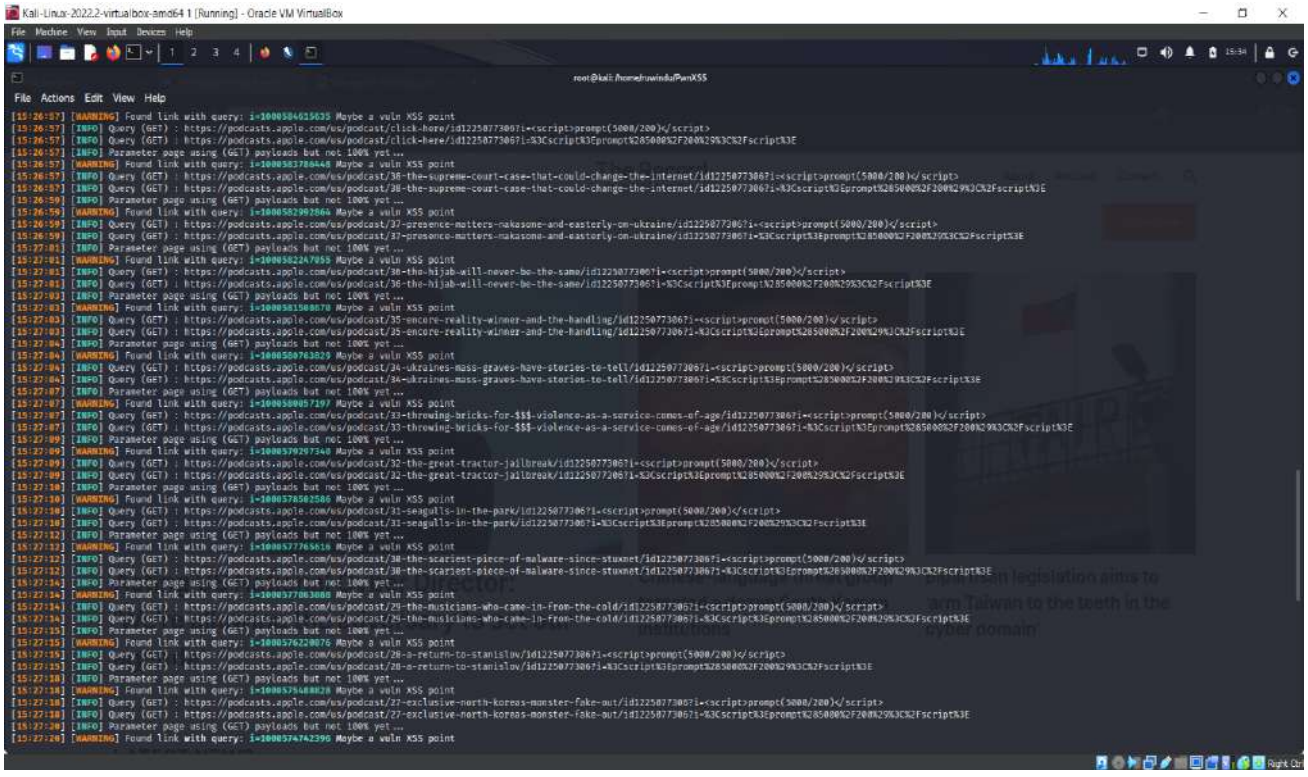
We were able to learn some of the information that was held by third parties by navigating to this region of the website, which is why it is referred to as the third-party sector of the website. During the course of this investigation, a number of web addresses, also known as universal resource locators (URLs), were uncovered.

Using PwnXSS tool



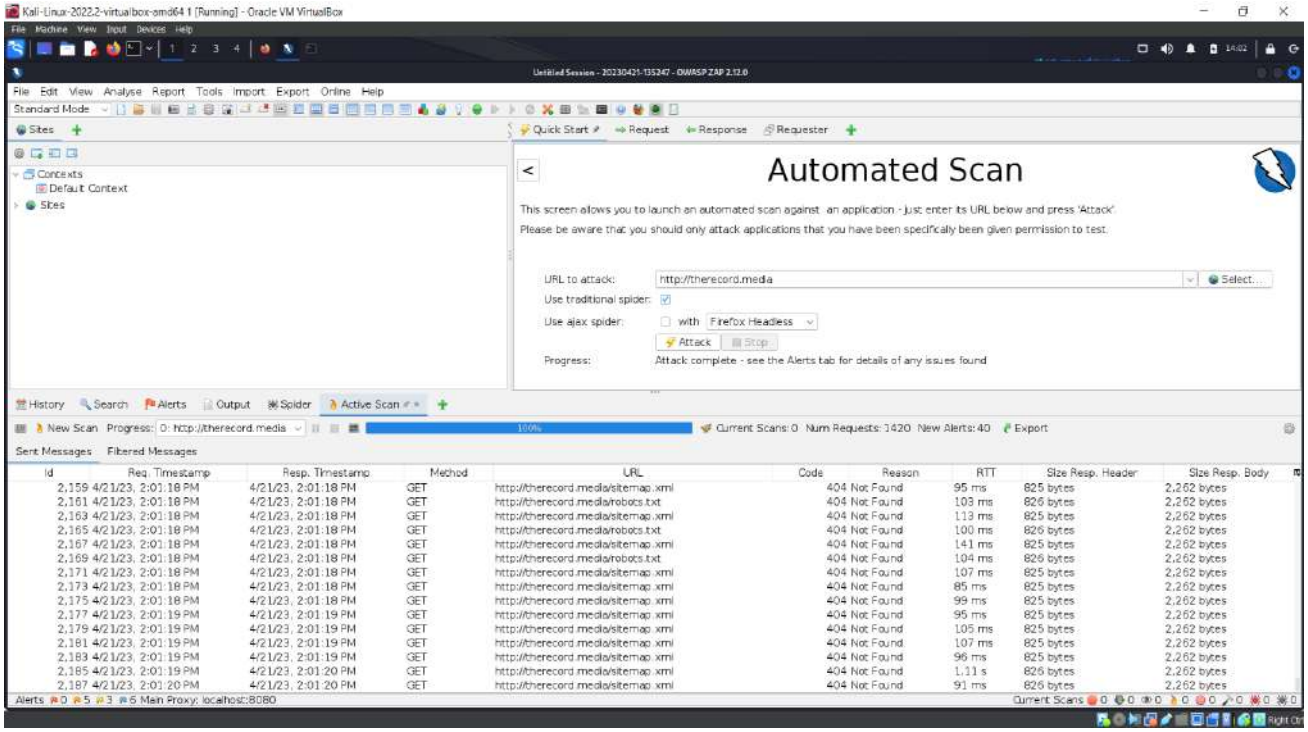






Both scans are PwnXss. Found them. https://therecord.media contains several unknown XSS vulnerabilities. Hackers might steal visitor data using these vulnerabilities.The new list contains open XSS vulnerabilities not covered in the presentation. Two helped. Payloads lack critical components, making exploitation difficult.

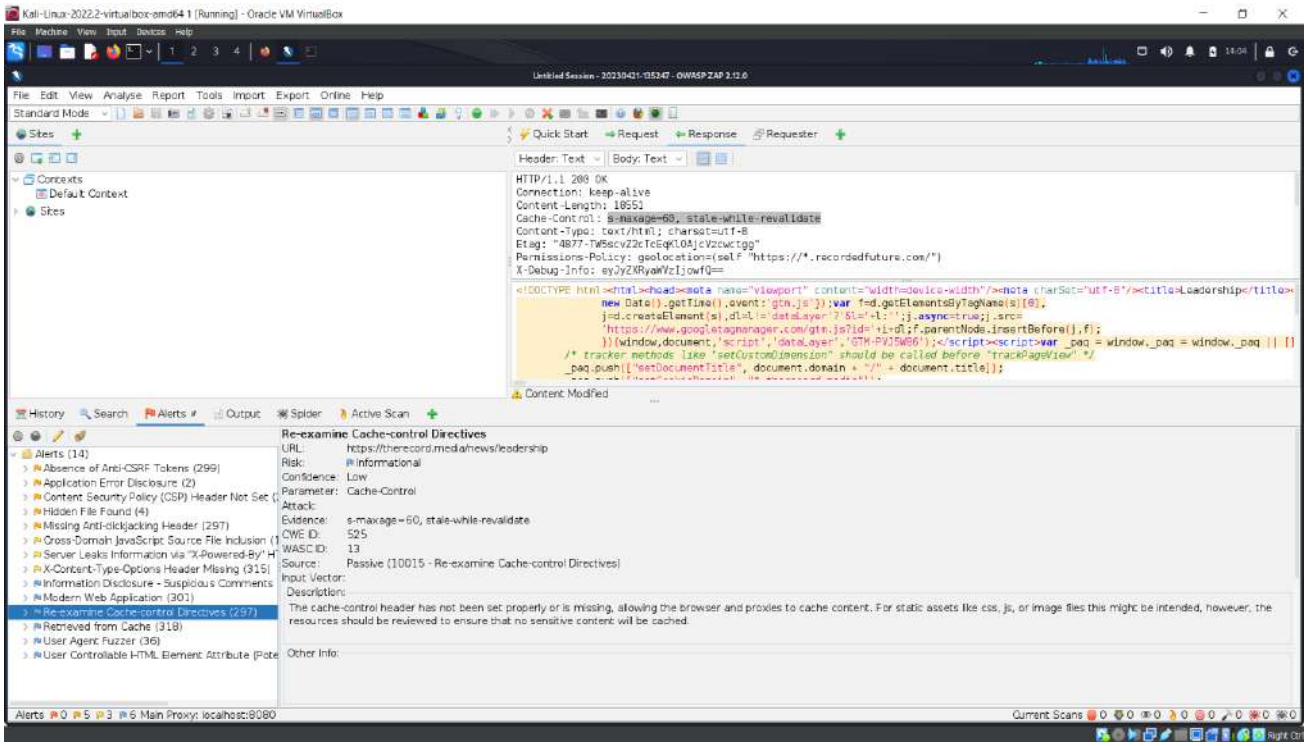
Using OWASP-ZAP tool



Found 1420 URLS.

On the main page of the tool, the websites that you are targeting will be shown on the left side, and you will be able to attack websites by supplying the URL of the website that you wish to target on the right side. This point of view is the single most important component in order to make efficient use of the instrument. You will also be able to check the effects of your assault based on your scan at the very bottom of the screen. These findings will be determined by what you scanned into your computer. When we get to this part of the map, we may choose "active scan" from the menu that pops up when we click on the green plus symbol.

When we have completed the procedure, our website will be shown on the far left of the screen. If we choose it with our mouse, then we will be able to see the outcomes. By choosing the alert tab, which is located at the very bottom of the window, we are able to see information that is of the highest significance to us. You will be given the opportunity to see a list of all of the vulnerabilities that have been detected inside that region. This list will be made available to you. If we choose one of these, we will be presented with further details on the specific vulnerability that we have chosen to investigate further.



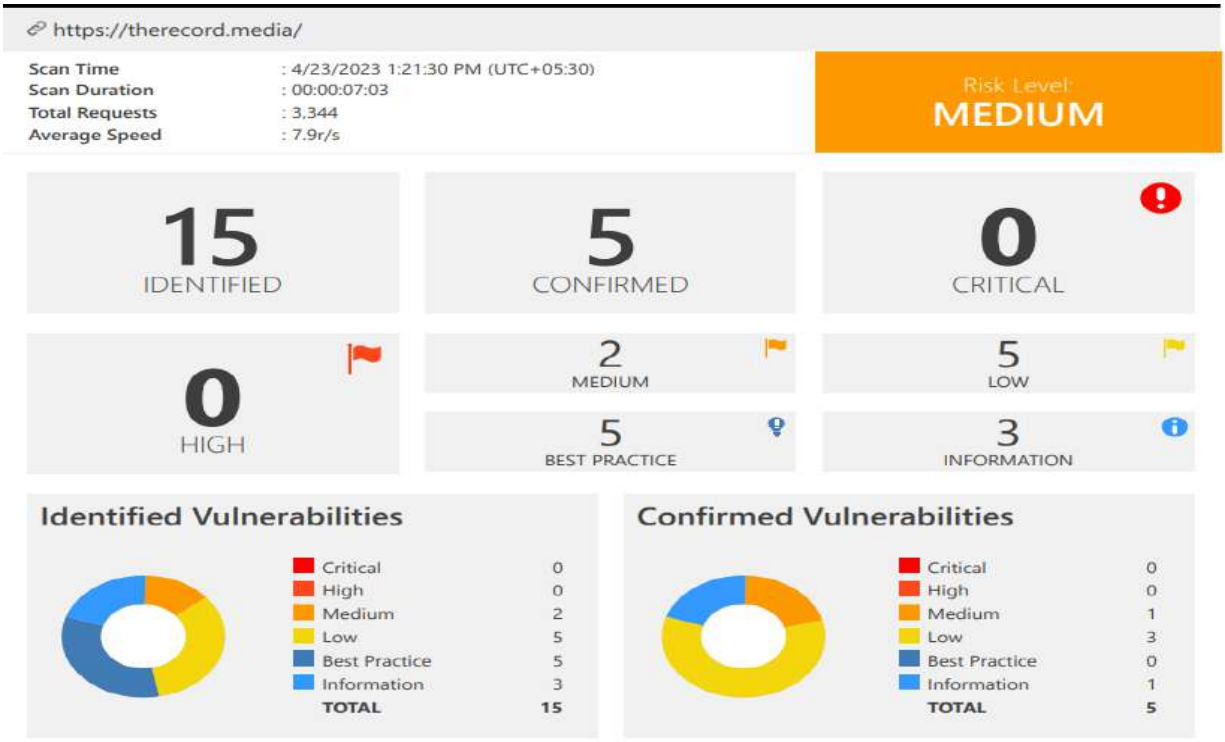
Found 23 Alerts.

Vulnerabilities found

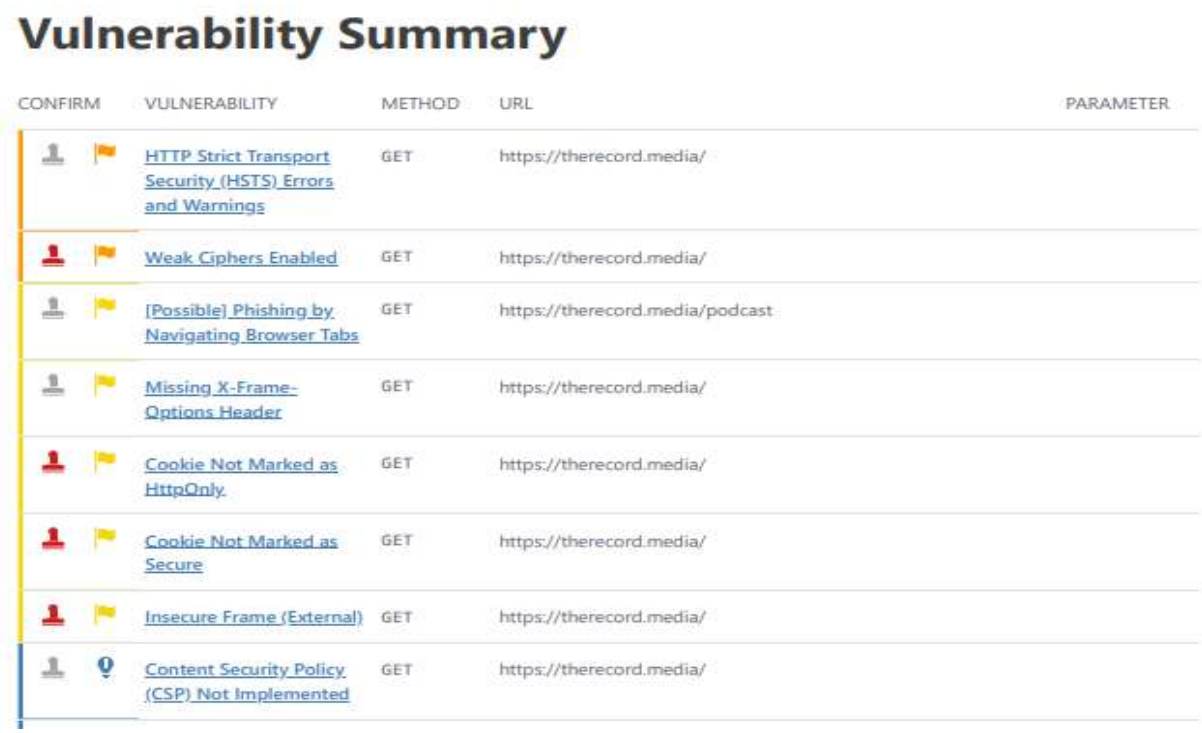
We did not get any alarms that had a high priority when we were doing our vulnerability scan; on the other hand, we did receive a considerable number of alarms that had a low priority. I chose one of them at random, and after I found a vulnerability in it, I exploited it so that I could look for more vulnerabilities elsewhere in the system.

Using Netsparker

I'm doing a vulnerability scan of therecord.media with the help of Netsparker professional Edition (V), which I'm using for my Audit.



After doing a scan of the domain, I was able to identify a total of 15 vulnerabilities related to the domain, including 2 vulnerabilities with a medium risk.



Weak Ciphers Enabled	GET	https://therecord.media/	
[Possible] Phishing by Navigating Browser Tabs	GET	https://therecord.media/podcast	
Missing X-Frame-Options Header	GET	https://therecord.media/	
Cookie Not Marked as HttpOnly	GET	https://therecord.media/	
Cookie Not Marked as Secure	GET	https://therecord.media/	
Insecure Frame (External)	GET	https://therecord.media/	
Content Security Policy (CSP) Not Implemented	GET	https://therecord.media/	
Expect-CT Not Enabled	GET	https://therecord.media/	
Missing X-XSS-Protection Header	GET	https://therecord.media/	
Referrer-Policy Not Implemented	GET	https://therecord.media/	
Subresource Integrity (SRI) Not Implemented	GET	https://therecord.media/sudan-internet-shut-down-amid-fighting	
Email Address Disclosure	GET	https://therecord.media/_next/static/chunks/735-7645aca2d71731dd.js	
Generic Email Address Disclosure	GET	https://therecord.media/_next/static/chunks/735-7645aca2d71731dd.js	
Forbidden Resource	GET	https://therecord.media/?nsextt=%0d%0ans%3anetsparker056650%3dvuln	nsextt

therecord.media has been found to have the following identified vulnerabilities

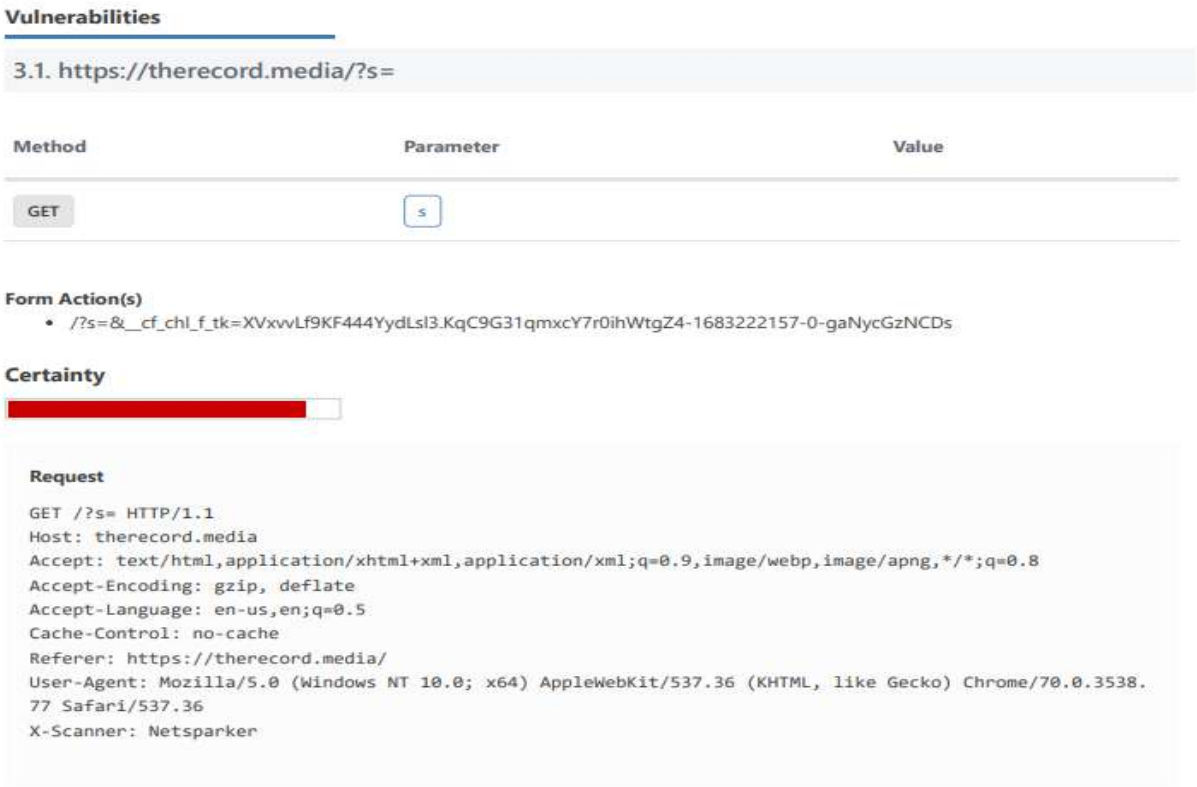
Identified vulnerabilities in therecord.media

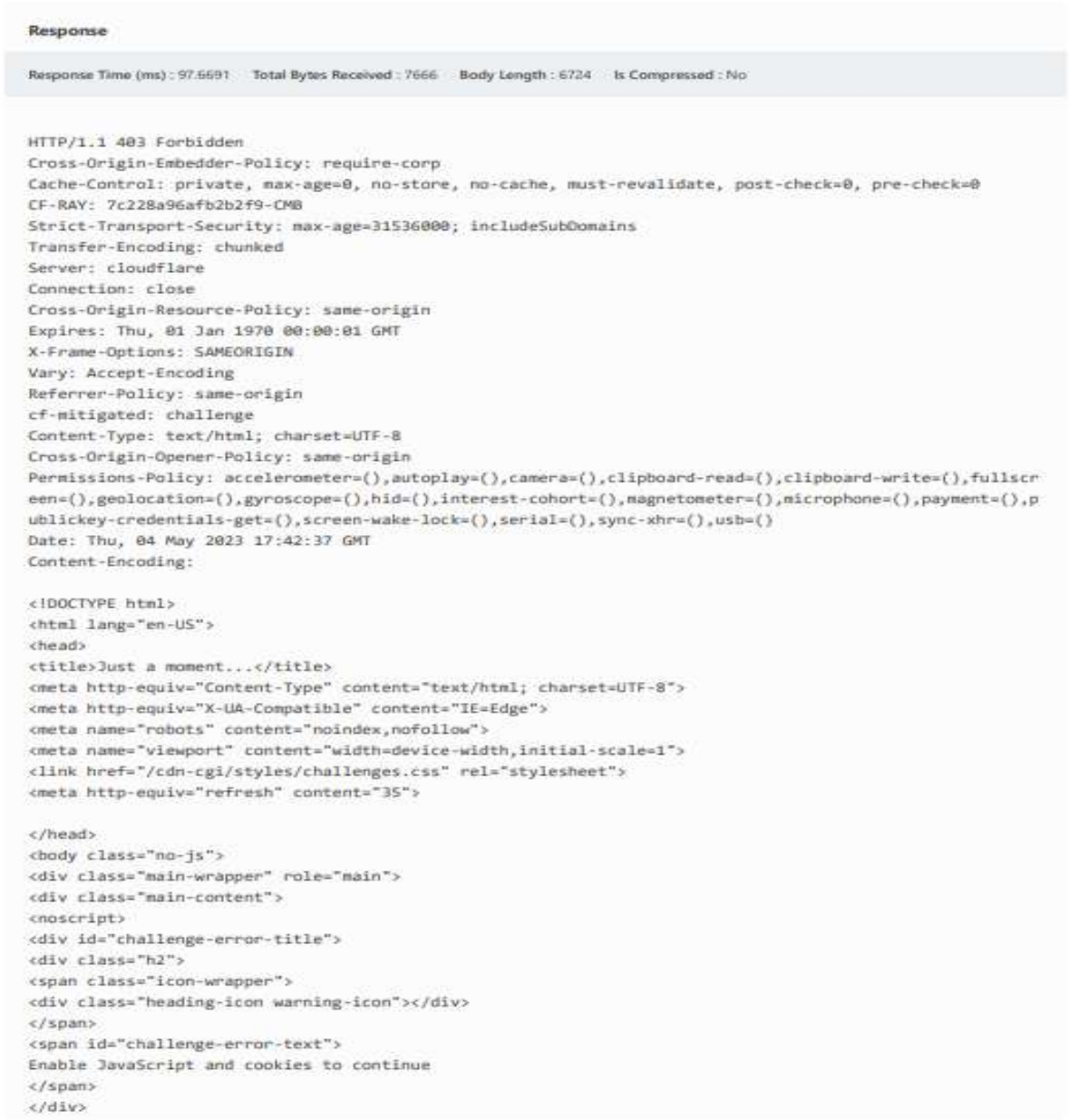
Vulnerability 03 - [Possible] Cross-site Request Forgery

Netsparker found something that it believes to be a CSRF vulnerability and reported its findings. The CSRF is observed a fair amount of the time. It forces authorized users to take out actions inside online programs even if such activities are in direct opposition to the preferences those users have stated about those activities.

Impact

An attacker may imitate any of the actions that can be carried out by a user on an application, such as adding a user, modifying content, or deleting data. This includes simulating the deletion of data. This varies from program to program. The person who committed the attack has access to all of the same features that are available to the victim. A website that requires extra information that only the authentic user is able to know (such as the user's password) is the one and only exception to this rule.





Solution

- Send more information with each HTTP request that can be used to figure out if it came from a trusted source. This "validation token" should be hard to guess for an attacker who doesn't already have access to the user's account. If a request is missing a validation token or the token does not match the expected value, the server should turn down the request.

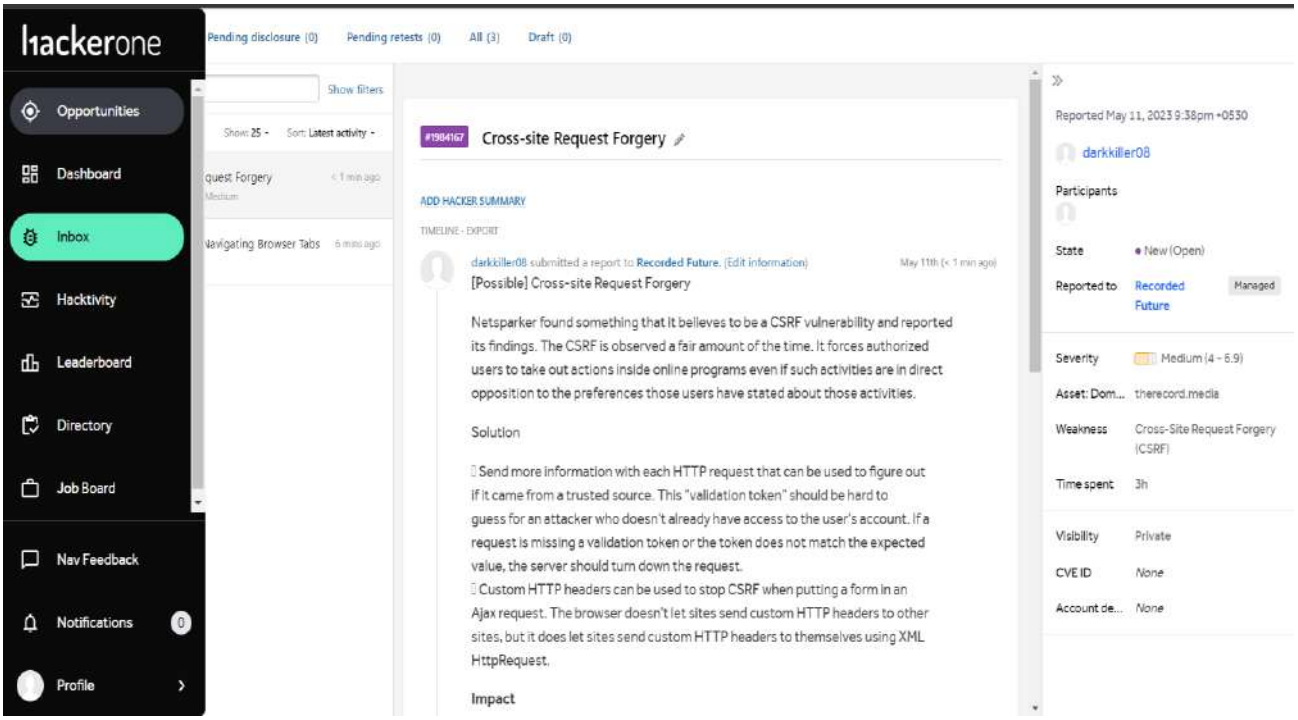
- Custom HTTP headers can be used to stop CSRF when putting a form in an Ajax request. The browser doesn't let sites send custom HTTP headers to other sites, but it does let sites send custom HTTP headers to themselves using XML HttpRequest.

Conclusion of the Report 03

We began by researching the company's actions and legislation. First step. The talk included many statistics and figures. We start our bug research by gathering some key data. The hosting company's IP address and the domain's technology are also included. We then migrate all subdomains to the same server and notice that each domain has the same IP address. Sometimes we need many tools to get additional information and verify it. This is necessary to verify our data. After that, we checked netcraft for files and directives to create a diagram of our domain. Thus, similar files and directives exist. Thus, such files or instructions do not exist. It greatly clarified the topic matter.

Next, we assess system faults. We learned about the domain's vulnerabilities and how to utilise certain tools to find them at the time. We also learned about domain vulnerabilities. After that, we use other websites to analyse the vulnerability to better understand the problem with this online application. After identifying vulnerabilities, we tried to establish one had a potentially dangerous concern. We proved it was dangerous. We had determined that the vulnerability was not significant, but we received a lot of fascinating information. We received a lot of information despite determining the vulnerability was unimportant.

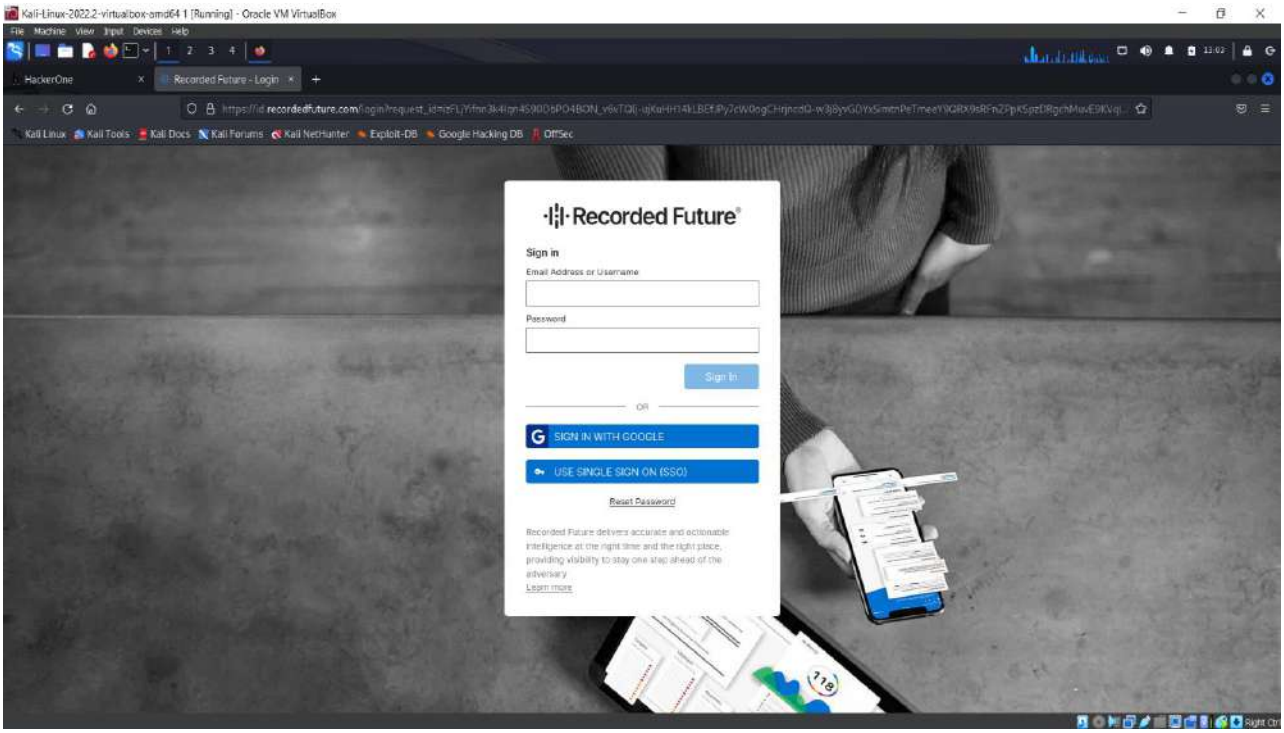
HackerOne Submitted Report Screenshot



iv. Report 04

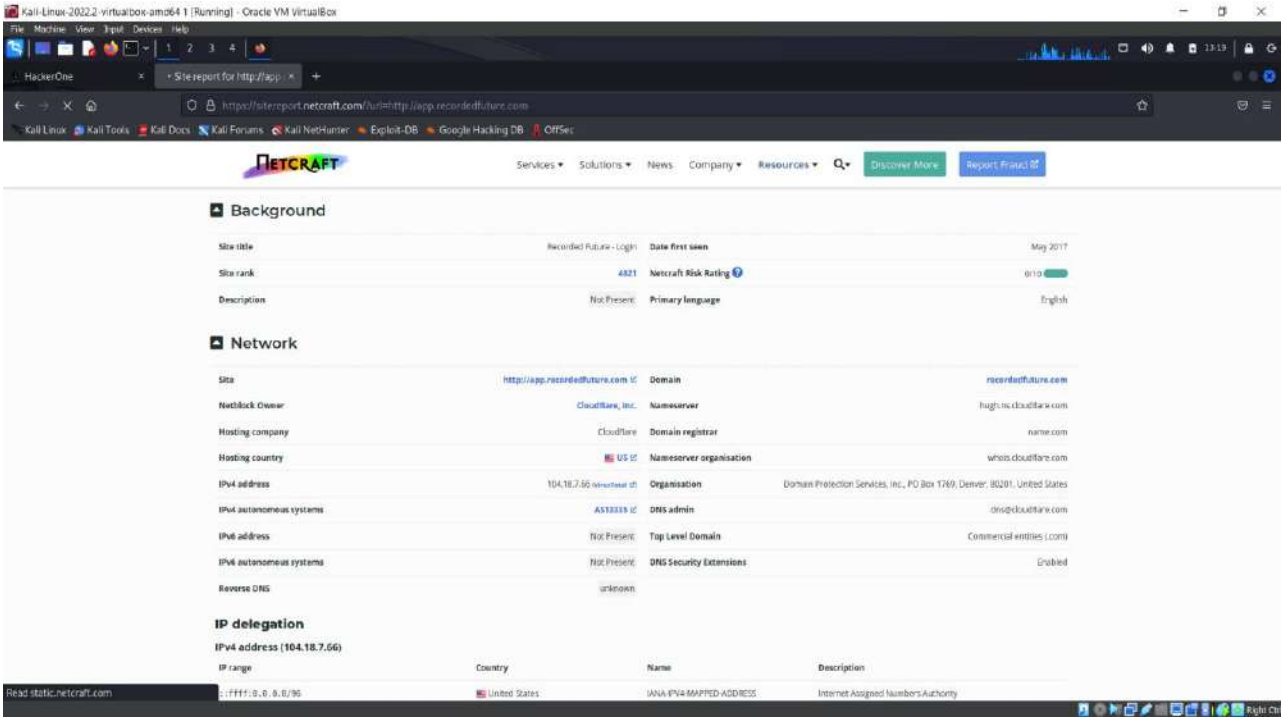
Target information: app.recordedfuture.com

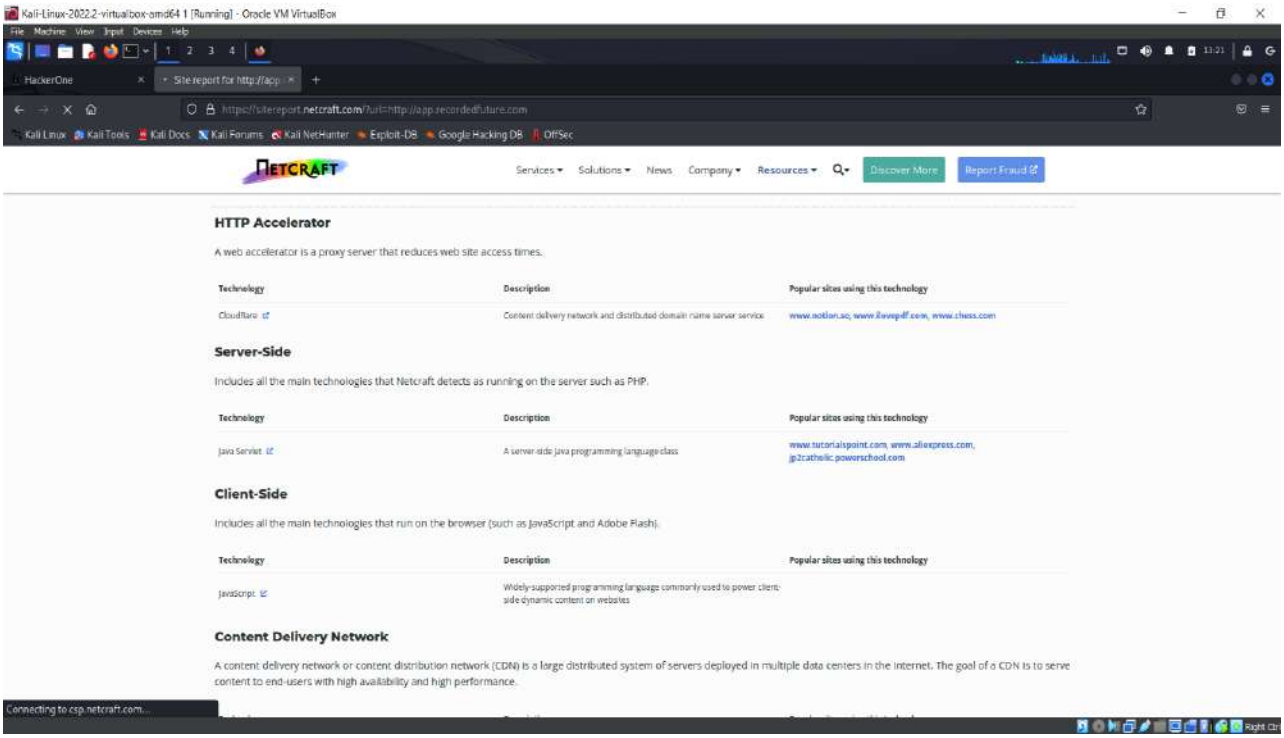
The purpose of this investigation is to determine whether or whether the target domain (app.recordedfuture.com) has any vulnerabilities, and if it does, to determine how serious a risk each of those vulnerabilities represents. If the target domain does have flaws, the investigation will also seek to determine how serious a risk each vulnerability poses. In the case that vulnerabilities are found while the investigation is being conducted, extra work will be done to determine whether or not the target domain also has vulnerabilities. The primary purpose of the inquiry is to ascertain whether or not the target domain has any subdomains that are lacking in any facet that adds to their capacity to be defined.



Information Gathering For Target Domain

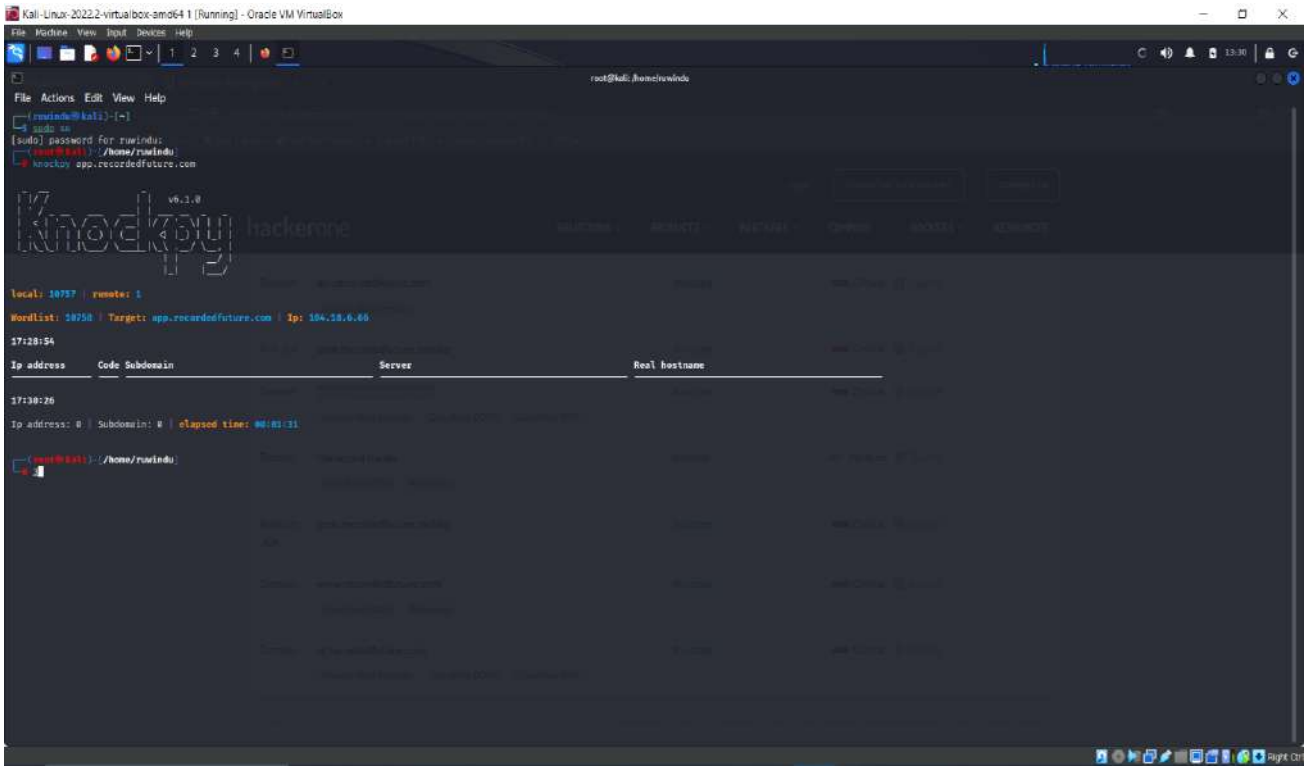
We'll look at our choices to see what app.recordedfuture.com can do technologically and what other information is important to the case. Since Netcraft is the only tool we have, let's sign up for it and look into what it knows. Since Netcraft is all we have, let's put in our name and see what it says. Right now, we're using Netcraft, so let's look at what we know about it.


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
HackerOne
Site report for http://app
https://sitereport.netcraft.com/?url=http://app.recordedfuture.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Background
Site title
Recorded Future - Login
Date first seen
May 2017
Site rank
4821
Netcraft Risk Rating
Description
Not Present
Primary language
English
Network
Site
http://app.recordedfuture.com
Domain
recordedfuture.com
Netblock Owner
Cloudflare, Inc.
Nameserver
hugh.ns.cloudflare.com
Hosting company
Cloudflare
Domain registrar
name.com
Hosting country
US
Nameserver organisation
whois.cloudflare.com
IPv4 address
104.18.7.66
Organisation
Domain Protection Services, Inc., PO Box 1769, Denver, 80201, United States
IPv4 autonomous systems
AS13335
DNS admin
dns@cloudflare.com
IPv6 address
Not Present
Top Level Domain
Commercial entities (.com)
IPv6 autonomous systems
Not Present
DNS Security Extensions
Enabled
Reverse DNS
unknown
IP delegation
IPv4 address (104.18.7.66)
IP range
Country
Name
Description
::ffff:0.0.0.0/96
United States
IANA-IPV4-MAPPED-ADDRESS
Internet Assigned Numbers Authority
Read static.netcraft.com


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
HackerOne
Site report for http://app
https://sitereport.netcraft.com/?url=http://app.recordedfuture.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
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
www.notion.so, www.ilovepdf.com, www.chess.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
Java Servlet
A server-side Java programming language class
www.tutorialspoint.com, www.aliexpress.com, jp2catholic.powerschool.com
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
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites
Content Delivery Network
A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the internet. The goal of a CDN is to serve content to end-users with high availability and high performance.
Connecting to csp.netcraft.com...

Using knockpy tool

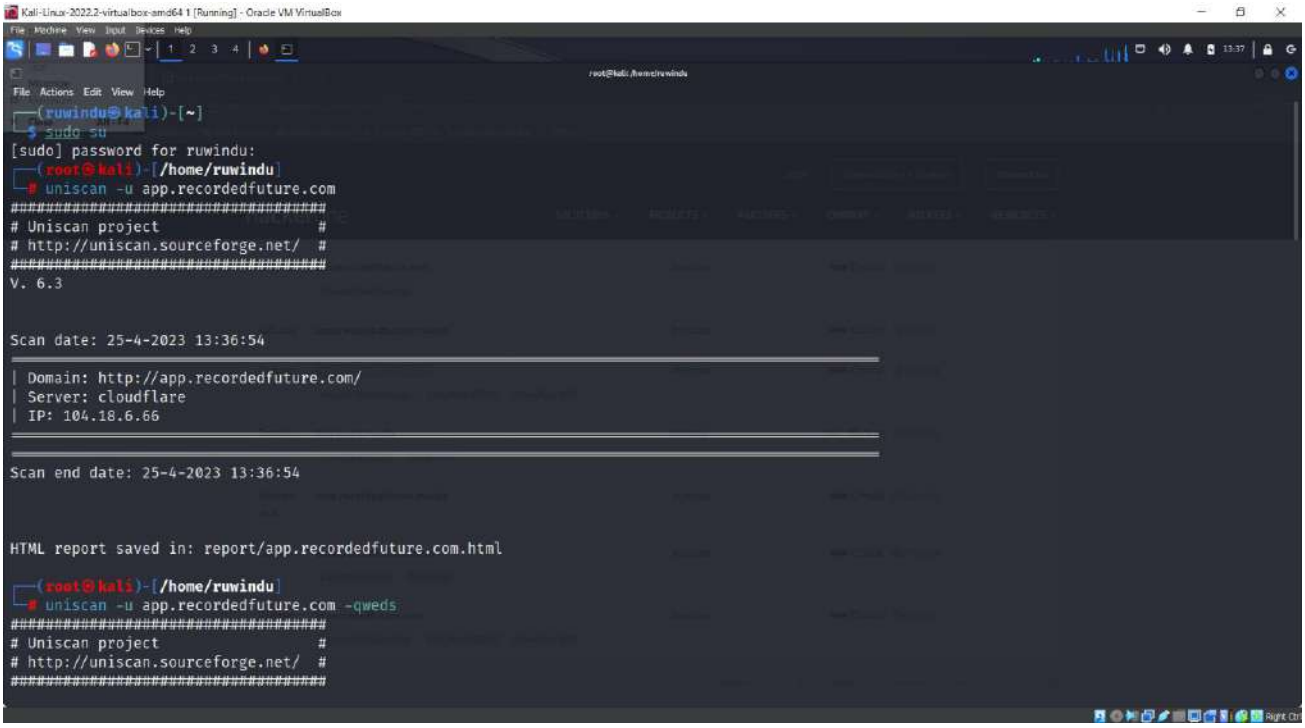
Using the knockpy tool, it is possible to collect subdomain names through scraping data sources, carrying out reverse DNS sweeping, and taking part in recursive brute forcing.



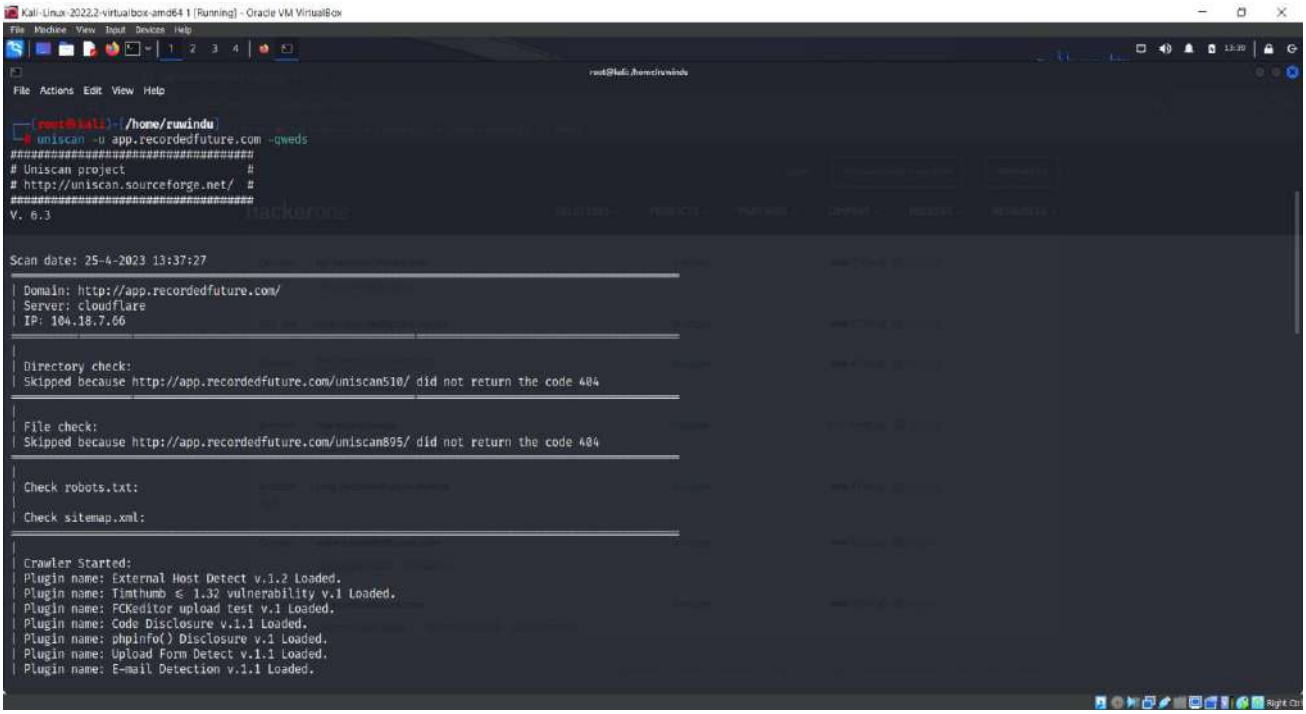
Since the app.recordedfuture.com subdomains have been recorded, we are now permitted to see them in this way after the completion of the enumeration of the subdomains that are associated with app.recordedfuture.com. It really shouldn't come as much of a surprise to anybody that the IP address and name server that are used by each and every one of the subdomains that are kept under the app.recordedfuture.com domain are the same ones that are used by the main domain itself. These details are shared by all of the subdomains that are stored under the app.recordedfuture.com domain. We are able to identify that this is a mobile application due to the fact that the application's true hostname is shown. The fact that the correct hostname is shown here serves as the foundation for our conclusion. We are now in a position to make use of it as a direct consequence of this, which has made it possible for us to do so.

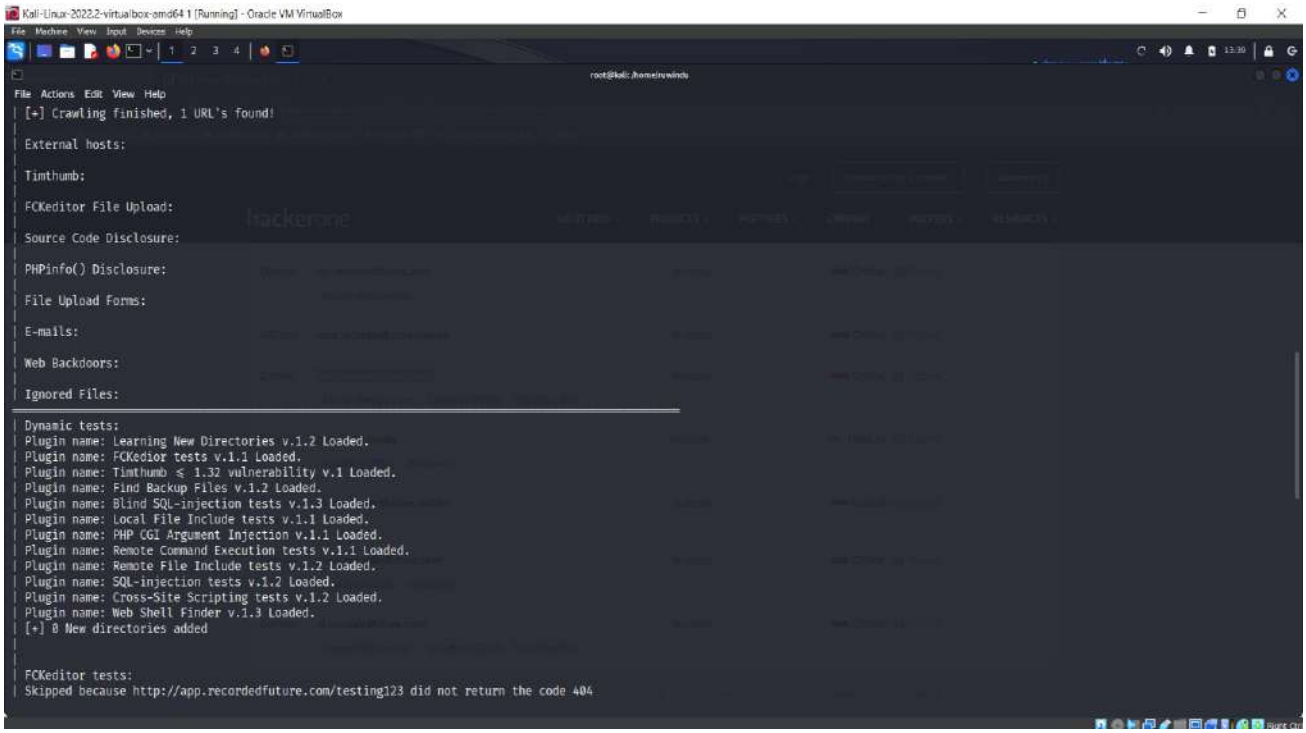
Using Uniscan tool

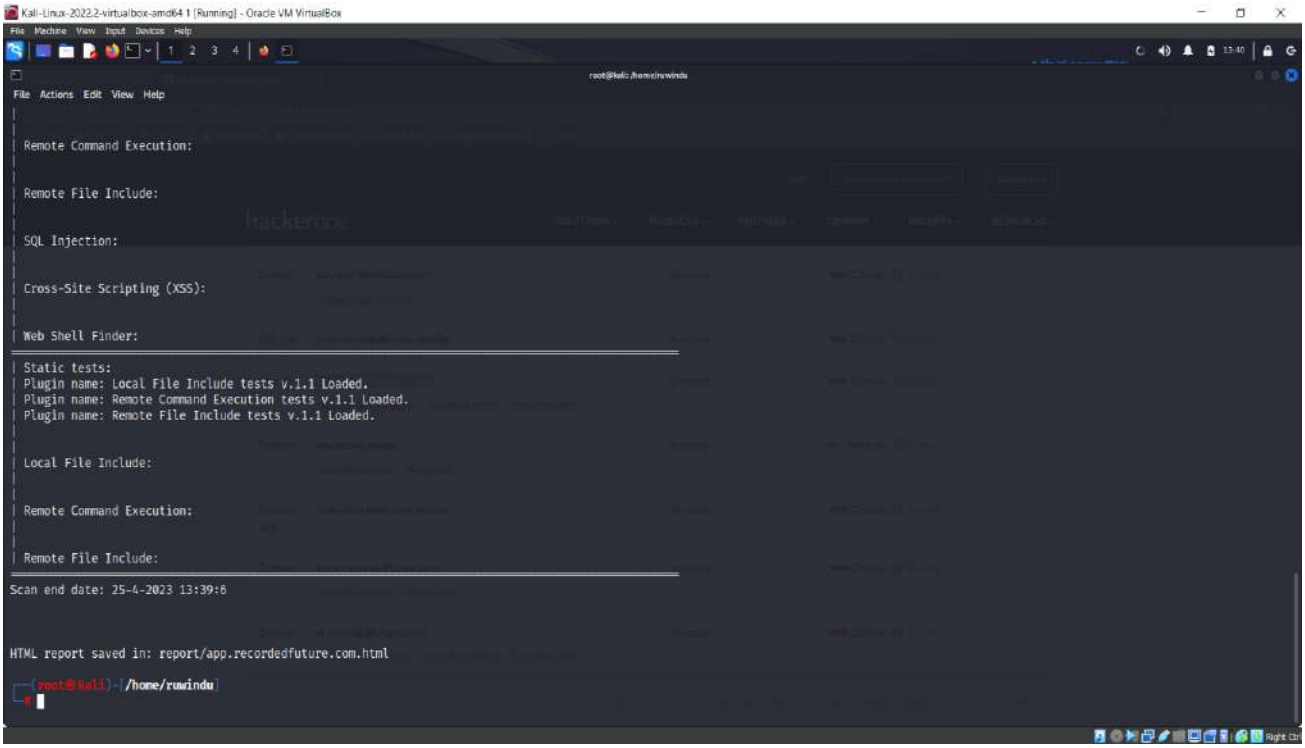
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u app.recordedfuture.com -qweds command:

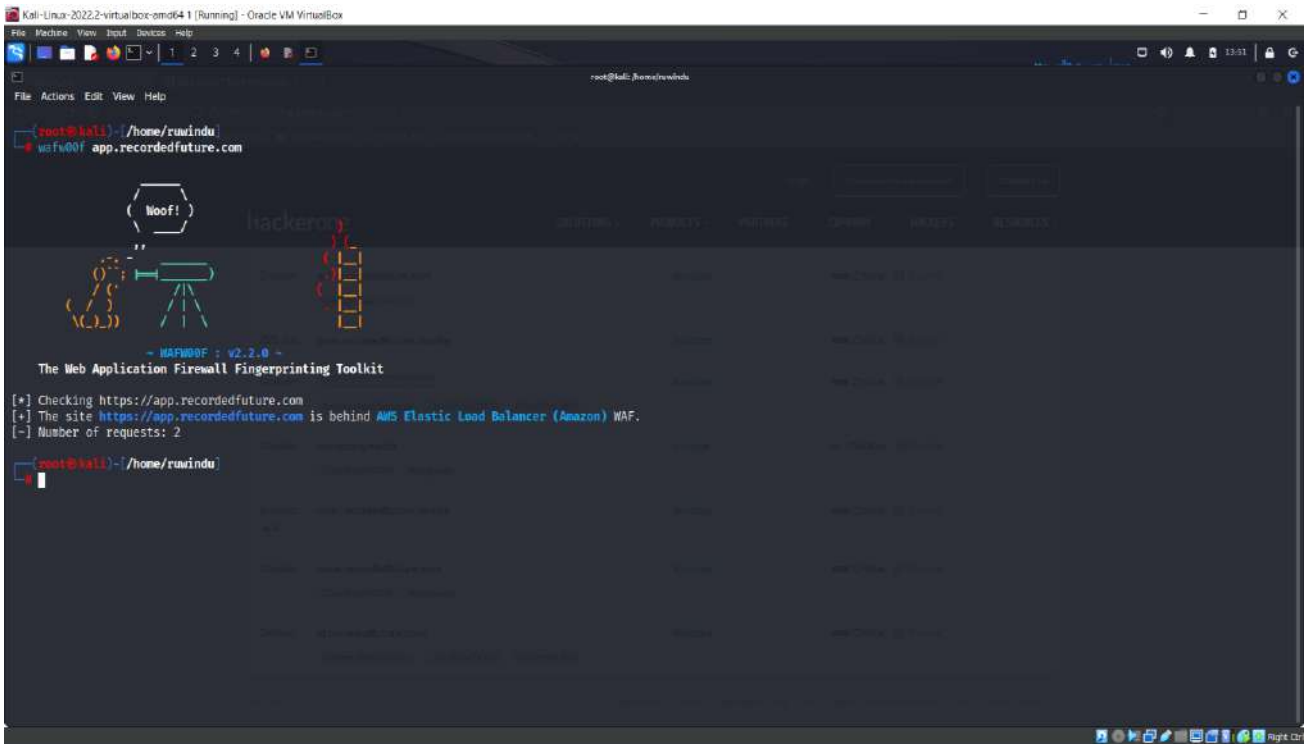



Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/ruwindu
File Actions Edit View Help
[+] Crawling finished, 1 URL's found!
External hosts:
Timthumb:
FCKeditor File Upload:
Source Code Disclosure:
PHPinfo() Disclosure:
File Upload Forms:
E-mails:
Web Backdoors:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKedior tests v.1.1 Loaded.
Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.2 Loaded.
Plugin name: SQL-injection tests v.1.2 Loaded.
Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
Plugin name: Web Shell Finder v.1.3 Loaded.
[+] 0 New directories added
FCKeditor tests:
Skipped because http://app.recordedfuture.com/testing123 did not return the code 404


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: /home/ruwindu
File Actions Edit View Help
Remote Command Execution:
Remote File Include:
SQL Injection:
Cross-Site Scripting (XSS):
Web Shell Finder:
Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.
Local File Include:
Remote Command Execution:
Remote File Include:
Scan end date: 25-4-2023 13:39:8
HTML report saved in: report/app.recordedfuture.com.html
┌──(root㉿kali)-[/home/ruwindu]
└─#

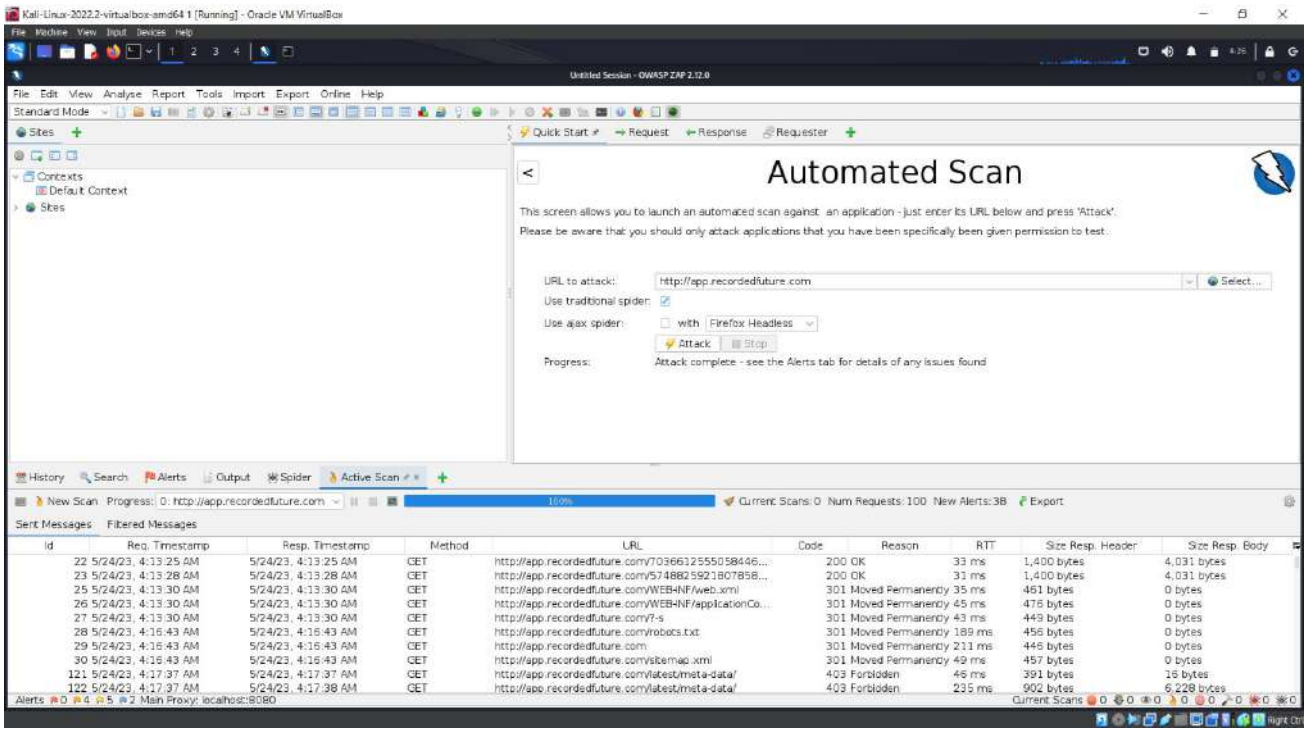
Using Wafw00f tool

When we run the wafw00f scan with the URL that we are targeting, we are able to see that the website app.recordedfuture.com seems to be protected by a web application firewall (WAF) or some other form of security solution. This is something that we are able to validate via our own direct experience. Because we had completed the scan, we were able to get this information and make the appropriate judgements.

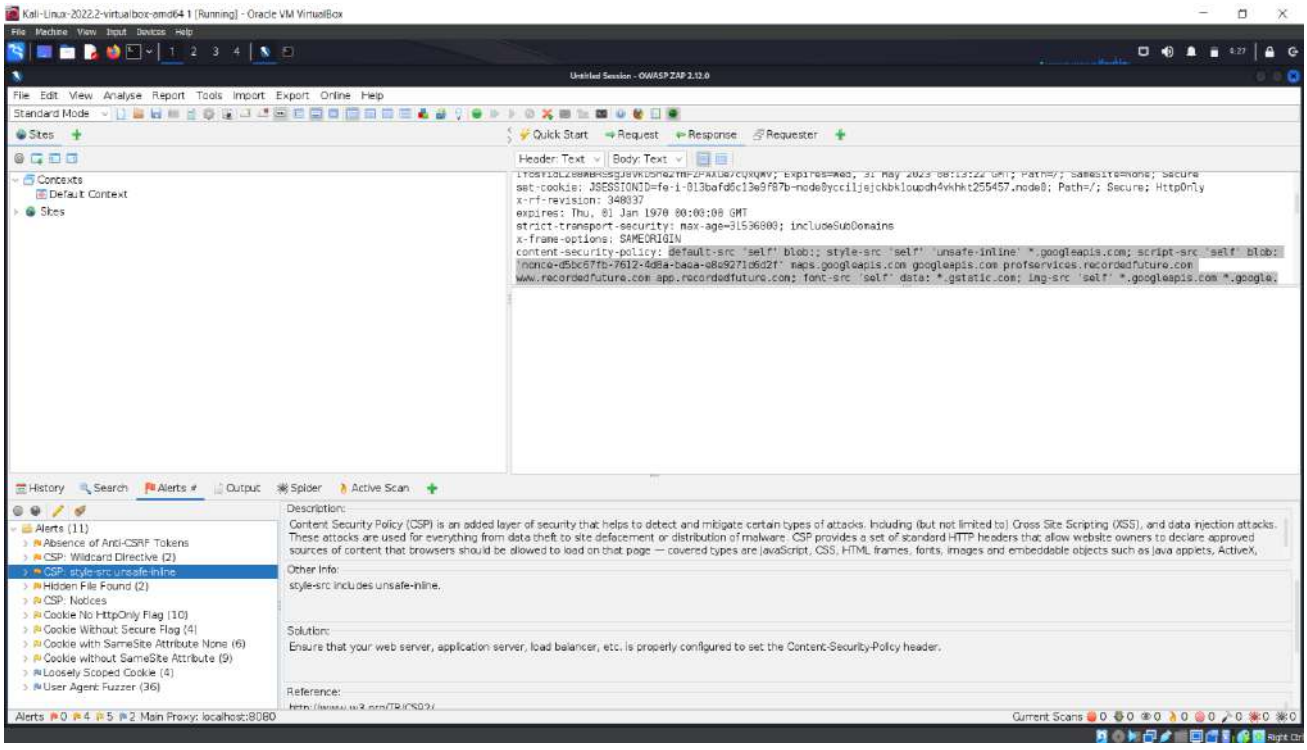


After doing the quick scan, we were able to locate and analyze the robust firewall that was a part of this domain.

Using OWASP-ZAP tool



Found 100 Requests.



Found 11 Alerts.

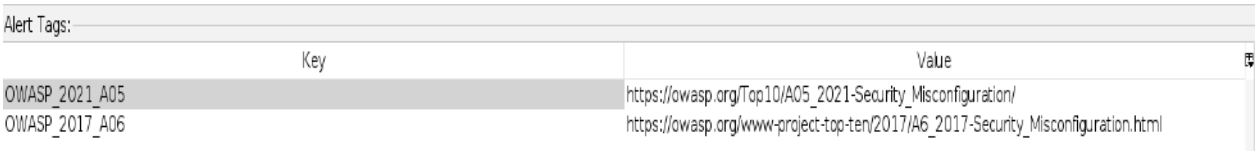
Vulnerabilities found

CSP: style-src unsafe-inline

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

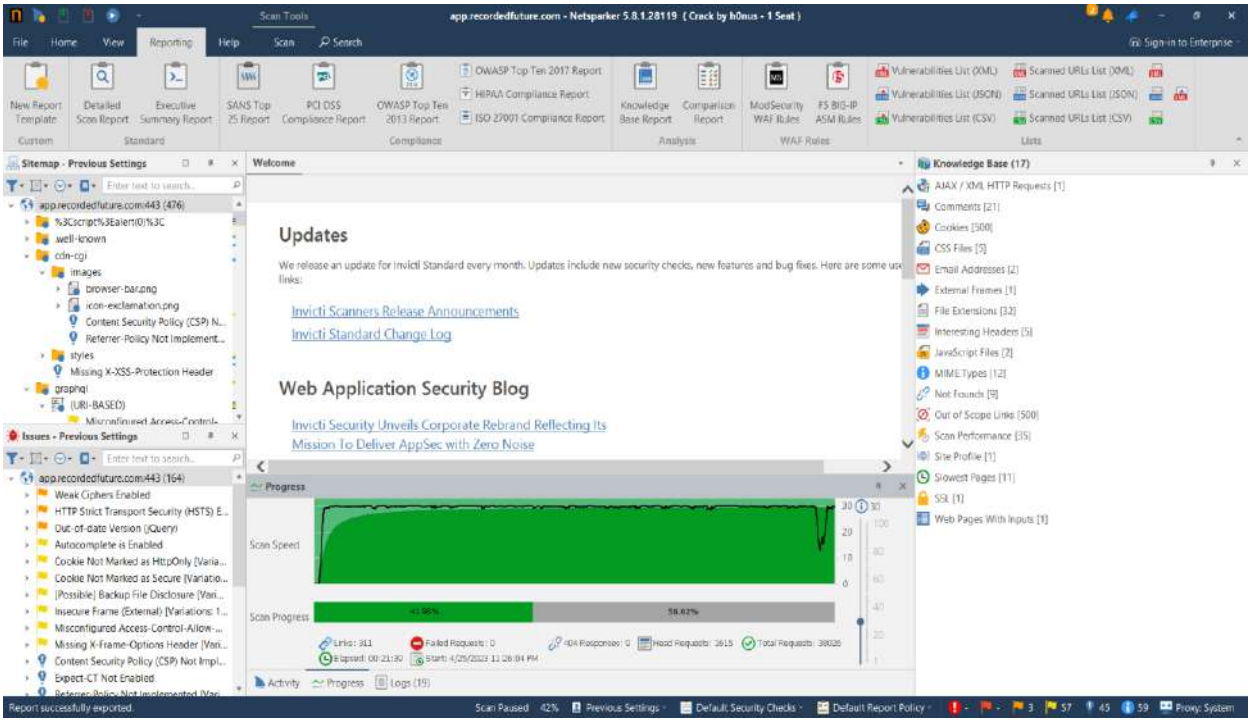
Solution

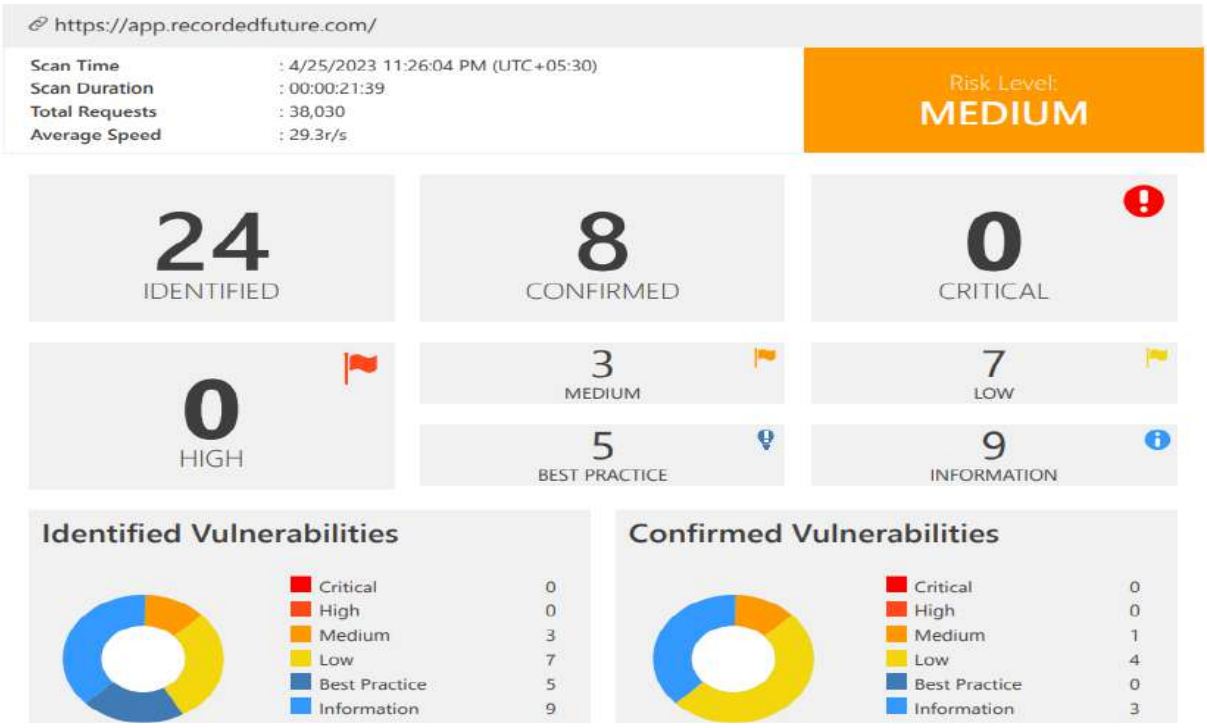
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.



Using Netsparker

In the course of my Audit, I performed a vulnerability check on app.recordedfuture.com with the aid of Netsparker professional Edition (V), which proved to be of great service to me in my endeavor. For the purpose of this specific audit, the website was analyzed.





After doing a scan of the domain, I was able to identify a total of 24 vulnerabilities related to the domain, including 3 vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://app.recordedfuture.com/	
	Out-of-date Version (jQuery)	GET	https://app.recordedfuture.com/rf/kobra/js/libs/jquery/jquery-3.4.1.min.js	
	Weak Ciphers Enabled	GET	https://app.recordedfuture.com/	
	[Possible] Backup File Disclosure	GET	https://app.recordedfuture.com/portal/o.config~	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://app.recordedfuture.com/graphql/	URI-BASED
	Missing X-Frame-Options Header	GET	https://app.recordedfuture.com/rf/kobra/js/libs/jquery/	
	Autocomplete is Enabled	GET	https://app.recordedfuture.com/live/login/?orig_url=%2527	orig_url
	Cookie Not Marked as HttpOnly	GET	https://app.recordedfuture.com/	
	Cookie Not Marked as Secure	GET	https://app.recordedfuture.com/	
	Insecure Frame (External)	GET	https://app.recordedfuture.com/portal/	
	Content Security Policy (CSP) Not Implemented	GET	https://app.recordedfuture.com/cdn-cgi/images/	
	Expect-CT Not Enabled	GET	https://app.recordedfuture.com/	
	Missing X-XSS-Protection Header	GET	https://app.recordedfuture.com/cdn-cgi/	
	Referrer-Policy Not Implemented	GET	https://app.recordedfuture.com/cdn-cgi/images/	
	SameSite Cookie Not Implemented	GET	https://app.recordedfuture.com/	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://app.recordedfuture.com/portal/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://app.recordedfuture.com/portal/	
	Email Address Disclosure	GET	https://app.recordedfuture.com/portal/static/js/main.e417f52a.js	
	Generic Email Address Disclosure	GET	https://app.recordedfuture.com/portal/static/js/main.e417f52a.js	
	Web Application Firewall Detected	GET	https://app.recordedfuture.com/%3Cscript%3Ealert(0)%3C/script%3E	URI-BASED
	Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://app.recordedfuture.com/portal/	
	Autocomplete Enabled (Password Field)	GET	https://app.recordedfuture.com/live/login/?orig_url=%2527	orig_url
	Forbidden Resource	GET	https://app.recordedfuture.com/rf/api-doc/index.html#!/wellknown	
	OPTIONS Method Enabled	OPTIONS	https://app.recordedfuture.com/live/	

app.recordedfuture.com has been found to have the following identified vulnerabilities:

Identified vulnerabilities in app.recordedfuture.com

Vulnerability 04 - Missing X-XSS-Protection Header

Because the X-XSS-Protectionheader for this website was found to be absent when it was analyzed by Netsparker, there is a possibility that it is susceptible to Cross-site Scripting (XSS) attacks. Cross-site scripting is what "cross-site scripting" is abbreviated as in the phrase "cross-site scripting."

Impact

At this time, supplemental data is all that is being offered in regard to this issue. As a direct consequence of this situation, there will be no immediate implications.

Vulnerabilities

5.1. http://recordedfuture.com/cdn-cgi/

Certainty

Request

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

Solution

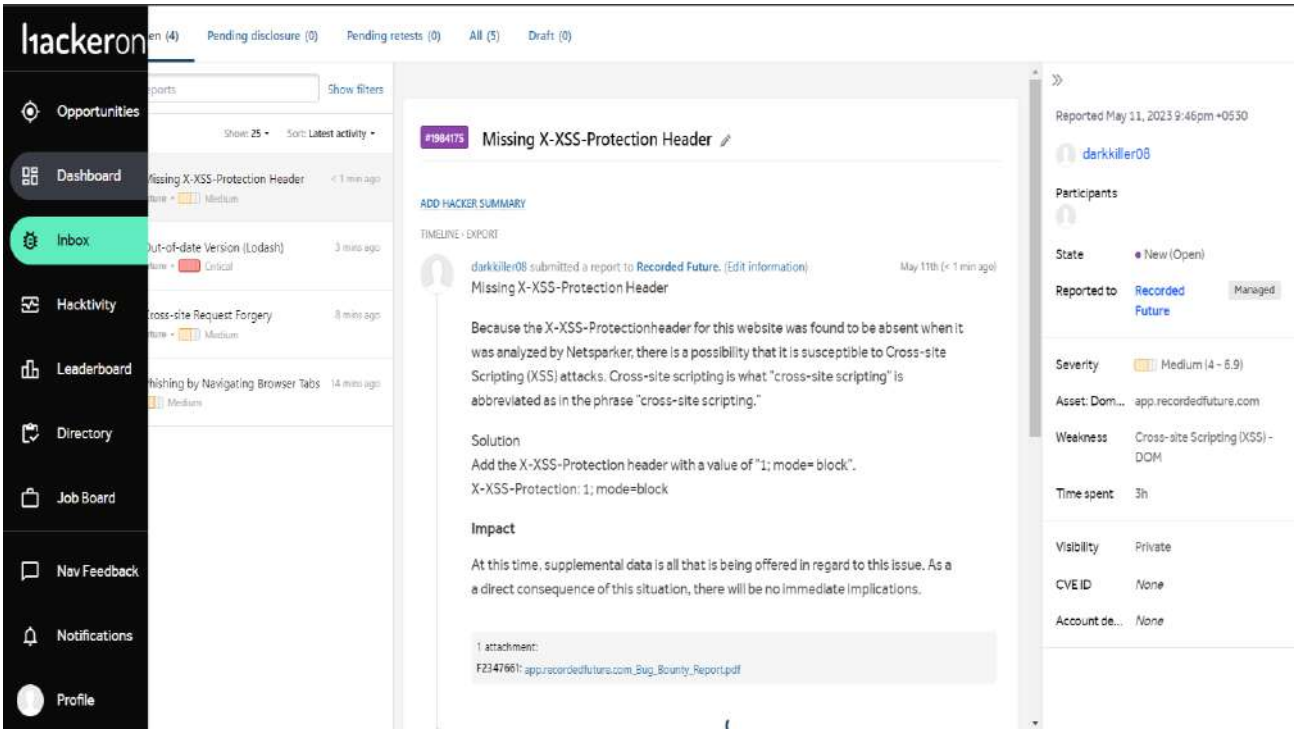
Add the X-XSS-Protection header with a value of "1; mode= block".

X-XSS-Protection: 1; mode=block

Conclusion of the Report 04

We have made the decision to check and assess the recorded future bug bounty plan in order to ensure that the information included in this report is correct, and we will do so as soon as possible. In the course of our study, one of our primary objectives was to determine whether or not we were effective in discovering an issue with the program. This will provide us the ability to determine whether or not the efforts we put in were beneficial. After then, we made an effort to compile information not only on the technologies themselves, but also about the IP addresses, the subdomains, and a few other locations here and there. Following the completion of the site content scan, we moved on to doing the vulnerability analysis. This step followed directly after the previous one. We were able to identify all 24 distinct categories of critical flaws in the system by using a piece of software called as a netsparker. This tool helped us do so. Following considerable consideration, we arrived to the conclusion that the primary focus of our investigation need to be on the possible threats that are presented by cooperating with groups that are not connected to us in any way. In the end, we were successful in gaining an understanding of exactly what it is that this vulnerability entails, as well as the possibly adverse circumstances that may contribute to it, as well as the potential remedies to this problem.

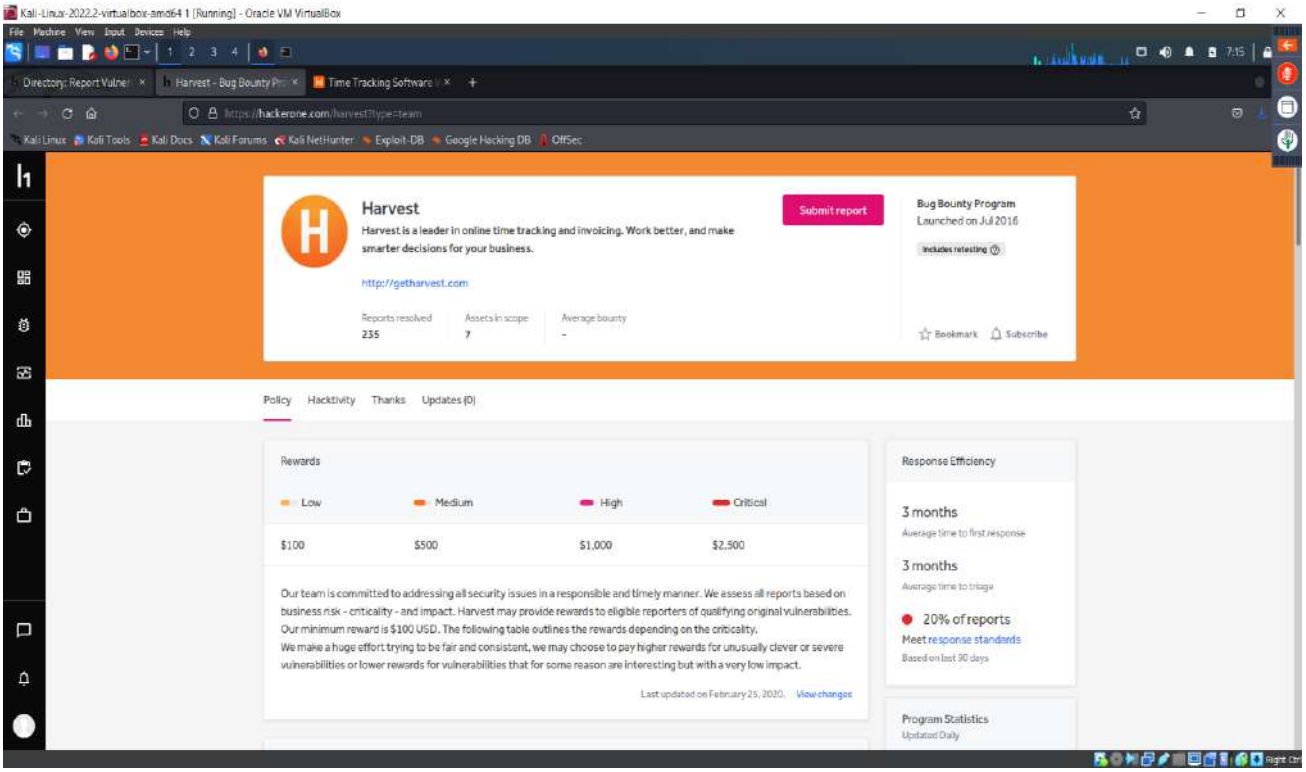
HackerOne Submitted Report Screenshot



v. Report 05

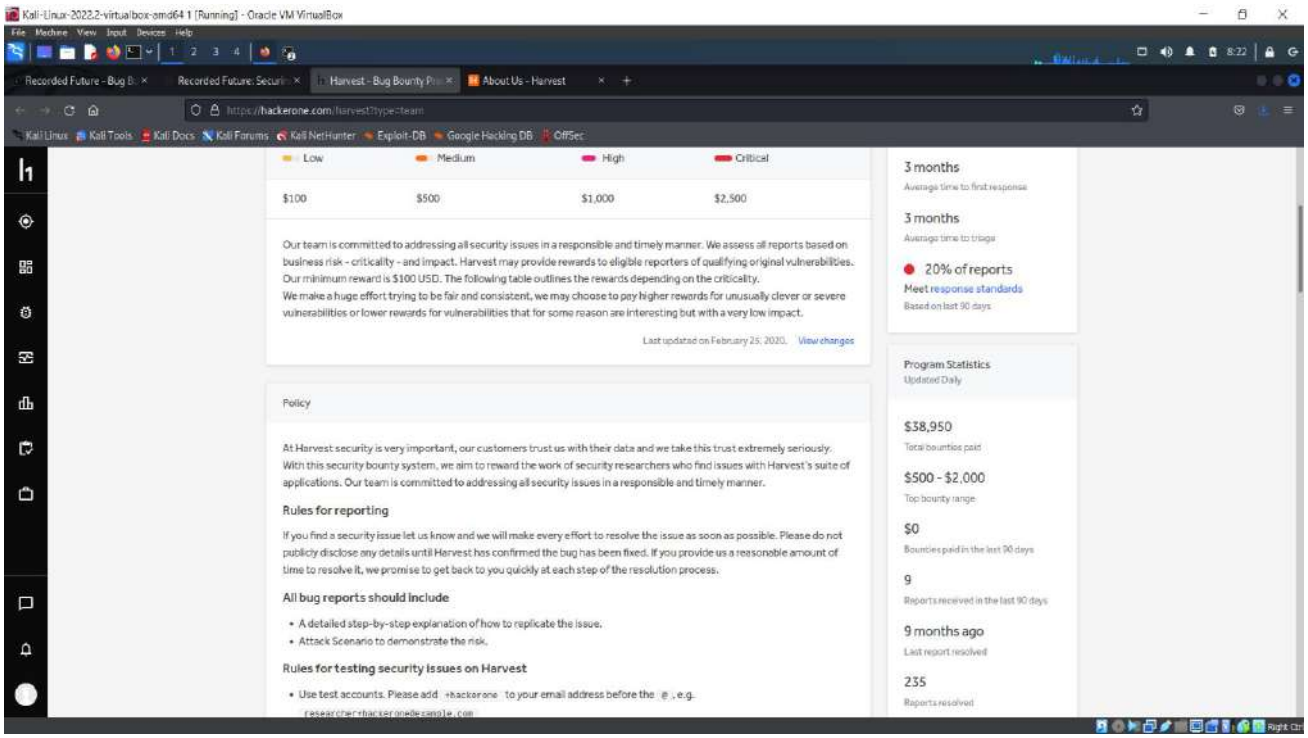
Target information: https://www.getharvest.com

Finding vulnerabilities in the target domain (https://www.getharvest.com/) and determining the risk level associated with such vulnerabilities is the purpose of this assessment. The aim of the assessment is to uncover vulnerabilities in the target domain.

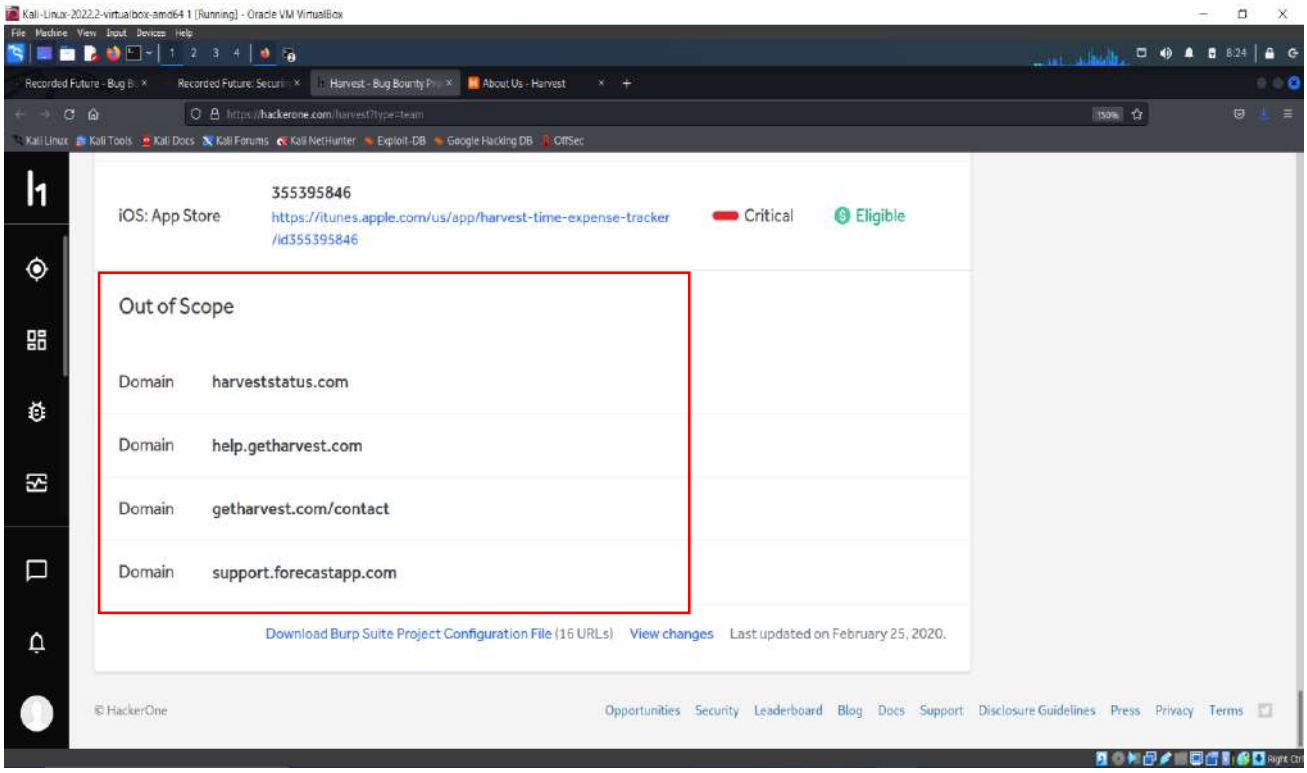


Harvest was first created in 2006 by two designers as a tool for the designers' personal use to aid in the development of their company. It was named "Harvest" at the time of its inception. Danny Wen and Shawn Liu, who were both employees at a web design business located in the financial area of New York City, collaborated on the development of an application that is notable for its aesthetically pleasing design as well as its originality. The application is used to record client time and generate invoices. They built the Harvest into being. Since that time, it has evolved into a platform that thousands of teams all around the world use to monitor and analyse the time that they spend working together.
To get started, we are obligated to study the policies as well as any additional information that may be included within the description. After that, we will have a better comprehension of the operations that take place inside this company, in addition to our scope and the other issues that are associated with it. They started by

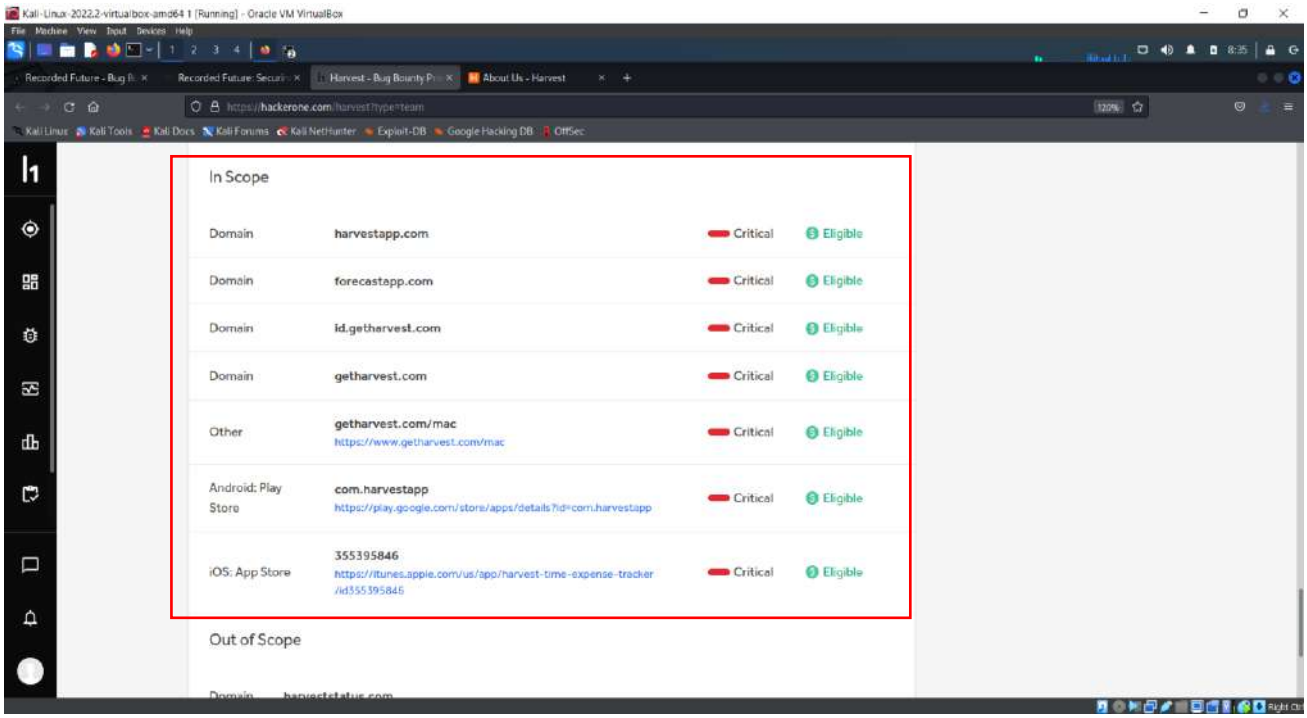
distributing the advantages in a manner that was proportional to the amount of hazard. We analyze each report with regard to the business risk, also known as criticality, and impact. It is possible for Harvest to pay incentives to qualified individuals who disclose qualifying original vulnerabilities. The minimum amount of prize we provide is $100 USD. The table that follows provides an overview of the prizes in accordance with the level of difficulty. Following that, they proceed to discuss the policies that govern their project. It is essential that we behave ourselves in accordance with the instructions that have been offered to us since we will be examining their online application. These guidelines have been presented to us.



After that, they will discuss any potential vulnerabilities that are beyond the scope of the project before going on to the next step. Because of the nature of these security problems, we are unable to make any efforts to detect a bug or include their findings in our report. Additionally, we are unable to include their results in our report. The aforementioned list mandates that we investigate and identify an error that should not be present. It is essential for us to act in this manner.

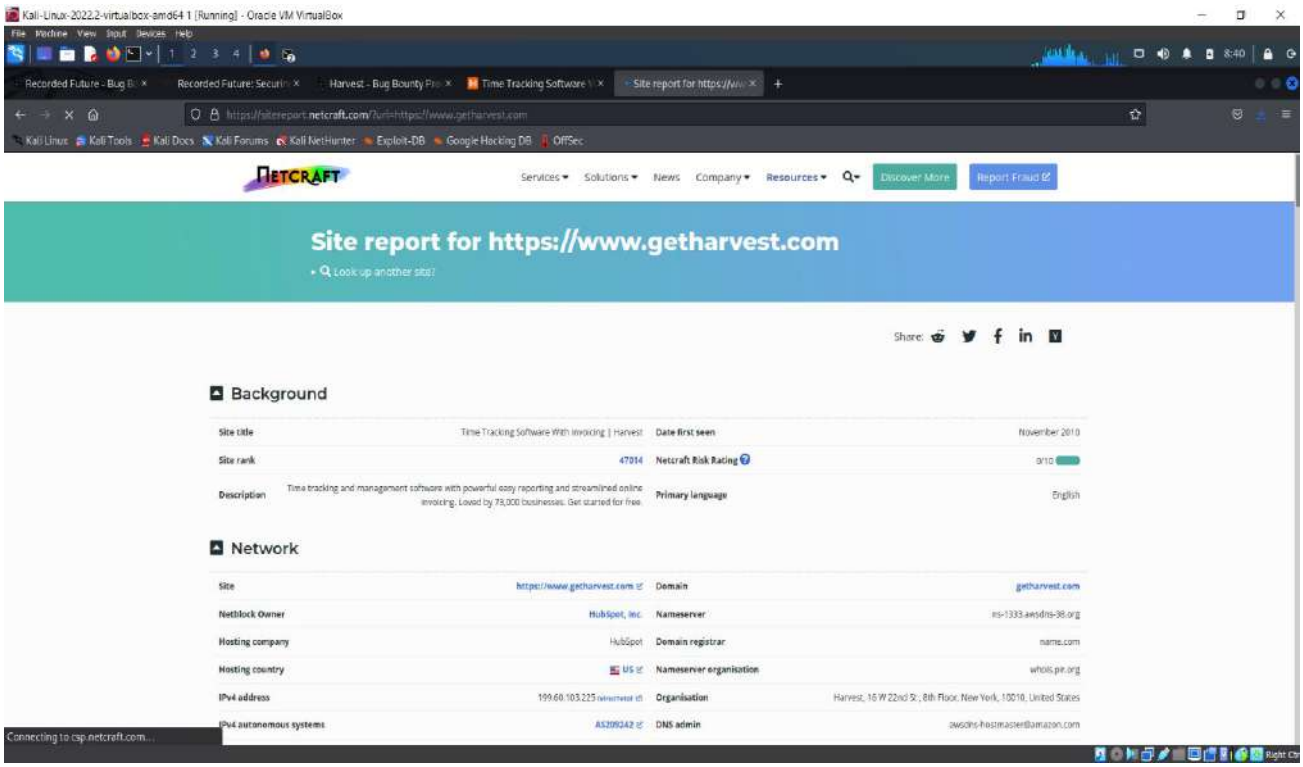


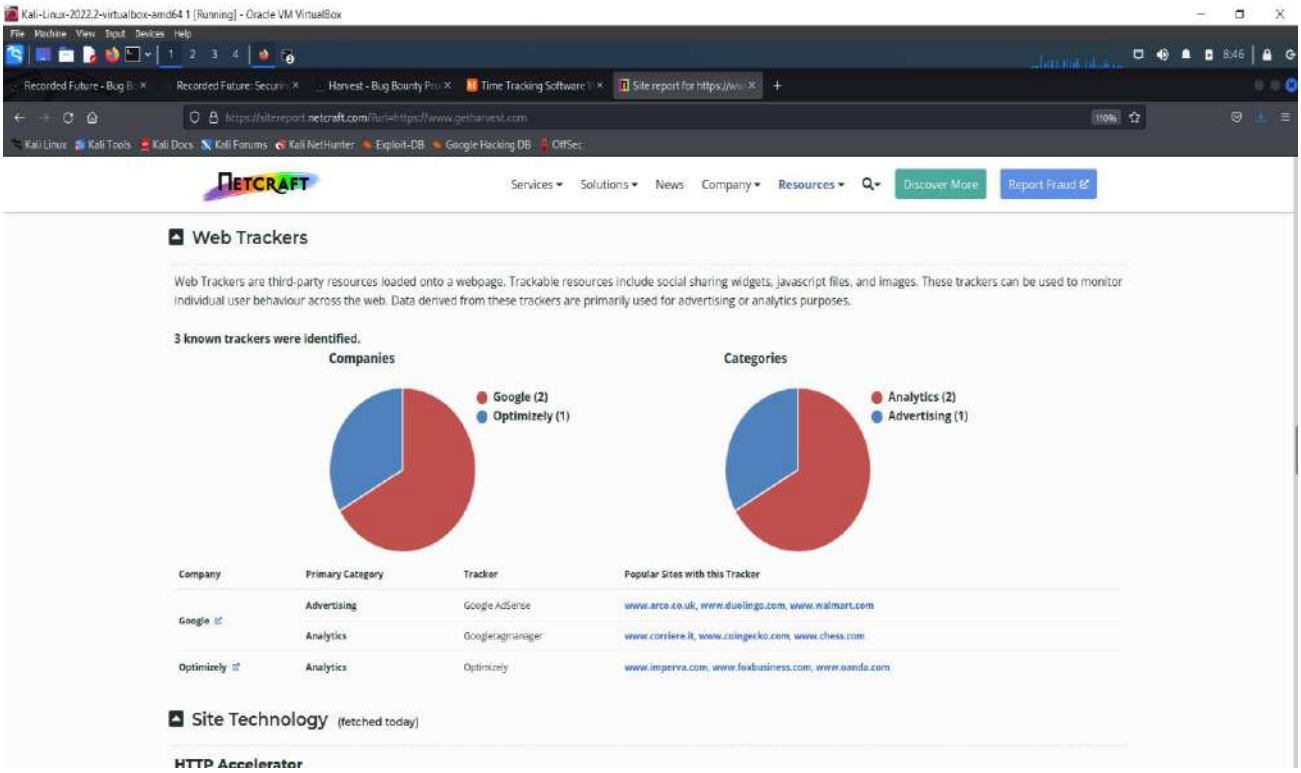
The in-scope region is extremely important to us when it comes to the process of hunting for bugs that have been awarded bounties. This is because every scan that we do looks only for domains that are included within the in-scope umbrella. This is due to the fact that each scan that we conduct searches for flaws only in domains that are included within the umbrella of the in-scope. In the event that things do not go according to plan, we are going to be put up against a variety of challenges of varying kinds.

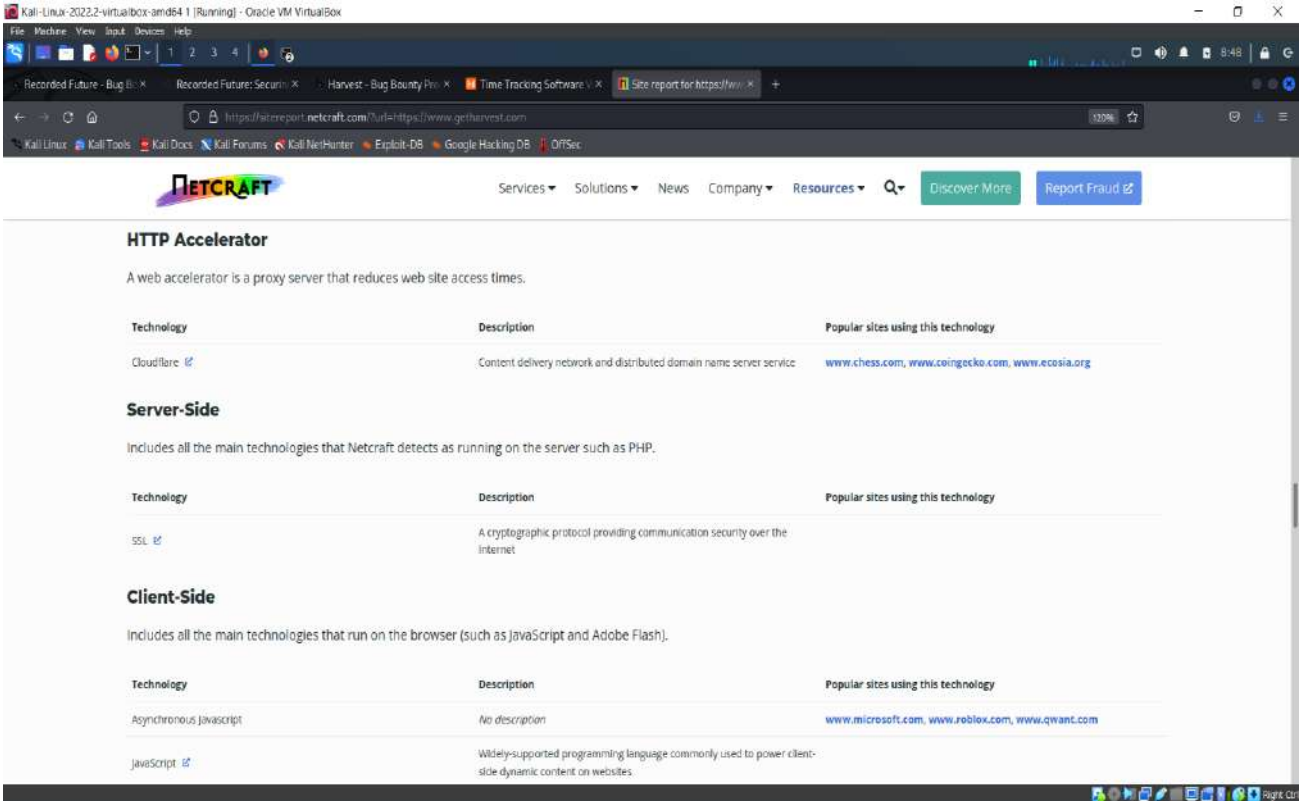


Information Gathering For Target Domain

Let's have a look at the many different approaches that we may use in order to get information not only on the technical capabilities of http://getharvest.com but also about other pertinent facts. Since we are only using Netcraft at the moment, let's put in our domain and research the information that can be obtained by using Netcraft. There are a number of programmes and websites that are capable of doing this, but since we are only using Netcraft at the moment, let's enter in our domain and investigate the information that can be obtained by using Netcraft.

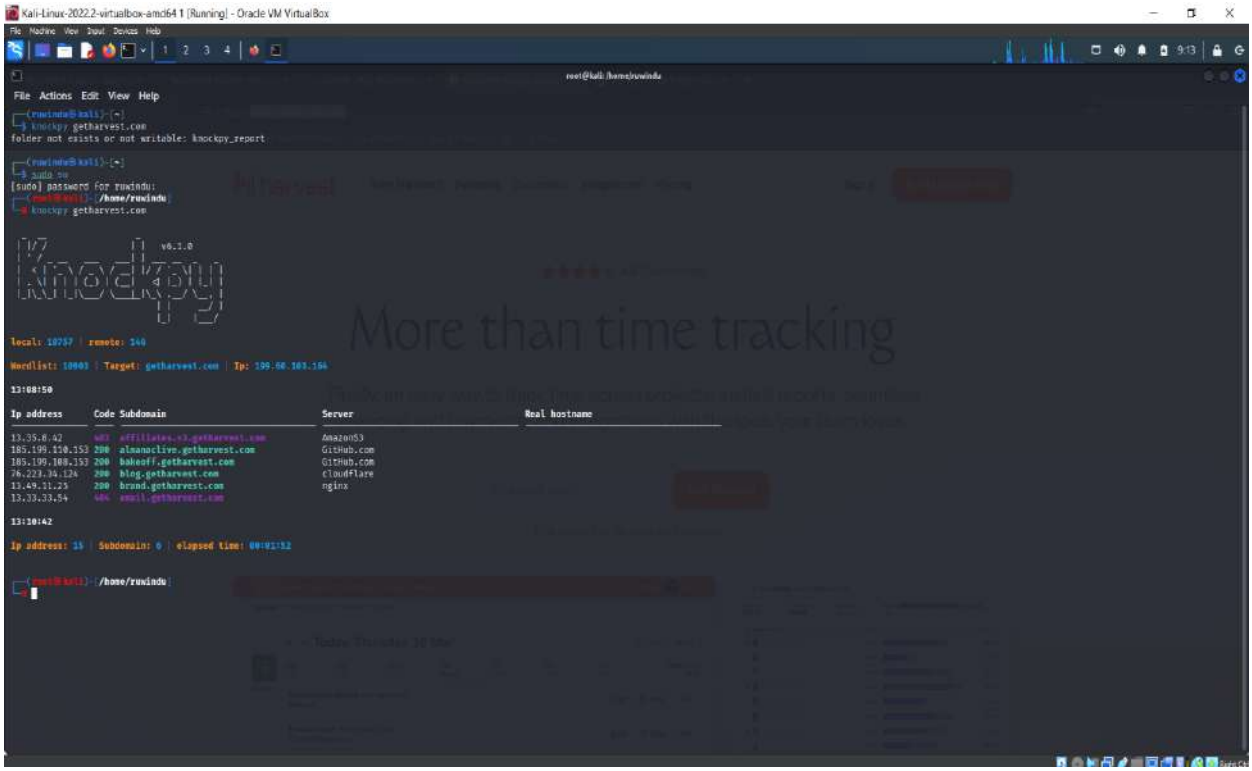



Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Web Trackers
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. 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
Google (2)
Optimizely (1)
Categories
Analytics (2)
Advertising (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Google
Advertising
Google AdSense
www.arco.co.uk, www.duolingo.com, www.walmart.com
Analytics
Googletagmanager
www.corriere.it, www.coingecko.com, www.chess.com
Optimizely
Analytics
Optimizely
www.imperva.com, www.foxbusiness.com, www.oanda.com
Site Technology (fetched today)
HTTP Accelerator


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
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
www.chess.com, www.coingecko.com, www.ecosia.org
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
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.microsoft.com, www.roblox.com, www.qwant.com
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites

Using knockpy tool

In order for us to get to the bottom of what has really taken place here, we are going to need to do a subdomain scanning using software that is created specifically for that purpose. Only then will we be able to get all of the questions we have answered. First, we give knockpy a go on both domains, and then we keep an eye on the output to see what kind of results it generates for us. This is the first phase in the process.

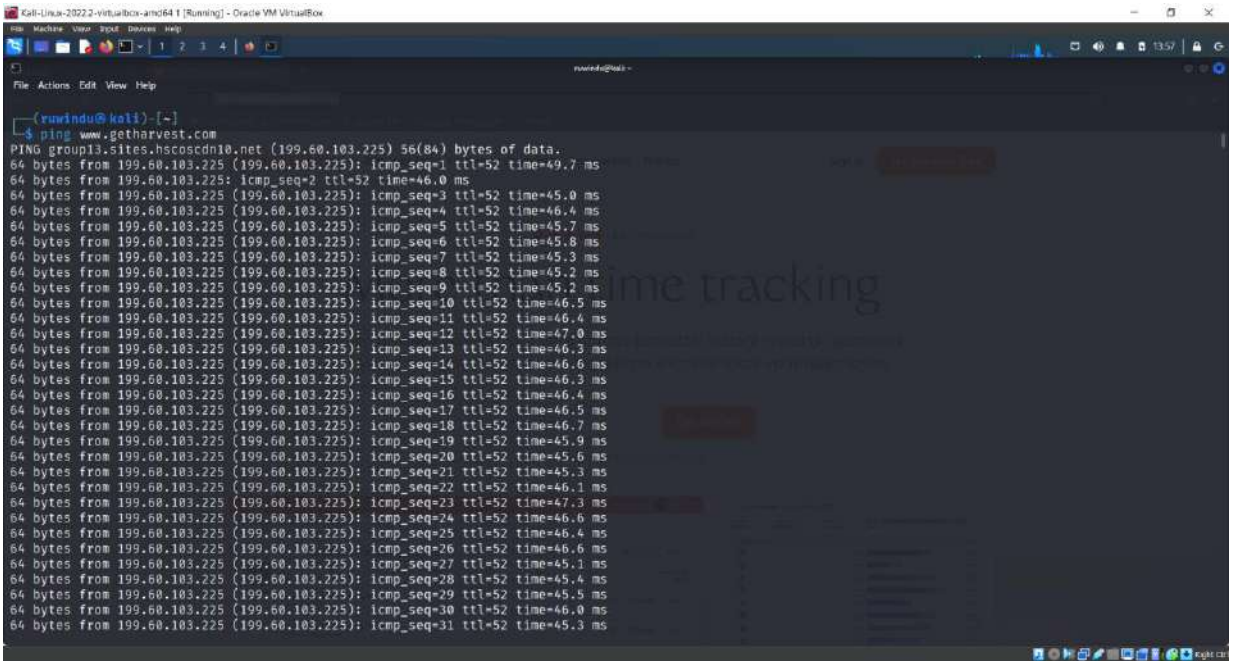


After going through the process of enumerating subdomains, we are now able to examine the formatted versions of https://www.getharvest.com's subdomains. It is extremely clear that each unique subdomain that falls under the www.getharvest.com domain makes use of the same IP address and name server. This is shown by the fact that this information is very obvious. The real hostname that is shown enables us to determine that this is a mobile application. As a result, we are able to detect that this is the case. Let's have a look at the results.

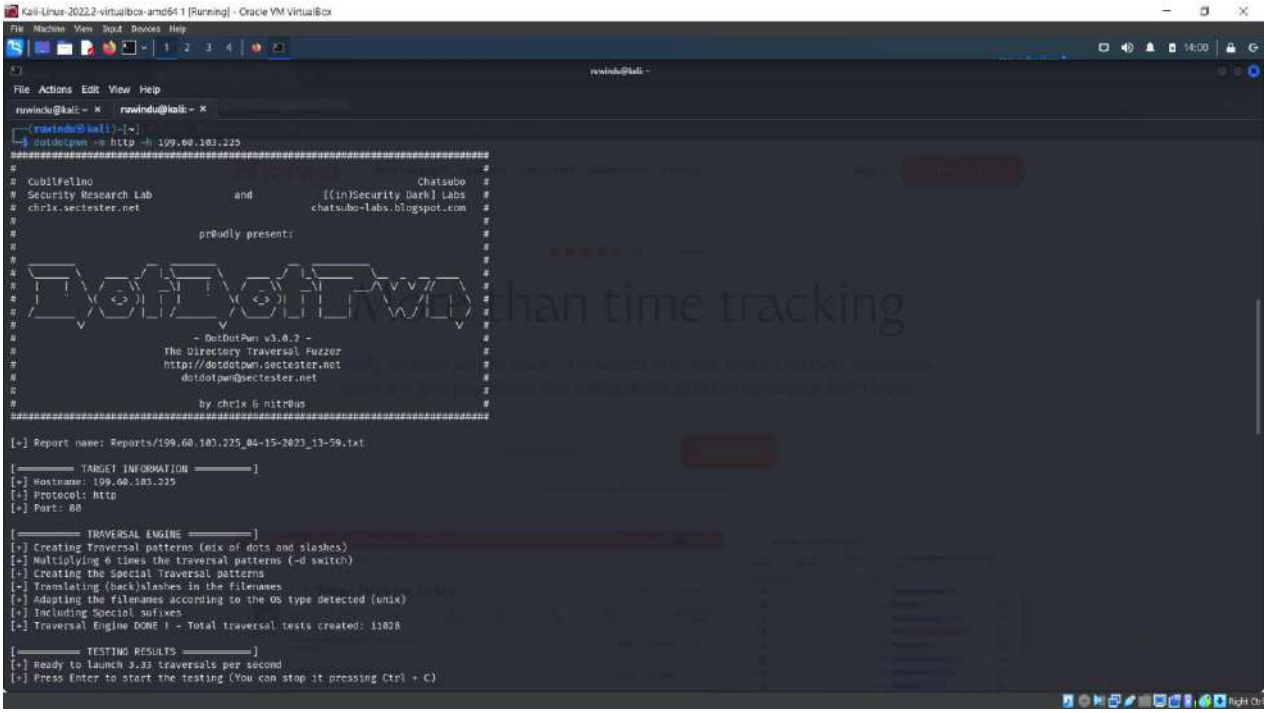
Using dotdotpwn tool

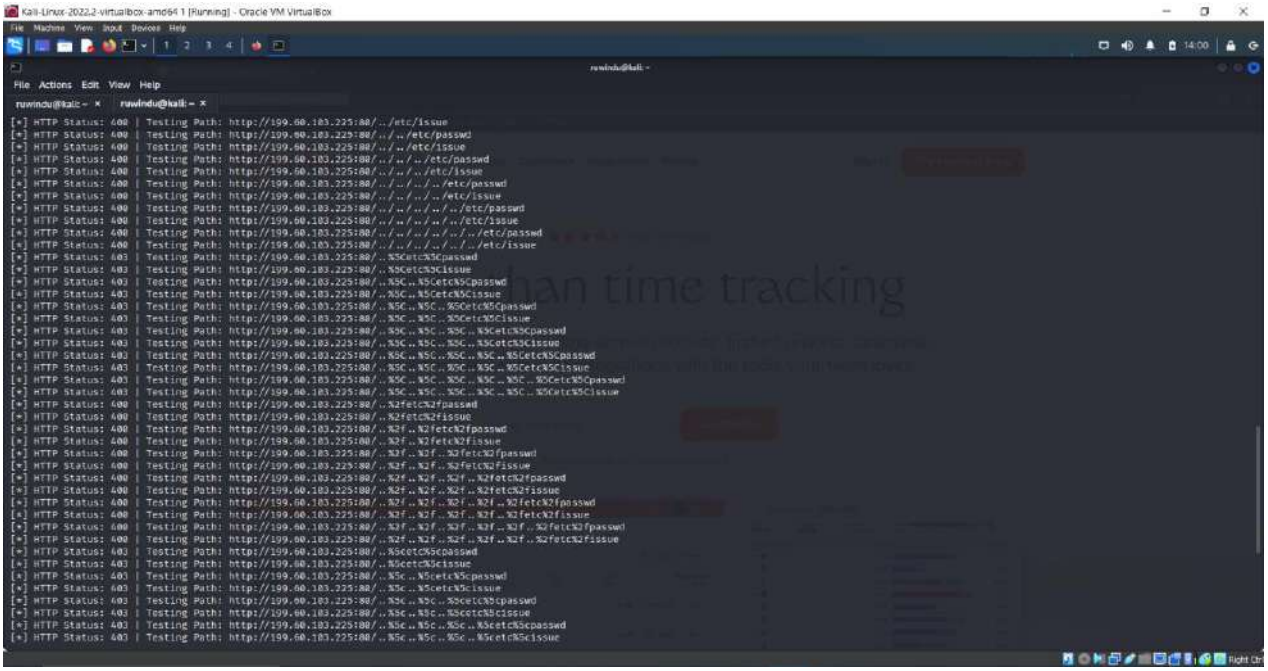
Users are able to find vulnerabilities in a wide number of protocols, servers, and apps with the help of DotDotPwn, which is a tool for doing penetration testing. DotDotPwn is open-source. Throughout the whole of its operation, the malware makes use of several methods, such as directory traversal and file inclusion, in order to find and exploit vulnerabilities that are present on target computers.

Use ping command and fid the IP address



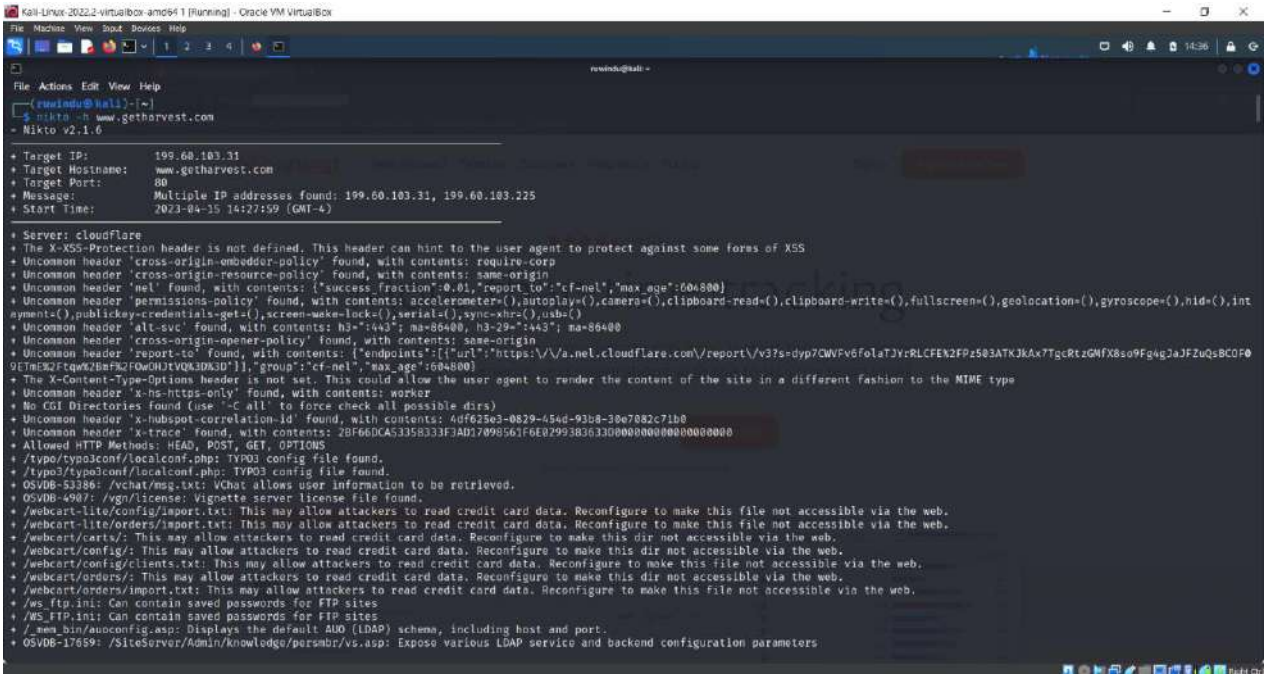
Get the IP address and use the dotdotpwn tool



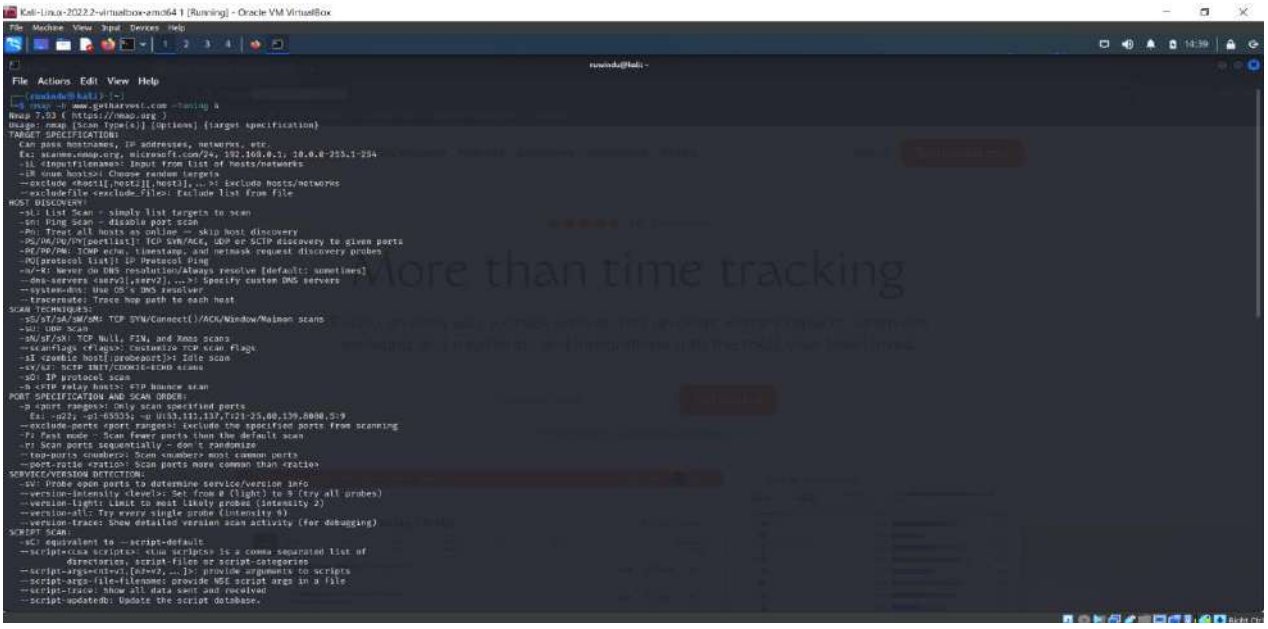


Using Nikto tool

The first scan did not make any mention of the available options, rather, it was only a routine scan of the targeted website.



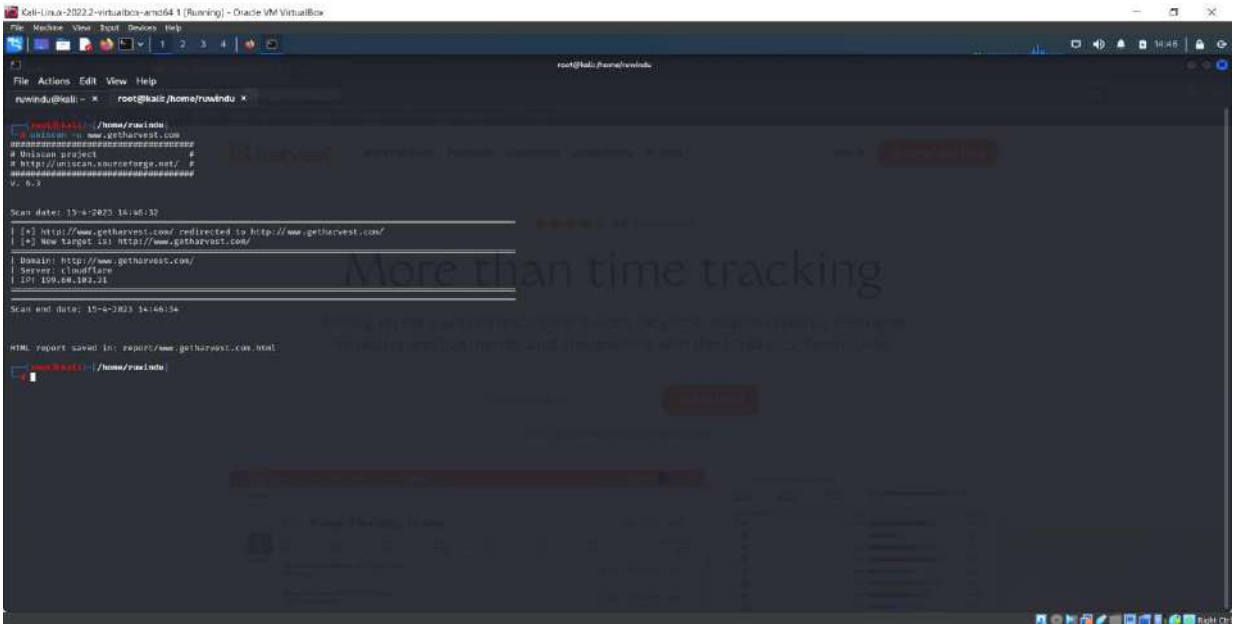
After that, we look at the option number 4 for the injection command.



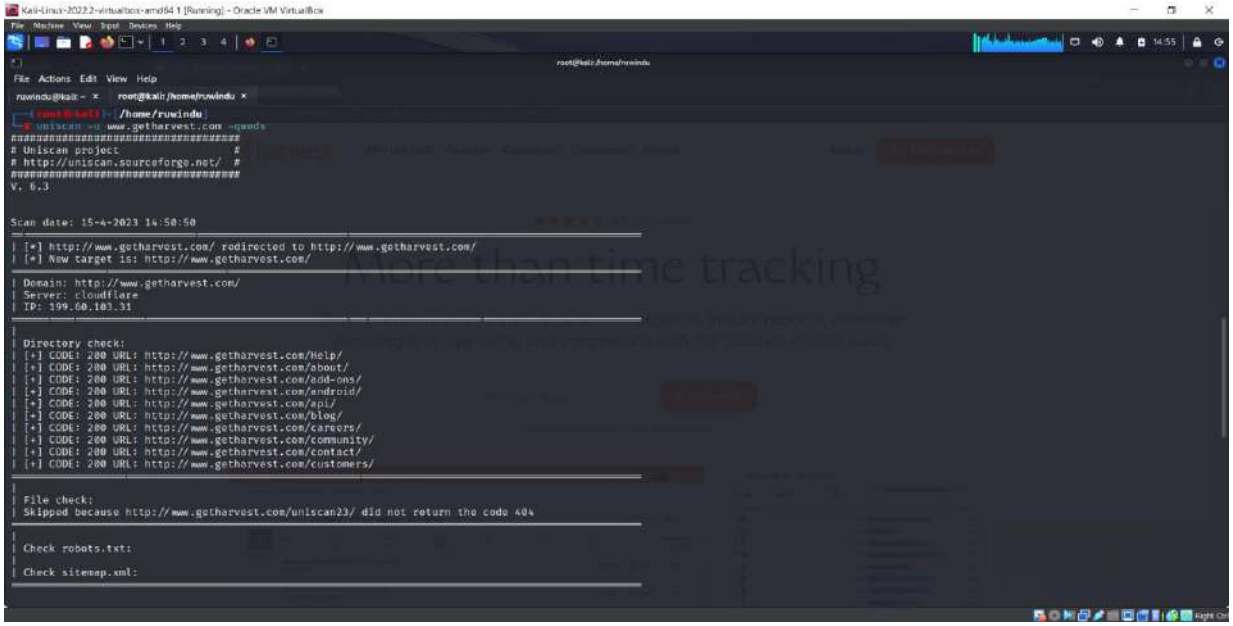
This scanner did not uncover any vulnerabilities in the system throughout its investigation. Despite the fact that a number of errors have been pointed out, as well as the availability of certain information that, according to the information P5 scale, also contains errors.

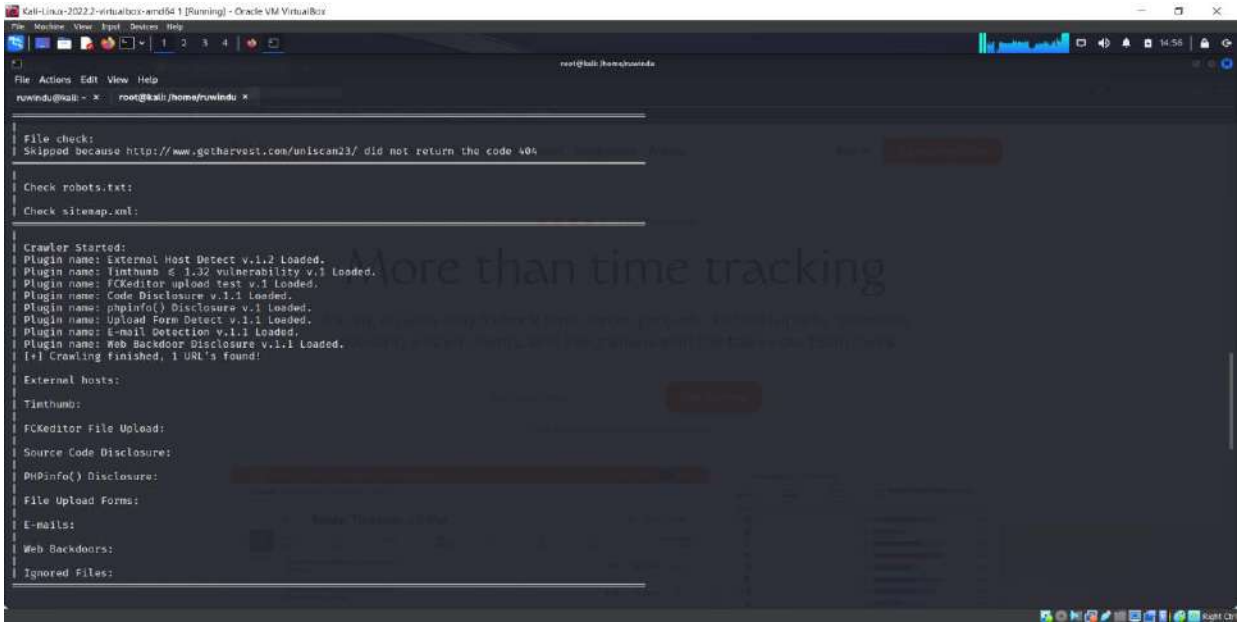
Using Uniscan tool

In order to do a speedy scan, use the –u option, and then as the input, supply either the IP address or the URL.

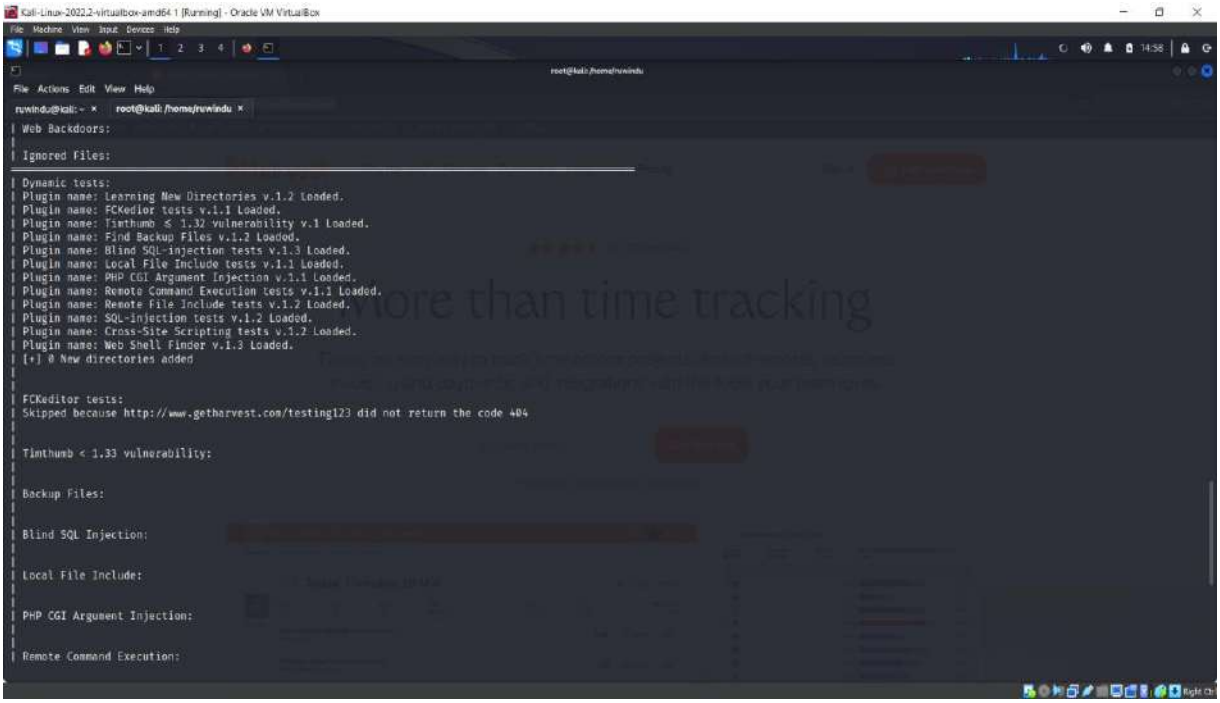


After the command used uniscan –u www.getharvest.com -qweds



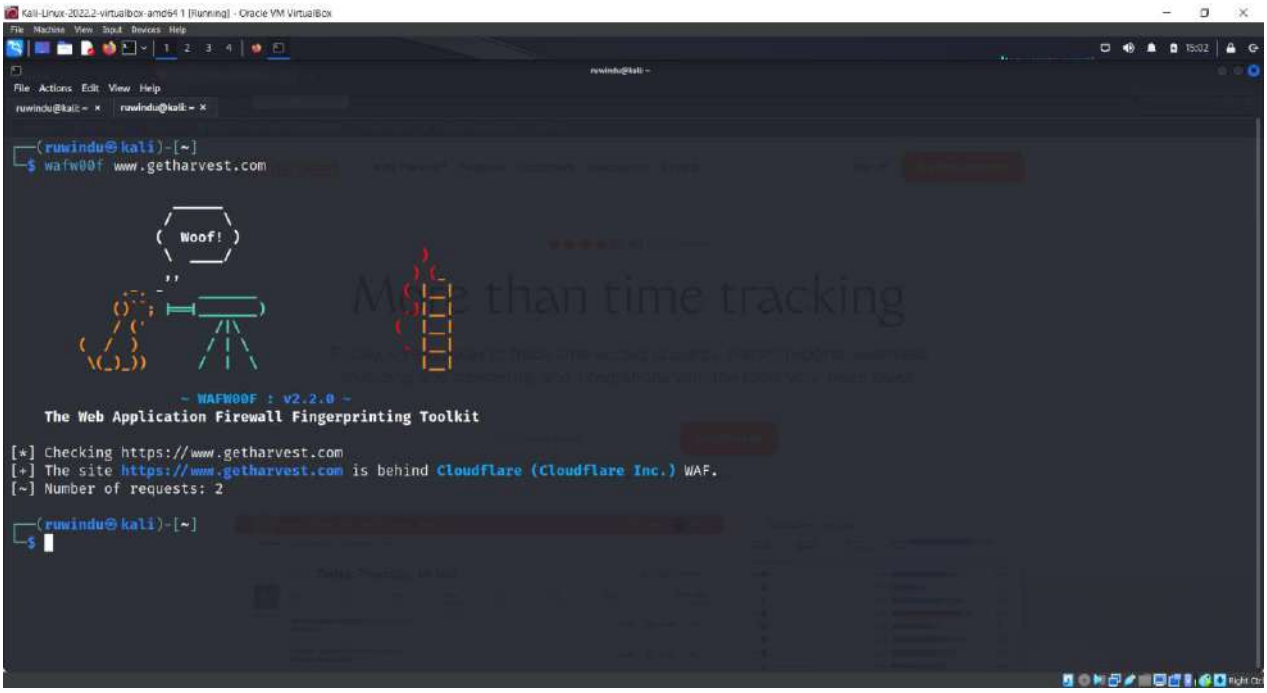


This is the section of the website where we were able to find some of the material that was hosted by other parties. In this specific case, web addresses, or URLs, were found.



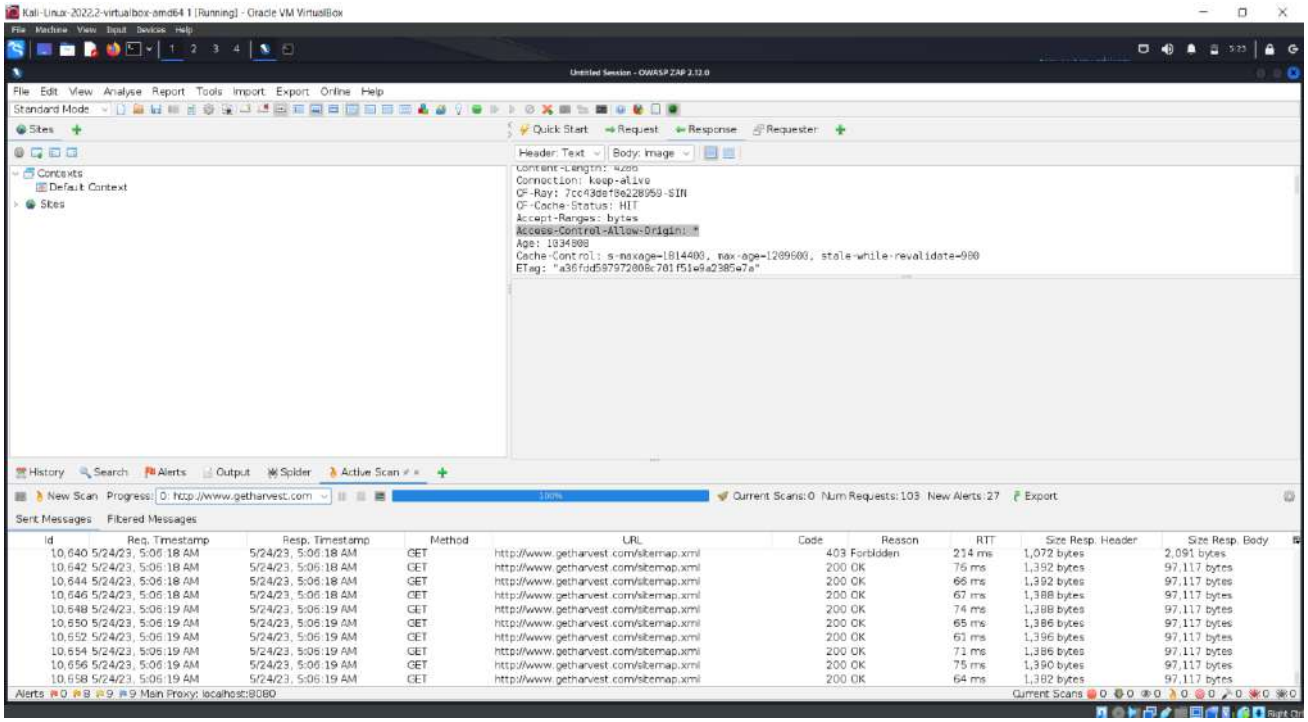
Using wafw00f tool

The website www.getharvest.com seems to be secured by a WAF or some other form of security solution when we run the wafw00f program with the targeted URL. This is something that we are able to witness when we run the tool.

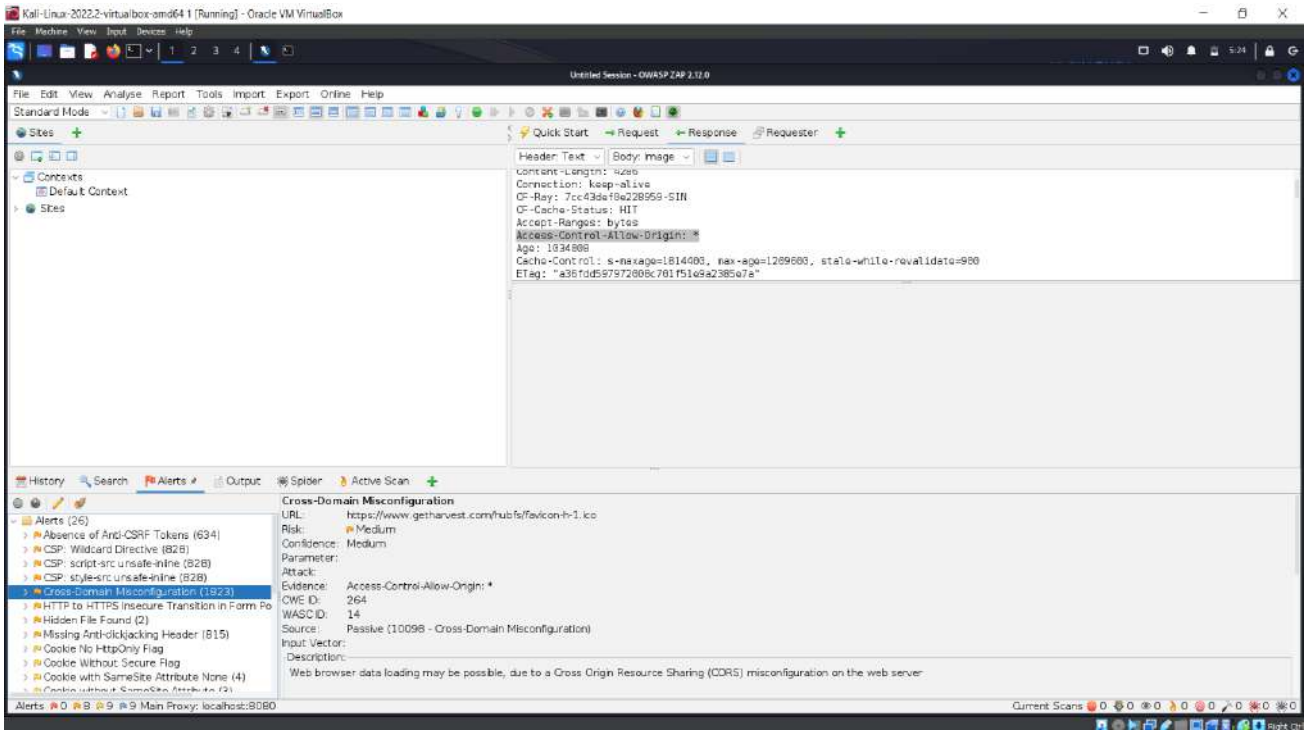


We were able to determine that there is an operational firewall by doing this rather straight forward test.

Using OWASP-ZAP tool



Found 103 Requests.



Found 26 Alerts.

Vulnerabilities found

Cross-Domain Misconfiguration

Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) Misconfiguration on the web server

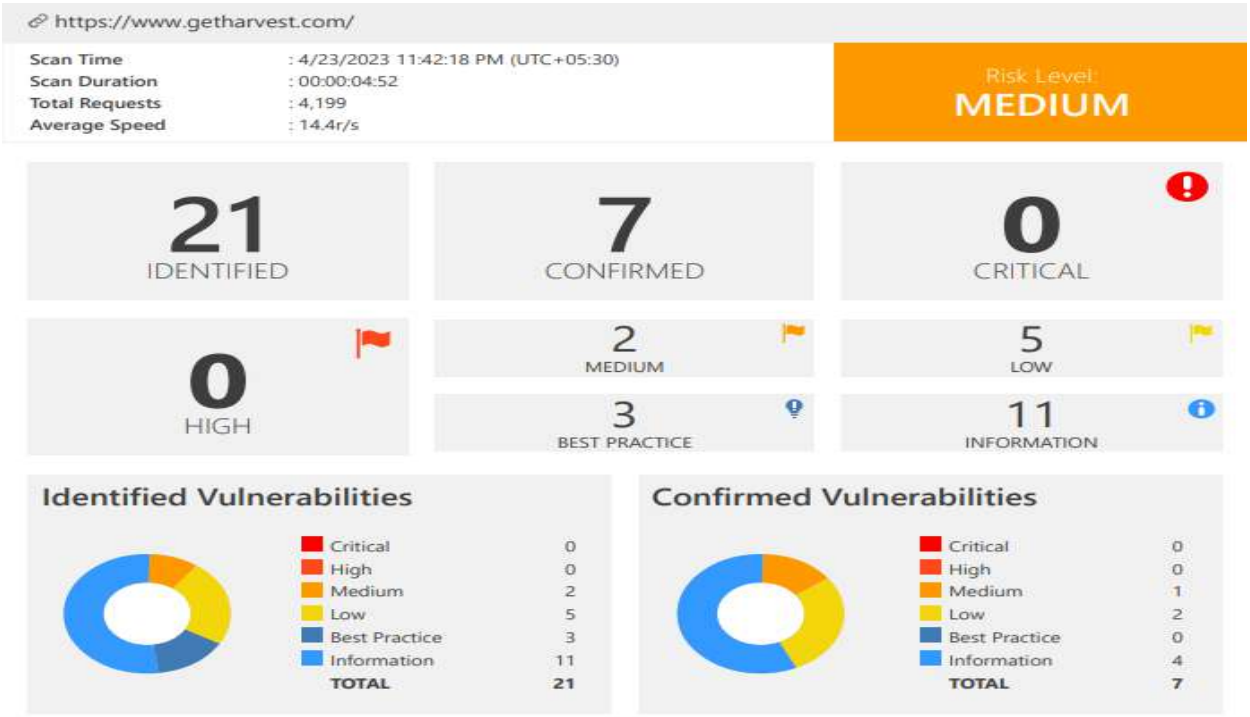
Solution

Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).

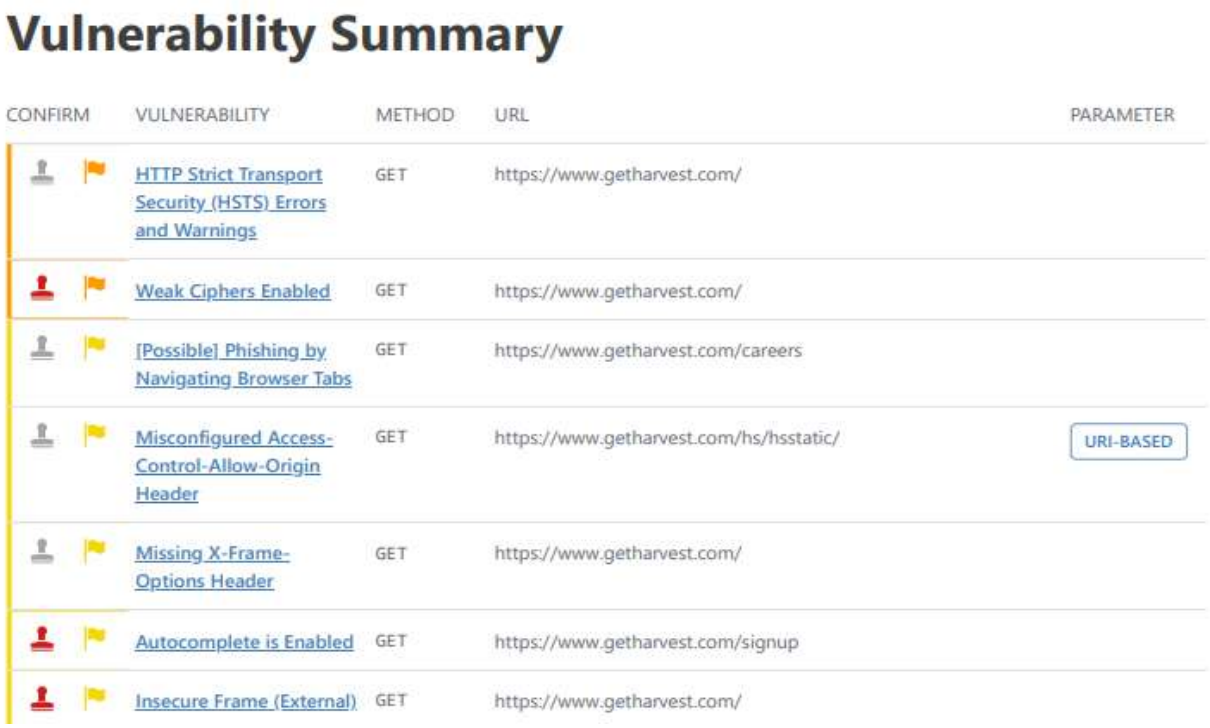
Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.

Using Netsparker

I'm doing a vulnerability scan of www.getharvest.com with the help of Netsparker professional Edition (V), which I'm using for my Audit.



After doing a scan of the domain, I was able to identify a total of 21 vulnerabilities related to the domain, including 2 vulnerabilities with a medium risk.



Expect-CT Not Enabled	GET	https://www.getharvest.com/	
Missing X-XSS-Protection Header	GET	https://www.getharvest.com/	
Subresource Integrity (SRI) Not Implemented	GET	https://www.getharvest.com/	
Email Address Disclosure	GET	https://www.getharvest.com/security	
Generic Email Address Disclosure	GET	https://www.getharvest.com/contact	
Missing object-src in CSP Declaration	GET	https://www.getharvest.com/	
Out-of-date Version (jQuery)	GET	https://www.getharvest.com/customers	
Reverse Proxy Detected (Envoy)	GET	https://www.getharvest.com/hs-fs/	
Sitemap Detected	GET	https://www.getharvest.com/sitemap.xml	

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Web Application Firewall Detected	GET	https://www.getharvest.com/%3Cscript%3Ealert(0)%3C/script%3E	URI-BASED
	Cross-site Referrer Leakage through Referrer-Policy	GET	https://www.getharvest.com/	
	File Upload Functionality Detected	GET	https://www.getharvest.com/contact	
	Forbidden Resource	POST	https://www.getharvest.com/	
	OPTIONS Method Enabled	OPTIONS	https://www.getharvest.com/	

www.getharvest.com has been found to have the following identified vulnerabilities

Identified vulnerabilities in www.getharvest.com

Vulnerability 05 - [Possible] Phishing by Navigating Browser Tabs (Medium)

Netsparker was able to discover possible phishing by cycling through the tabs of the browser; however, it was unable to verify that the vulnerability existed.

Open windows that make use of ordinary hrefs that have the tag target="_blank" are eligible to have their own window.opener.location has been altered. Alter the content of the parent site to something else at a later time, even if it is hosted on a different domain.

Impact

Although this vulnerability does not make it possible to execute scripts, it does make it possible to conduct phishing attacks in which the parent tab is silently replaced. In the event that the links do not have the rel="noopener noreferrer" tag, a third-party website is able to alter the URL of the source tab by utilizing the window.opener.location.assign property.users may be duped into believing that they are still on a reliable page, which would then encourage them to provide their personal information on the malicious website.

Vulnerabilities

3.1. https://www.getharvest.com/careers

External Links

- https://apply.workable.com/harvest/j/D9227FC3D9/
- https://apply.workable.com/harvest/j/81E091FA7F/
- https://apply.workable.com/harvest/j/C2D2137D75/

Certainty

Request

```
GET /careers HTTP/1.1
Host: www.getharvest.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: __cf_bm=e_OUfI7OKWL2grbGLgFqeHD9Jr82bUk7N_P.JFkjTNE-1682273541-0-AZ6VlpaHP5tCTlvc383hS0sFSR3JOf
Jxn2dRpP+X1jKGDPgVMXFPIJztAls9CvRP8klOdAaPrs3OQKBfvN8mg40=; __cfruid=5e8a9e4f9a7f56b92e59609bdec07f3217
bad546-1682273541
Referer: https://www.getharvest.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 1481.6599 Total Bytes Received : 47610 Body Length : 45846 Is Compressed : No

```
HTTP/1.1 200 OK
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=8y0SA4sonFAI0hVbQig9SLgsk
IOY59%20NRdh0E3svXEsgTUXrA6VZDRVAev7IKhpNzk3HhQr%2FbFLevmB5N3GiYZE4hjdkF%2ByvtAqIaXVzXglxKnCmET%2BnHQiG
2zKG4DPi%2Fq55XKh3MkFa6M2b8xuPxg%3O%3D"}],"group":"cf-nel","max_age":604800}
X-Hs-Https-Only: worker
X-HS-Cache-Config: BrowserCache-5s-EdgeCache-180s
Cache-Control: s-maxage=10800, max-age=0
ETag: W/"6dc27699bbda086Sc560a1ccb8eb350d"
CF-RAY: 7bc81422cb1db94b-AMS
Strict-Transport-Security: max-age=31536000
Transfer-Encoding: chunked
X-HS-Content-Id: 49165356092
Server: cloudflare
Link: </hs/hsstatic/HubspotToolsMenu/static-1.154/js/index.js>; rel=preload; as=script,</hs/hsstatic/co
s-i18n/static-1.53/bundles/project.js>; rel=preload; as=script
X-HS-Hub-Id: 19495563
X-HS-Prerendered: Thu, 20 Apr 2023 14:33:39 GMT
X-HS-CF-Cache-Status: MISS
Connection: keep-alive
Referrer-Policy: no-referrer-when-downgrade
Vary: Accept-Encoding
Edge-Cache-Tag: CT-49165356092,P-19495563,W-43417846325,CW-63498358272,D8-5244780,E-63498340476,E-63498
340511,E-63498365851,E-63501167527,E-63501334614,E-63501334620,E-63501347970,E-63501347972,E-6350137205
6,MENU-43833013427,MENU-43833013670,RA-63498358574,RA-63501360907,RA-66499715655,RA-66500174772,RA-6650
0225656,RA-66500293048,RA-66500301225,RA-68214555691,PGS-ALL,SW-1,GC-63501624645,GC-64232839204,TS-6350
1334655
X-HS-Cache-Control: s-maxage=10800, max-age=0
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
Last-Modified: Thu, 20 Apr 2023 14:33:39 GMT
Content-Type: text/html; charset=UTF-8
NEL: {"success_fraction":0.01,"report_to":"cf-nel","max_age":604800}
Content-Security-Policy: upgrade-insecure-requests
Date: Sun, 23 Apr 2023 18:13:07 GMT
Con
…
<div class="flex-col col-large">
<ul class="jobs-listings link-list">



<li><a href="https://apply.workable.com/harvest/j/D9227FC3D9/" target="_blank">Marketing Operations Man
ager</a></li>

<li><a href="https://apply.workable.com/harvest/j/81E091FA7F/" target="_blank">Senior Data Analyst</a>
</li>
```

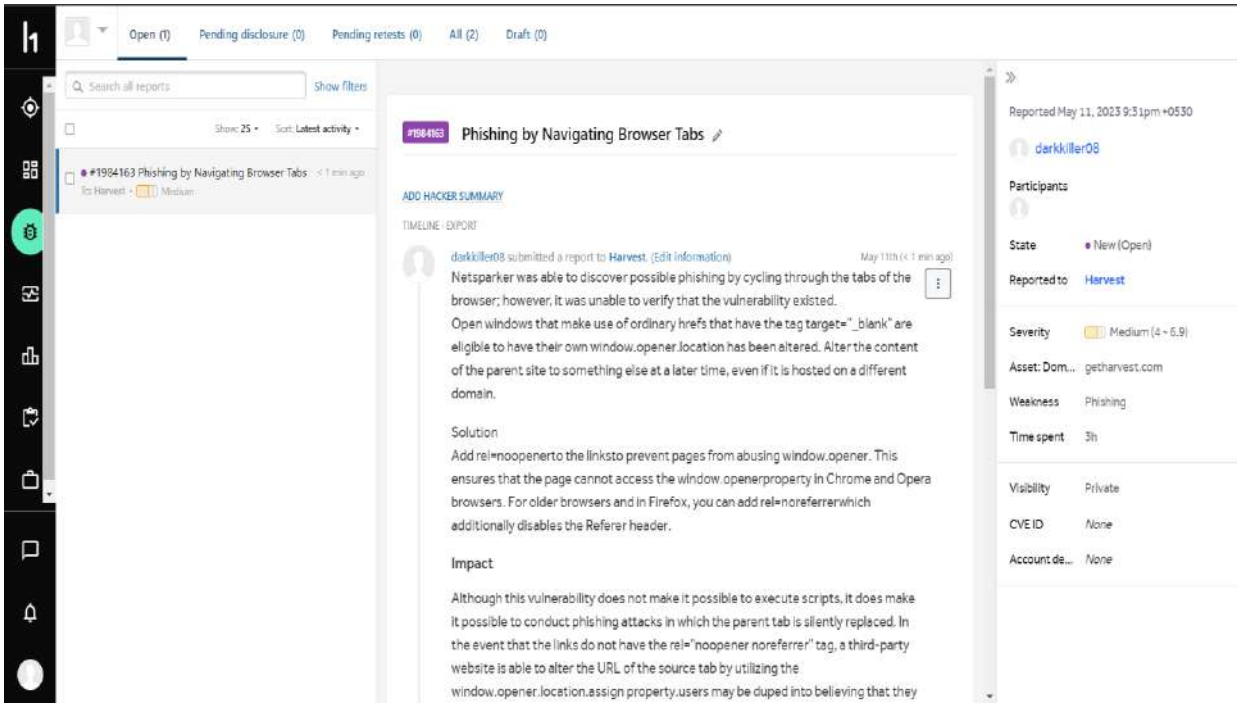
Solution

Add rel=noopenerto the linksto prevent pages from abusing window.opener. This ensures that the page cannot access the window.openerproperty in Chrome and Opera browsers. For older browsers and in Firefox, you can add rel=noreferrerwhich additionally disables the Referer header.

Conclusion of the Report 05

We were told of the vulnerabilities that the domain possessed, as well as the manner in which we may utilise particular technologies to discover them and fix them. A few examples of the sorts of tools that may be used are knockpy, dotdotpwn, nikto, uniscan, wafw00f, owsap-zap and Netsparker. Other examples include wafw00f and uniscan. Following that, we do an investigation of the vulnerability by using a few additional websites in order to get a more in-depth knowledge of the nature of the problem that is present with this web application. Following the discovery of vulnerabilities, we made an effort to put one of those vulnerabilities to the test and demonstrate that it had a potentially damaging issue. This attempt was performed after the vulnerabilities had been identified. We were successful in proving that there was a problem that had the potential to cause harm. Despite the fact that we had arrived at the conclusion that the vulnerability was not a significant one at the time, we were given a great amount of details that we found to be rather fascinating. Despite the fact that we had determined that the vulnerability did not pose a significant threat, we were given a significant amount of information.

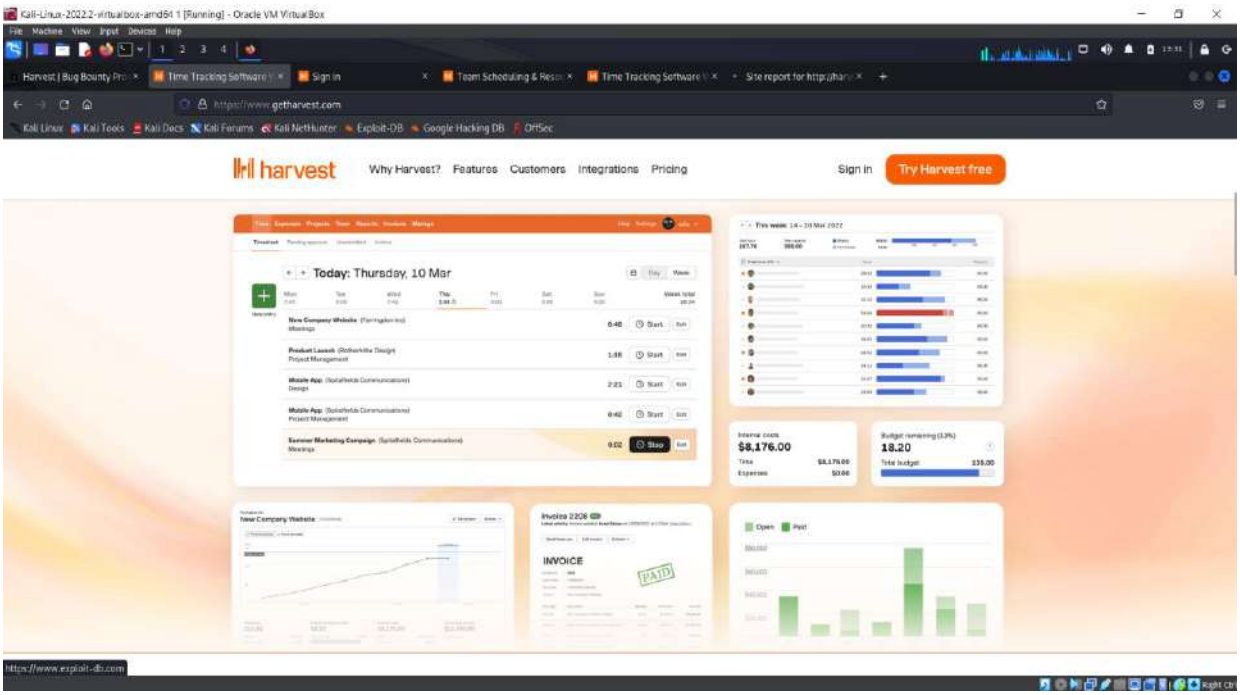
HackerOne Submitted Report Screenshot



vi. Report 06

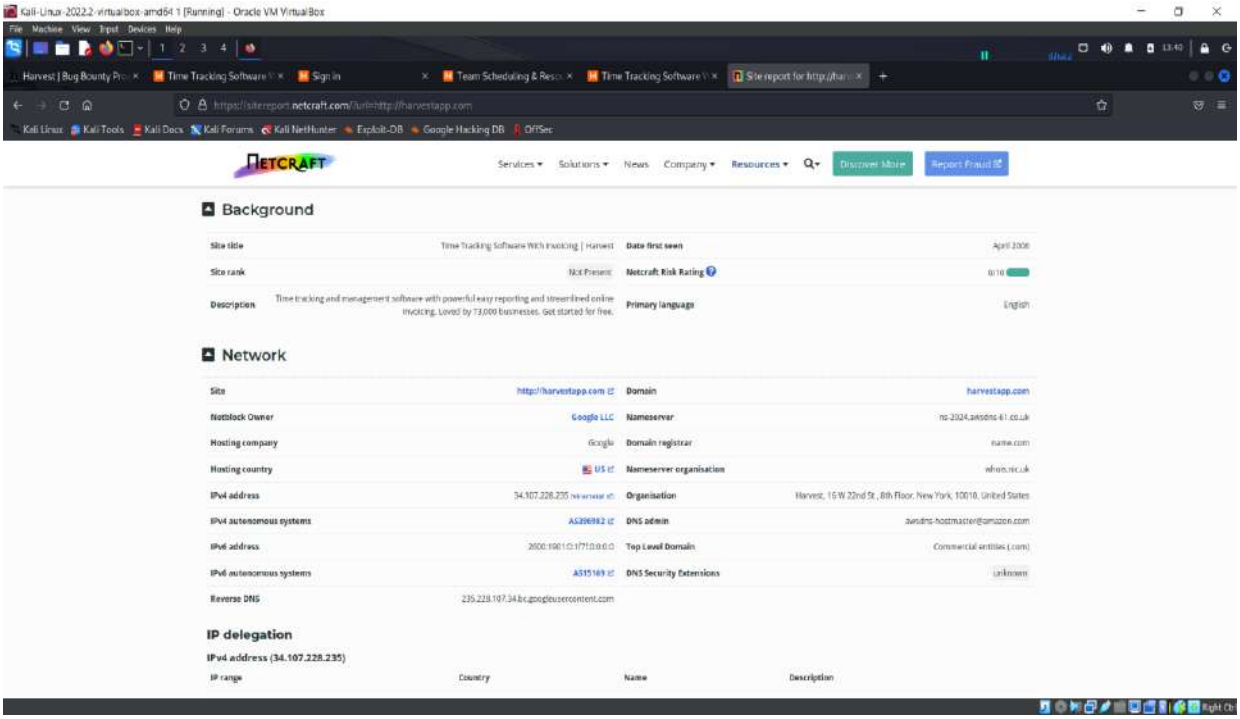
Target information: http://harvestapp.com

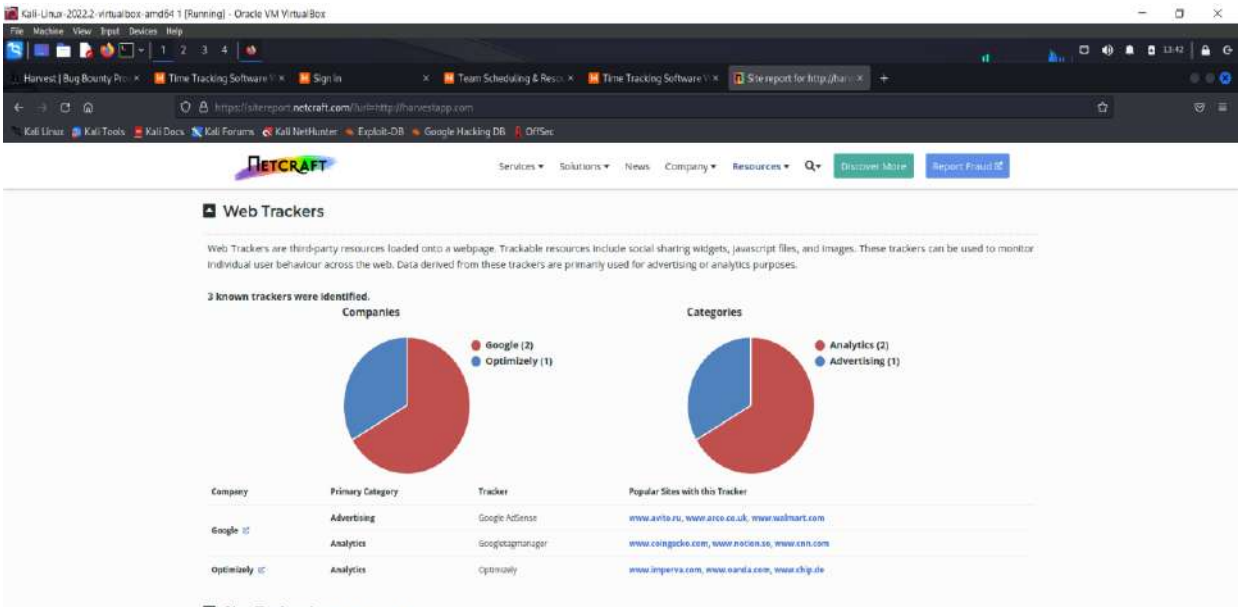
This investigation's goals are twofold: first, to ascertain whether or not the target domain (http://harvestapp.com) has any vulnerabilities, and second, to ascertain the degree of peril that is connected with each of those flaws in the event that it does. This study will also evaluate how much danger is connected with each of those concerns if it turns out that the target domain does indeed comprise vulnerabilities. If vulnerabilities are discovered while the investigation is being carried out, more work will be done to establish whether or not the target domain also contains vulnerabilities. This will be done in the event that vulnerabilities are discovered. The fundamental objective of the investigation is to establish whether or not the target domain has any subdomains that are deficient in any characteristic that would enhance their capability to be described.

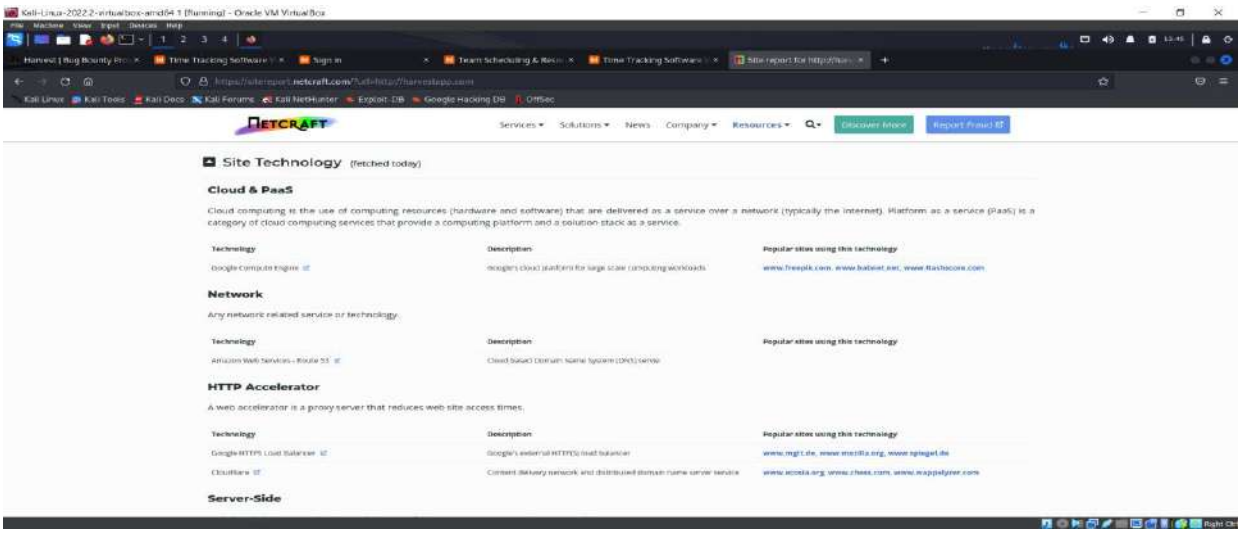


Information Gathering For Target Domain

Let's have a look at the myriad of various options we have at our disposal so that we may not only find out what the technical capabilities of http://harvestapp.com are, but also other information that is pertinent to the situation. Since Netcraft is the only tool we now have access to, let's create an account for it and do some research on the information we may get by using it. Let's put Netcraft to the test and search for ourselves to see what type of information we can unearth given that this is the only resource we now have access to. Let's have a look at the information that can be collected from utilizing Netcraft because that is all we are doing for the time being

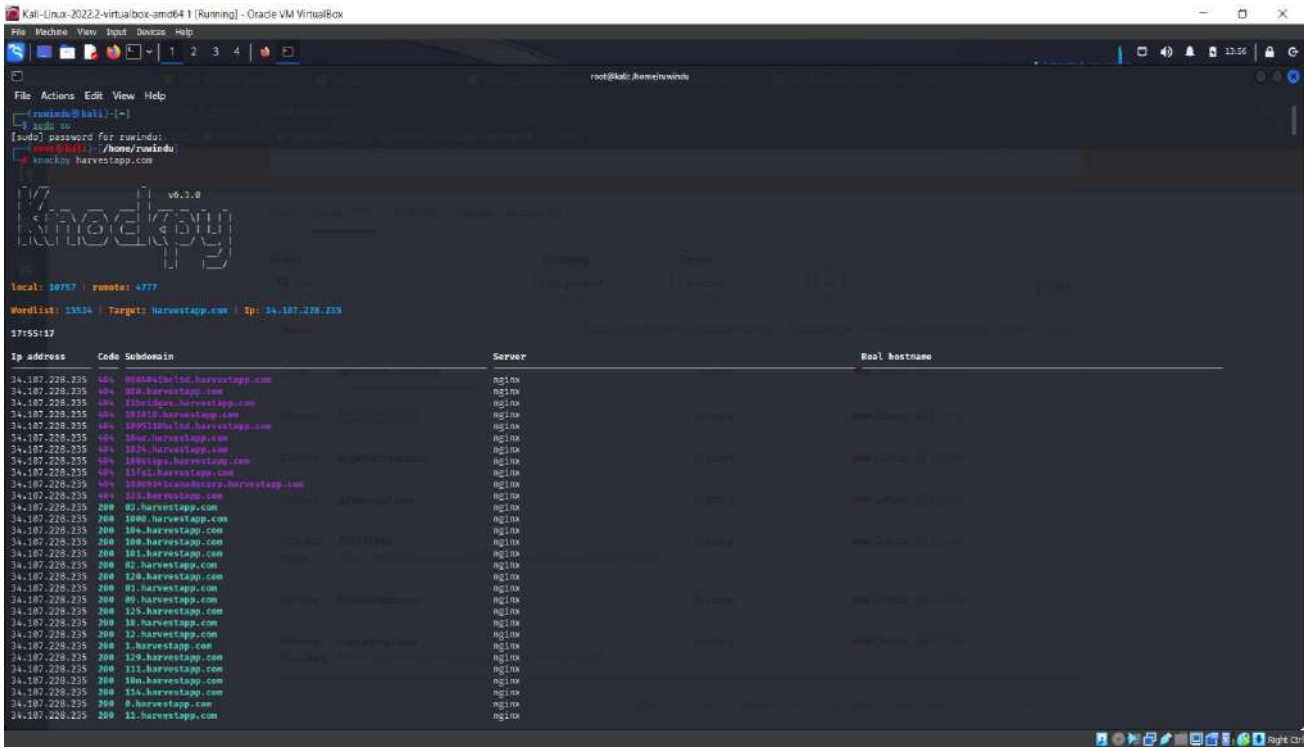

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Background
Network
IP delegation

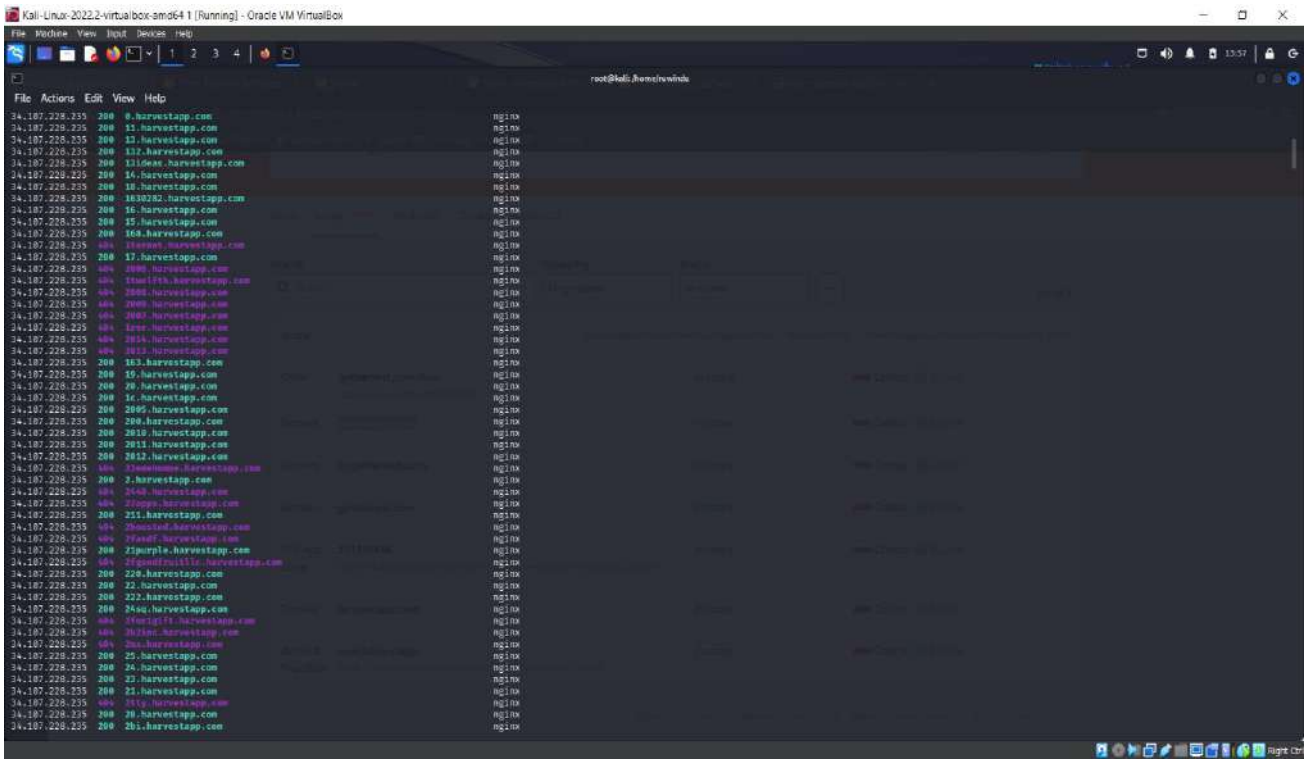

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Web Trackers
3 known trackers were identified.
Companies
Categories
Google (2)
Optimizely (1)
Analytics (2)
Advertising (1)

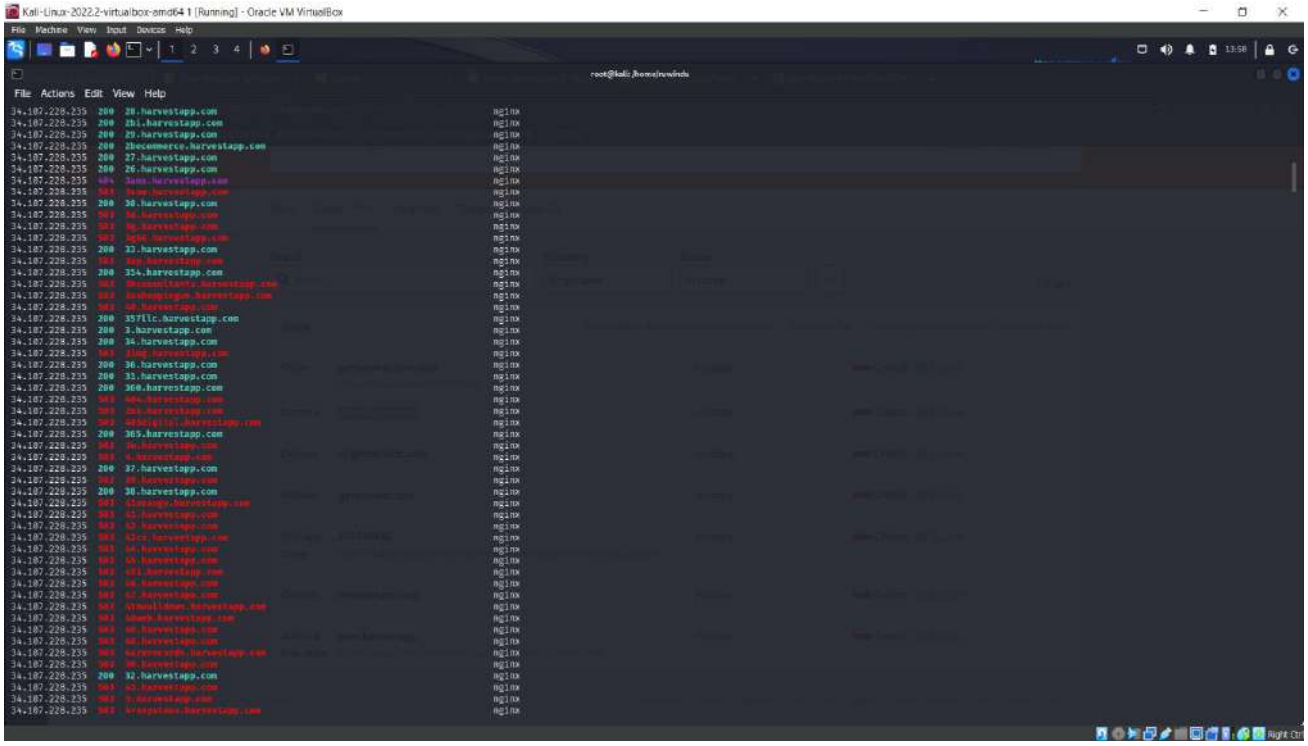

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Site Technology (fetched today)
Cloud & PaaS
Network
HTTP Accelerator
Server-Side

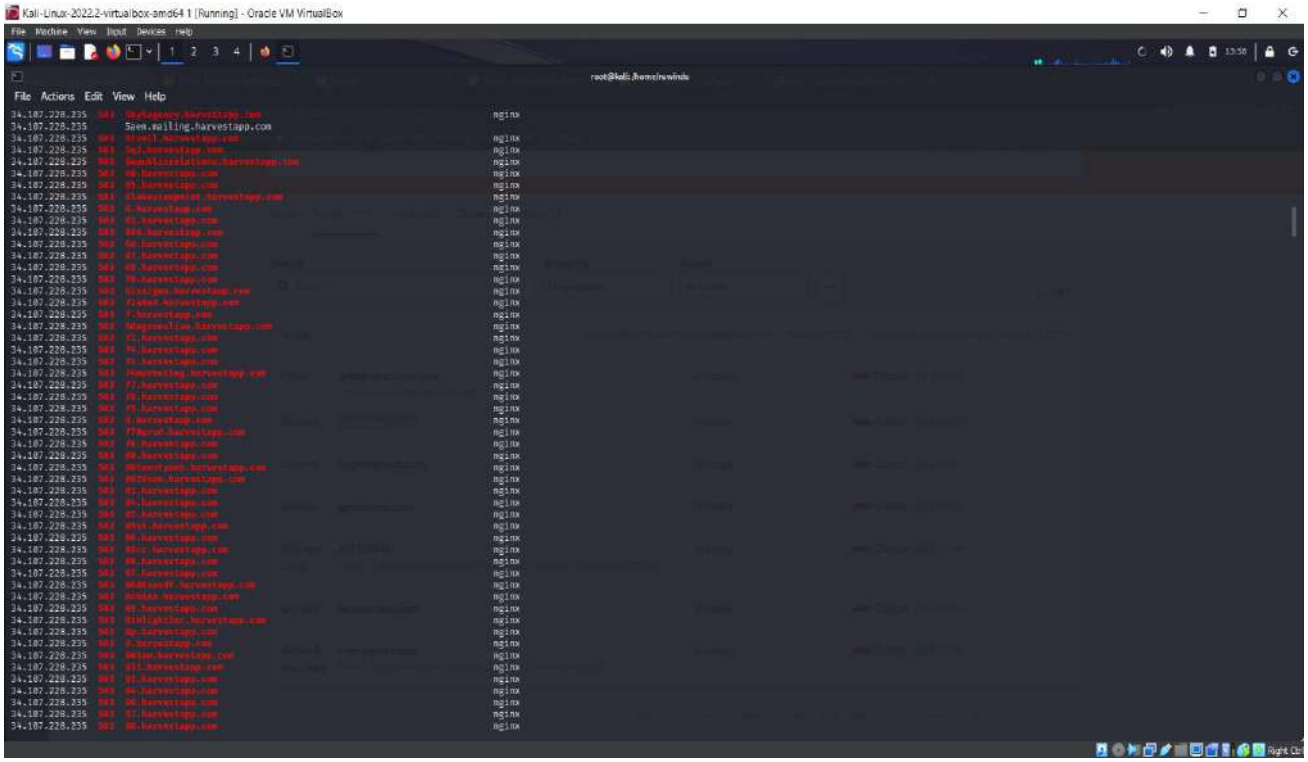
Using knockpy tool

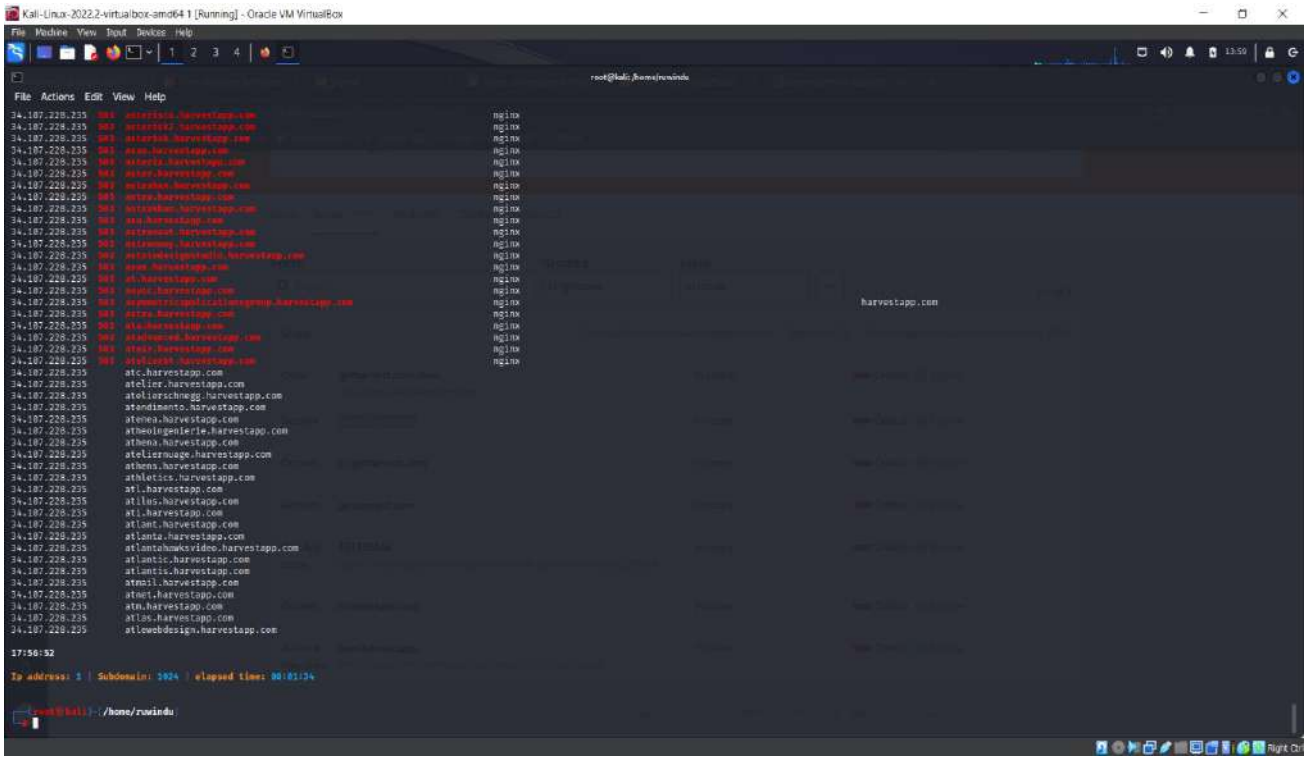
Using the knockpy tool, it is possible to collect subdomain names through scraping data sources, carrying out reverse DNS sweeping, and taking part in recursive brute forcing.






Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help

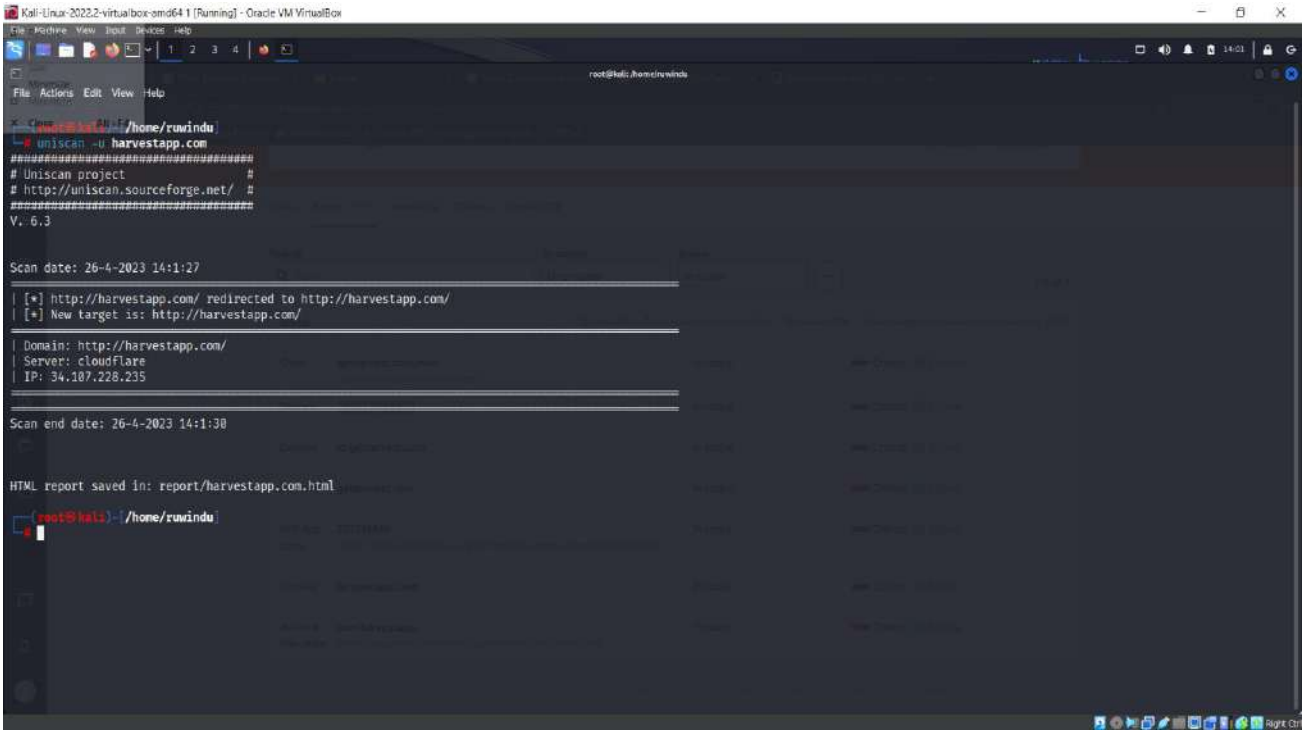

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help



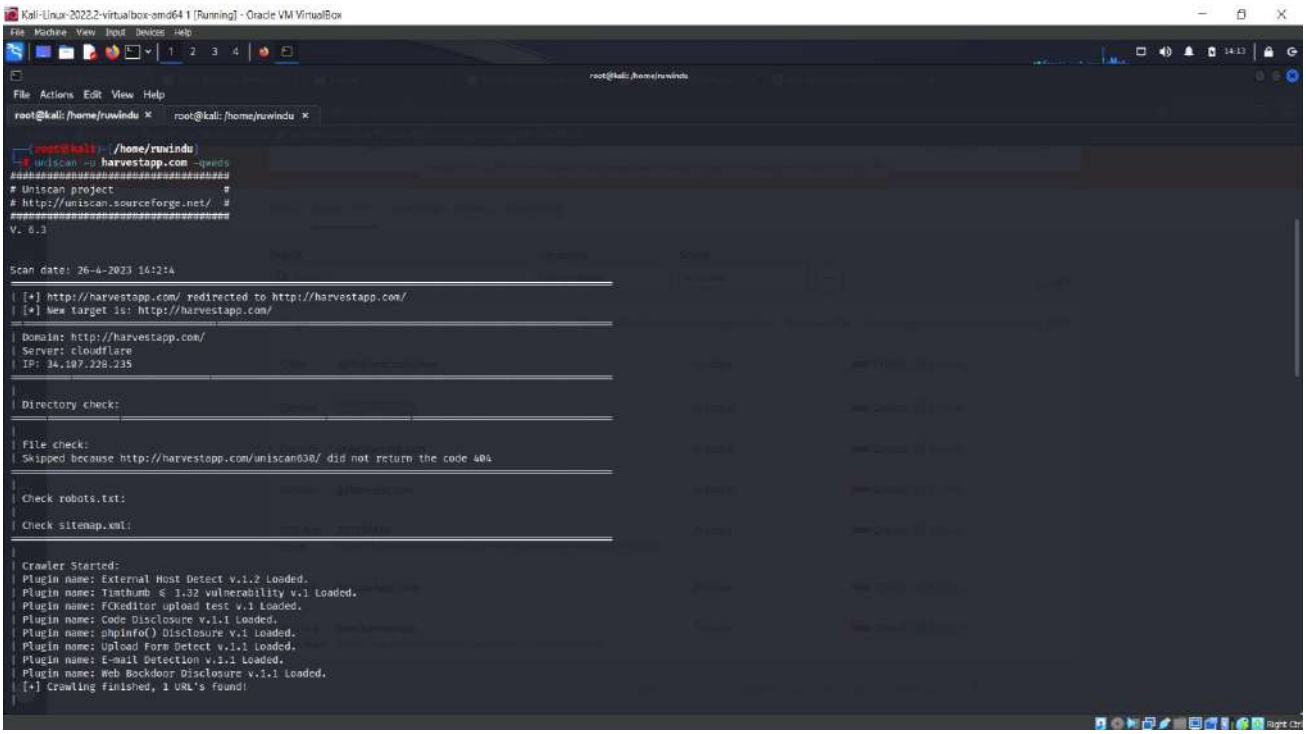
Since the harvestapp.com subdomains have been recorded, we are now able to see them in this way after the completion of the enumeration of the subdomains that are associated with harvestapp.com. It really shouldn't come as much of a surprise to anybody that the IP address and name server that are used by each and every one of the subdomains that are kept under the harvestapp.com domain are the same ones that are used by the main domain itself. These details are shared by all of the subdomains that are maintained under the harvestapp.com domain. All of the subdomains that are managed under the harvestapp.com domain have access to these common information. All of the subdomains that are included under the harvestapp.com domain are in agreement with one another about these particulars. It is possible for us to identify that this is a mobile application due to the fact that the program's real hostname is shown. Because of this, we are able to deduce that it is a mobile application. The fact that the correct hostname is shown here serves as the basis for our conclusion and provides the structure around which it is built. We are now in a position to make use of it as a direct consequence of this, which has opened up opportunities for us to do so and has made it feasible for us to do so. Because of this, it is now within our means to do so.

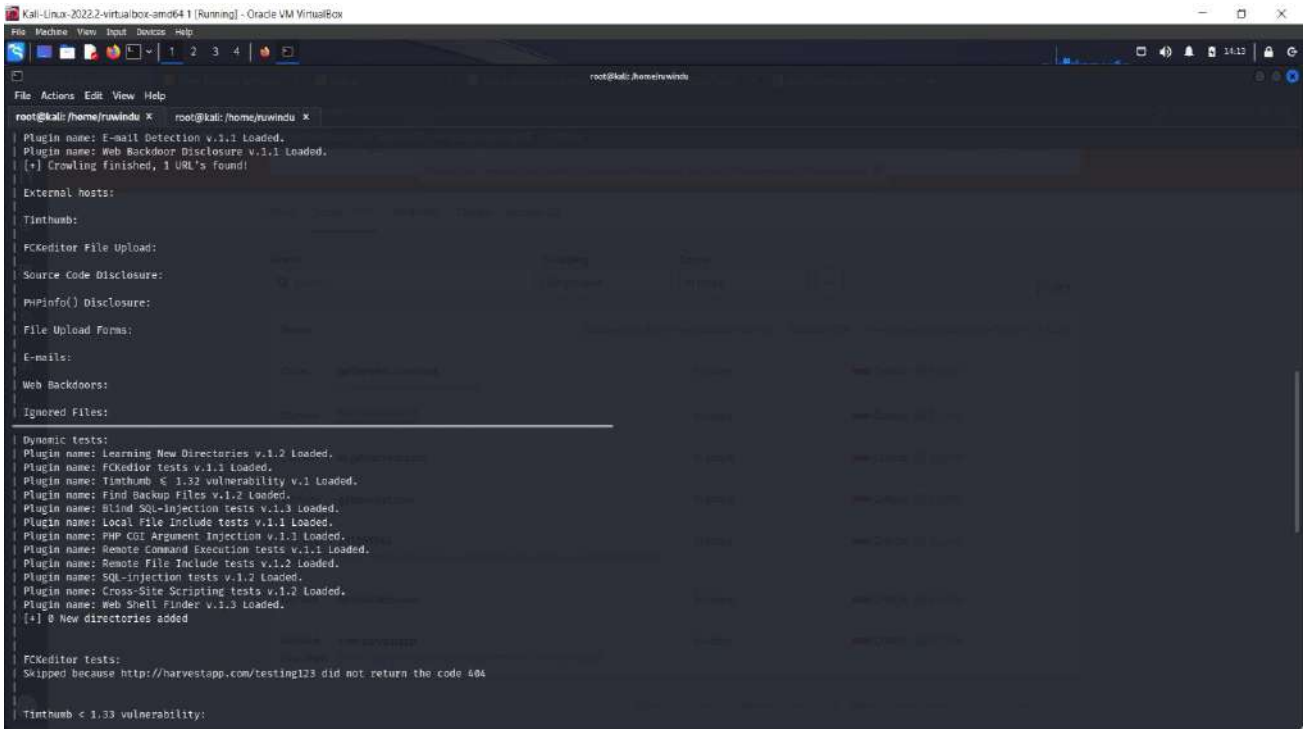
Using Uniscan tool

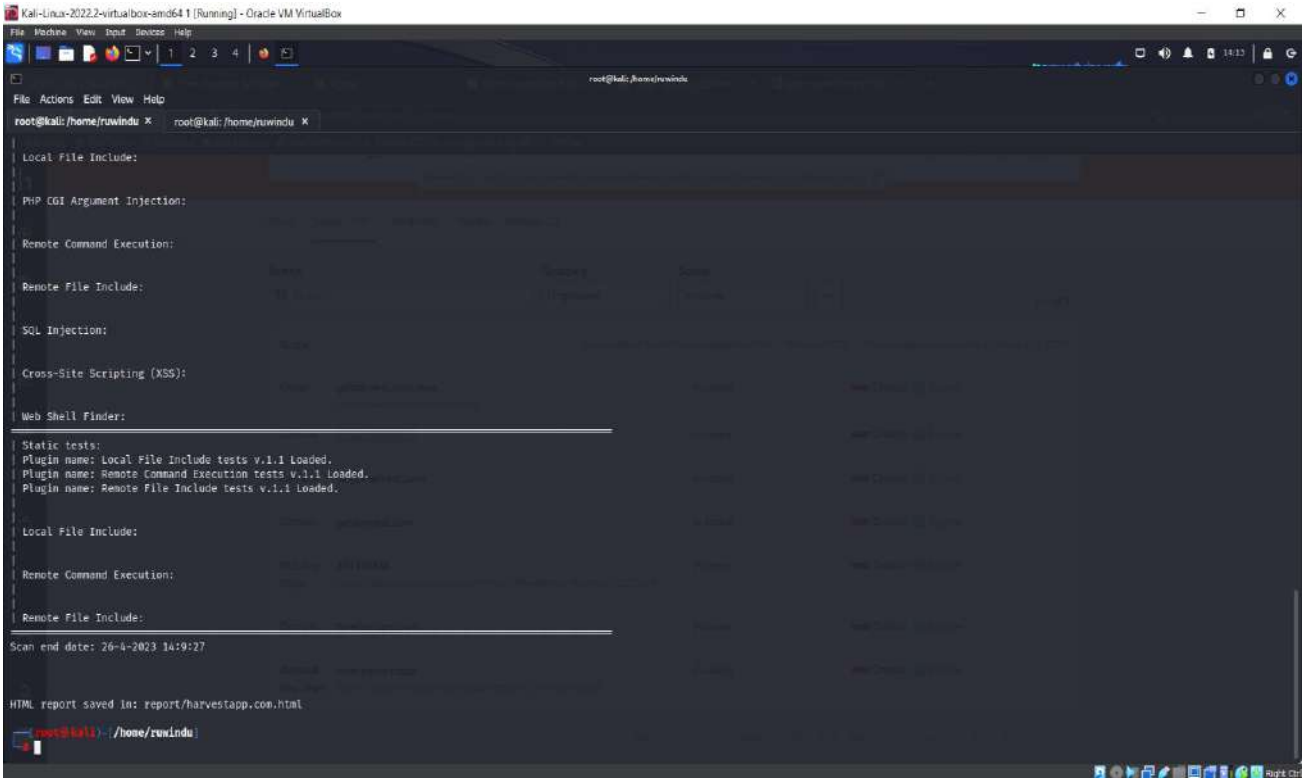
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u domain -qweds command:

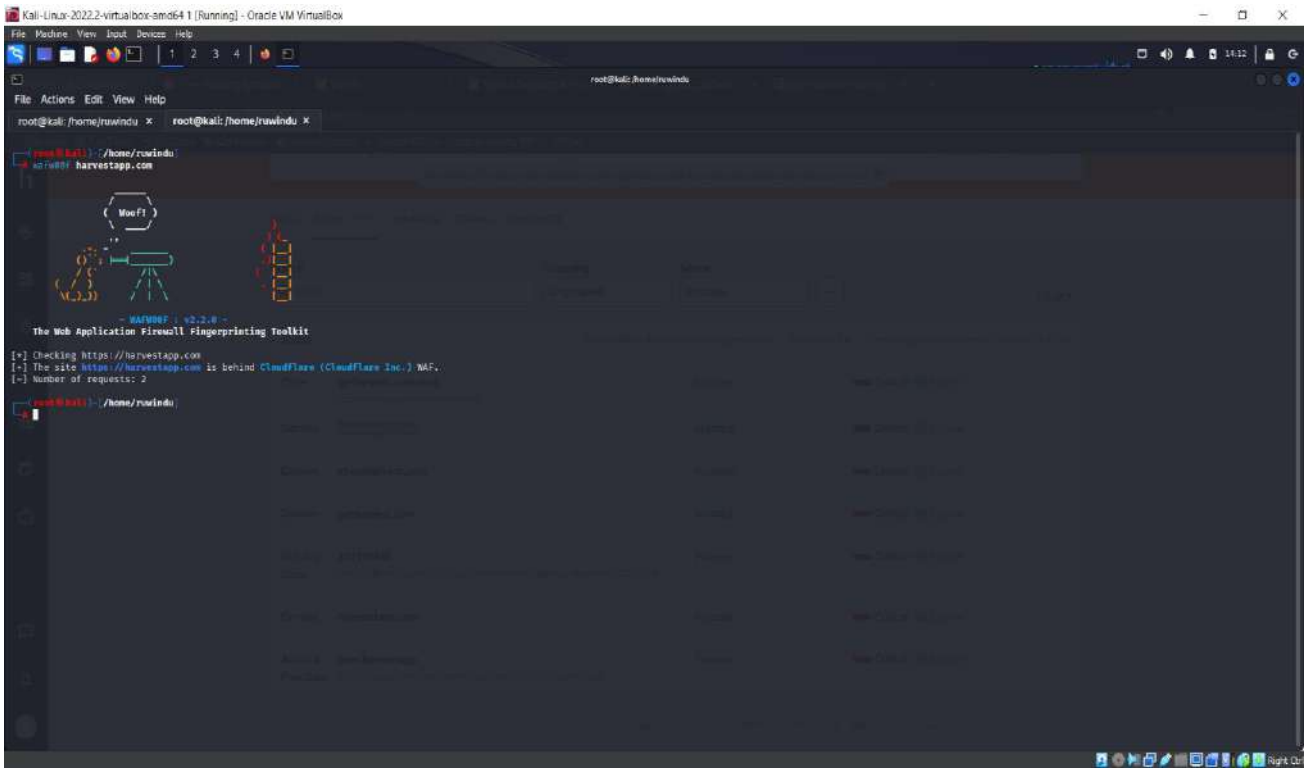



Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: /home/ruwindu
root@kali: /home/ruwindu
| Plugin name: E-mail Detection v.1.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| [+] Crawling finished, 1 URL's found!
| External hosts:
| Timthumb:
| FCKeditor File Upload:
| Source Code Disclosure:
| PHPinfo() Disclosure:
| File Upload Forms:
| E-mails:
| Web Backdoors:
| Ignored Files:
| Dynamic tests:
| Plugin name: Learning New Directories v.1.2 Loaded.
| Plugin name: FCKedior tests v.1.1 Loaded.
| Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
| Plugin name: Find Backup Files v.1.2 Loaded.
| Plugin name: Blind SQL-injection tests v.1.3 Loaded.
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.2 Loaded.
| Plugin name: SQL-injection tests v.1.2 Loaded.
| Plugin name: Cross-Site Scripting tests v.1.2 Loaded.
| Plugin name: Web Shell Finder v.1.3 Loaded.
| [+] 0 New directories added
| FCKeditor tests:
| Skipped because http://harvestapp.com/testing123 did not return the code 404
| Timthumb < 1.33 vulnerability:


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali: /home/ruwindu
root@kali: /home/ruwindu
| Local File Include:
| PHP CGI Argument Injection:
| Remote Command Execution:
| Remote File Include:
| SQL Injection:
| Cross-Site Scripting (XSS):
| Web Shell Finder:
| Static tests:
| Plugin name: Local File Include tests v.1.1 Loaded.
| Plugin name: Remote Command Execution tests v.1.1 Loaded.
| Plugin name: Remote File Include tests v.1.1 Loaded.
| Local File Include:
| Remote Command Execution:
| Remote File Include:
Scan end date: 26-4-2023 14:19:27
HTML report saved in: report/harvestapp.com.html
/home/ruwindu

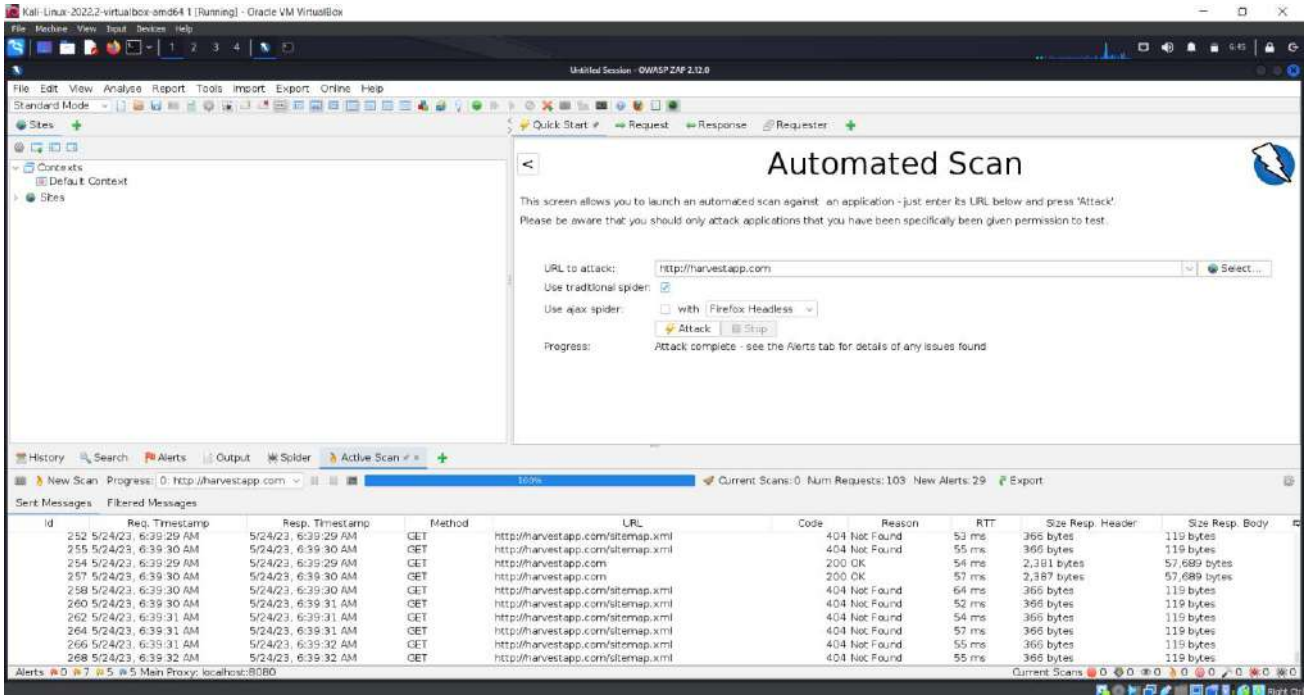
Using Wafw00f tool

When we run the wafw00f scan with the URL that we are targeting, we are able to see that the website harvestapp.com seems to be protected by a web application firewall (WAF) or some other form of security solution. This is something that we are able to validate via our own direct experience. Because we had completed the scan, we were able to get this information and make the appropriate judgements.

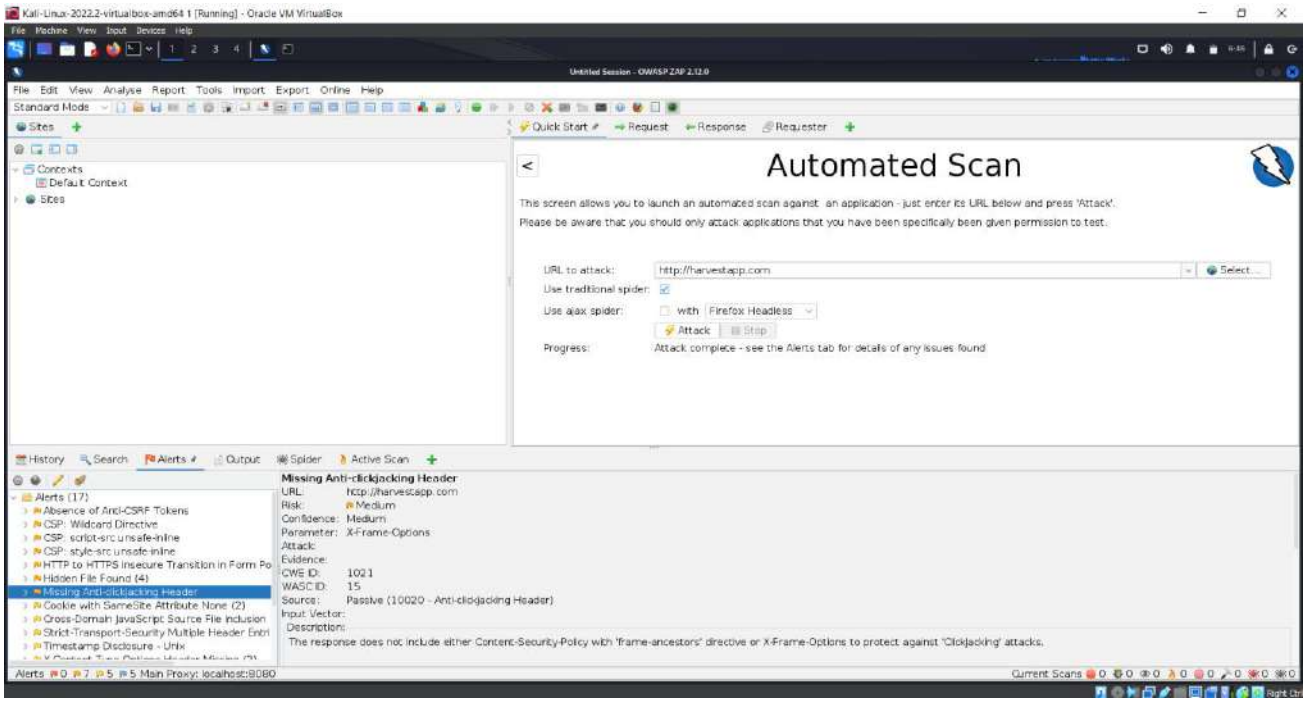


After doing the quick scan, we were able to locate and analyze the robust firewall that was a part of this domain.

Using OWASP-ZAP tool



Found 103 Requests.

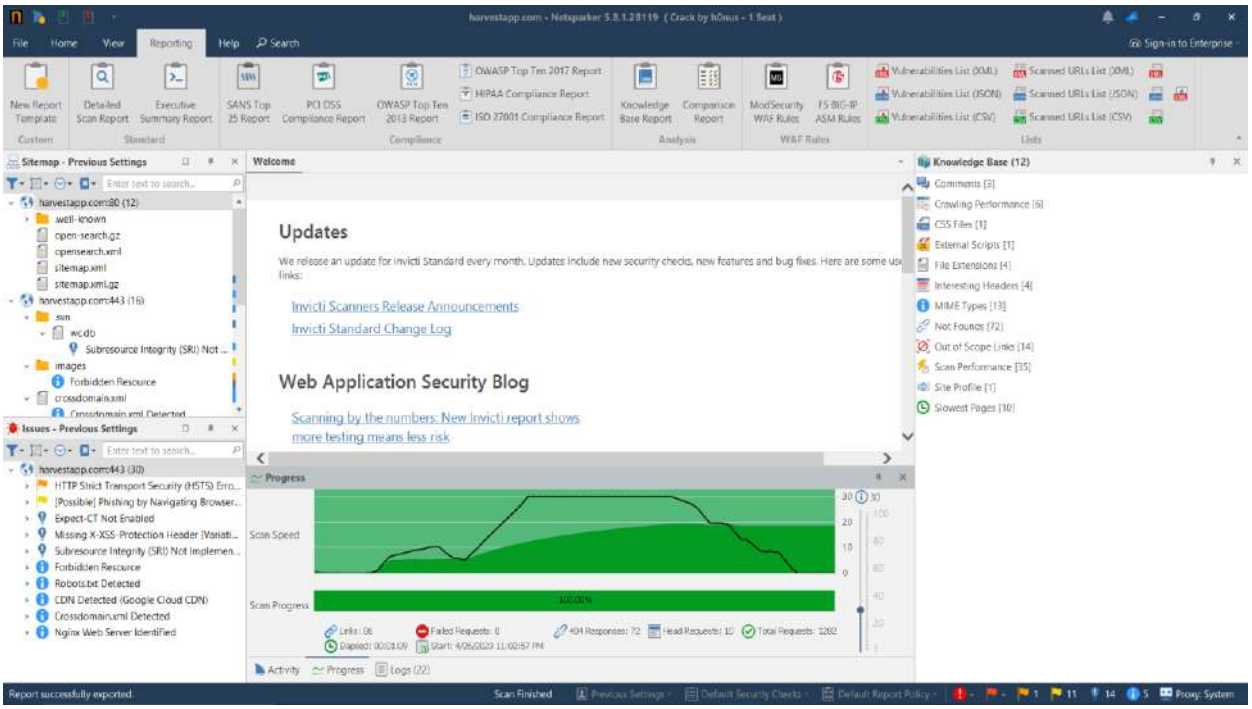


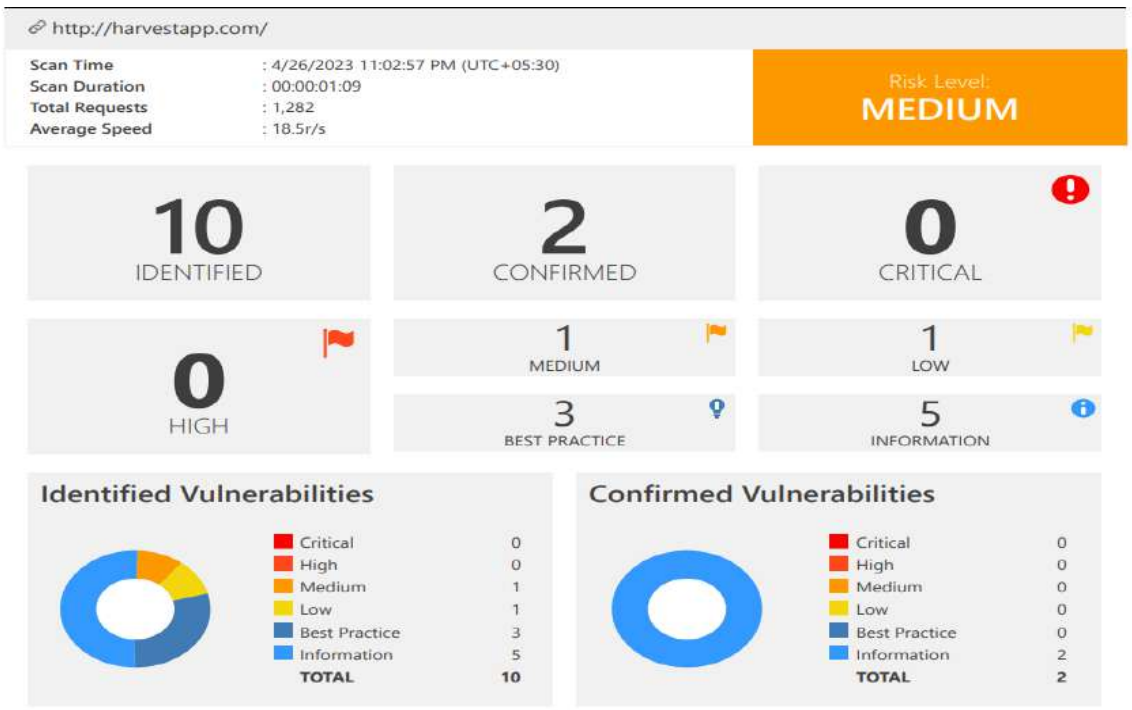
Found 26 Alerts.

Vulnerabilities found

Using Netsparker

In the course of my Audit, I performed a vulnerability check on harvestapp.com with the aid of Netsparker professional Edition (V), which proved to be of great service to me in my endeavor. For the purpose of this specific audit, the website was analyzed.





After doing a scan of the domain, I was able to identify a total of 10 vulnerabilities related to the domain, including 1 vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETEI
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://harvestapp.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://harvestapp.com/trace.axd	
	Expect-CT Not Enabled	GET	https://harvestapp.com/	
	Missing X-XSS-Protection Header	GET	https://harvestapp.com/opensearch.xml	
	Subresource Integrity (SRI) Not Implemented	GET	https://harvestapp.com/.svn/wc.db	
	CDN Detected (Google Cloud CDN)	GET	https://harvestapp.com/	
	Crossdomain.xml Detected	GET	https://harvestapp.com/crossdomain.xml	
	Nginx Web Server Identified	GET	https://harvestapp.com/	
	Forbidden Resource	GET	https://harvestapp.com/images/	
	Robots.txt Detected	GET	https://harvestapp.com/robots.txt	

http://harvestapp.com has been found to have the following identified vulnerabilities:

Identified vulnerabilities in http://harvestapp.com

Vulnerability 06 - Robots.txt Detected

Netsparker uncovered a file named Robots.txt that included information that may be classified as confidential.

Impact

A competitor may be able to uncover concealed folders and files contained inside a file; however, the success of this tactic is dependent on the information that is included within the file.

Response

Response Time (ms) : 260.954 Total Bytes Received : 441 Body Length : 238 Is Compressed : No

```
HTTP/1.1 301 Moved Permanently
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Location: https://harvestapp.com:443/robots.txt
Date: Wed, 26 Apr 2023 17:33:13 GMT
Cache-Control: private

# See https://developers.google.com/webmasters/control-crawl-index/docs/robots_txt for documentation
# and https://www.google.com/webmasters/tools/robots-testing-tool for testing

user-agent:*
disallow:/

user-agent:Googlebot
allow:/
```

Solution

Check to see that this file does not include any sensitive information that may be put to inappropriate use, such as the location of an administrative control panel. If the prohibited routes are essential to you and you want to prevent unauthorised access to them, you should avoid entering them in the Robots.txt file and instead make sure that they are adequately protected via means of authentication. This is because you should avoid writing them in the file if you want to prevent unauthorised access to them. Robots.txt is only used for one purpose: to inform search robots as to which sites should be indexed and which ones should not be crawled.

The following block can be used to tell the crawler to index files under /web/ and **ignore the rest**:

```
User-Agent: *
Allow: /web/
Disallow: /
```

Please note that when you use the instructions above, **search engines will not index your website** except for the specified directories.

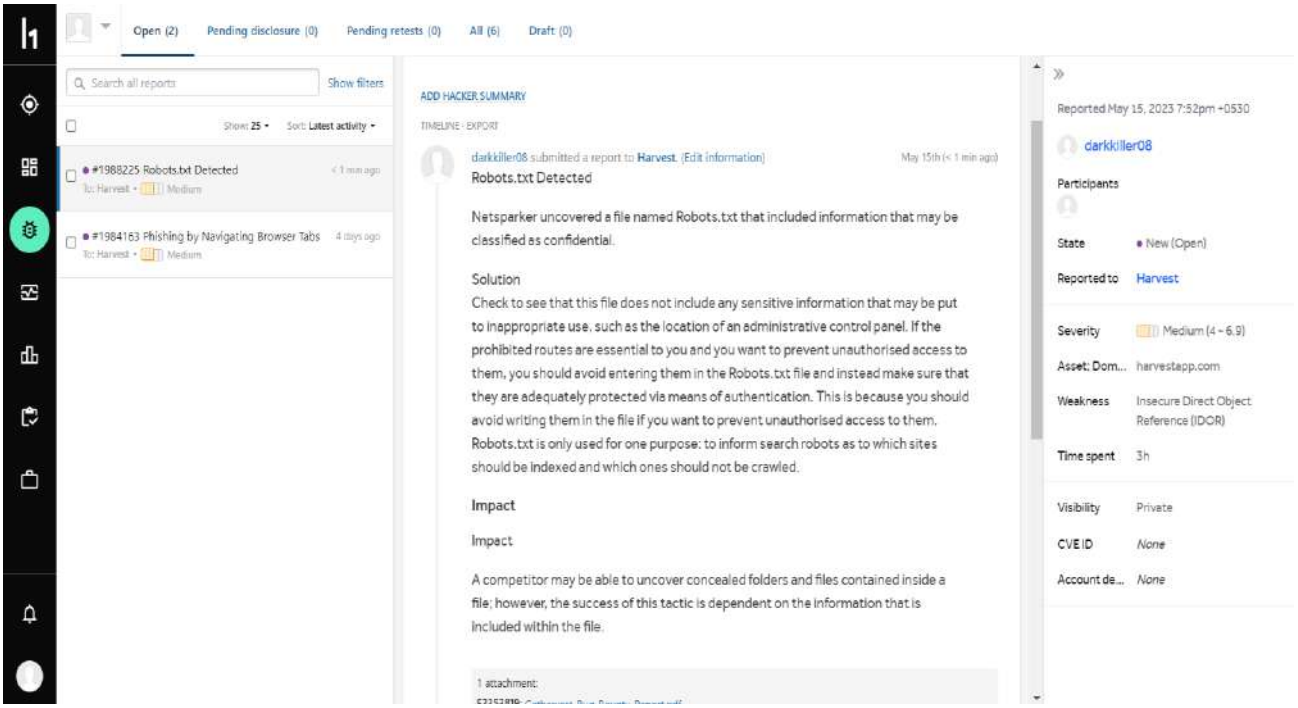
If you want to hide certain section of the website from the search engines `X-Robots-Tag`can be set in the response header to tell crawlers whether the file should be indexed or not:

```
X-Robots-Tag: googlebot: nofollow
X-Robots-Tag: otherbot: noindex, nofollow
```

Conclusion of the Report 06

To ensure the correctness of this report, we have chosen to research and analyze the recorded future bug reward program as soon as possible. To succeed, we must know the documented future bug reward structure. Thus, we must verify this report's data. We prioritized finding software bugs during the examination. We chose this to test our mission. Then our research was successful. With this data, we can assess our success. We collected data on the technologies, IP addresses, subdomains, and geographic locations. This is to better serve you, our valued customers. Vulnerability analysis followed content scanning. The next step was apparent. This approach followed the last. After the preceding step, this must have been the first. Netsparker found all ten critical system issues. The mechanism allowed this. Thus, we overcame our challenges. We needed this technology to succeed. Our inquiry will focus on the risks of cooperating with outsiders. After much deliberation, we decided. We deliberated and came up with this. We understood this vulnerability, its causes, and its solutions.

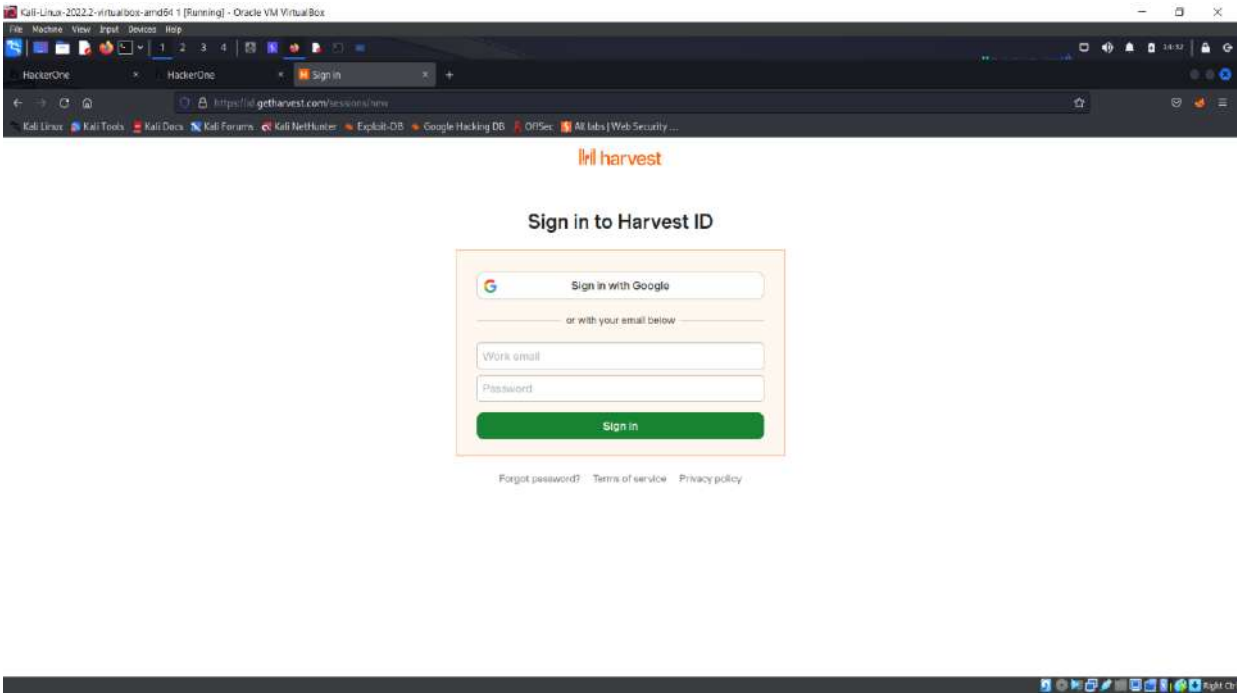
HackerOne Submitted Report Screenshot



vii. Report 07

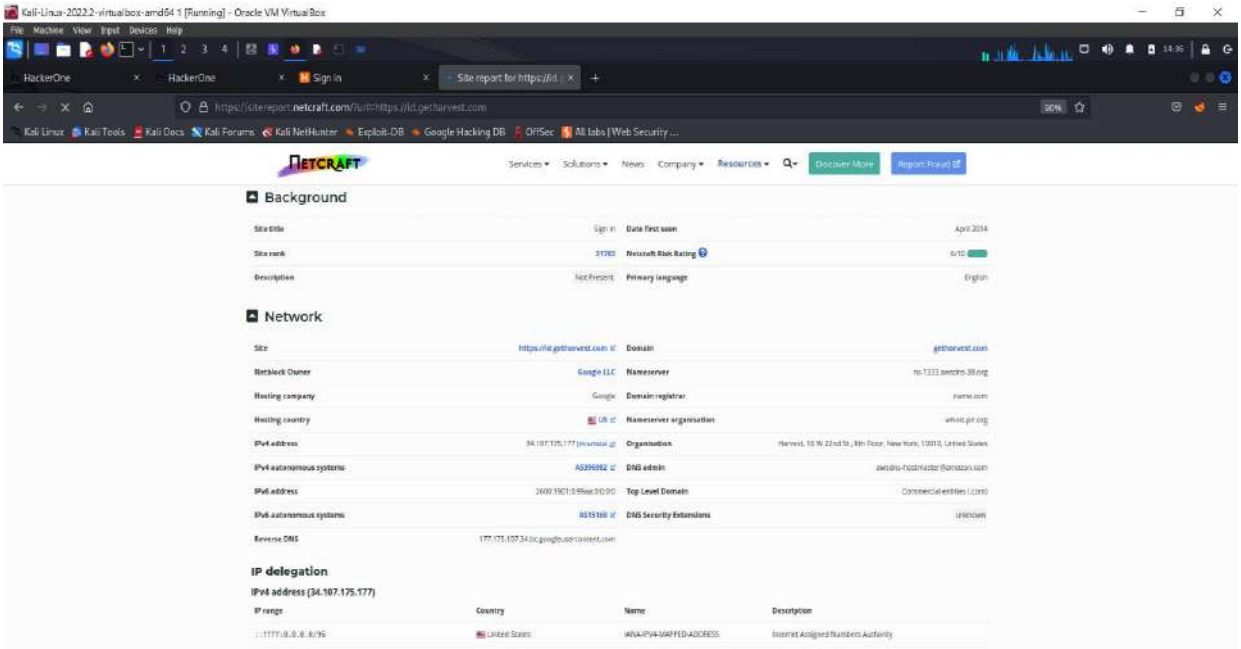
Target information: https://id.getharvest.com

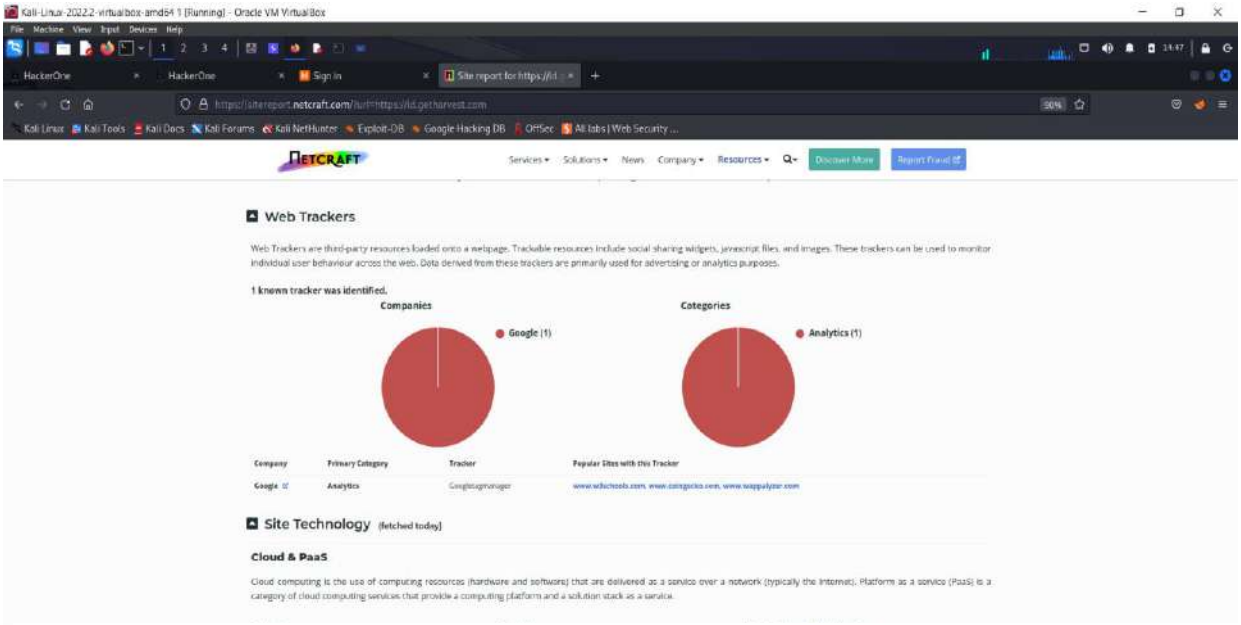
This assessment's goals are to determine both the degree of risk that is associated with the potential points of vulnerability that are found within the target domain (https://id.getharvest.com/sessions/new), as well as the potential points of vulnerability that are found within the target domain (https://id.getharvest.com/sessions/new). In addition, this evaluation's goals are to determine the potential points of vulnerability that are found within the target domain. The evaluation is going to be carried out so that we can achieve these objectives. The evaluation that is now being carried out has as its major objective the identification of problematic problems connected to the subject that is the focus of attention at this moment.

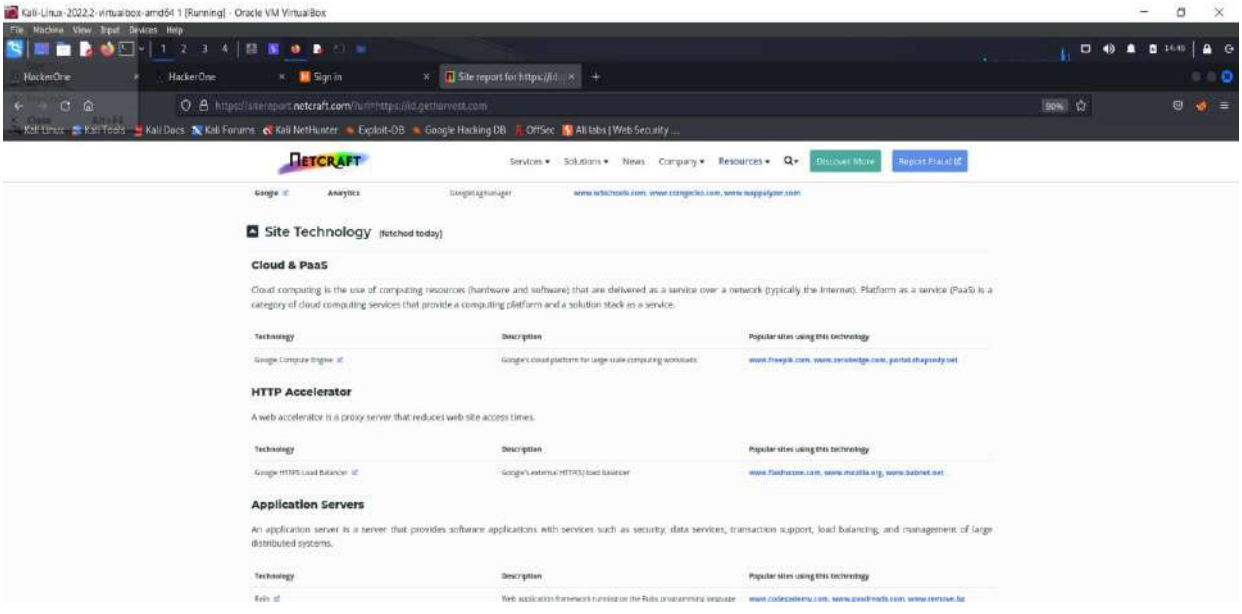


Information Gathering For Target Domain

Let's have a look at the variety of different choices we have available to us so that we may not only find out what the technical capabilities of https://id.getharvest.com/sessions/new are, but also additional information that is relevant to the circumstance that we are in. Since Netcraft is the only tool that we currently have access to, let's set up an account for it and do some investigation into the information that we could obtain by using it. Since this is the only resource at our disposal at the moment, let's put Netcraft to the test and conduct a search for ourselves to find out what kind of information we are able to unearth using this tool. Let's take a look at the information that can be gathered from using Netcraft since that is all we are

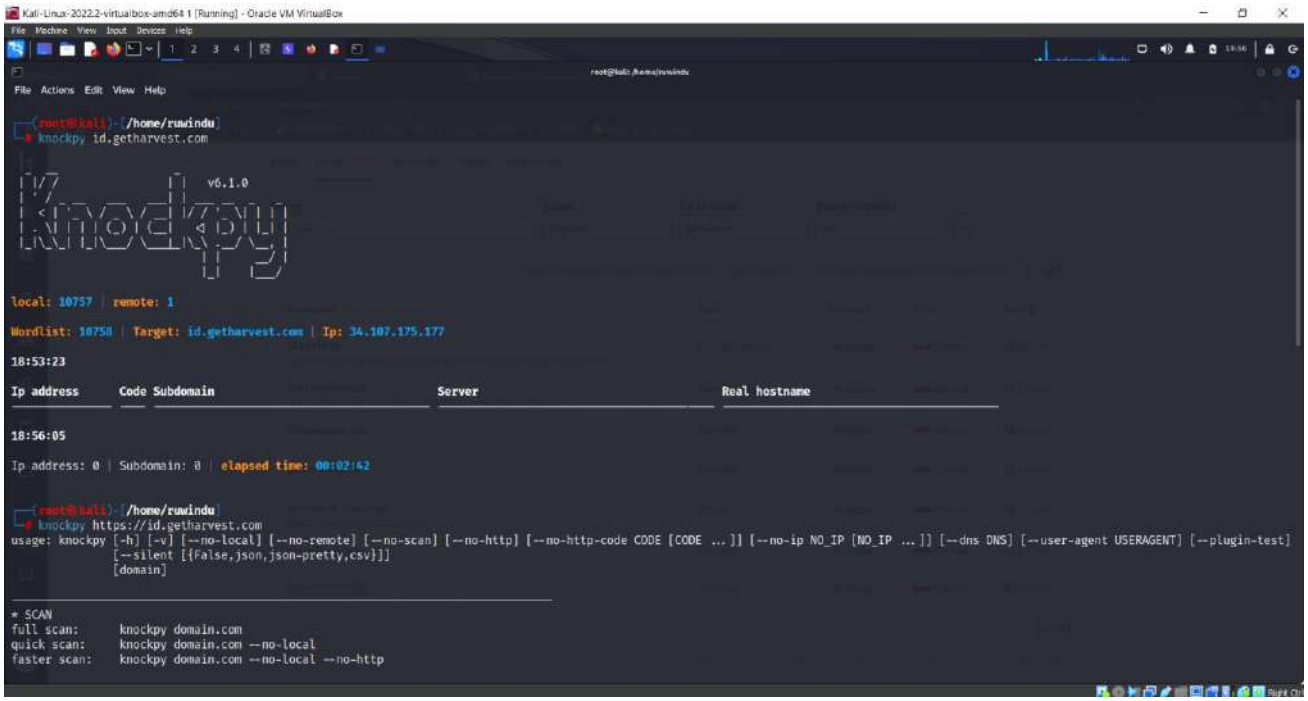

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
Background
Network
IP delegation
IPv4 address (34.107.175.177)


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
Web Trackers
1 known tracker was identified.
Companies
Google (1)
Categories
Analytics (1)
Site Technology (fetched today)
Cloud & PaaS


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
Site Technology (fetched today)
Cloud & PaaS
HTTP Accelerator
Application Servers

Using knockpy tool

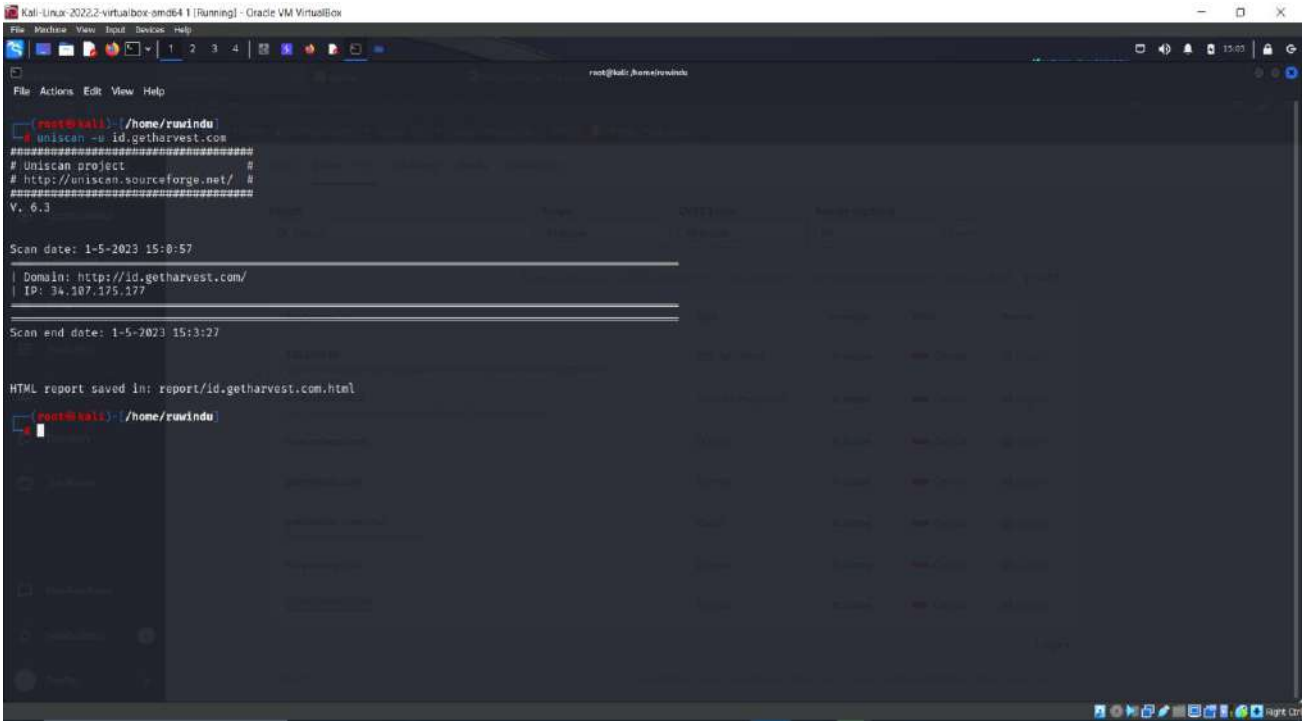
Using the knockpy tool, it is possible to collect subdomain names through scraping data sources, carrying out reverse DNS sweeping, and taking part in recursive brute forcing.



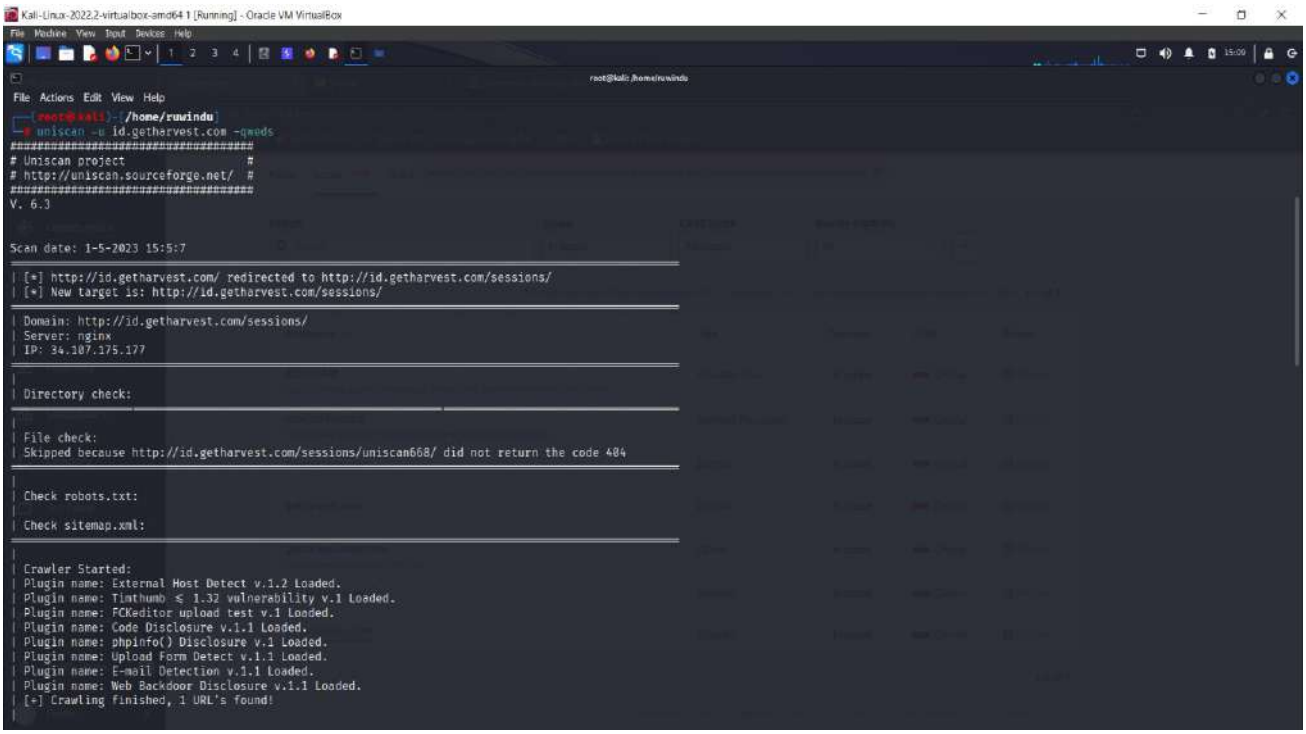
Since the id.getharvest.com subdomains have been logged, we can now see them in this way. This is because the listing of the id.getharvest.com subdomains is now complete. No one should be too surprised that the IP address and name server used by the main id.getharvest.com domain are also used by all of the subdomains. All of the sites that are taken care of under the id.getharvest.com domain share this information. All of the sites that are handled under the id.getharvest.com name can view this information. All of the sites that are part of the harvestapp.com name agree on these points. The real address of the program lets us know that this is a mobile app. Because of this, we can figure out that it's a mobile game. The fact that the right address is shown here serves as the foundation for our conclusion and gives it shape. We can now use it because of this, which has given us the chance and made it possible for us to do so. Because of this, we now have enough money to be able to do it.

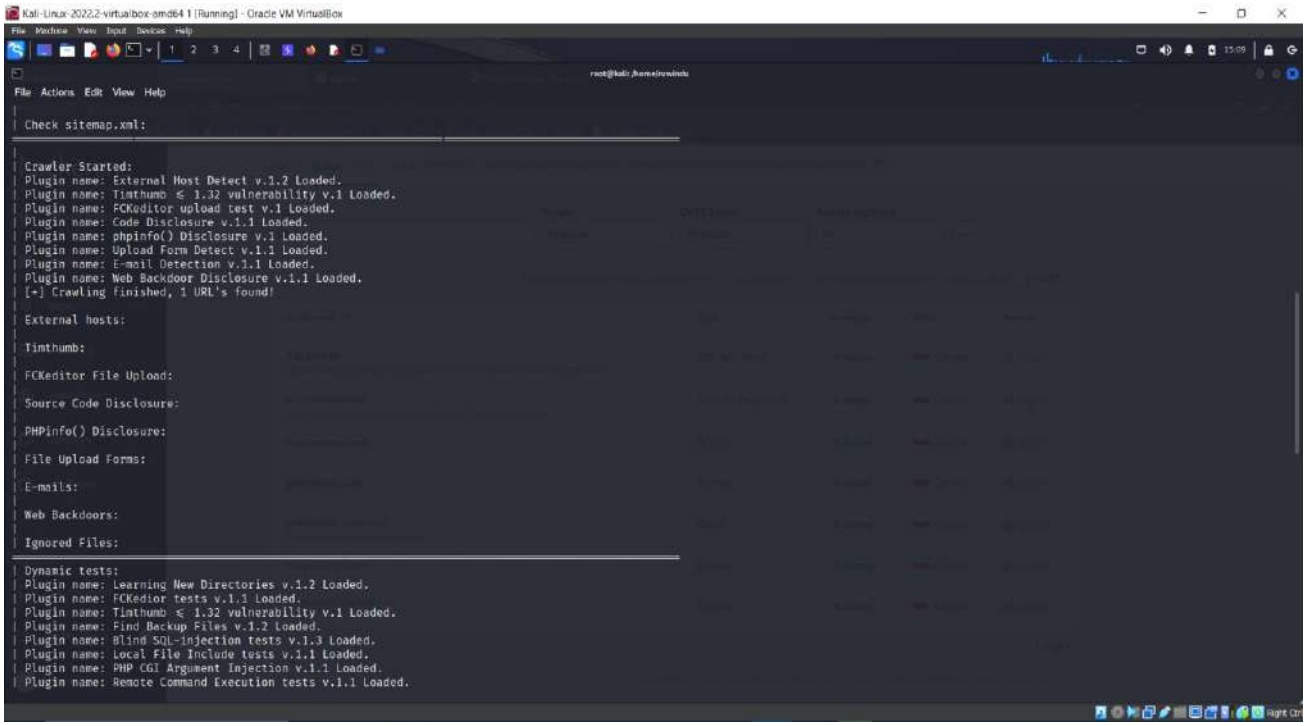
Using Uniscan tool

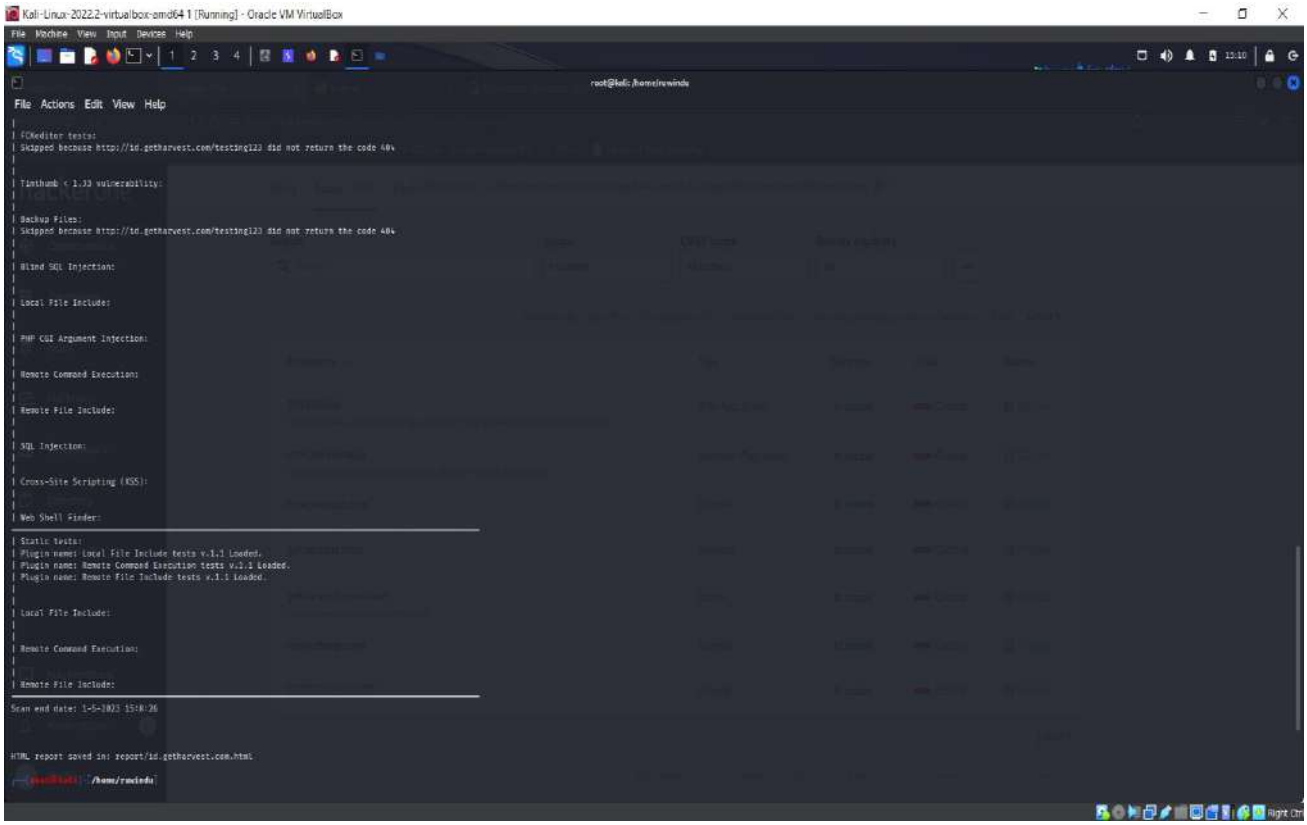
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u domain -qweds command:

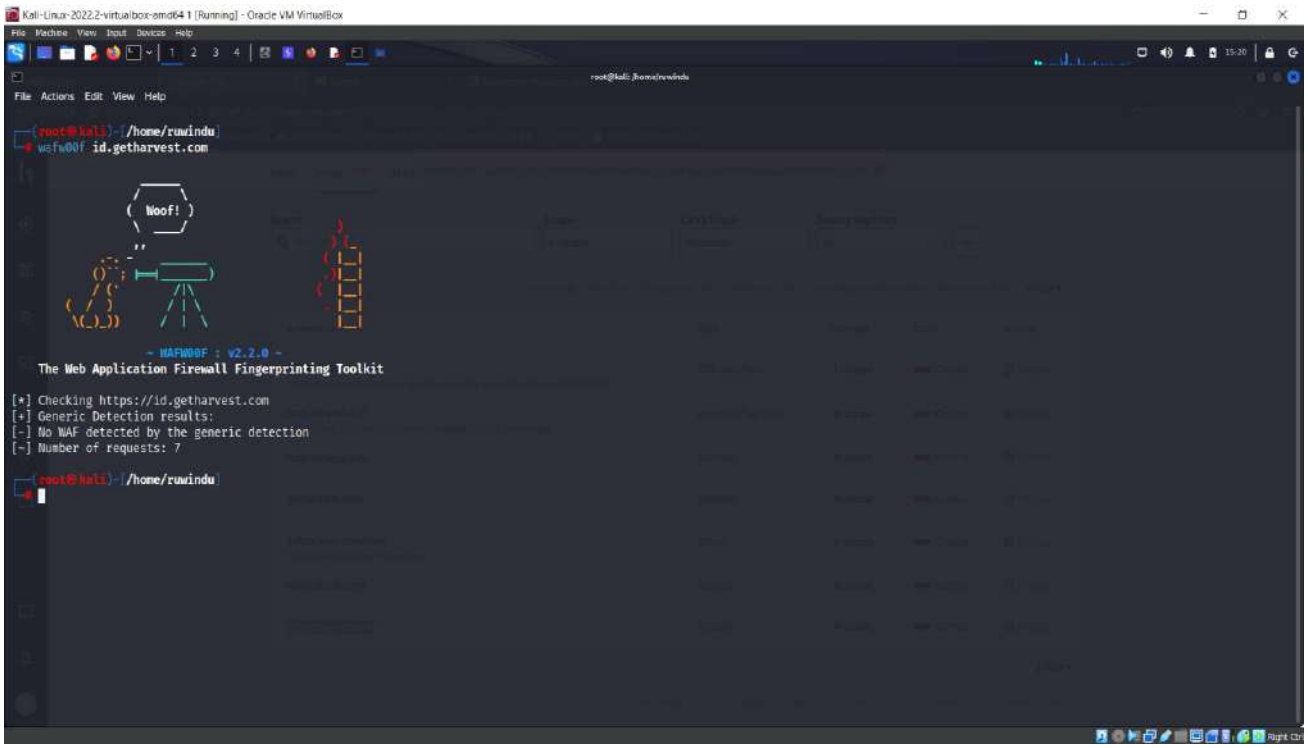



Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Check sitemap.xml:
Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
Plugin name: FCKeditor upload test v.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: phpinfo() Disclosure v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
[+] Crawling finished, 1 URL's found!
External hosts:
Timthumb:
FCKeditor File Upload:
Source Code Disclosure:
PHPinfo() Disclosure:
File Upload Forms:
E-mails:
Web Backdoors:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKedior tests v.1.1 Loaded.
Plugin name: Timthumb ≤ 1.32 vulnerability v.1 Loaded.
Plugin name: Find Backup Files v.1.2 Loaded.
Plugin name: Blind SQL-injection tests v.1.3 Loaded.
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: PHP CGI Argument Injection v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
FCKeditor tests:
Skipped because http://id.getharvest.com/testing123 did not return the code 404
Timthumb < 1.33 vulnerability:
Backup Files:
Skipped because http://id.getharvest.com/testing123 did not return the code 404
Blind SQL Injection:
Local File Include:
PHP CGI Argument Injection:
Remote Command Execution:
Remote File Include:
SQL Injection:
Cross-Site Scripting (XSS):
Web Shell Finder:
Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
Plugin name: Remote File Include tests v.1.1 Loaded.
Local File Include:
Remote Command Execution:
Remote File Include:
Scan end date: 1-5-2023 15:0:26
HTML report saved in: report/id.getharvest.com.html

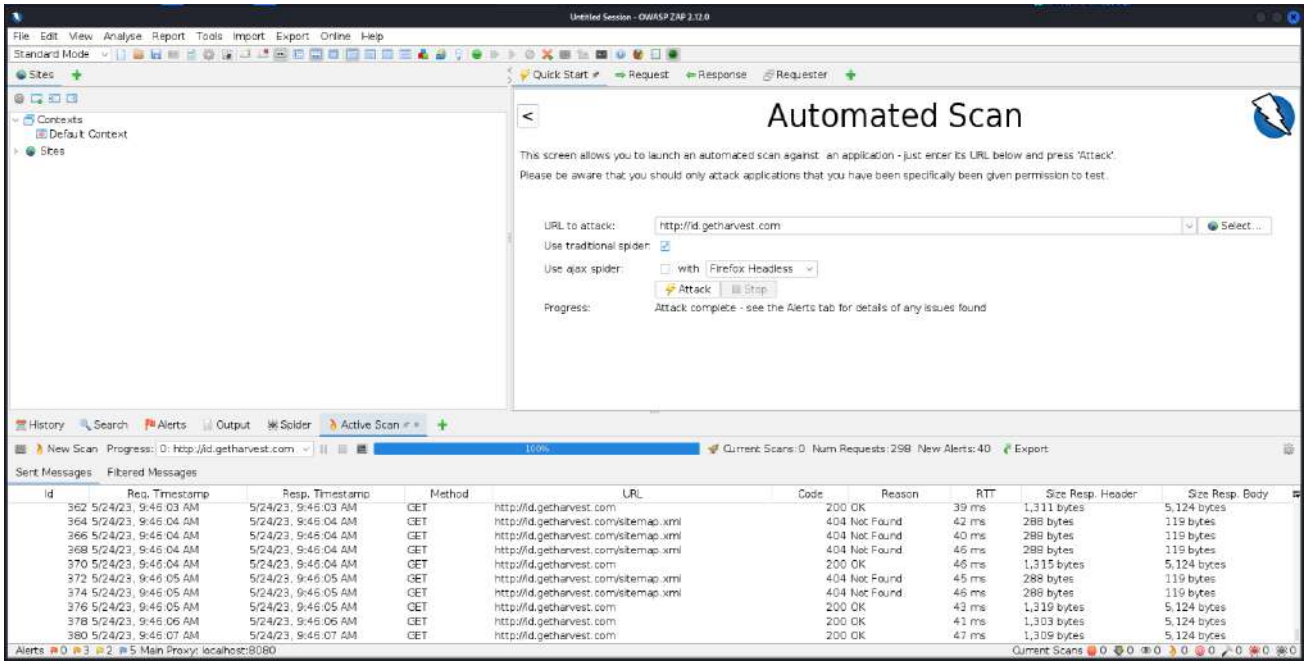
Using Wafw00f tool

When we run the wafw00f scan with the URL that we are targeting, we are able to see that the website harvestapp.com seems to be protected by a web application firewall (WAF) or some other form of security solution. This is something that we are able to validate via our own direct experience. Because we had completed the scan, we were able to get this information and make the appropriate judgements.

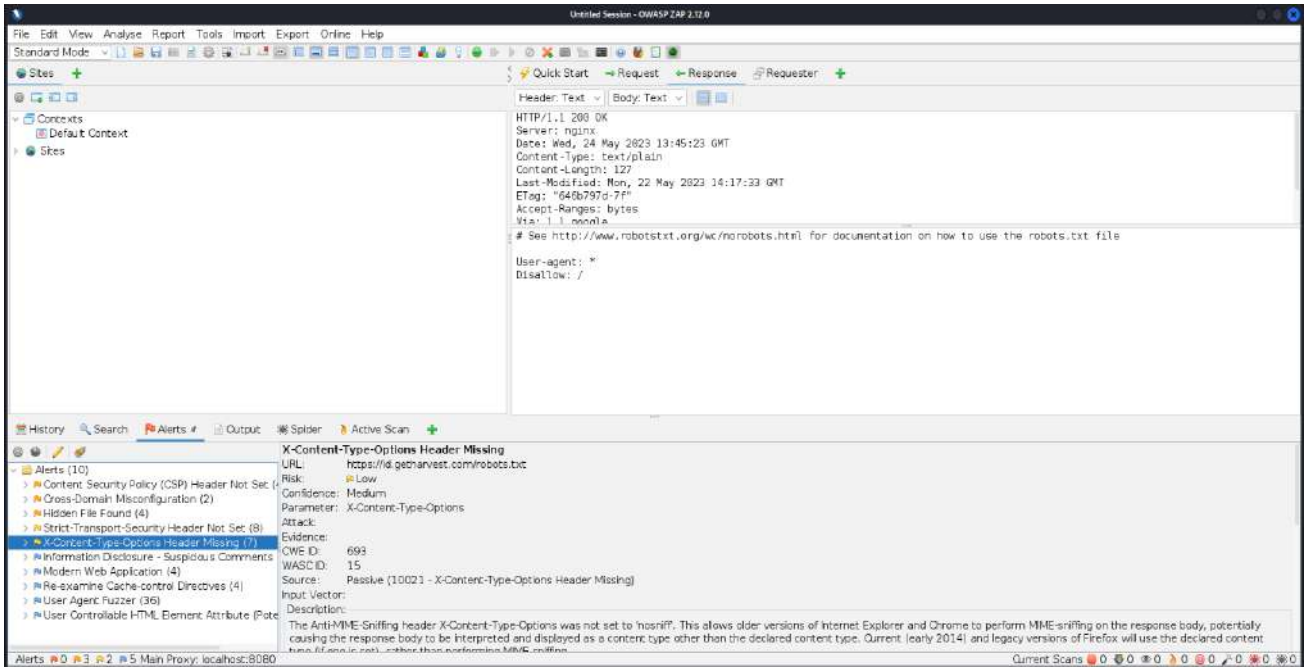


After doing the quick scan, we were able to locate and analyze the robust firewall that was a part of this domain.

Using OWASP-ZAP tool



Found 290 Requests.

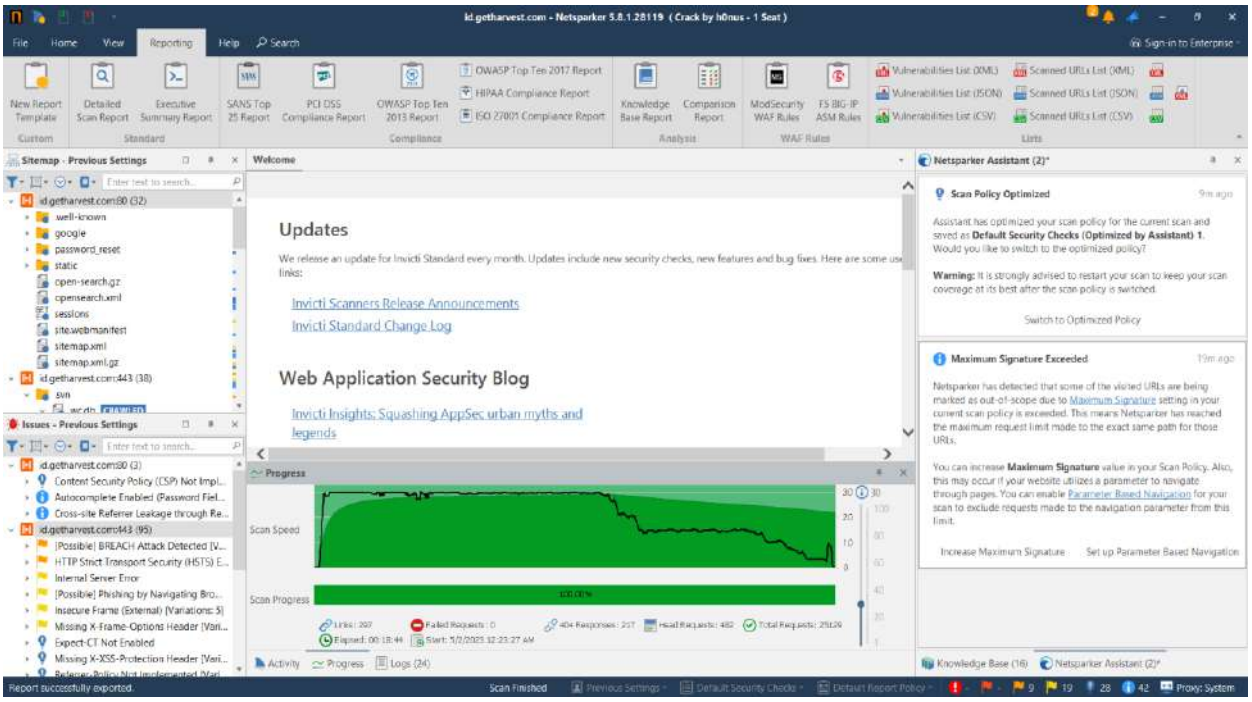


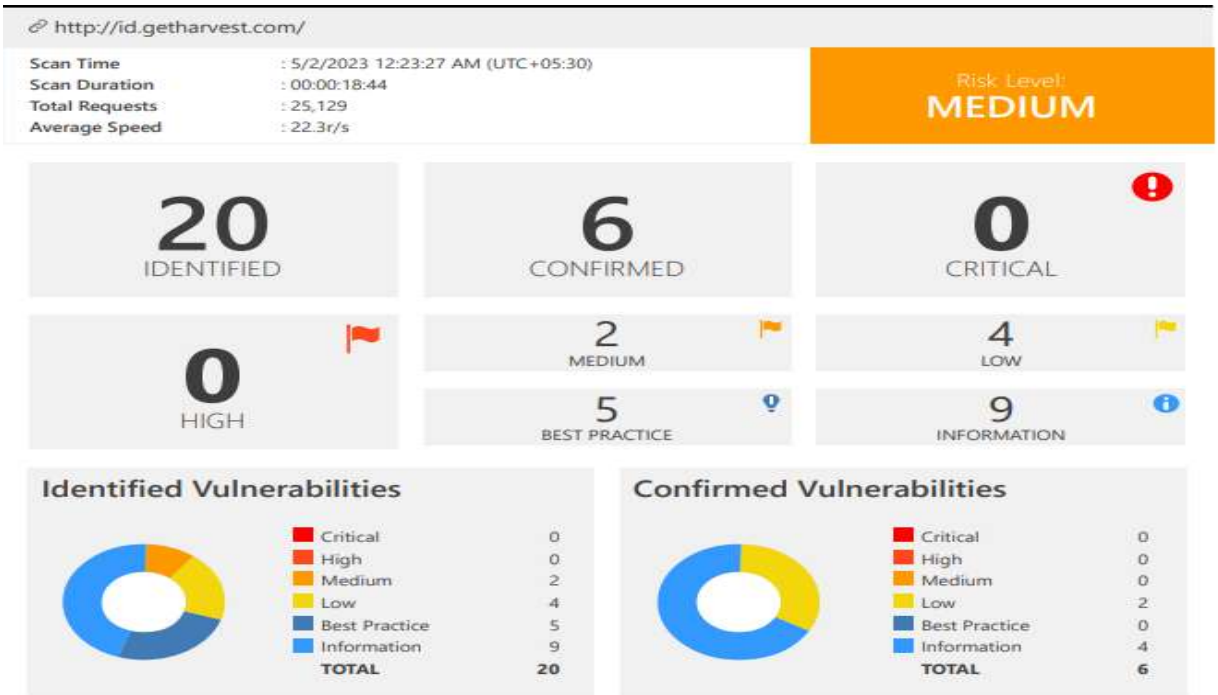
Found 10 Alerts.

Vulnerabilities found

Using Netsparker

In the course of my Audit, I performed a vulnerability check on harvestapp.com with the aid of Netsparker professional Edition (V), which proved to be of great service to me in my endeavor. For the purpose of this specific audit, the website was analyzed.





After doing a scan of the domain, I was able to identify a total of 20 vulnerabilities related to the domain, including 2 vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	[Possible] BREACH Attack Detected	POST	https://id.getharvest.com/sessions	
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://id.getharvest.com/	
	[Possible] Phishing by Navigating Browser Tabs	POST	https://id.getharvest.com/sessions/	
	Missing X-Frame-Options Header	POST	https://id.getharvest.com/sessions	
	Insecure Frame (External)	GET	https://id.getharvest.com/sessions/new	
	Internal Server Error	POST	https://id.getharvest.com/password_reset	
	Content Security Policy (CSP) Not Implemented	GET	https://id.getharvest.com/sessions/new	
	Expect-CT Not Enabled	GET	https://id.getharvest.com/opensearch.xml	
	Missing X-XSS-Protection Header	GET	https://id.getharvest.com/opensearch.xml	
	Referrer-Policy Not Implemented	POST	https://id.getharvest.com/sessions	
	Subresource Integrity (SRI) Not Implemented	GET	https://id.getharvest.com/.svn/wc.db	
	CDN Detected (Google Cloud CDN)	GET	https://id.getharvest.com/opensearch.xml	
	Disabled X-XSS-Protection Header	GET	https://id.getharvest.com/google/oauth2/new?state%5Bintent%5D=%2527	state%5Bintent%5D
	Email Address Disclosure	POST	https://id.getharvest.com/sessions/	
	Generic Email Address Disclosure	POST	https://id.getharvest.com/sessions/	
	Nginx Web Server Identified	GET	https://id.getharvest.com/opensearch.xml	

https://id.getharvest.com has been found to have the following identified vulnerabilities:

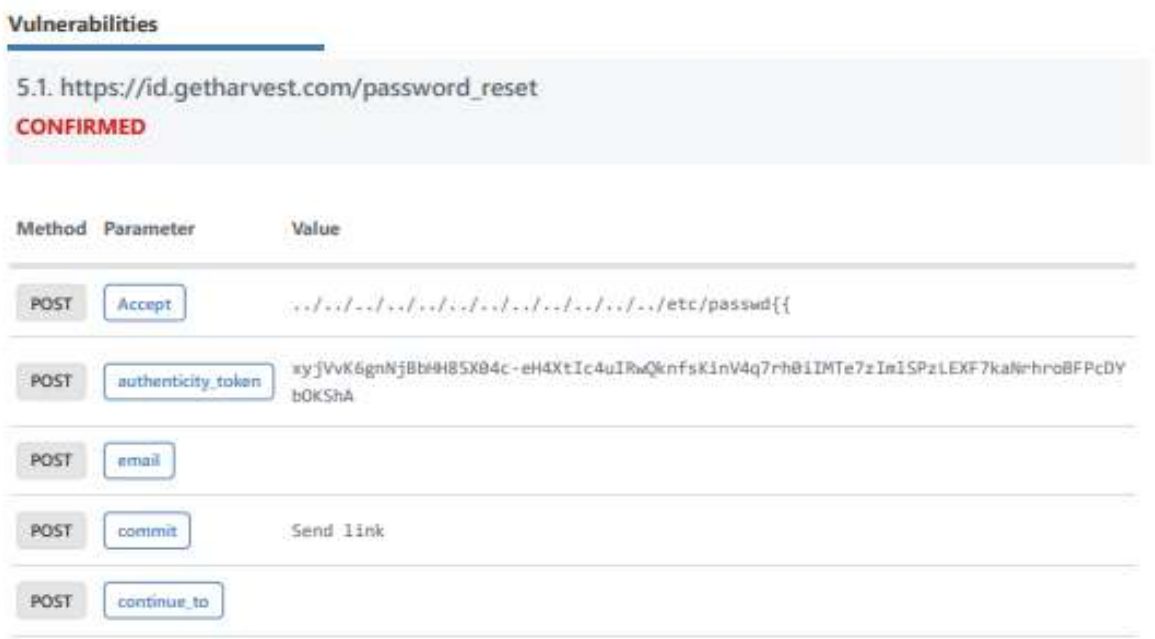
Identified vulnerabilities in https://id.getharvest.com

Vulnerability 07 - Internal Server Error

Netsparker identified an internal server fault.
The server replied with an HTTP status code of 500, which indicates that there was an issue on the server's end of the communication. It was necessary to conduct an exhaustive investigation of one's behavior since there were a number of possible explanations. If Netsparker is able to find another vulnerability in the same resource, it will report the new one as its own separate vulnerability.

Impact

It is possible that the effect will shift depending on the circumstances that are present. In the vast majority of instances, this is a sign of inappropriate coding approaches, such as an inadequate amount of error checking, sanitization, and whitelisting. On the other side, there is a possibility that there is a more major issue, such as SQL injection. In this scenario, Netsparker will explore any more possible issues and report each one separately if it discovers any.



Request

```
POST /password_reset HTTP/1.1
Host: id.getharvest.com
Accept: ../../../../../../../../../../../etc/passwd{{
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Content-Length: 142
Content-Type: application/x-www-form-urlencoded
Cookie: _iridesco-identity_session=sFUxURd94VcfX73GtCFrYOU6iVouZZ5WgU6smhMZRaXqSjEsZSsZzmnTzEW%2B8zH9Yc
iLHkFhJ8IiU2aZbsxi%2BS0UGkZ165m3Y53BREt0ojHJp5YA62B7R3r%2FPdLU5Dh3QZBrNPGhC93tS0ztZ72G1JtusVqXHbX72vFJJ
1%2BBwwOU8xi%2FuyH6gd%2BkKIjPPji%2FDf8SBTIBqiO7qG%2BixbcWsDg9XnzkbeHfI8SV01UOYzXFpB%2FhloK4T2B9UL9N1%2F
EuHFYQrvxC5OKazMvkFc5WXYZfC8LeXmE8bd6SyJk2wKnmT4odpxX23j%2FNvOTOHxNNvB5TM8XWKPm0scV9QE6soKh%2B9NexXg%3
D%3D--%2FIs0RNOSJPMJ5oeA--S0Tvr23CQ6fzVJAgK6czkA%3D%3D
Referer: https://id.getharvest.com/password_reset/new
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker

authenticity_token=xyjVvK6gnNjBbHH8SX04c-eH4XtIc4uIRwQknfsKinV4q7rh0iIMTe7zIm1SPzLEXF7kaNrhro8FPcDYbOKS
hA&email=&commit=Send+link&continue_to=
```

Response

Response Time (ms) : 290.7931 Total Bytes Received : 192 Body Length : 0 Is Compressed : No

```
HTTP/1.1 500 Internal Server Error

Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Server: nginx
Via: 1.1 google
Transfer-Encoding: chunked
Date: Mon, 01 May 2023 19:10:30 GMT
```

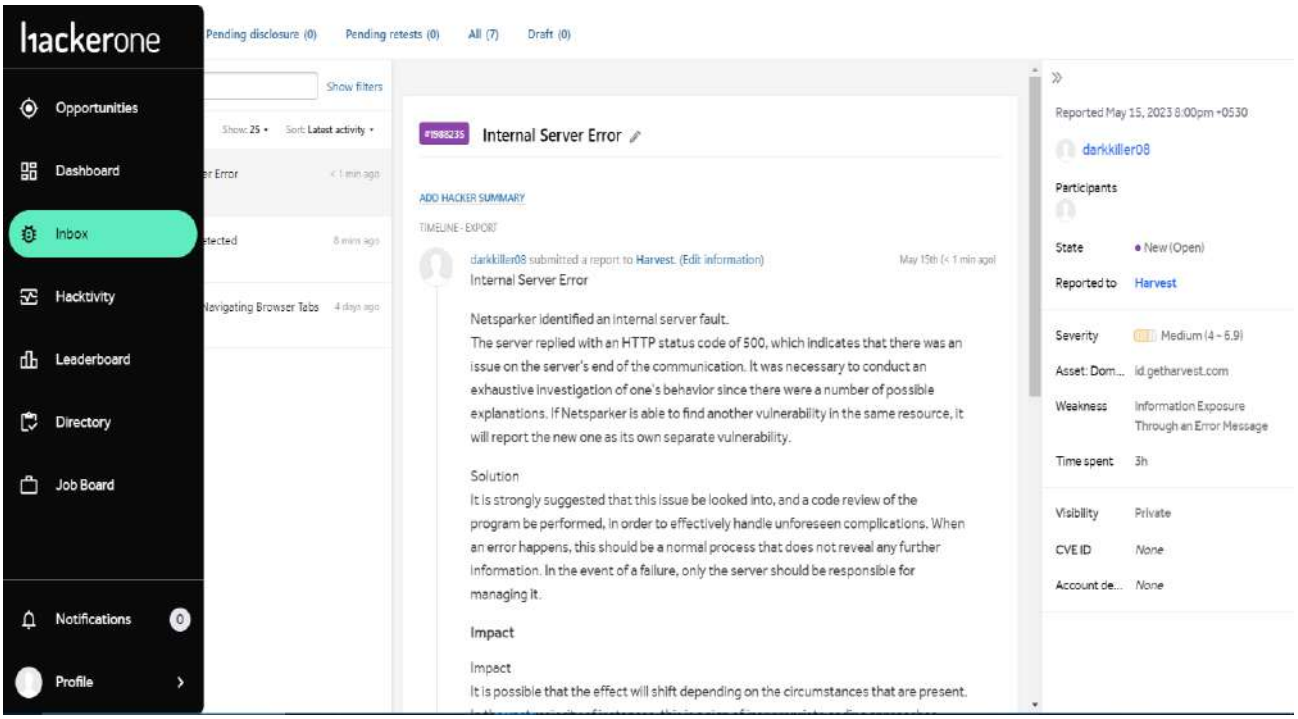
Solution

It is strongly suggested that this issue be looked into, and a code review of the program be performed, in order to effectively handle unforeseen complications. When an error happens, this should be a normal process that does not reveal any further information. In the event of a failure, only the server should be responsible for managing it.

Conclusion of the Report 07

The purpose of this report prompted us to make the decision to take part in a bug bounty program that was offered by HackerOne. To start things off, we had a discussion on the bug bounty program and went through the material that was provided, such as the criteria and the regulations. We started by selecting one domain from the list of in-scope domains that was provided to us, and then we gathered information that was relevant to that particular domain. We carried out the process of information collection under a wide range of various categories, such as technologies, subdomains, files and folders, and so on and so forth. After that, we proceeded to the next step, which was the vulnerability assessment. After that, we were done. There, we learned that there is a potential of obtaining one warning with a degree of severity that falls somewhere in the middle. We decided to take action on the warning that had a degree of severity that was somewhere in the center since all of the other warnings had a low level of severity. We spoke about the concept of vulnerability as well as the historical roots of such a weakness, as far as my understanding of the conversation goes.

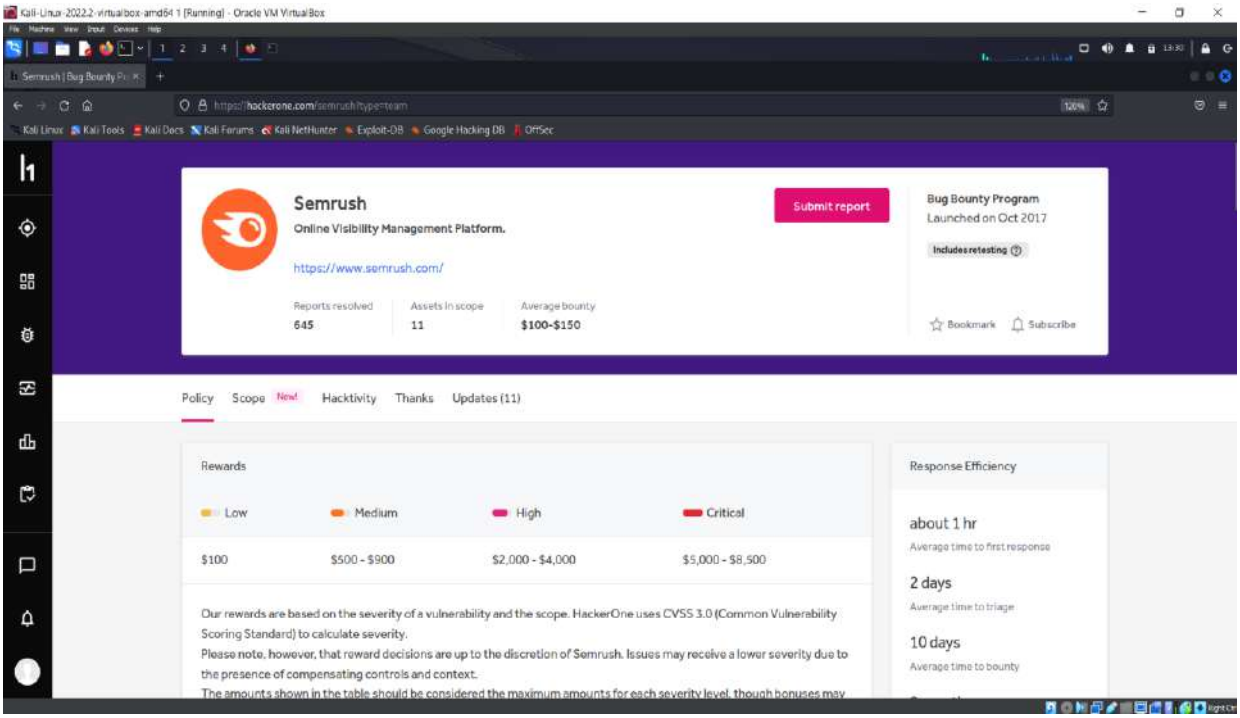
HackerOne Submitted Report Screenshot



viii. Report 08

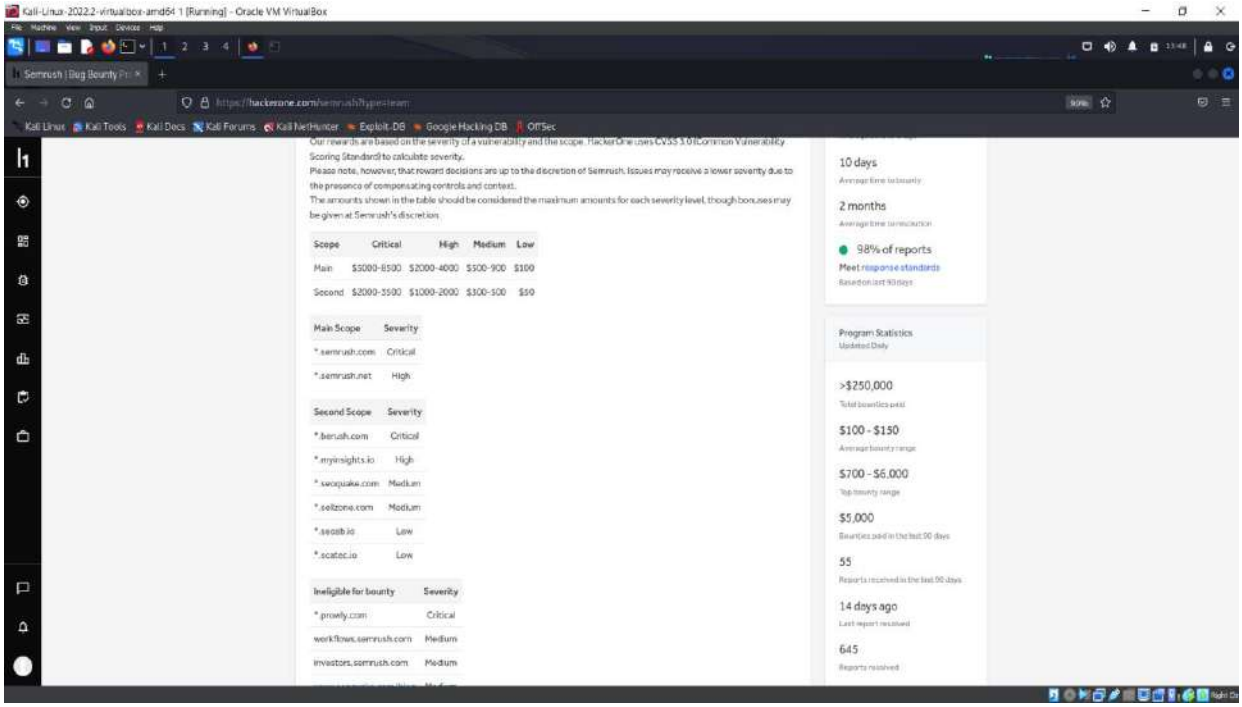
Target information: https://www.semrush.com/

The purpose of this evaluation is to determine both the degree of risk that is connected with the possible points of vulnerability that are found within the target domain (https://www.semrush.com/), as well as the potential points of vulnerability that are found within the target domain. The objective of the evaluation that is now being carried out is to search for flaws in the subject area that is the focus of attention.

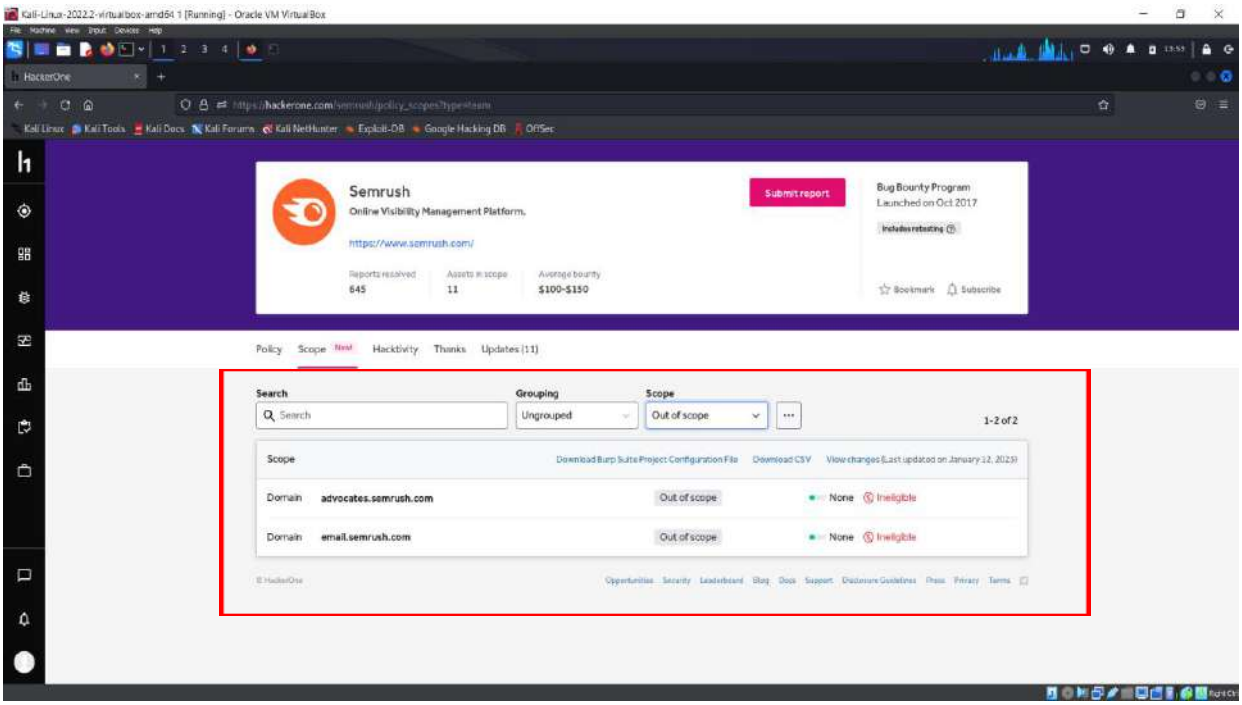


Semrush was established in 2008 by a small group of specialists specialising in search engine optimisation (SEO) and information technology (IT), with the intention of making online competition fair and transparent, and of offering equal opportunities for all players. After another ten years of development, it eventually become a powerful platform that now supports marketers from all over the world in expanding their presence on the internet.

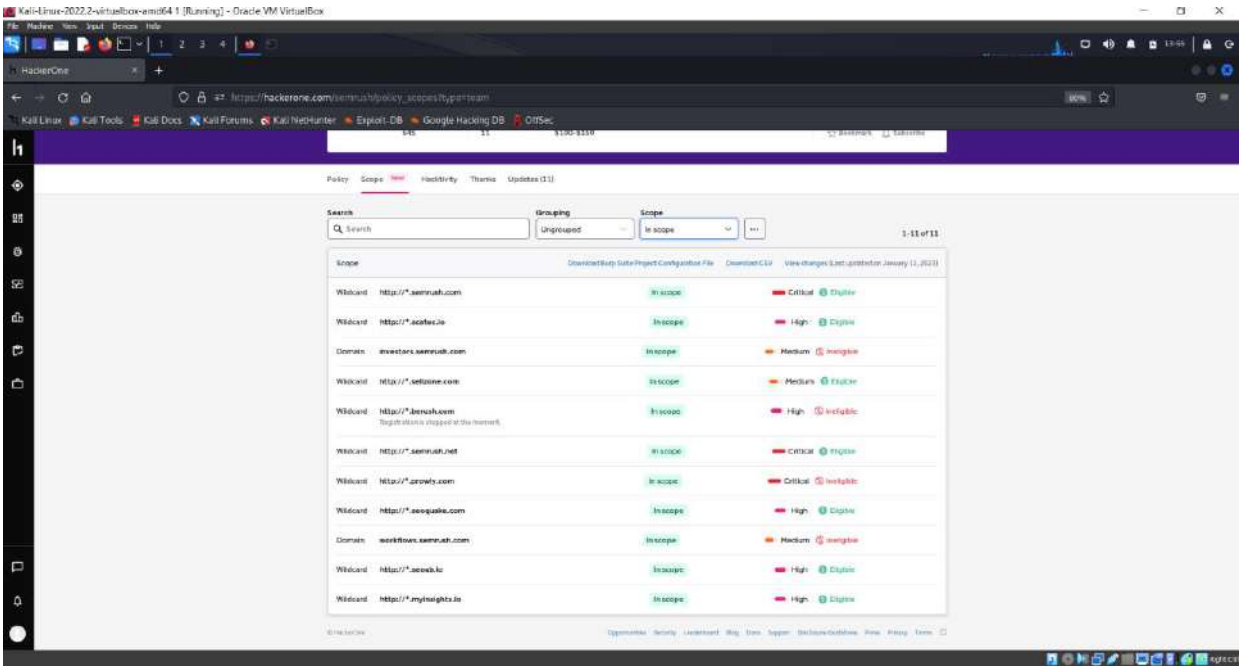
incentives. It is likely that the addition of compensating controls and context will result in problems obtaining a severity rating that is lower than they otherwise would have. The quantities that are displayed in the table need to be treated as the maximum amounts that are available for each severity level. Even if bonuses may be provided at Semrush's discretion, the amounts that are listed in the table.



After that, prior to going on to the subsequent stage, they will first have a conversation regarding any potential vulnerabilities that go outside the remit of the project. Because of the nature of these security vulnerabilities, we are unable to make any efforts to find a bug or include the results of such attempts in our report. This prevents us from using their findings in our report. Because of this, we are unable to include their results into our own report as well. In addition to this, we are forbidden to use any of their results or conclusions in any form in our report. The aforementioned list places an obligation on us to carry out an inquiry and determine the nature of an error that ought not to be present. It is very necessary for us to behave ourselves in this manner.

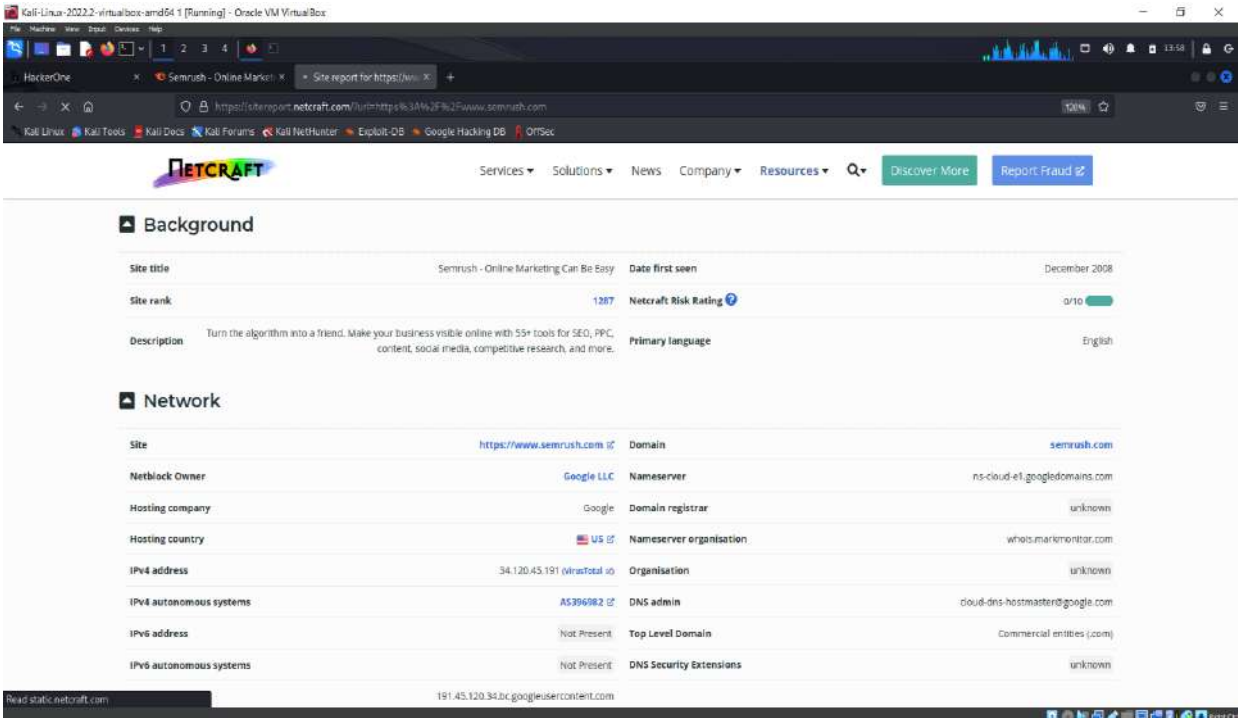


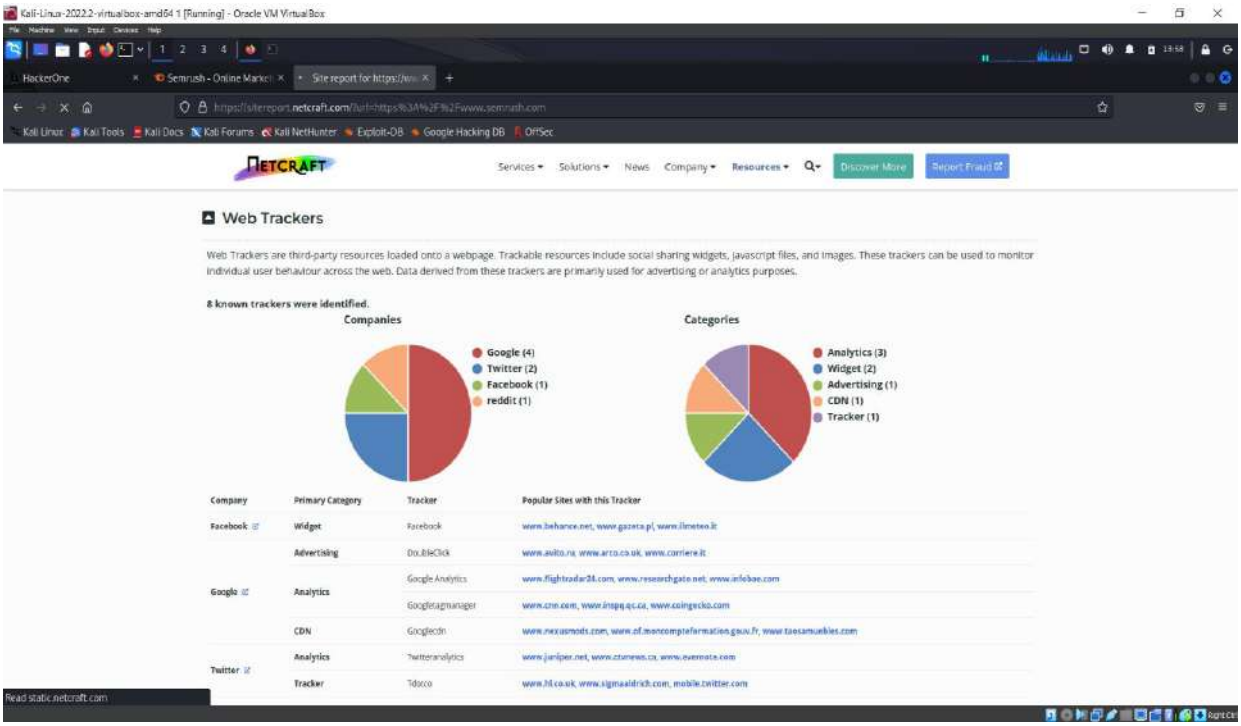
When it comes to the process of looking for bugs that have been granted bounties, the in-scope area is of the utmost importance to us. This is due to the fact that each and every scan that we do searches only for domains that fall under the banner of being "in-scope." This is because each scan that we run looks for defects only in domains that are included inside the umbrella of the in-scope. As a result, this limitation causes this result. In the event that things do not go according to plan, we are going to be confronted with a number of different sorts of problems. These challenges will be of varied degrees of difficulty.

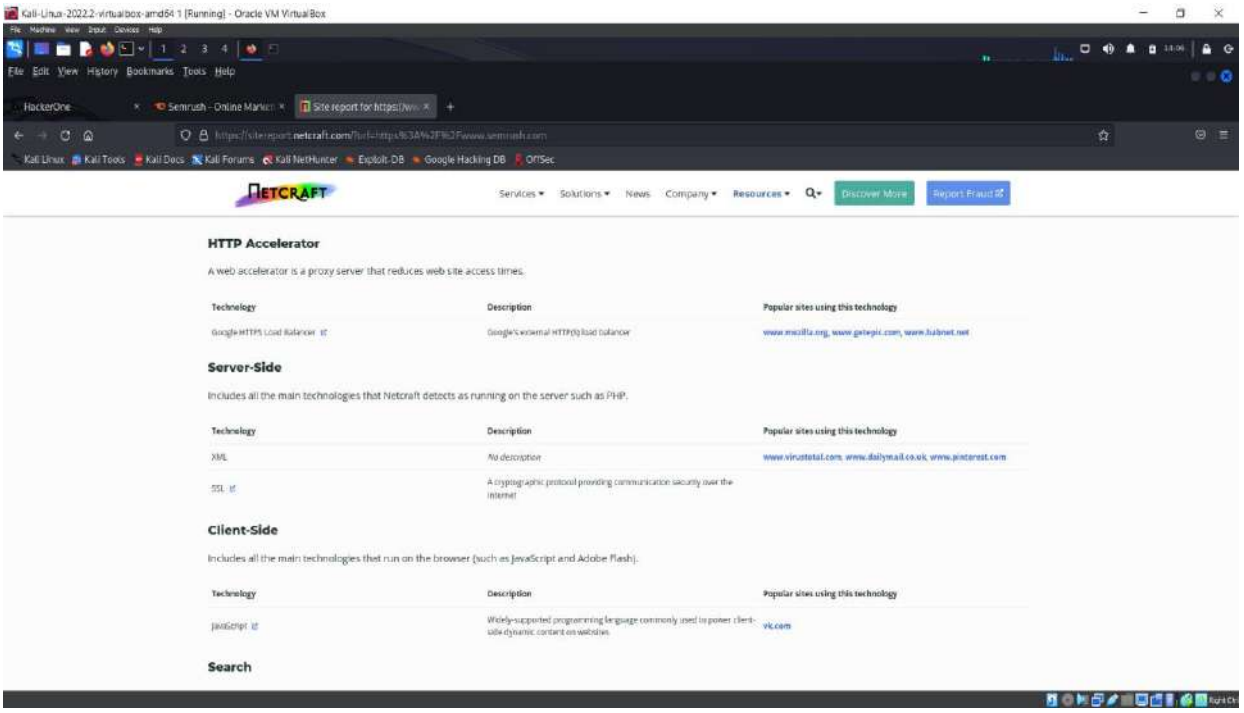


Information Gathering For Target Domain

Let's have a look at the multiplicity of different approaches that we might take in order to get information not just on the technical capabilities of https://www.semrush.com but also on other important facts. There are a lot of different ways that we may go about this. Let's put in our domain and do some research on the information that can be acquired by simply employing Netcraft for the time being since that is the only tool we have access to right now. Let's put in our domain and do some research on the information that can be gained by solely utilising Netcraft. Let's enter in our domain and investigate the information that can be obtained by using Netcraft as it is the only tool that we have access to at the time. Since we are only using Netcraft at the moment, let's examine the information that can be gained via the use of Netcraft. There are a number of programmes and websites that are capable of performing this, but since we are only using Netcraft at the moment, let's examine the information that can be obtained through the use of Netcraft.

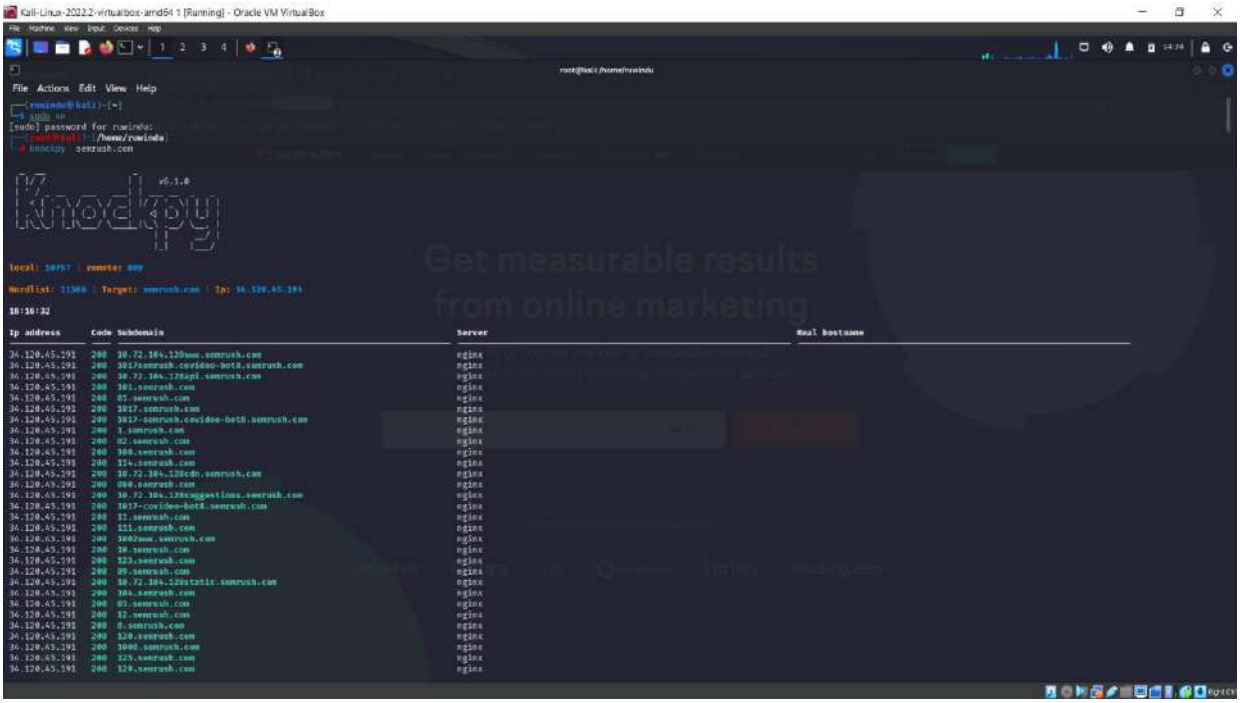


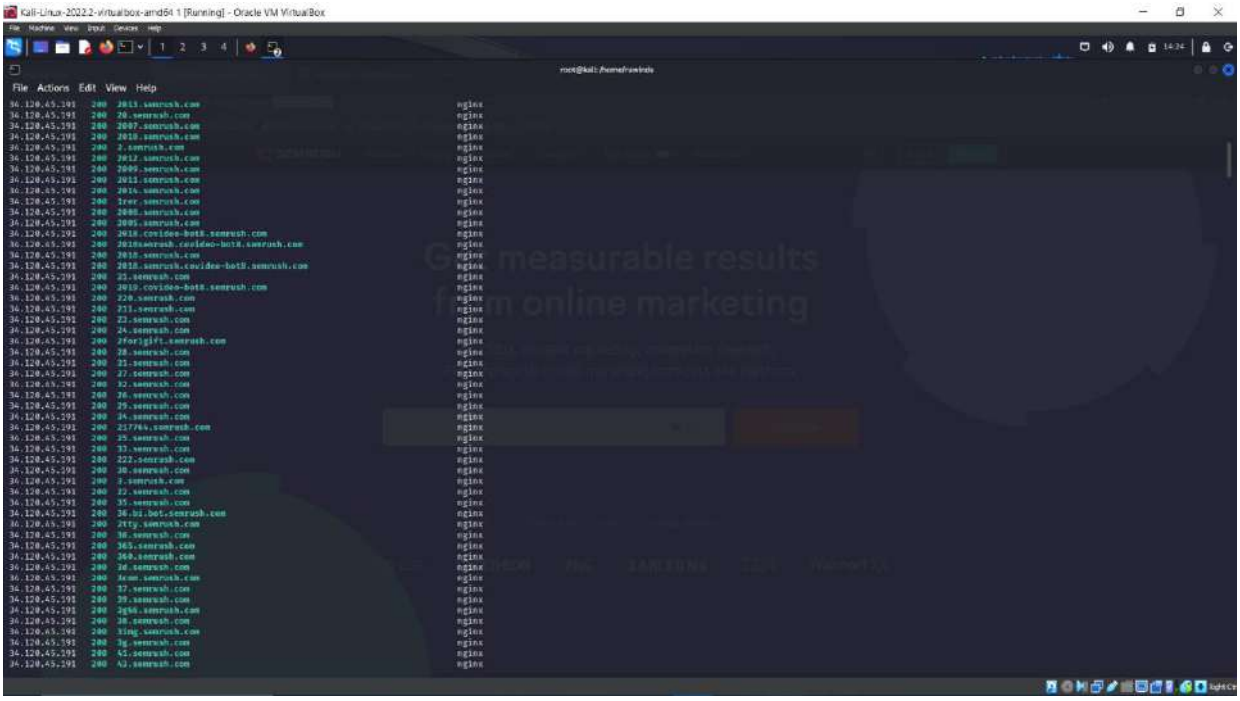

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
HackerOne
Semrush - Online Marketi
Site report for https://ww
https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.semrush.com
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
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.
8 known trackers were identified.
Companies
Google (4)
Twitter (2)
Facebook (1)
reddit (1)
Categories
Analytics (3)
Widget (2)
Advertising (1)
CDN (1)
Tracker (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Facebook
Widget
Facebook
www.behance.net, www.gazeta.pl, www.ilmeteo.it
Advertising
DoubleClick
www.avito.ru, www.arco.co.uk, www.corriere.it
Google
Analytics
Google Analytics
www.flightradar24.com, www.researchgate.net, www.infobae.com
Googletagmanager
www.cnn.com, www.inspq.qc.ca, www.coingecko.com
CDN
Googlecdn
www.nexusmods.com, www.cf.moncompteformation.gouv.fr, www.toutsameubles.com
Twitter
Analytics
Twitteranalytics
www.janiper.net, www.ctvnews.ca, www.evernote.com
Tracker
Tdocco
www.hl.co.uk, www.sigmaaldrich.com, mobile.twitter.com
Read static.netcraft.com

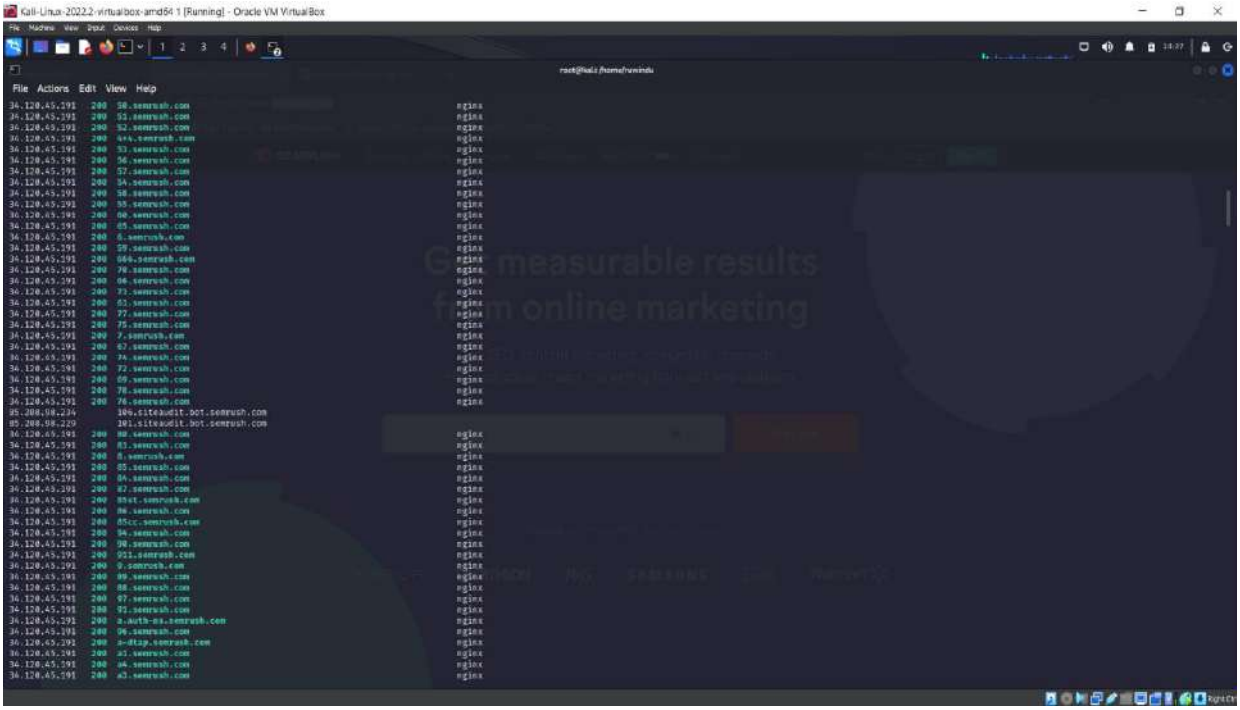

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Edit View History Bookmarks Tools Help
HackerOne
Semrush - Online Marketi
Site report for https://ww
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
HTTP Accelerator
A web accelerator is a proxy server that reduces web site access times.
Technology
Description
Popular sites using this technology
Google HTTPS Load Balancer
Google's external HTTP(S) load balancer
www.mozilla.org, www.gstatic.com, www.fastnet.net
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
XML
No description
www.virustotal.com, www.dailymail.co.uk, www.pinterest.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
JavaScript
Widely-supported programming language commonly used to power client-side dynamic content on websites
vk.com
Search

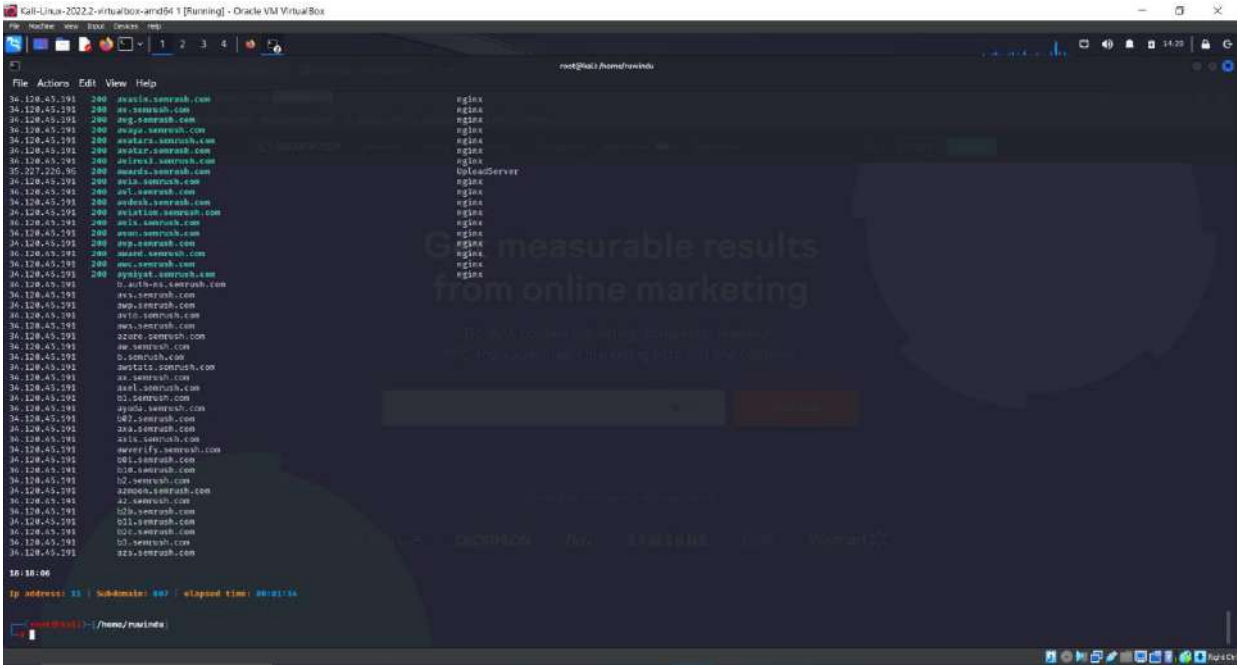
Using knockpy tool

In order for us to get to the bottom of what has really taken place here, we are going to need to do a subdomain scanning using software that has been built specifically for the purpose of carrying out a job such as this one. After that, and only after that, will we be able to get answers to all of the questions that we now have. The first thing that we do is run knockpy on both domains, and after that, we pay attention to the output to see what kind of results it provides us with. The first stage of the procedure will now begin after this step has been completed.





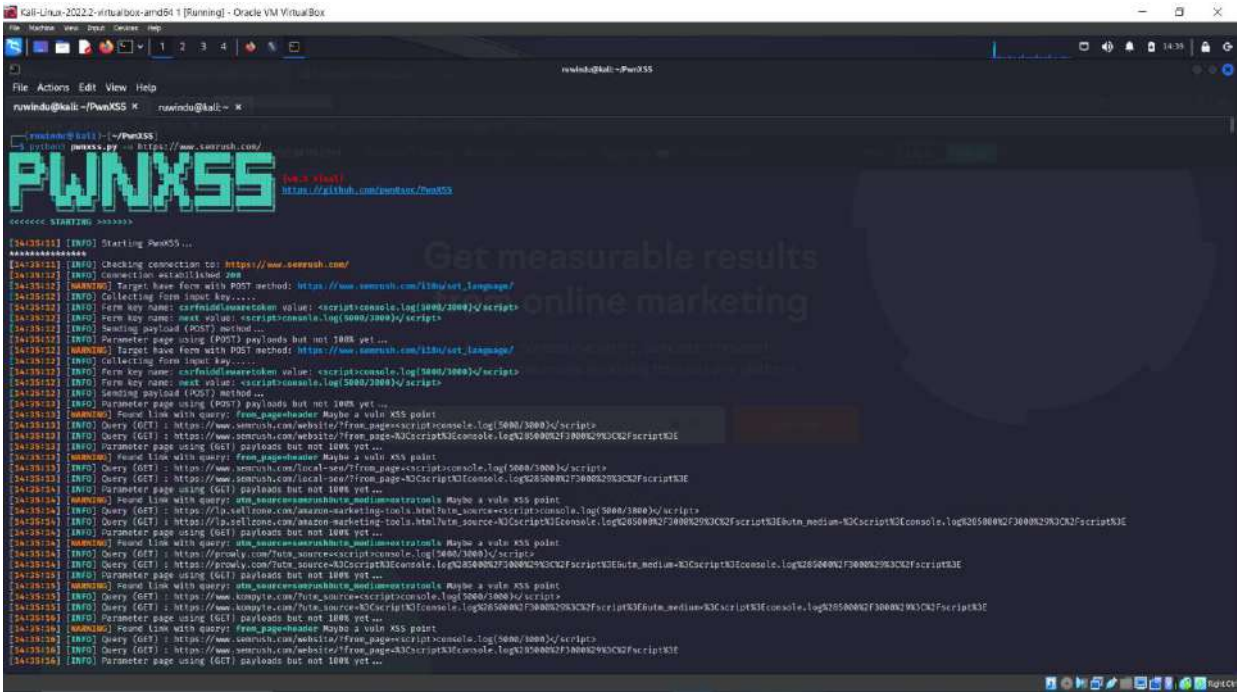


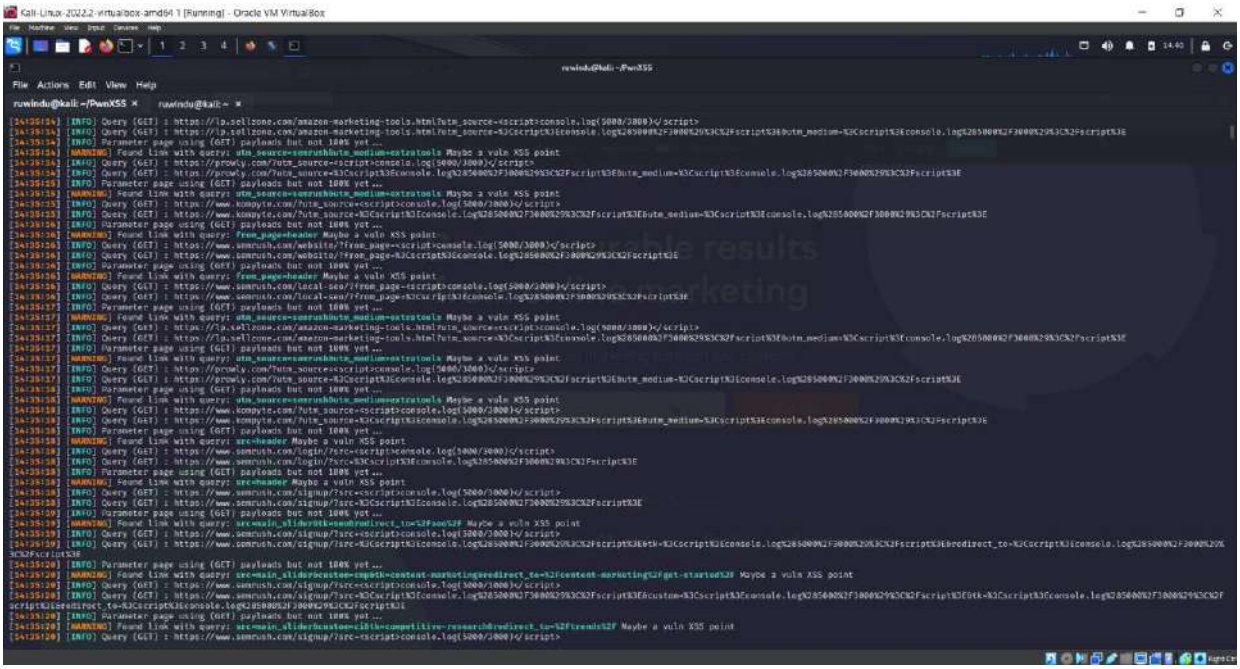


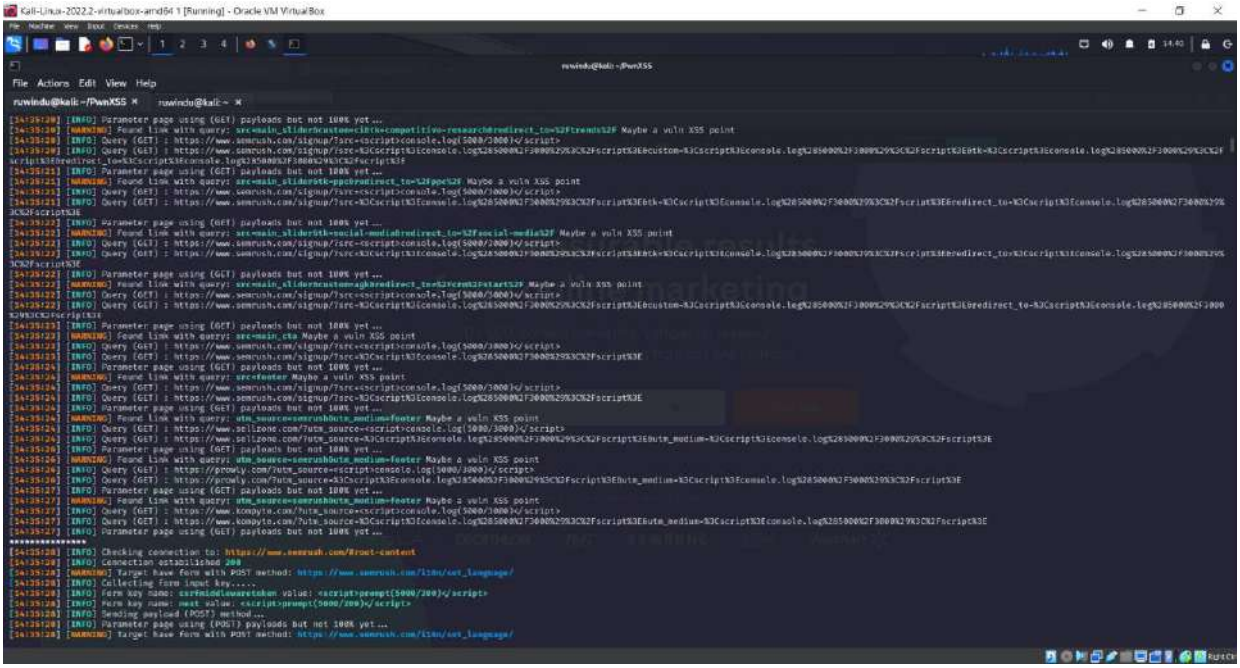
After having finished the process of enumerating subdomains, we are now in a position to study the formatted versions of the subdomains that can be located at www.semrush.com. This is because we have completed the method of enumerating subdomains. It is plainly clear that each and every subdomain that is included inside the www.semrush.com domain makes use of the same IP address and name server. This is the case since all of the subdomains are part of the same domain. You may get this information by going to the website www.semrush.com. This is shown by the fact that the specific information in question is very plainly visible to the naked eye. The fact that the program's actual hostname is shown provides more evidence to support our conclusion that this is a mobile application. Because of this, we are in a position to

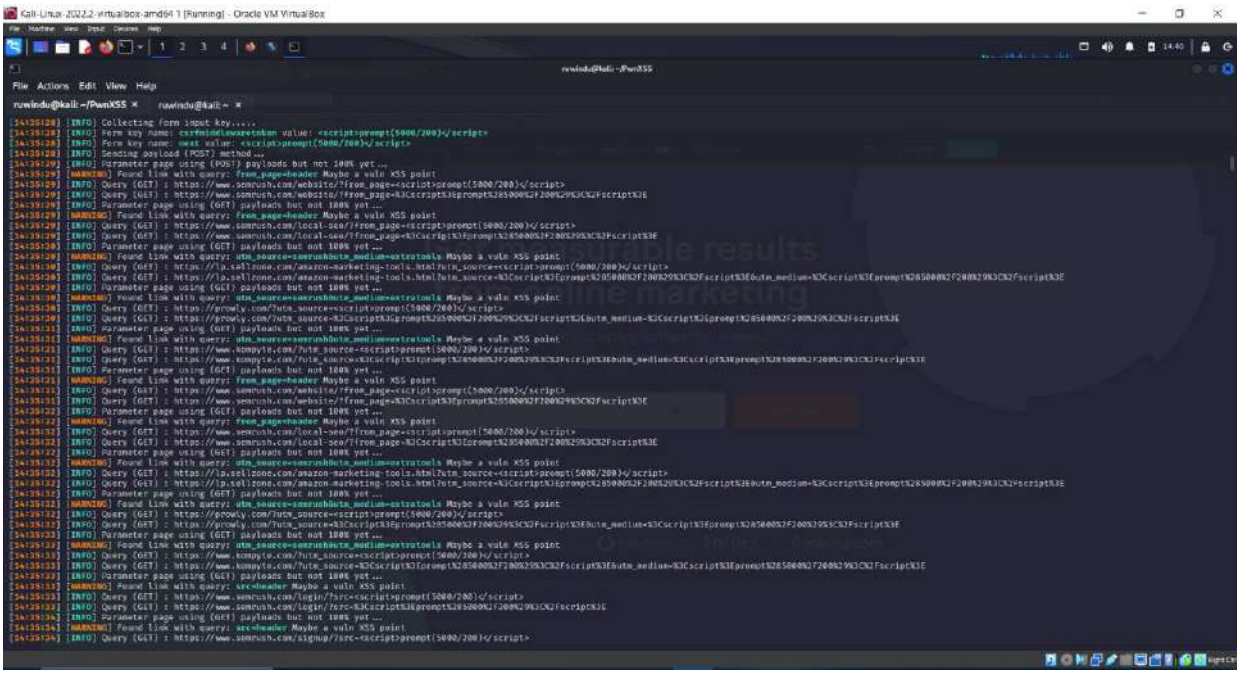
see that this is the current state of affairs. This is a direct result of what has occurred. Let's have a look at the results of the experiment, shall we? This particular website found a total of 807 subdomains and 11 different IP addresses for them.

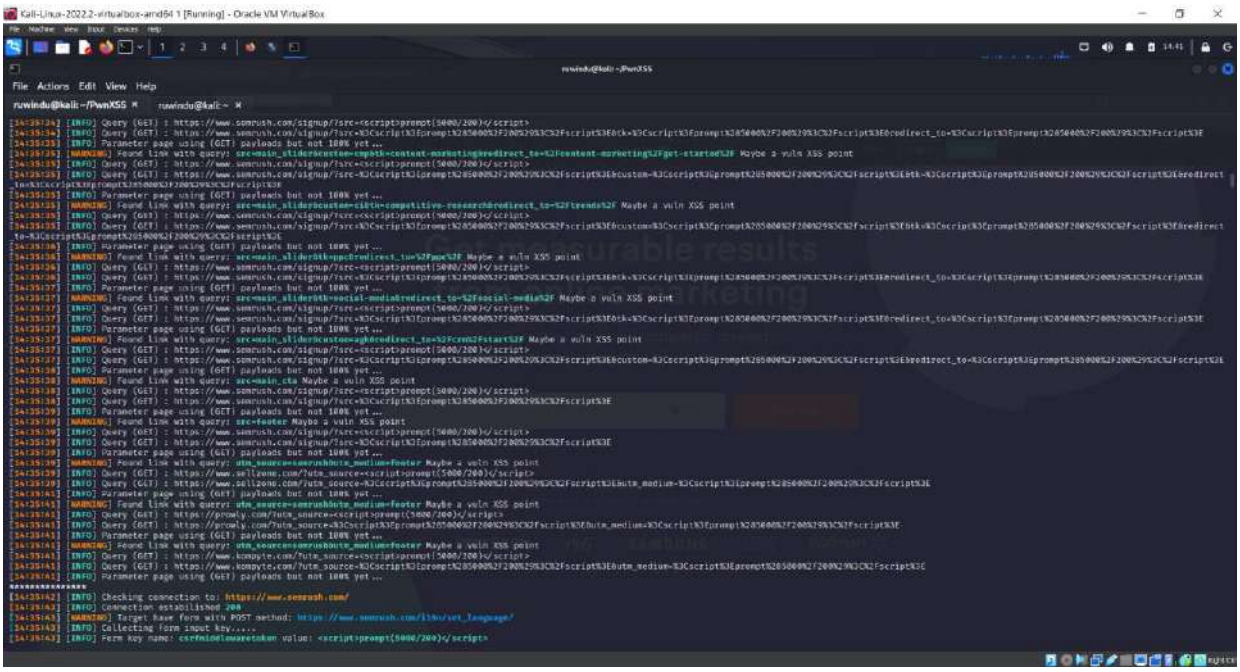
Using PwnXSS tool

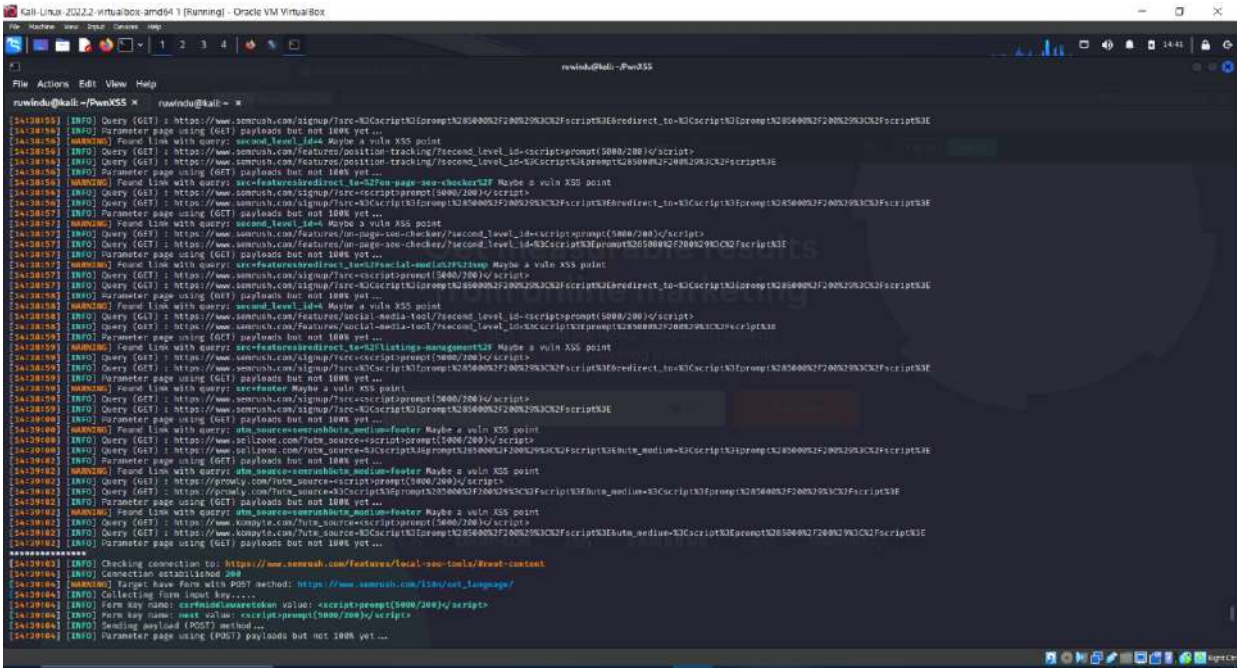





Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
ruwindu@kali: ~/PwnXSS
ruwindu@kali: ~


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
ruwindu@kali: ~/PwnXSS
ruwindu@kali: ~



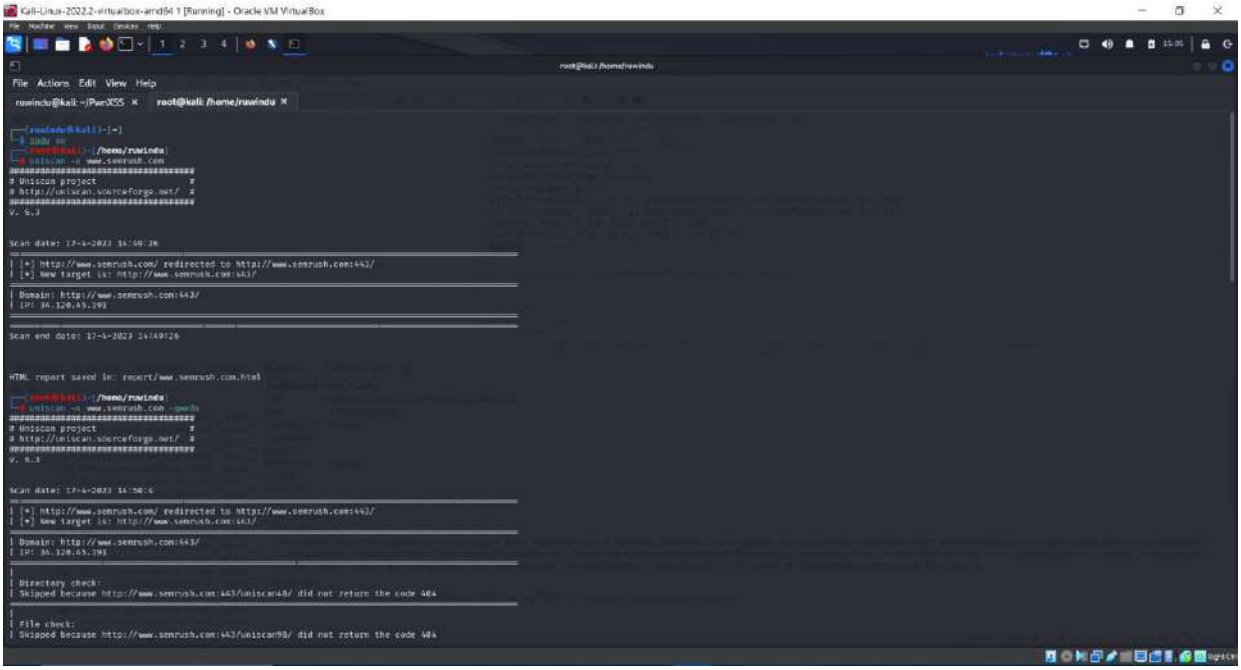


The findings of the scans that are presented both above and below were acquired with the assistance of the PwnXss scanner. As a direct consequence of these results, a number of previously unidentified XSS vulnerabilities that were found to exist on the website located at https://www.semrush.com have been brought to the attention of the general public.

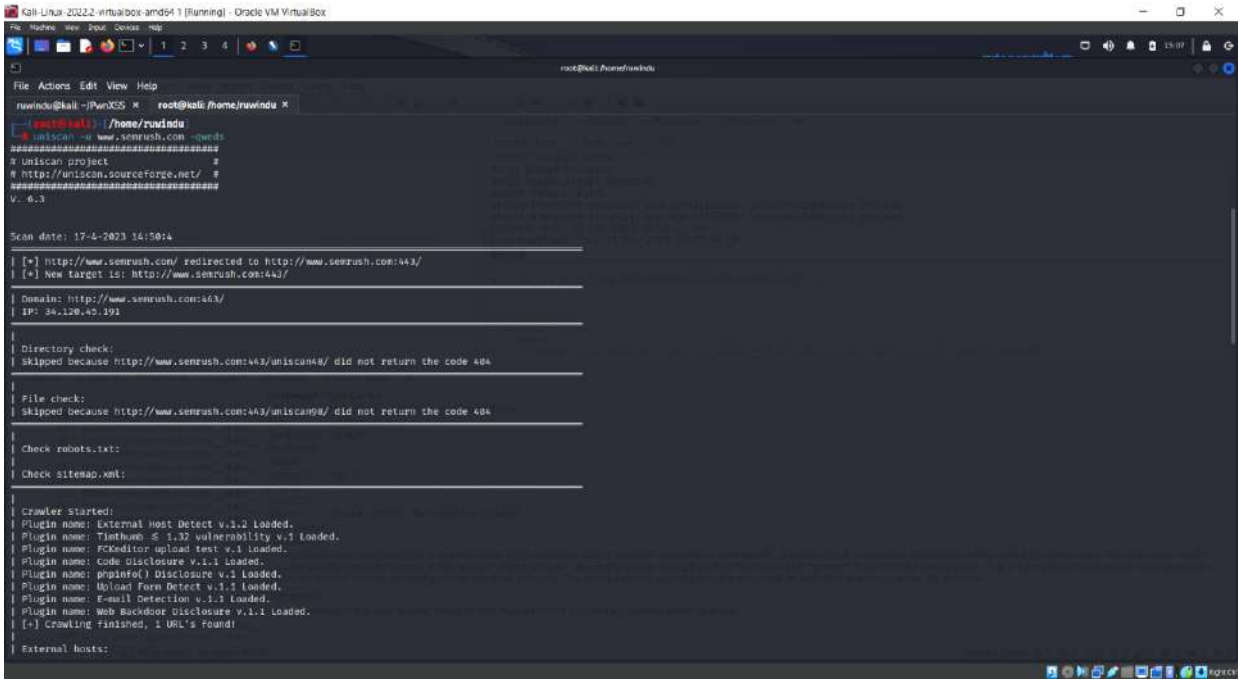
The list that was just presented comprises a significant number of open XSS vulnerabilities that were not mentioned anywhere in the discussion. I gave a few of them a go at being useful, and I'm delighted to say that my efforts were rewarded with favourable outcomes. Due to the fact that the payloads are missing essential vital components, exploiting these vulnerabilities has proved to be a challenging endeavour for those who have attempted it.

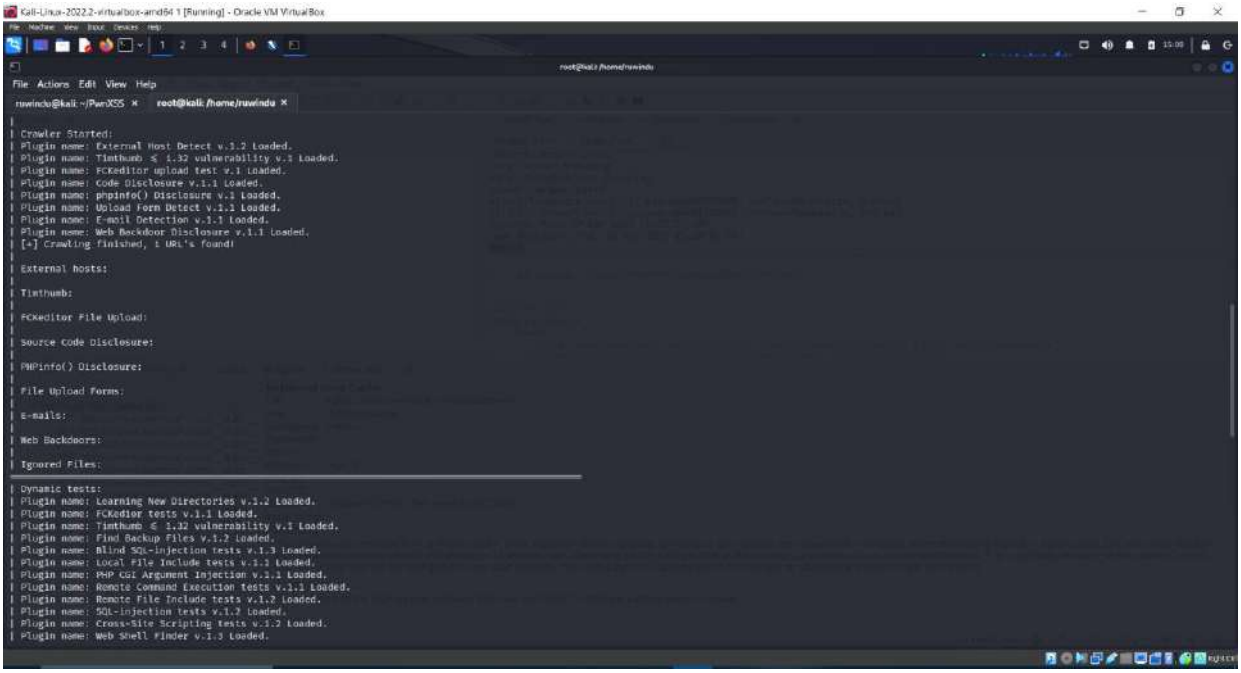
Using Uniscan tool

Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u www.semrush.com -qweds command:

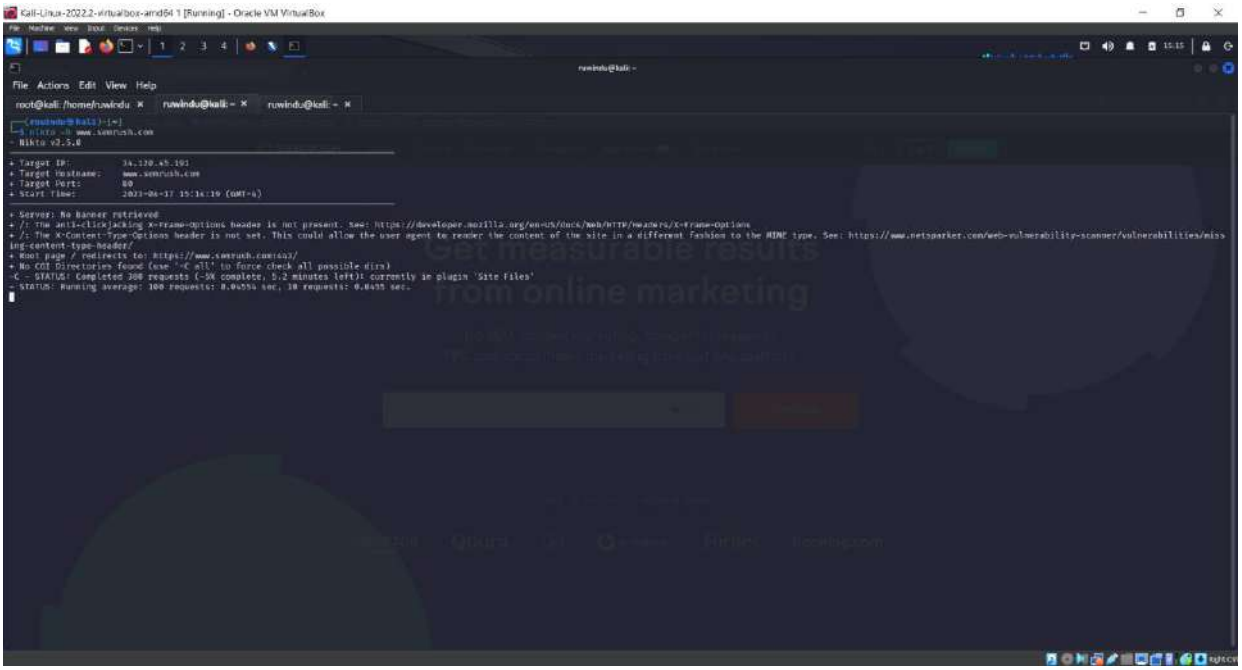




We were able to find some of the information that was housed by third parties by navigating to this region of the website, which is why it is referred to as the third-party sector of the website. In this specific investigation, web addresses, which are also often referred to as URLs, were found.

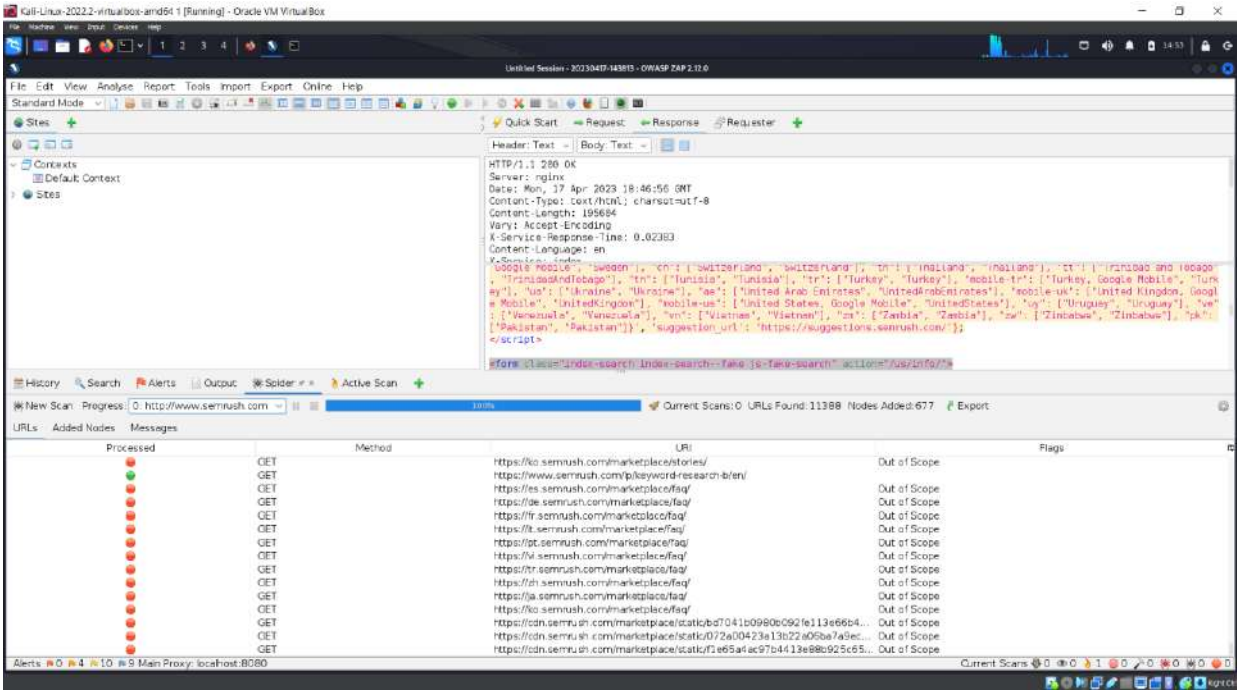
Using Nitko tool

We are provided with a greater number of high-level options and the nikto tool is utilised to cane the target domain when we run the command with the –h switch.



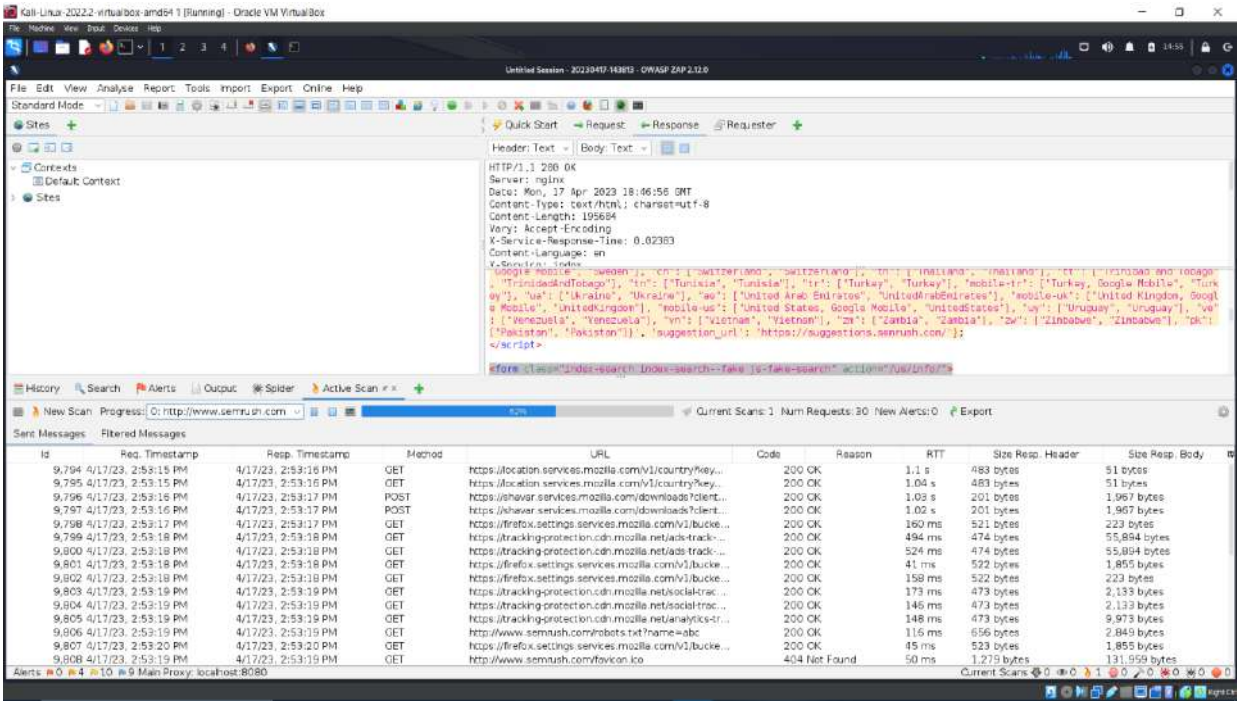
This scanner was not successful in discovering any vulnerabilities inside the system.

Using OWASP-ZAP tool



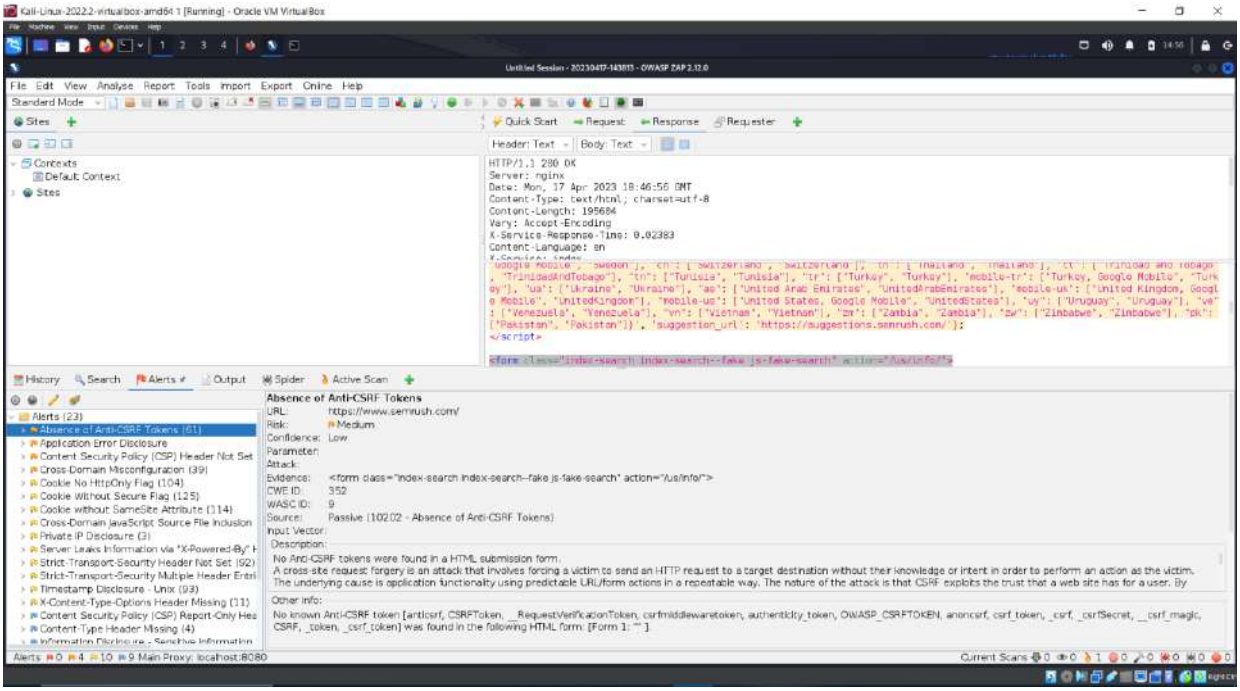
Found 11388 URLS.

On the left side of the primary screen of the tool, you will see the websites that you are targeting, and on the right side, you will be able to attack by giving the URL of the website you want to target. This view is the most important one for using the instrument. You will also obtain the outcomes of your assault depending on your scan at the very bottom of the display screen. Once we have arrived at this location, we can choose "active scan" from the drop-down option that displays when we click on the green plus symbol. And we need to establish our scan policy manager; moreover, you have the choice of either creating a scan policy or using the one that is already standard. In addition, you have the opportunity to change it and tailor the intensity of the attack to your own needs. When we click on the attack first, it will find all of the URLs that are related, and it will make an effort to attack those URLs in line with the scan method that we set up in advance.



Available Active scans.

When we are through with the procedure, our website will be shown on the left side of the screen; we can then choose it to see the results. On the alert tab, which is located at the bottom of the window, we are able to see highly significant information. You will be able to see a list of all the vulnerabilities that have been found inside that section. If we choose one of them, we will be presented with further information on the specific vulnerability.



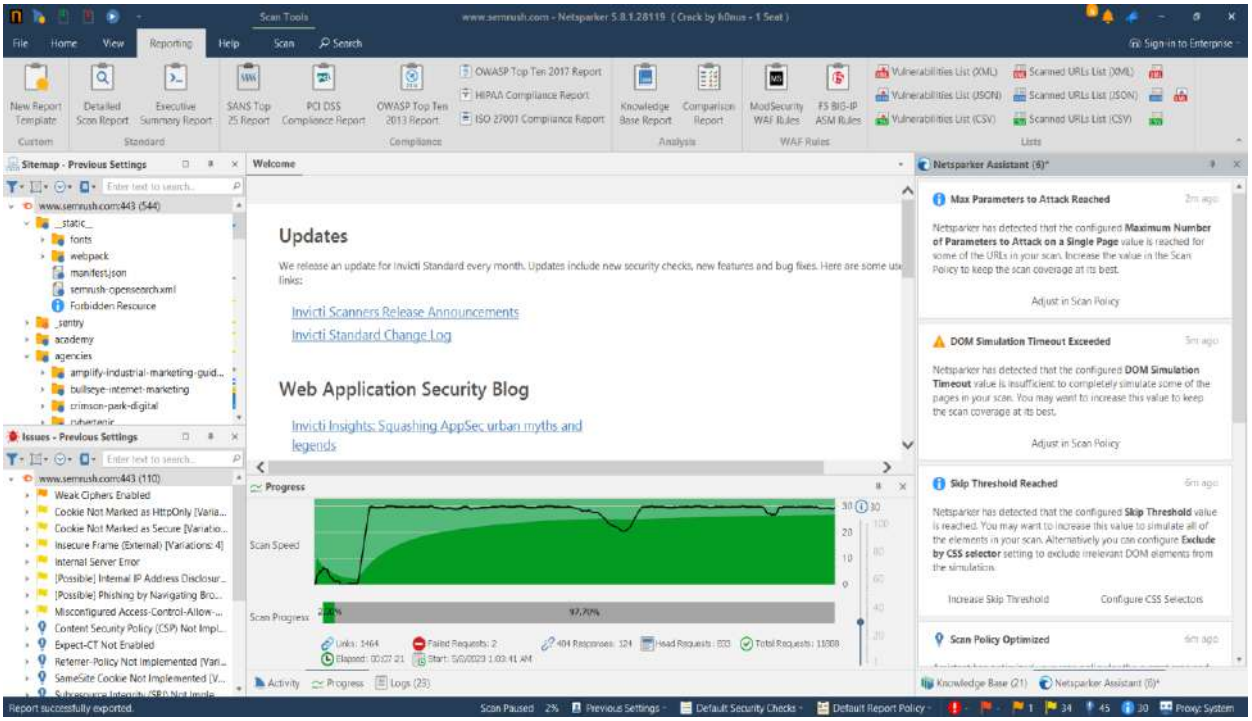
Found 23 Alerts.

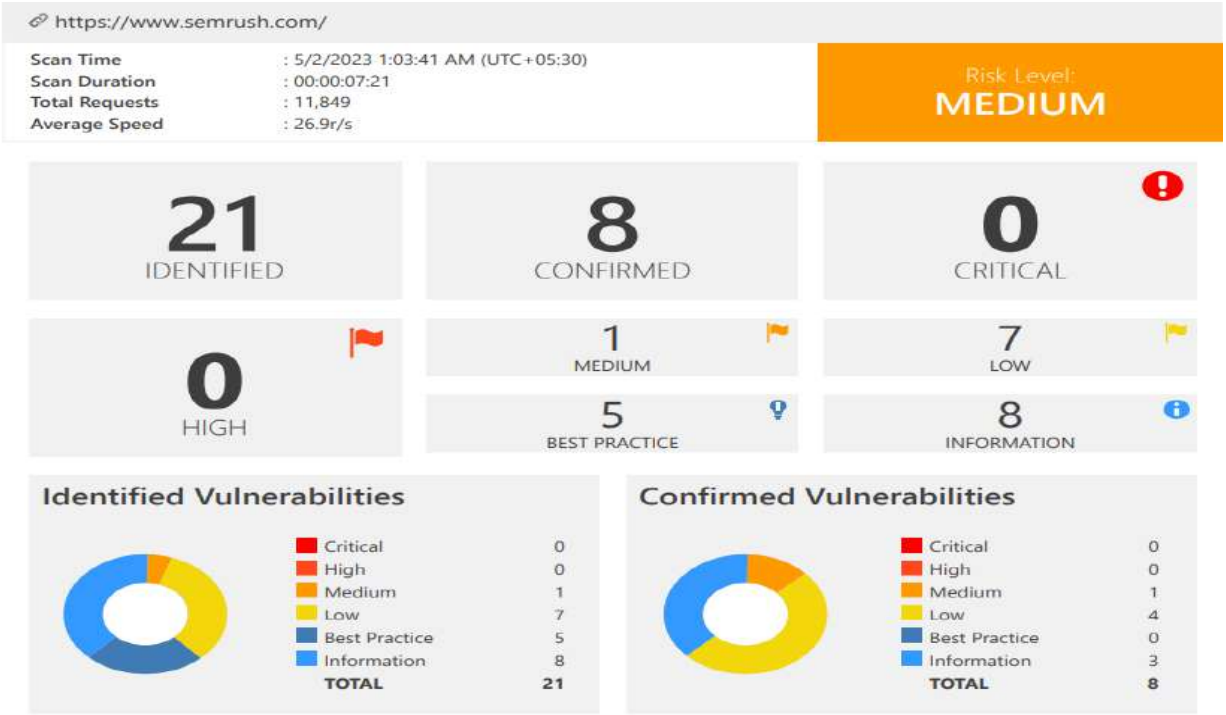
Vulnerabilities found

We did not get any warnings with a high priority throughout our vulnerability scan; however, we did receive a great deal of alarms with a low priority. I chose one of them at random and made advantage of the weakness it had in order to look for another fault elsewhere in the system.

Using Netsparker

In the course of my Audit, I performed a vulnerability check on harvestapp.com with the aid of Netsparker professional Edition (V), which proved to be of great service to me in my endeavor. For the purpose of this specific audit, the website was analyzed.





After doing a scan of the domain, I was able to identify a total of 21 vulnerabilities related to the domain, including 1 vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Weak Ciphers Enabled	GET	https://www.semrush.com/	
	[Possible] Internal IP Address Disclosure	GET	https://www.semrush.com/marketplace/?nsextt=%2522%252bnetsparker(0x004278)%252b%2522	nsextt
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.semrush.com/kb/?nsextt=%0ans%3anetsparker056650%3dvuln	nsextt
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.semrush.com/splitsignal/	
	Cookie Not Marked as HttpOnly	POST	https://www.semrush.com/i18n/set_language/	
	Cookie Not Marked as Secure	GET	https://www.semrush.com/	
	Insecure Frame (External)	GET	https://www.semrush.com/webinars/	
	Internal Server Error	GET	https://www.semrush.com/news/categories/WS_FTP.log	URI-BASED
	Content Security Policy (CSP) Not Implemented	GET	https://www.semrush.com/	
	Expect-CT Not Enabled	GET	https://www.semrush.com/	
	Referrer-Policy Not Implemented	GET	https://www.semrush.com/	
	SameSite Cookie Not Implemented	GET	https://www.semrush.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.semrush.com/	
	CDN Detected (Google Cloud CDN)	GET	https://www.semrush.com/	
	Email Address Disclosure	GET	https://www.semrush.com/	
	ExpressJS Identified	GET	https://www.semrush.com/agencies/?hTTp://r87.com/n	

https://www.semrush.com/ has been found to have the following identified vulnerabilities:

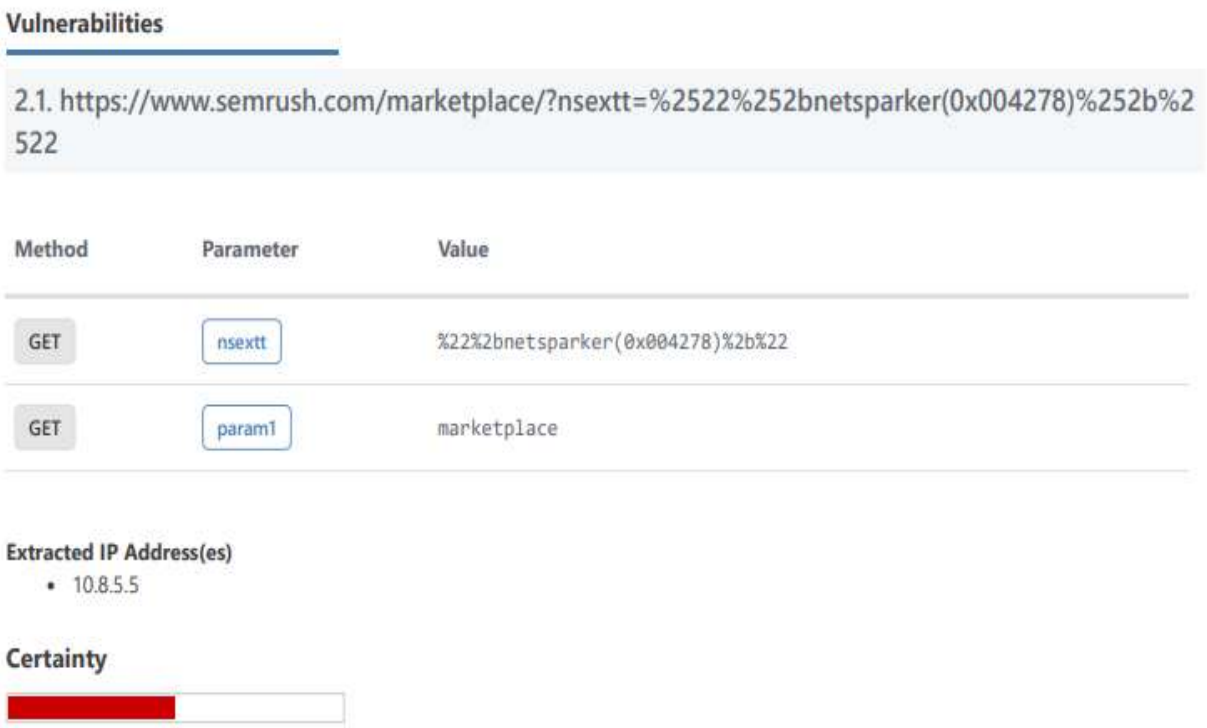
Identified vulnerabilities in https://www.semrush.com/

Vulnerability 08 - [Possible] Internal IP Address Disclosure (Medium)

The results of Netsparker suggest that the page in issue may be leaking confidential information regarding IP addresses.
Because it was impossible to tell whether the IP address belonged to the system itself or to an internal network, it was unknown to which of the two types of networks it was associated.

Impact

There is no immediate effect; nonetheless, this information may be beneficial to an enemy in uncovering new vulnerabilities or in developing methods to exploit holes that have already been identified and disclosed. Although there is no immediate impact, there is the potential for an adversary to utilize this knowledge.



Request

```
GET /marketplace/?nsextt=%2522%252bnetsparker(0x004278)%252b%2522 HTTP/1.1
Host: www.semrush.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: GCLB=CM2RtpWFyrXEoAE; PHPSESSID=8ae51cda77ff18c1dbe889989f0e27a8; SSO-JWT=eyJhbGciOiJFUzI1NiIsI
nR5cCI6IkpXVCJ9.eyJqdGkiOiI4YWU1MWNkYTc3ZmYxOGMxZGJlODg5OTg5ZjBlMjdhOCIsImlhdCI6MTY4Mjk2OTYxNywiaXNzIjo
ic3NvIn0.RtusJabvCSmeuD5i-Q4D7W_ud3l49480aLzi13s6QTxBgI_JrbcLpLBXNZKL4jz-mzAXDvVXvlatkqOctiNIRg; app_ce
nter_csrf_token=142239eac0cf4dcbb4dafd048b94a5f6; site_csrftoken=e9QzgUKHQ42xWalPEMdifwtoi5Ih5SUbyiZYDS
EK0sXw08rJUxBs0nfxE2dU9hsI; localization=%7B%22locale%22%3A%22en%22%7D; XSRF-TOKEN=eyJpdiI6InJWSGtQQ3ls
R0UrS05ESUpabjUxY0E9PSIsInZhbHVlIjoiZSsxUm5nM3VBTUhIU1BsR2VISGpVS0dhNGZGb0dGVldnSExqRjFlSTNleVNaWG5hQ1R
1a3hjd3NvVzdzTEtcLzYiLCJtYWMiOiIwNTRhOTllNWU4ZjVlZGExMmUzMDYxMjM0ZjY1MzE4YWY2MTJiZDhhZjkxYjM1YzU0YjcyZD
M2ODNkYzVmN2M1In0%3D; webinars_session=nJKDkUJk5Gqh1dRd7x1arb7Oz0WEit18Y3D8nn1Q; csrftoken=fF84v2UDzYZo
JBqq3PizXuuVU3bvDfGKY8dMlvgFDC3k3zlXhFSNUyiQuQhLZClc
Referer: https://www.semrush.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 539.8527 Total Bytes Received : 467846 Body Length : 467160 Is Compressed : No

```
HTTP/1.1 200 OK
X-Service: projects.marketplace
Cache-Control: no-cache
ETag: W/"6da90-oABtJH+HDP+ZXm09mug15MLe8Kg"
Strict-Transport-Security: max-age=31536000; includeSubdomains; preload
Transfer-Encoding: chunked
Server: nginx
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Via: 1.1 google
X-Frame-Options: DENY
Vary: Accept-Encoding
sm-log-id: f1b-6ac28edf51311a38f77df8fa3d1904bc
Server-Timing: service;dur=90.26085, backend;dur=110.33305
X-Service-Response-Time: 0.08896
Content-Language: en
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
Content-Type: text/html; charset=utf-8
Date: Mon, 01 May 2023 19:36:47 GMT
Con
…
5.6-2.6-.1-6-3-7.4-4.7-3.2-5.6-1.7-.6.8 15.3 7.5-10.7 9-12.6-1.2-2.5-9 9.3-14.2 16.7-12.3 7.5 2 12.9 8.
9 19.5 12.8a.5.5 0 00.7.5zm-14 11.6c-3.2-1-14.6 8.3-14.2 11.5a.5.5 0 00.7-.1 26.1 26.1 0 0113.2-10.8.5.
50 00.3-.6zm33.3-126.7a180.2 180.2 0 00-9 16.4 13.3 13.3 0 004.2.6c3.2-5.6 6.5-11.3 9.6-17a11.8 11.8 0
 00-3.2-2.6l-1.6 2.6zm-10 16l10.8-19a13.5 13.5 0 00-6.9-1.3c-3.2 5.4-6.2 10.9-9 16.4a11.9 11.9 0 0
…
296.1 114c-8 3.8-10-3.2-3.8-8 .7-1.2 2-.2.6.7-1 1-4.3 4.1-3.1 6.3 1.3 2.4 5.8.2 5.9.2a.5.5 0 01.4.9zm8.
4 3.7c-4.4-5.5-11.3 3.8-7.1 8 5.4 5.3 10.5-3.4 7.1-8zm-39.2 88a.5.5 0 00.7-.1 26.1 26.1 0 0113.2-10.8.
5.50 00.3-.6c-3.2-1-14.6 8.3-14.2 11.5zm254-13.9c-4 23.9-35.8 25-59.7 26.3 2.4 23.3 9.1 45.5 16.6 64.9h
-1a252.9 252.9 0 01-16.6-65c-7 .2-14.3-.2-21.2-.6-3.8 12.3-13 20.4-27.6 23.8l17.7 41.8h-1.1l-17.6-4
…
```

Solution

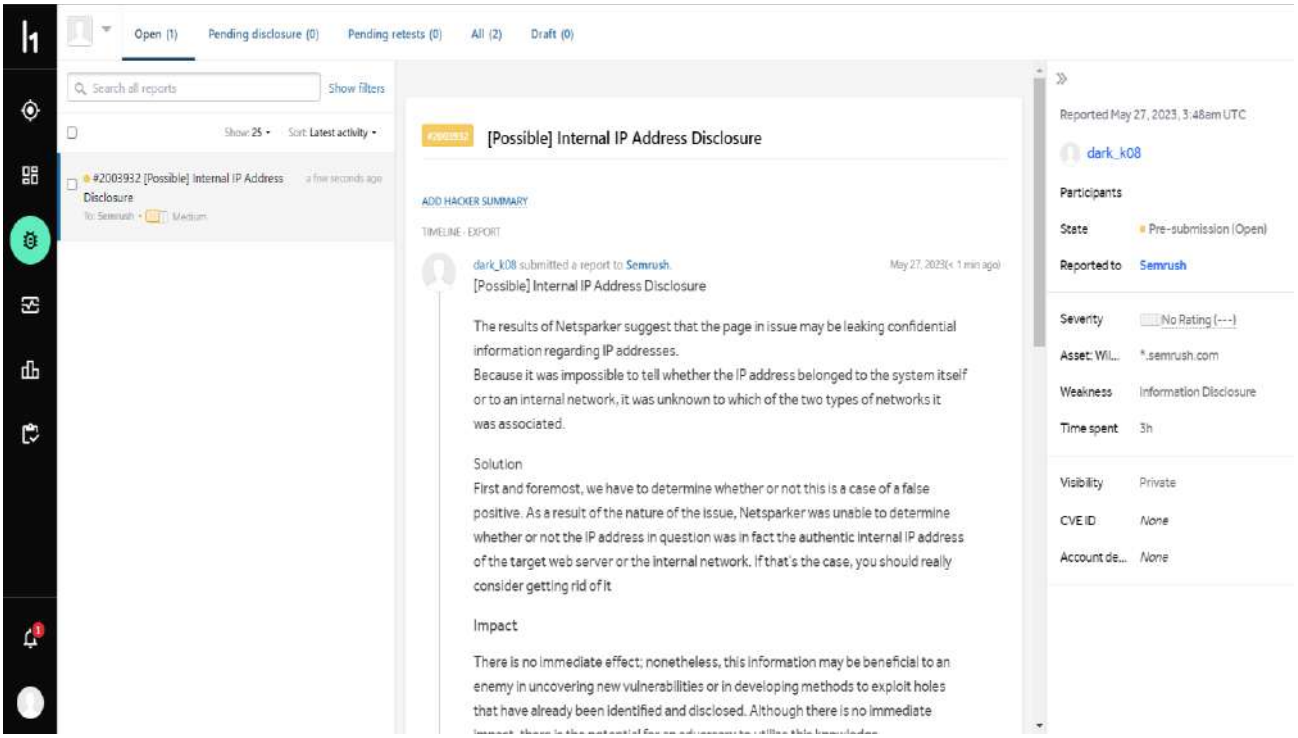
First and foremost, we have to determine whether or not this is a case of a false positive. As a result of the nature of the issue, Netsparker was unable to determine whether or not the IP address in question was in fact the authentic internal IP address of the target web server or the internal network. If that's the case, you should really consider getting rid of it.

Conclusion of the Report 08

We started by researching the backdrop, including the company's actions and legislation. Several topics were covered. Then We start our bug hunt by gathering some crucial data. These include the hosting company's IP address and the domain's technology. We then move all subdomains to the same server and discover that each domain has the same IP address.Sometimes we need to utilize many tools to get additional information and verify it. After that, we checked netcraft for files and directives to analyze our domain diagram. We concluded there are no such files or instructions. It clarified the entire subject.

Next, we assess possible vulnerabilities. We learned about the domain's vulnerabilities and how to use tools to find them at that time. To further understand this web application's vulnerability, we use other websites to test it. After discovering flaws, we tried to prove one was dangerous.We had decided the vulnerability was not substantial, but we were supplied with a lot of fascinating information.

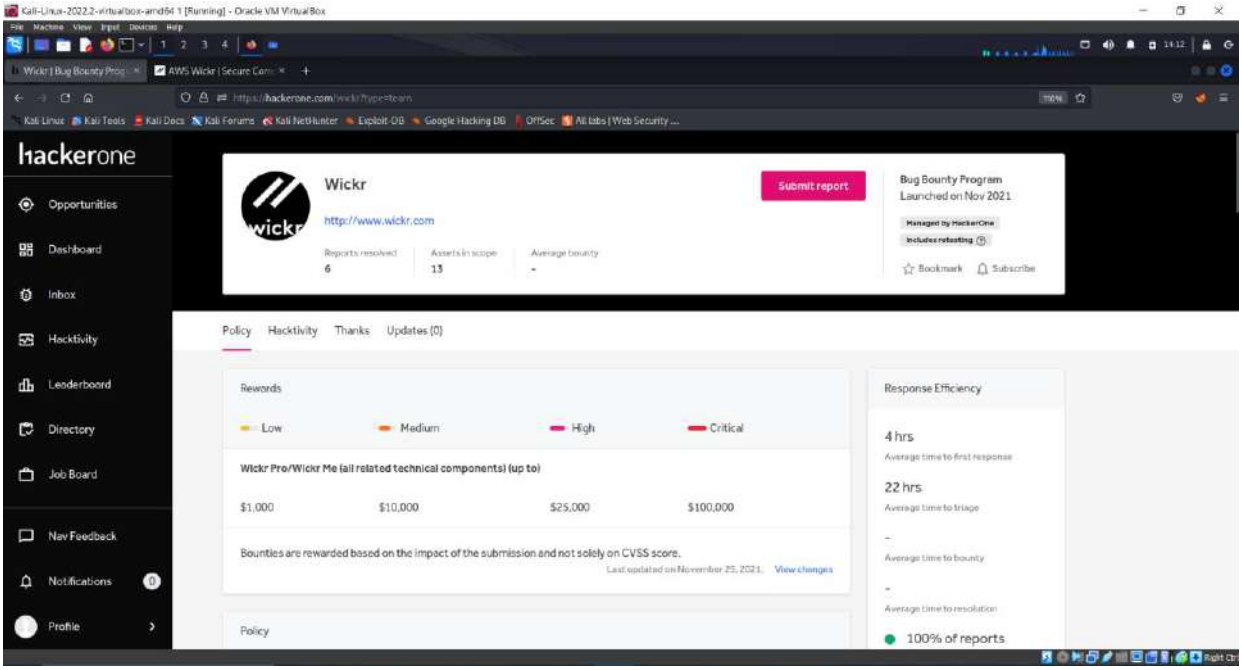
HackerOne Submitted Report Screenshot

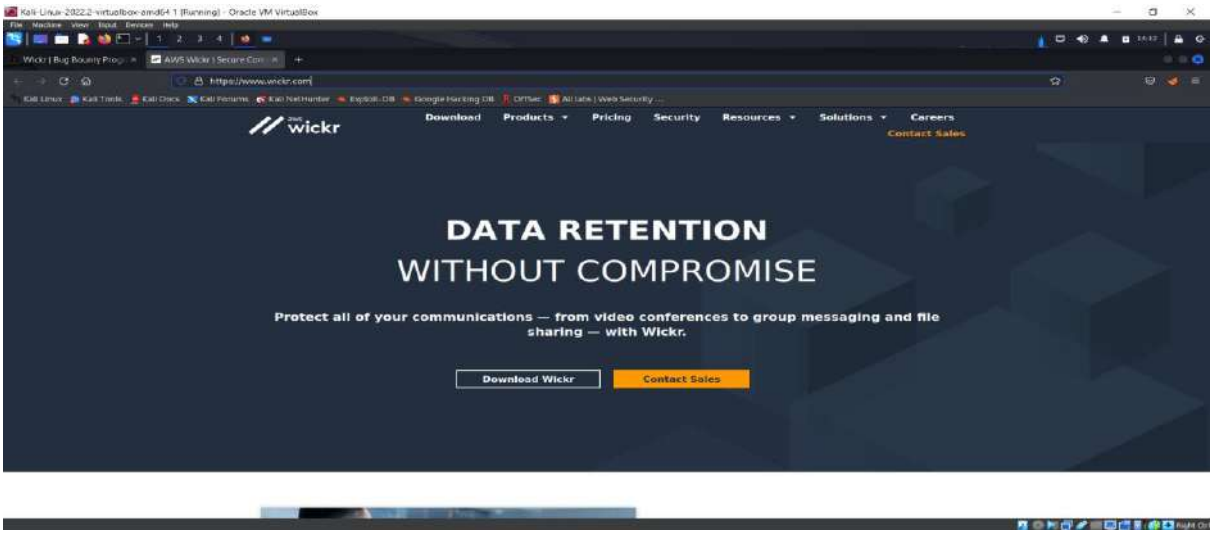


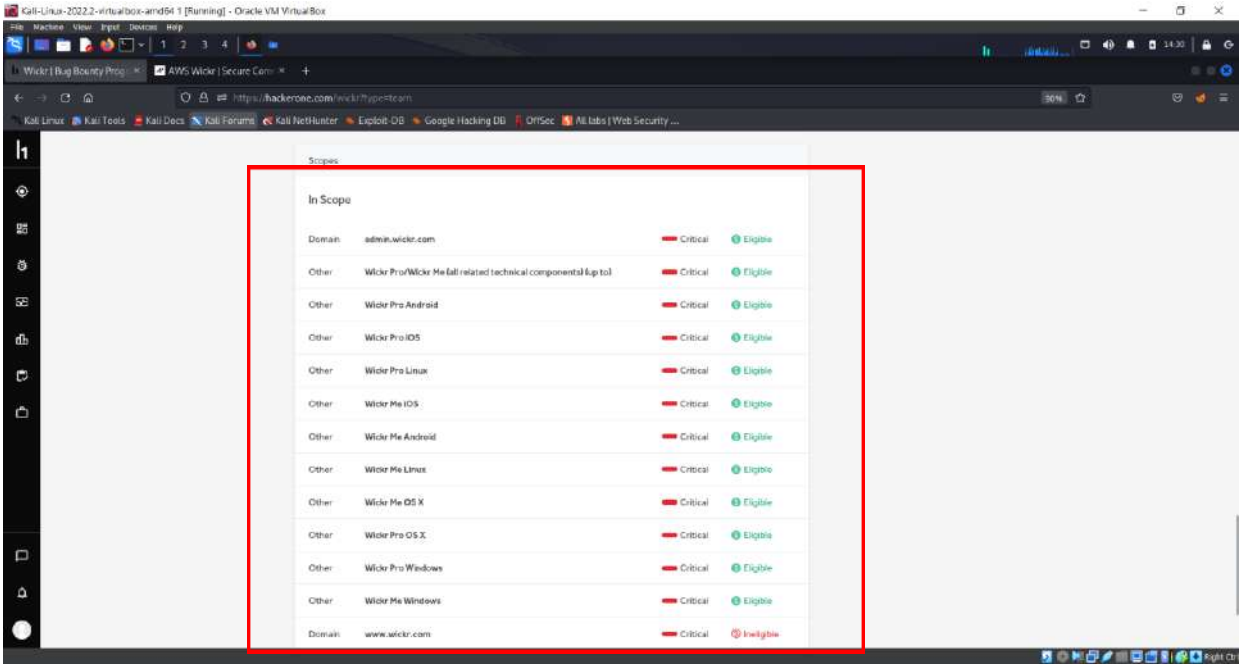
ix. Report 09

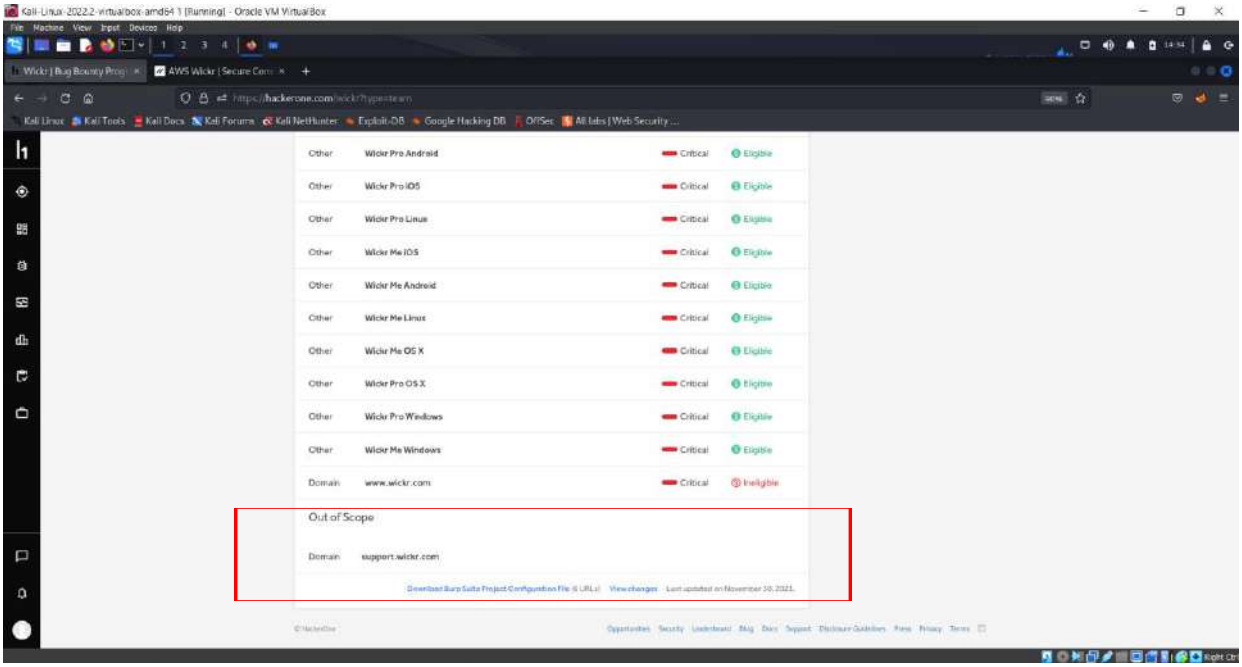
Target information: https://www.wickr.com/

This assessment's goals are to establish both the degree of risk that is associated with the potential points of vulnerability that are found within the target domain (https://www.wickr.com/), as well as the potential points of vulnerability that are discovered within the target domain. In other words, the goal of this evaluation is to evaluate both the degree of risk that is associated with the potential points of vulnerability that are found within the target domain. The assessment that is now being carried out has as its primary goal the identification of problematic aspects associated with the topic that is the center of attention.



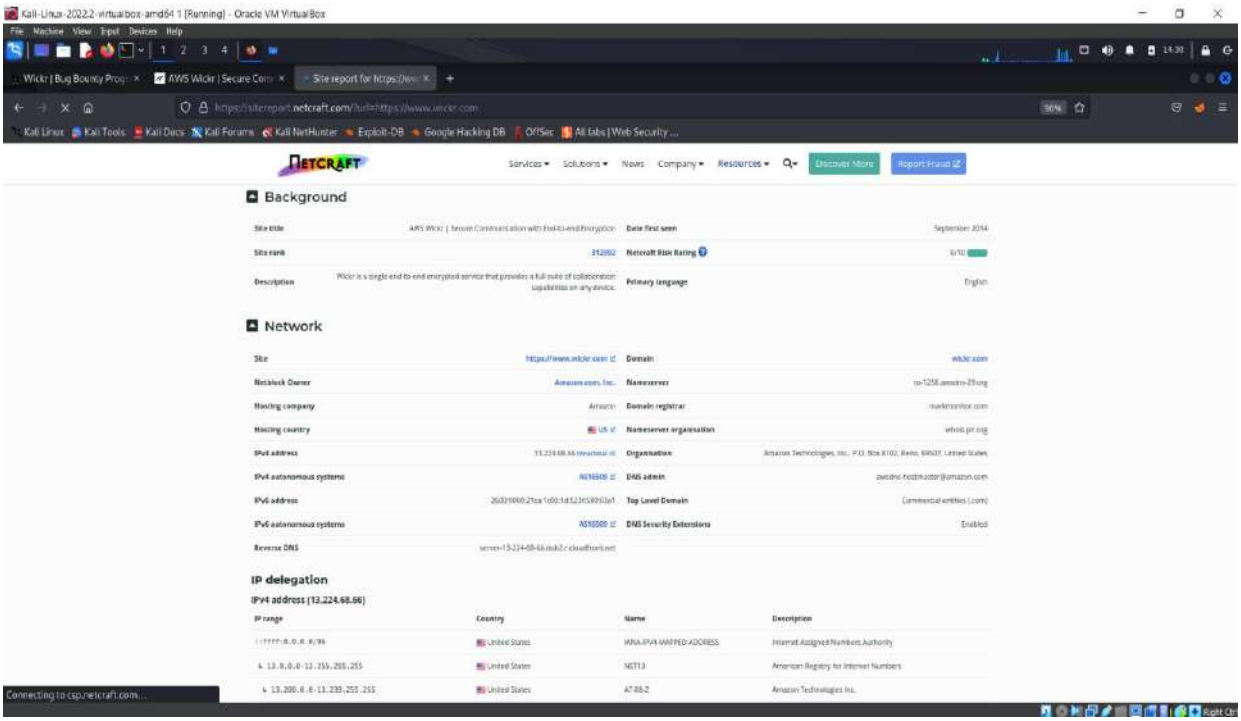


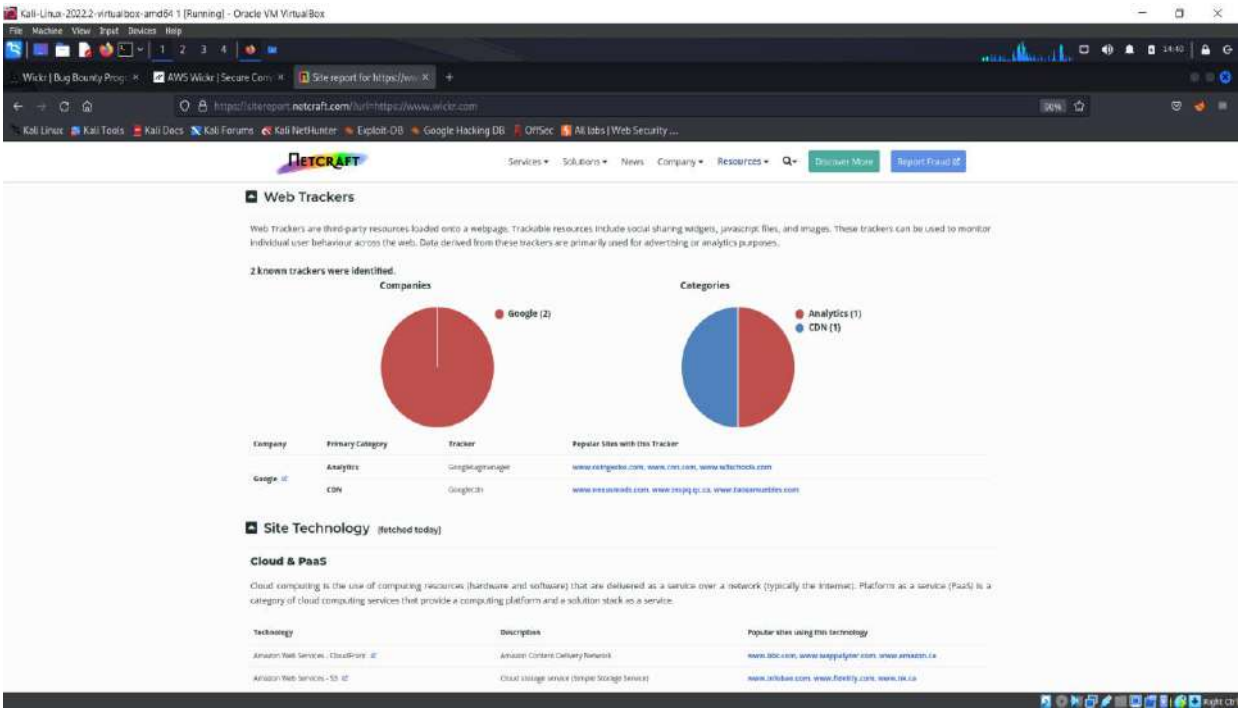

Scopes
In Scope
Domain admin.wickr.com Critical Eligible
Other Wickr Pro/Wickr Me (all related technical components) (up to) Critical Eligible
Other Wickr Pro Android Critical Eligible
Other Wickr Pro iOS Critical Eligible
Other Wickr Pro Linux Critical Eligible
Other Wickr Me iOS Critical Eligible
Other Wickr Me Android Critical Eligible
Other Wickr Me Linux Critical Eligible
Other Wickr Me OS X Critical Eligible
Other Wickr Pro OS X Critical Eligible
Other Wickr Pro Windows Critical Eligible
Other Wickr Me Windows Critical Eligible
Domain www.wickr.com Critical Ineligible

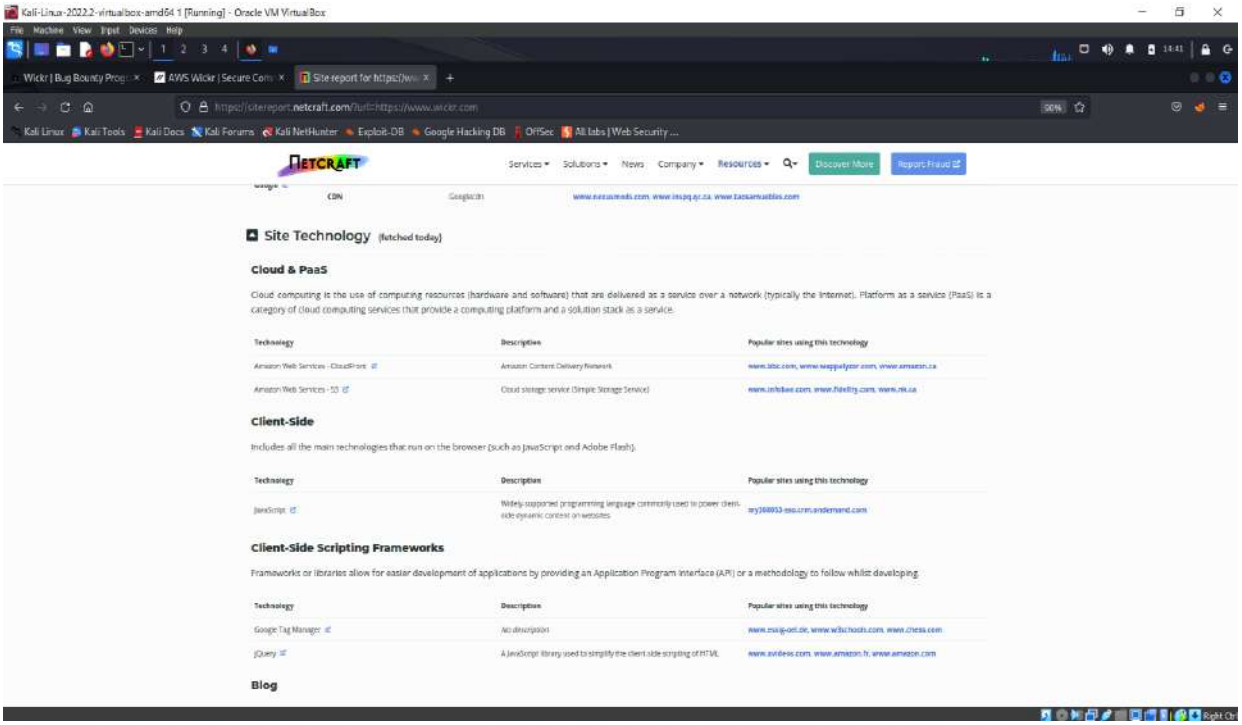

Other Wickr Pro Android Critical Eligible
Other Wickr Pro iOS Critical Eligible
Other Wickr Pro Linux Critical Eligible
Other Wickr Me iOS Critical Eligible
Other Wickr Me Android Critical Eligible
Other Wickr Me Linux Critical Eligible
Other Wickr Me OS X Critical Eligible
Other Wickr Pro OS X Critical Eligible
Other Wickr Pro Windows Critical Eligible
Other Wickr Me Windows Critical Eligible
Domain www.wickr.com Critical Ineligible
Out of Scope
Domain support.wickr.com

Information Gathering For Target Domain

Let's have a look at the many routes we may take to find out not just the technical specifications of https://www.wickr.com/, but also other essential information. Several methods are at our disposal for achieving this goal. Many different strategies exist for accomplishing this goal. Let's use the one and only resource we have at the moment, Netcraft, to enter our domain name and see what information it returns. Let's use Netcraft to get into the specifics that can't be accessed anywhere else by entering our domain name. Since we are now limited to using Netcraft, let's see what information we can glean from a scan of our network. Doing this will be a good use of our time. Let's take a look at what we can learn from Netcraft because it's our only option for now. Since Netcraft is currently our only option, let's examine the information it can supply. We will look at the information that can be gleaned from Netcraft for the time being even if there are other software and websites that can do this purpose.

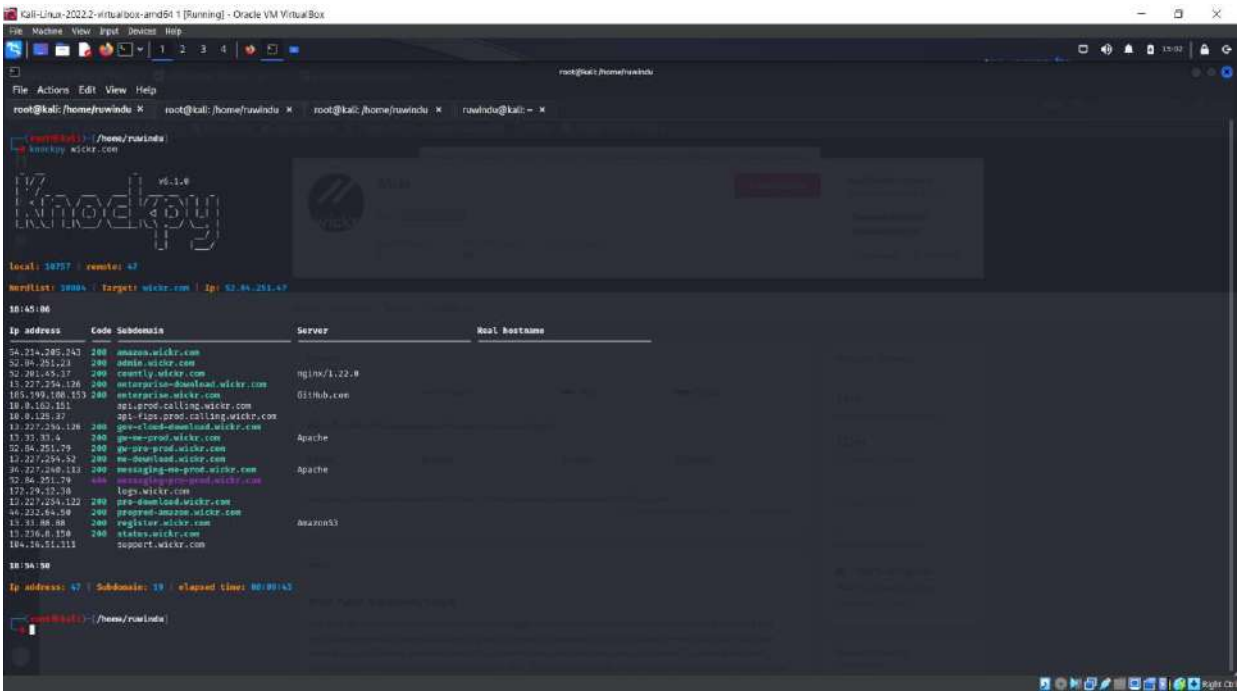



Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Web Trackers
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. 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.
2 known trackers were identified.
Companies
Google (2)
Categories
Analytics (1)
CDN (1)
Company
Primary Category
Tracker
Popular Sites with this Tracker
Google
Analytics
CDN
Site Technology (fetched today)
Cloud & PaaS
Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.
Technology
Description
Popular sites using this technology
Amazon Web Services - CloudFront
Amazon Content Delivery Network
Amazon Web Services - S3
Cloud storage service (Simple Storage Service)


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
CDN
Site Technology (fetched today)
Cloud & PaaS
Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). Platform as a service (PaaS) is a category of cloud computing services that provide a computing platform and a solution stack as a service.
Technology
Description
Popular sites using this technology
Amazon Web Services - CloudFront
Amazon Content Delivery Network
Amazon Web Services - S3
Cloud storage service (Simple Storage Service)
Client-Side
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).
JavaScript
Client-Side Scripting Frameworks
Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.
Google Tag Manager
No description
jQuery
A JavaScript library used to simplify the client-side scripting of HTML
Blog

Using knockpy tool

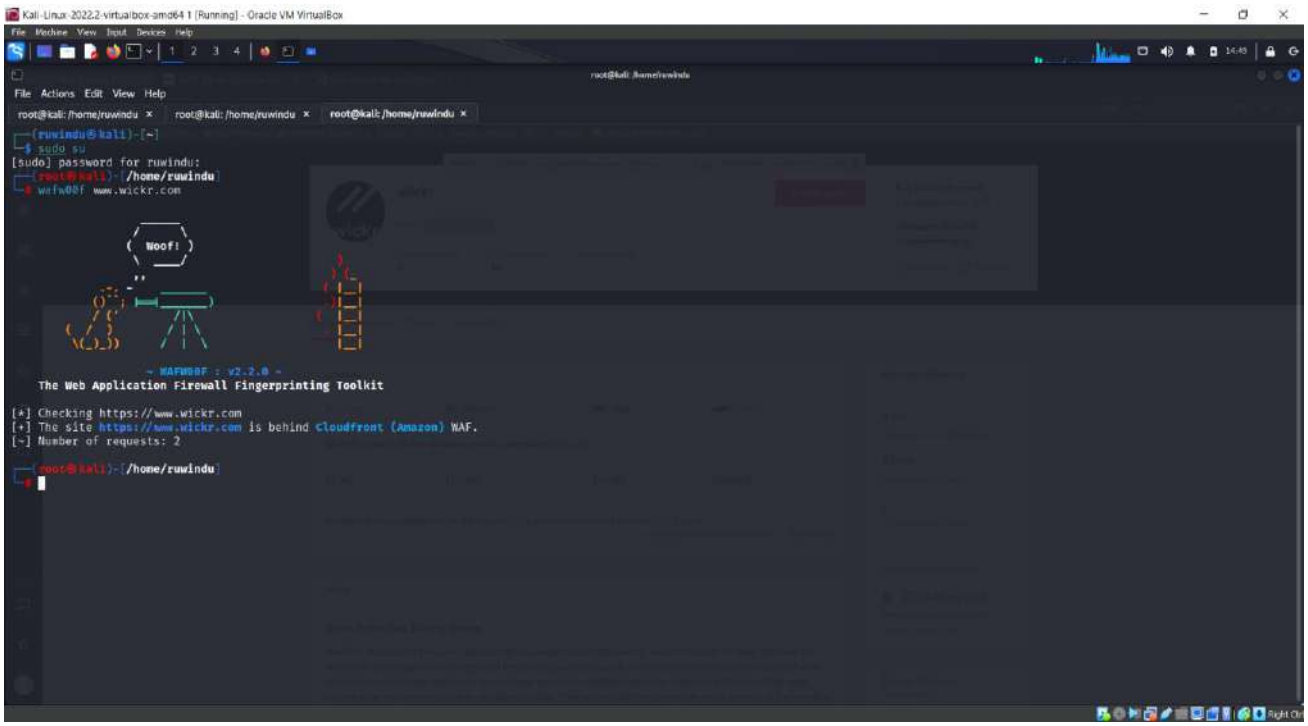
In order for us to get to the bottom of what has really taken place here, we are going to need to do out a subdomain scanning by using software that has been developed expressly for the purpose of carrying out a work such as this one. After that—and only after that—will we be able to get answers to each and every one of the queries that we now have. After we have finished running knockpy on both domains, the next thing that we do is pay attention to the output to see what type of results it has given us. Following the completion of this stage of the operation, we will now go on to the first stage of the process.



Following completion of the task of enumerating subdomains, we are now in a position to investigate the formatted versions of the subdomains that can be found at https://www.wickr.com/. These versions of the subdomains may be found on the website. This is due to the fact that we have finished enumerating all of the subdomains in the procedure. It should come as no surprise that the IP address and name server used by each and every subdomain that is included inside the https://www.wickr.com/ domain are the same. Because each of the subdomains is a component of the overall domain, this is the situation that exists. Visit the website at https://www.wickr.com/ in order to get the information that you are seeking. This is shown by the exact information in issue being very readily apparent to the naked eye, which is evidence that demonstrates this point. The fact that the program's real hostname is shown lends more credence to the idea that this is a mobile application, which is the conclusion that we have arrived at.

Using Wafw00f tool

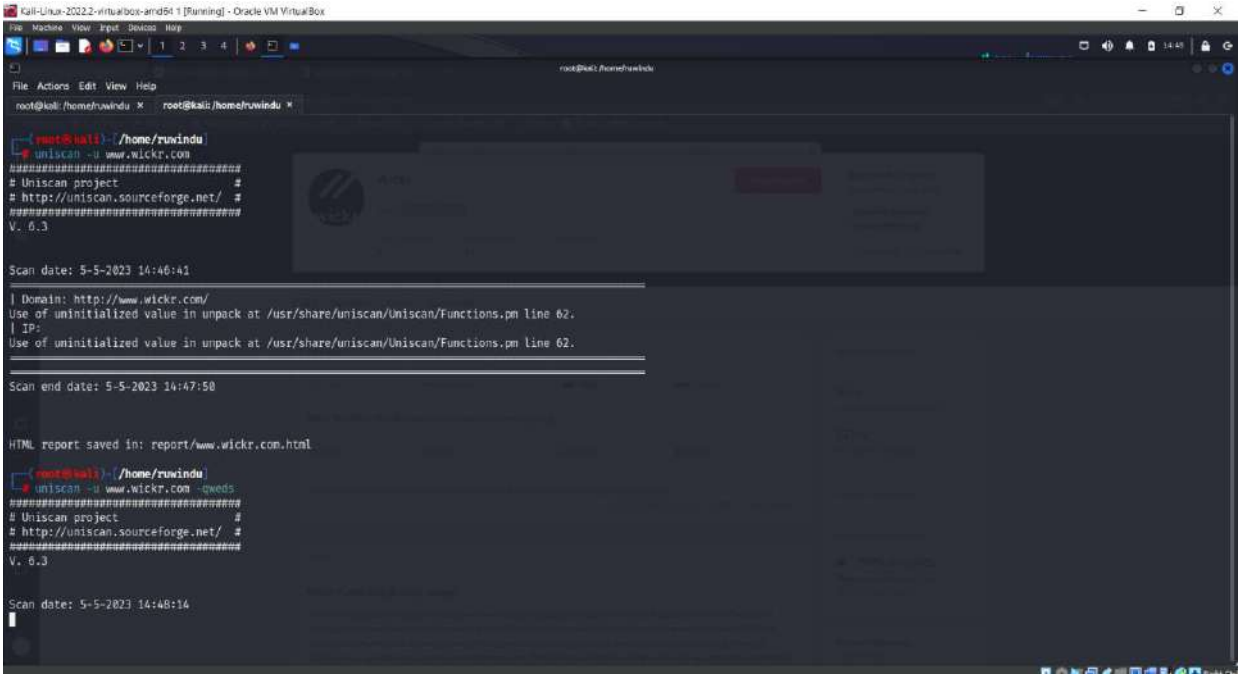
When we run the wafw00f scan with the URL that we are targeting, we are able to see that the website harvestapp.com seems to be protected by a web application firewall (WAF) or some other form of security solution. This is something that we are able to validate via our own direct experience. Because we had completed the scan, we were able to get this information and make the appropriate judgements.



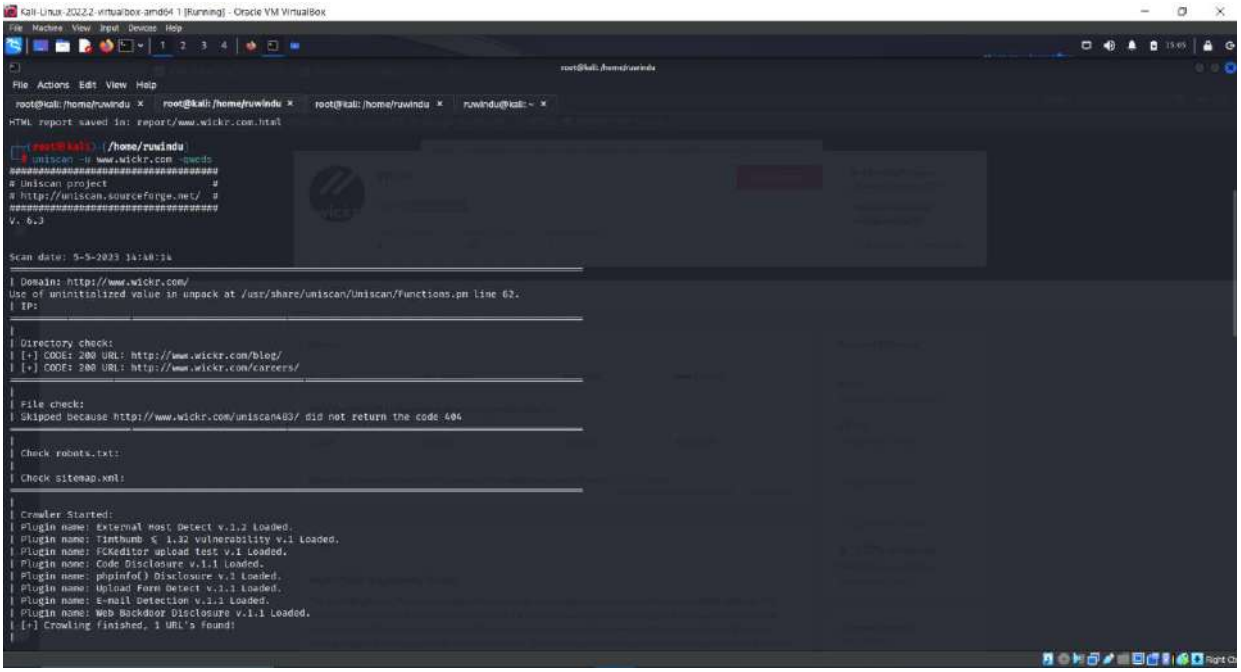
After doing the quick scan, we were able to locate and analyze the robust firewall that was a part of this domain

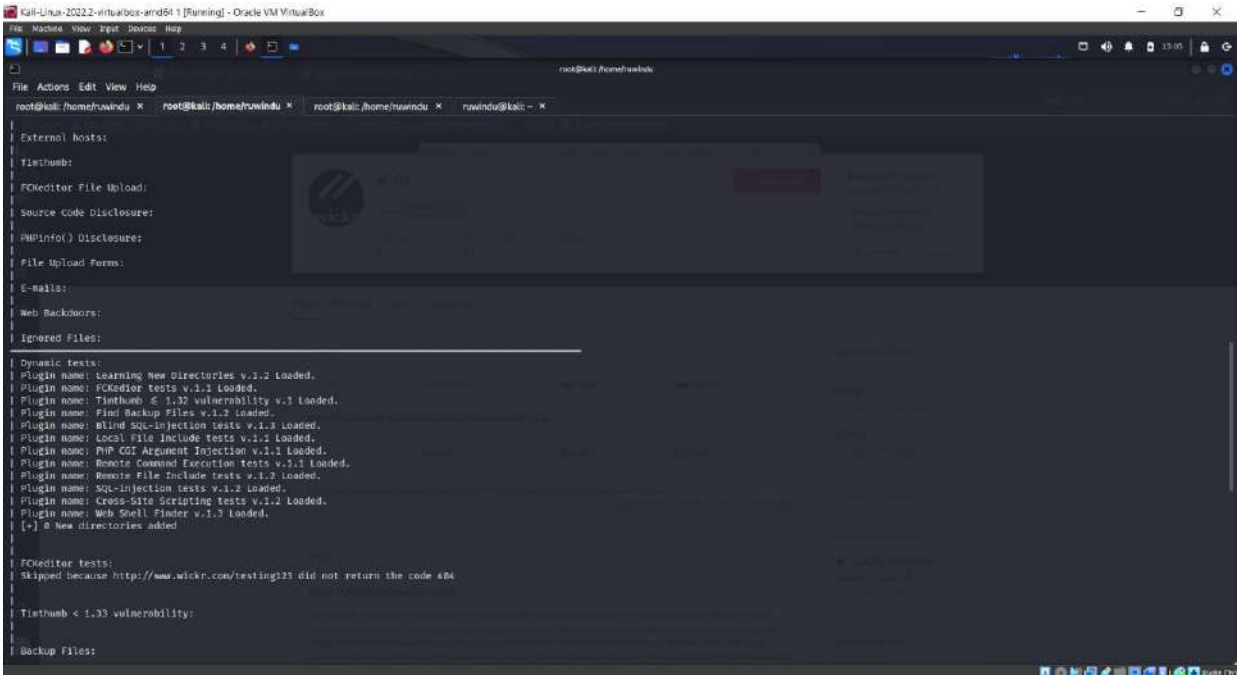
Using Uniscan tool

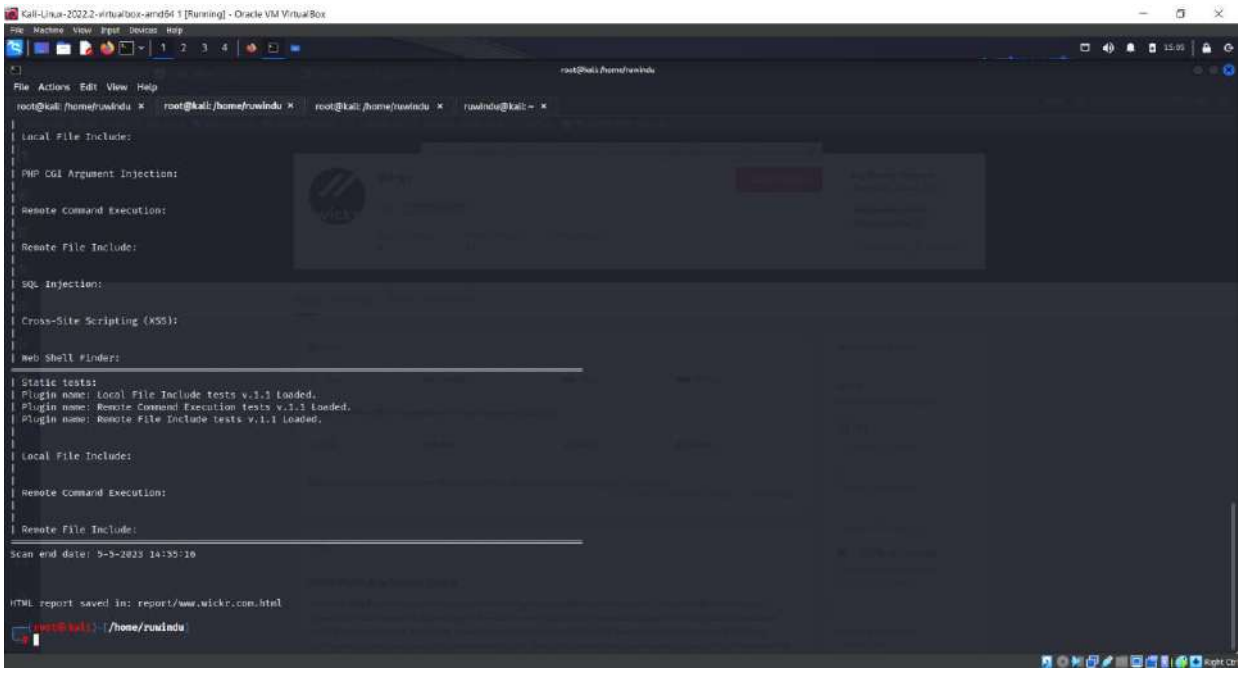
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u www.semrush.com -qweds command:



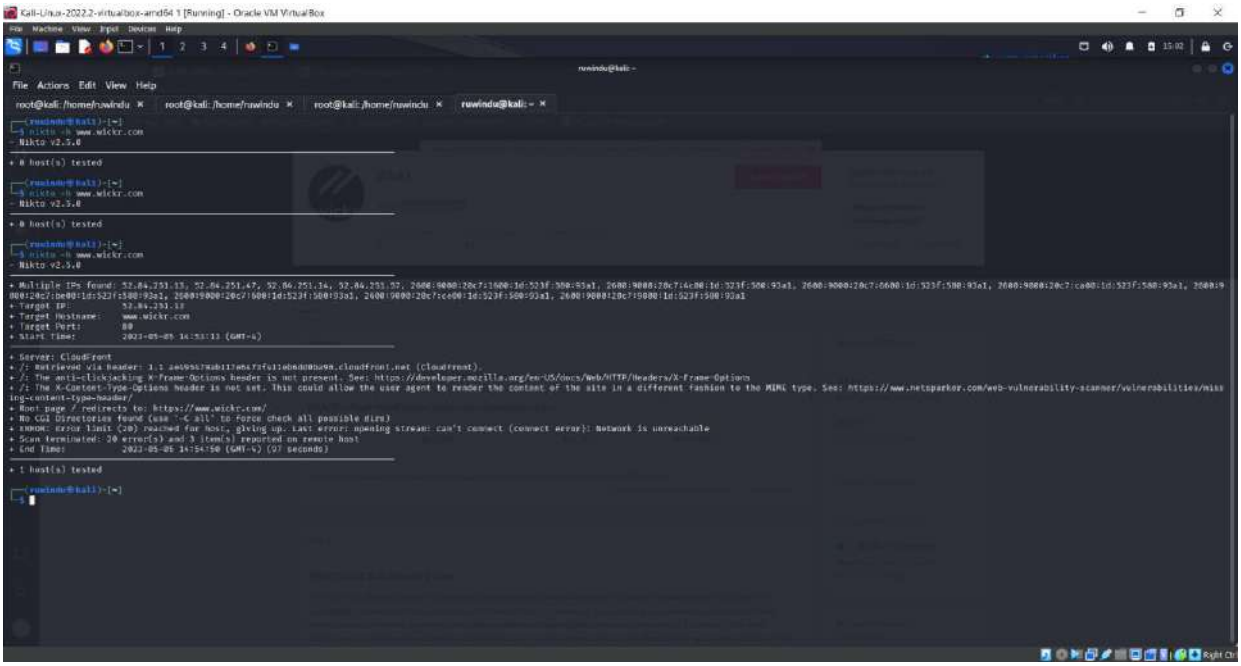




We were able to find some of the information that was housed by third parties by navigating to this region of the website, which is why it is referred to as the third-party sector of the website. In this specific investigation, web addresses, which are also often referred to as URLs, were found.

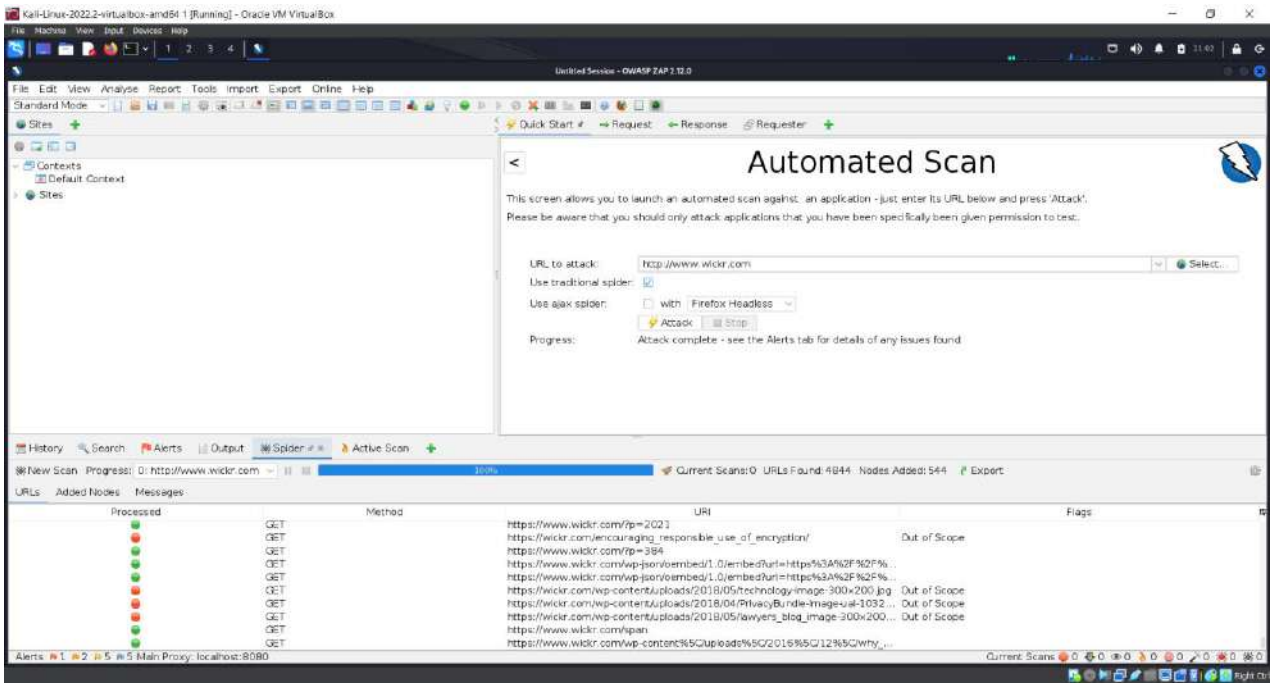
Using Nitko tool

We are provided with a greater number of high-level options and the nikto tool is utilised to cane the target domain when we run the command with the –h switch.

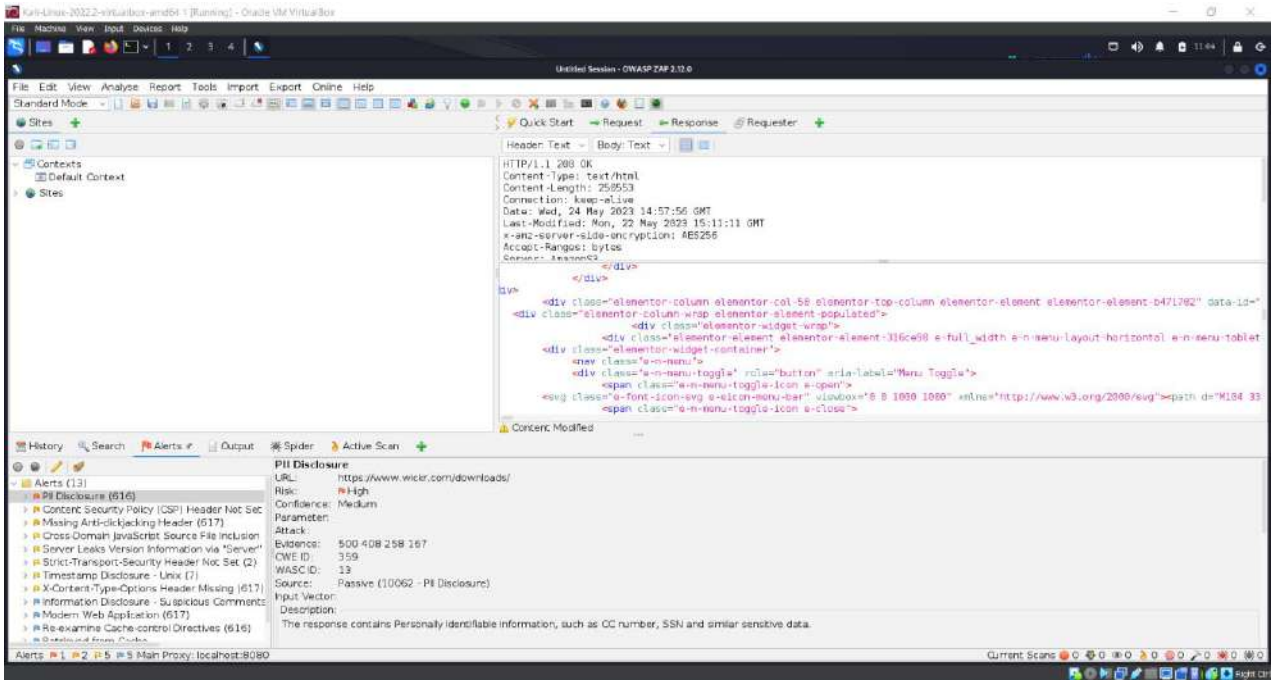


This scanner was not successful in discovering any vulnerabilities inside the system.

Using OWASP-ZAP tool



Found 4844 Requests.

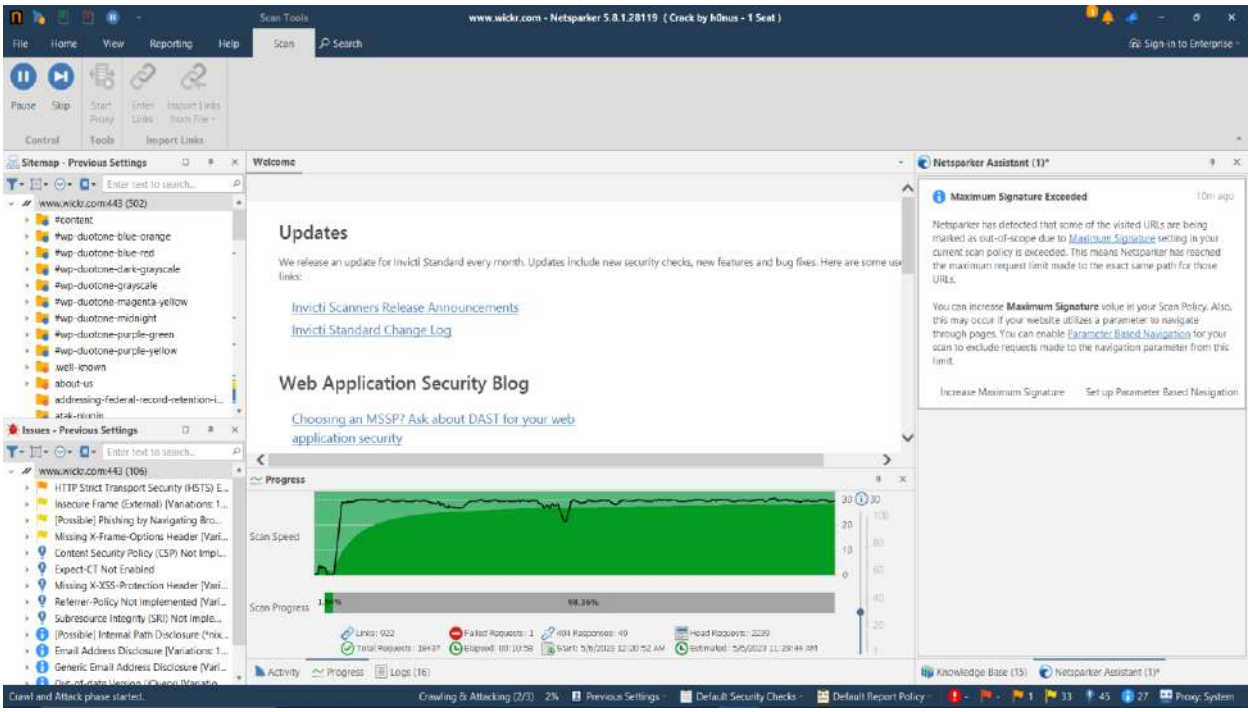


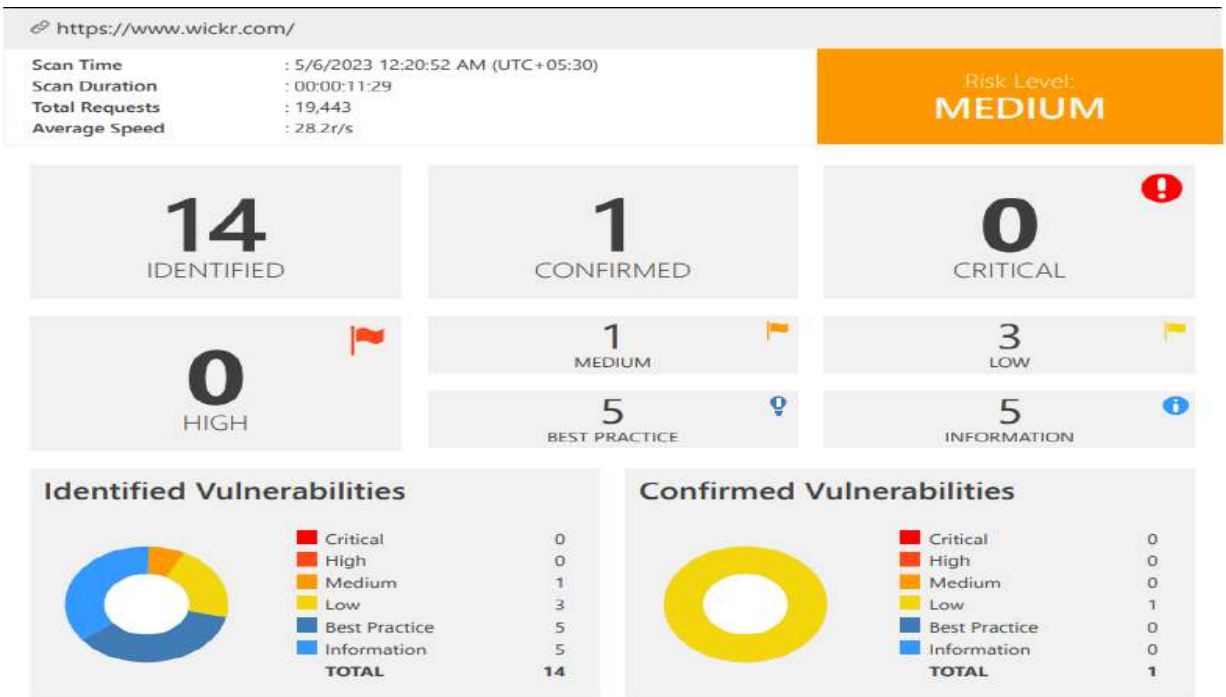
Found 13 Alerts.

Vulnerabilities found

Using Netsparker

In the course of my Audit, I performed a vulnerability check on harvestapp.com with the aid of Netsparker professional Edition (V), which proved to be of great service to me in my endeavor. For the purpose of this specific audit, the website was analyzed.





After doing a scan of the domain, I was able to identify a total of 14 vulnerabilities related to the domain, including vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://www.wickr.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.wickr.com/	
	Missing X-Frame-Options Header	GET	https://www.wickr.com/	
	Insecure Frame (External)	GET	https://www.wickr.com/	
	Content Security Policy (CSP) Not Implemented	GET	https://www.wickr.com/	
	Expect-CT Not Enabled	GET	https://www.wickr.com/	
	Missing X-XSS-Protection Header	GET	https://www.wickr.com/	
	Referrer-Policy Not Implemented	GET	https://www.wickr.com/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.wickr.com/	
	[Possible] Internal Path Disclosure (*nix)	GET	https://www.wickr.com/aws-wickr-a-secure-end-to-end-encrypted-communication-service-for-enterprises-with-auditing-and-regulatory-requirements/	
	Email Address Disclosure	GET	https://www.wickr.com/ram/	
	Generic Email Address Disclosure	GET	https://www.wickr.com/terms/?hTTp://r87.com/n	
	Out-of-date Version (jQuery)	GET	https://www.wickr.com/	
	Sitemap Detected	GET	https://www.wickr.com/sitemap.xml	

https://www.wickr.com/ has been found to have the following identified vulnerabilities:

Identified vulnerabilities in https://www.wickr.com/

Vulnerability 09 - Missing X-Frame-Options Header

This website has been identified by Netsparker as being susceptible to a clickjacking attack since it does not have an X-Frame-Options header. This vulnerability has caused this website to be classified as potentially dangerous.
The X-Frame-Options HTTP header field is used to express a policy that specifies whether the browser should show the transmitted resource inside of a frame or an iframe. This policy determines whether the browser should display the resource inside of a frame or an iframe. Servers have the option of declaring this policy in the header of their HTTP responses. Doing so offers them further defence against clickjacking attacks. This will ensure that their material is not included inside the frames or pages of any other websites.

Impact

An attacker uses multiple transparent or opaque layers to trick a user into hitting a button or link on a framed page instead of the top level page. Thus, the attacker is "hijacking" clicks for their website and forwarding them to another page, maybe controlled by another programme or domain.
Like keystroke hijacking. Stylesheets, iframes, and text boxes may be used to fool users into entering their email or bank account passwords.

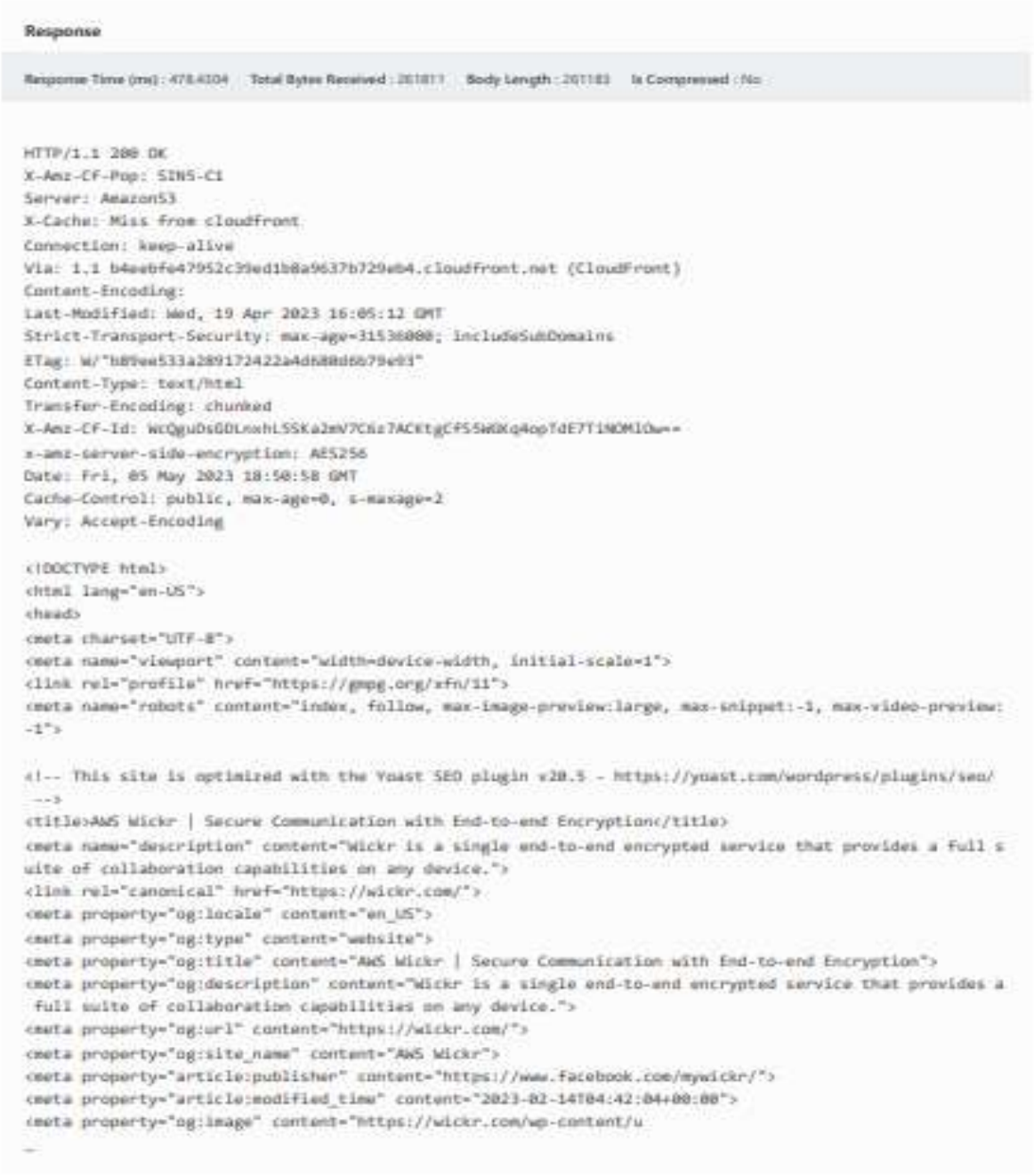
Vulnerabilities

4.1. https://www.wickr.com/

Certainty

Request

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



Response

Response Time (ms) : 478.4104 Total Bytes Received : 261817 Body Length : 261183 Is Compressed : No

```
HTTP/1.1 200 OK
X-Amz-CF-Pop: SIN5-C1
Server: AmazonS3
X-Cache: Miss from cloudfront
Connection: keep-alive
Via: 1.1 b4eebfe47952c39ed1b8a9637b729e04.cloudfront.net (CloudFront)
Content-Encoding:
Last-Modified: Wed, 19 Apr 2023 16:05:12 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: W/"b89ee533a289172422a4d688d6679e03"
Content-Type: text/html
Transfer-Encoding: chunked
X-Amz-CF-Id: WcQguDsGDLnxhLSSKa2mV7C6z7ACEtgCFS5WGXq4opTdE7TiNOMlOw==
x-amz-server-side-encryption: AES256
Date: Fri, 05 May 2023 18:50:58 GMT
Cache-Control: public, max-age=0, s-maxage=2
Vary: Accept-Encoding

<!DOCTYPE html>
<html lang="en-US">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="https://gmpg.org/xfn/11">
<meta name="robots" content="index, follow, max-image-preview:large, max-snippet:-1, max-video-preview:
-1">

<!-- This site is optimized with the Yoast SEO plugin v20.5 - https://yoast.com/wordpress/plugins/seo/
 -->
<title>AWS Wickr | Secure Communication with End-to-end Encryption</title>
<meta name="description" content="Wickr is a single end-to-end encrypted service that provides a full s
uite of collaboration capabilities on any device.">
<link rel="canonical" href="https://wickr.com/">
<meta property="og:locale" content="en_US">
<meta property="og:type" content="website">
<meta property="og:title" content="AWS Wickr | Secure Communication with End-to-end Encryption">
<meta property="og:description" content="Wickr is a single end-to-end encrypted service that provides a
 full suite of collaboration capabilities on any device.">
<meta property="og:url" content="https://wickr.com/">
<meta property="og:site_name" content="AWS Wickr">
<meta property="article:publisher" content="https://www.facebook.com/mywickr/">
<meta property="article:modified_time" content="2023-02-14T04:42:04+00:00">
<meta property="og:image" content="https://wickr.com/wp-content/u
```

Solution

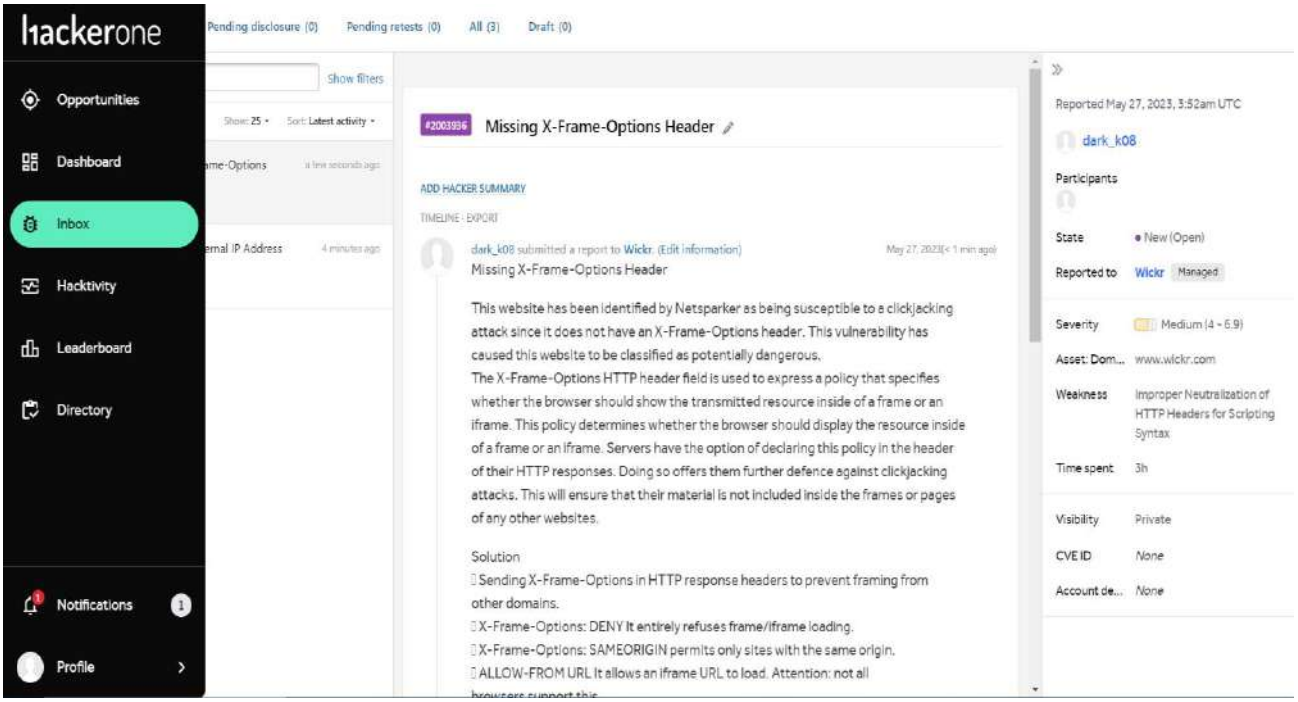
- Sending X-Frame-Options in HTTP response headers to prevent framing from other domains.
- X-Frame-Options: DENY It entirely refuses frame/iframe loading.
- X-Frame-Options: SAMEORIGIN permits only sites with the same origin.
- ALLOW-FROM URL It allows an iframe URL to load. Attention: not all browsers support this.
- Defensive UI code ensures that the current frame is the top-level window.

Conclusion of the Report 09

We began by researching the company's actions and laws. First step. The conversation covered many statistics and figures. We start our bug hunt by gathering environmental data. The hosting company's IP address and the domain's technology are also included. We then migrate all subdomains to the same server and notice that each domain has the same IP address. Sometimes we need many tools to gather more information and verify it. This is necessary to verify our data. Next, we used netcraft to find files and directives to create a diagram of our domain. Thus, similar files and directives exist. Thus, we concluded that specific files or instructions do not exist. It greatly clarified the topic matter.

Next, we assess system flaws. We learned about the domain's vulnerabilities and how to utilise certain tools to find them at the moment. We also learned about domain vulnerabilities. After that, we use other websites to analyse the vulnerability to better understand the issue with this online application. After identifying vulnerabilities, we tried to prove one had a potentially dangerous concern. We proved it was dangerous. Although we had determined that the vulnerability was not serious, we were given a lot of fascinating information. Despite our previous assessment that the vulnerability was minor.

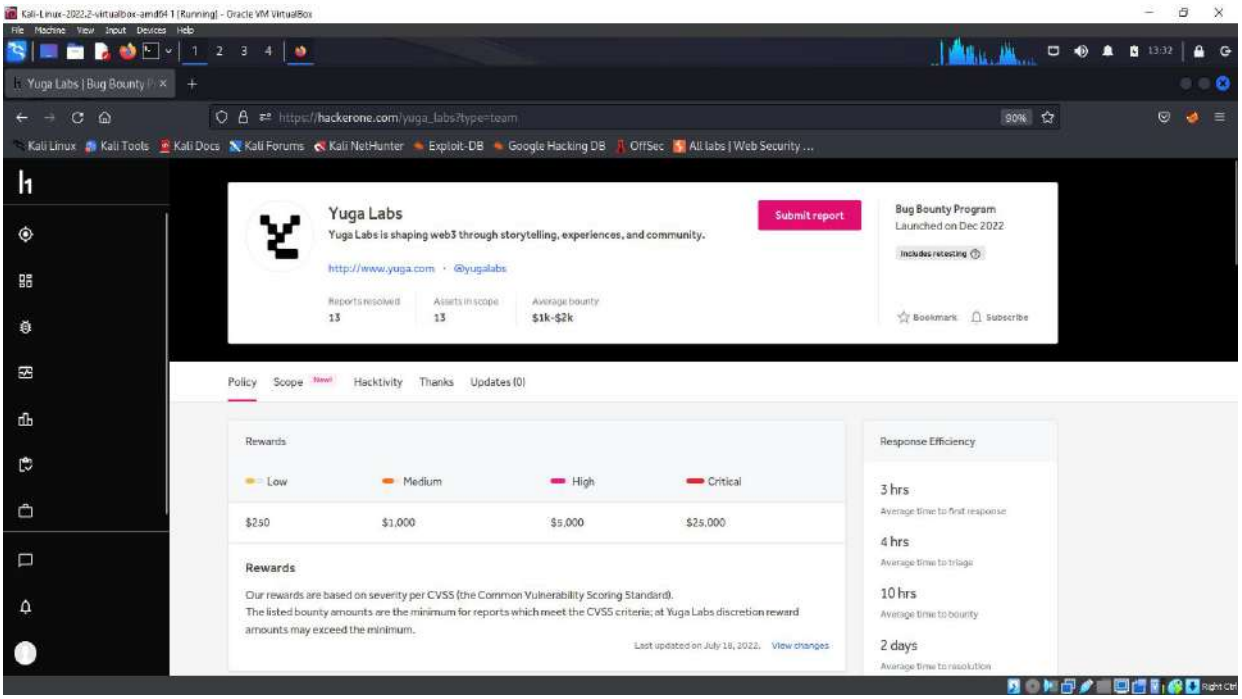
HackerOne Submitted Report Screenshot



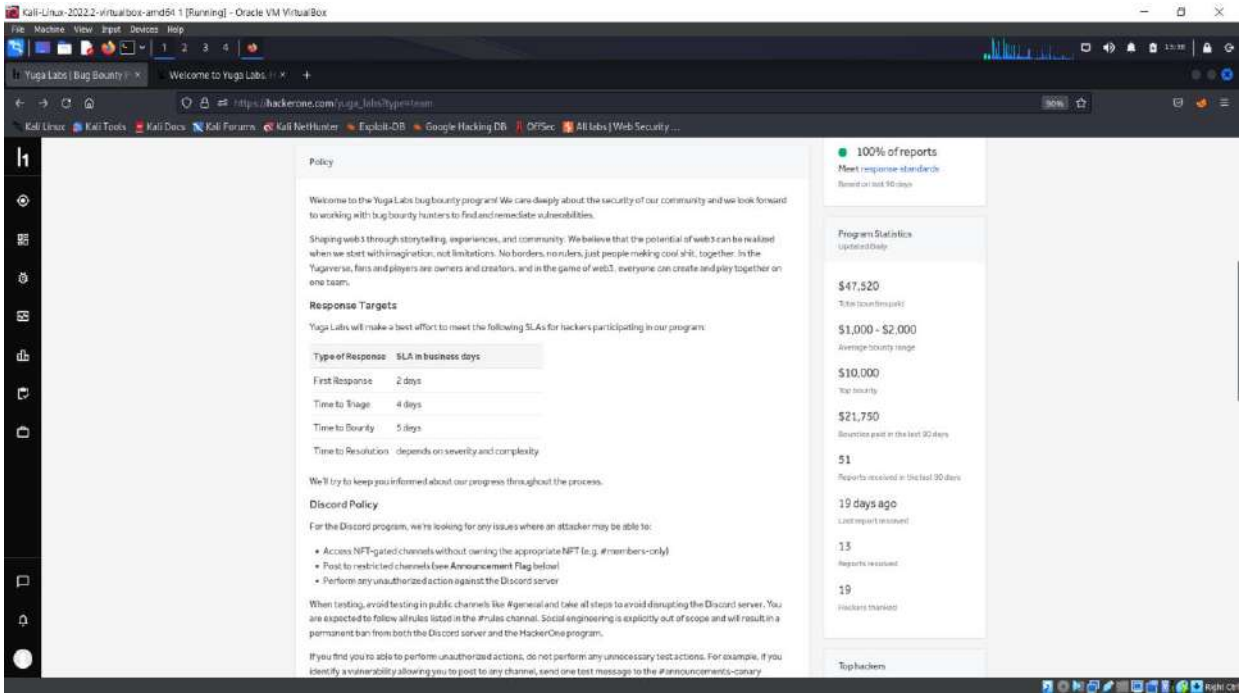
x. Report 10

Target information: https://www.yuga.com/

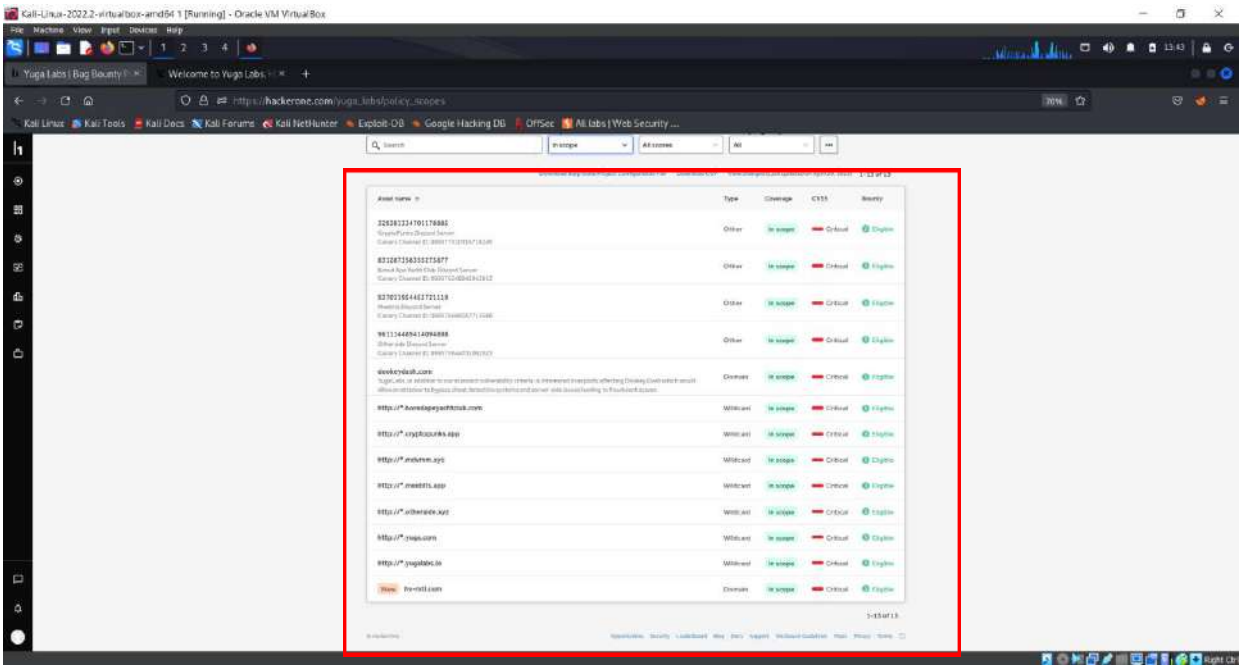
This evaluation aims to establish the risk associated with the target domain's (https://www.yuga.com/) possible vulnerabilities. The study also identifies target domain vulnerabilities. By identifying target domain vulnerabilities, we can attain these goals. To put it another way, this evaluation seeks to determine the risk associated with both the target domain and its potential sources of vulnerability. The current examination seeks to identify issues related to the current topic.



We place a high priority on the safety of our community, and we are excited to collaborate with bug bounty hunters to identify and address any vulnerabilities that may be discovered.
Storytelling, experience sharing, and community involvement are being used to shape web3. We are of the opinion that the potential of web3 can be achieved if, rather than beginning with limits, we begin with our ideas. People working together to create awesome things, with no borders and no leaders in the way. In the fans and players are the owners and creators of content, and in the game of web3, everyone can create together on the same team while still competing against each other.

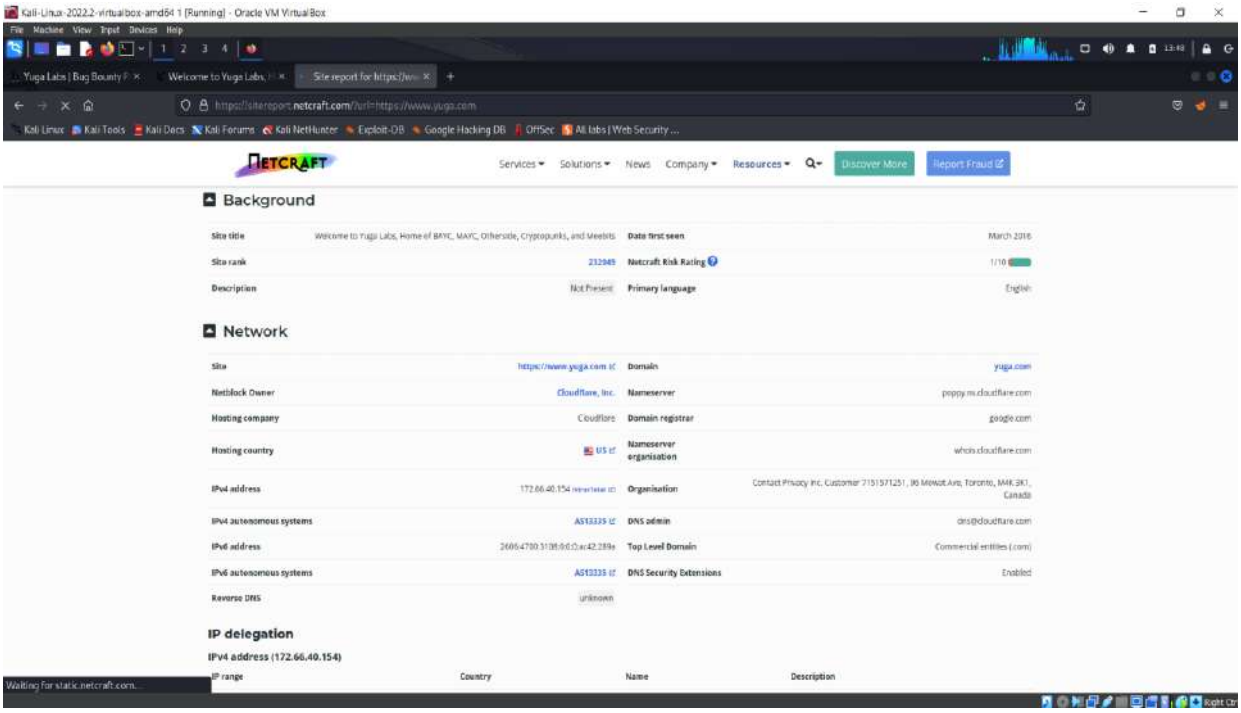


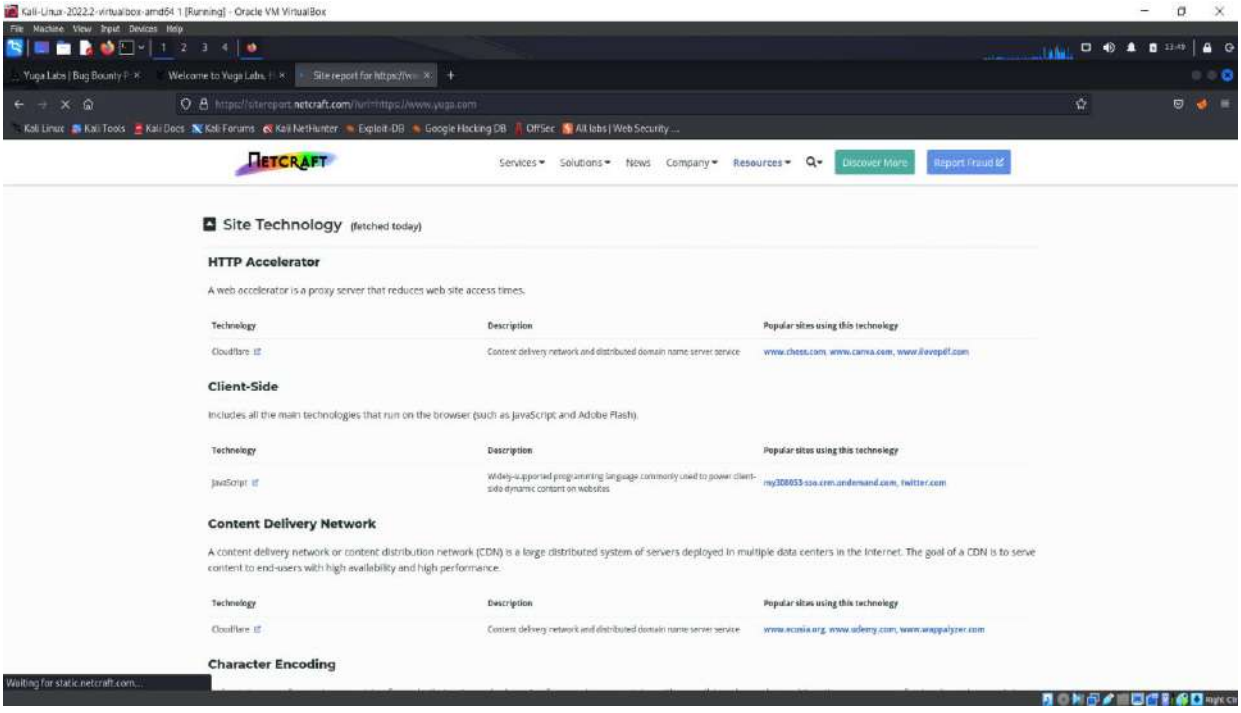
Then, before they move on to the next step, they will talk about any possible weaknesses that aren't part of the project. Before they move on to the next step, this will happen. Because of how these security holes work, we can't try to find a bug or include the results of our searches in our report. This means that we can't include the results of any such work. Since this is the case, we can't use their data in our study. Because of this, we can't use their results in the same way in our own report as they did. Also, we are not allowed to use any of their results or conclusions in any way in our report. Because of the list that was just shown, we have a duty to look into it and figure out what kind of mistake it is that shouldn't be there. It's really important that we act in the ways that were outlined above.



Information Gathering For Target Domain

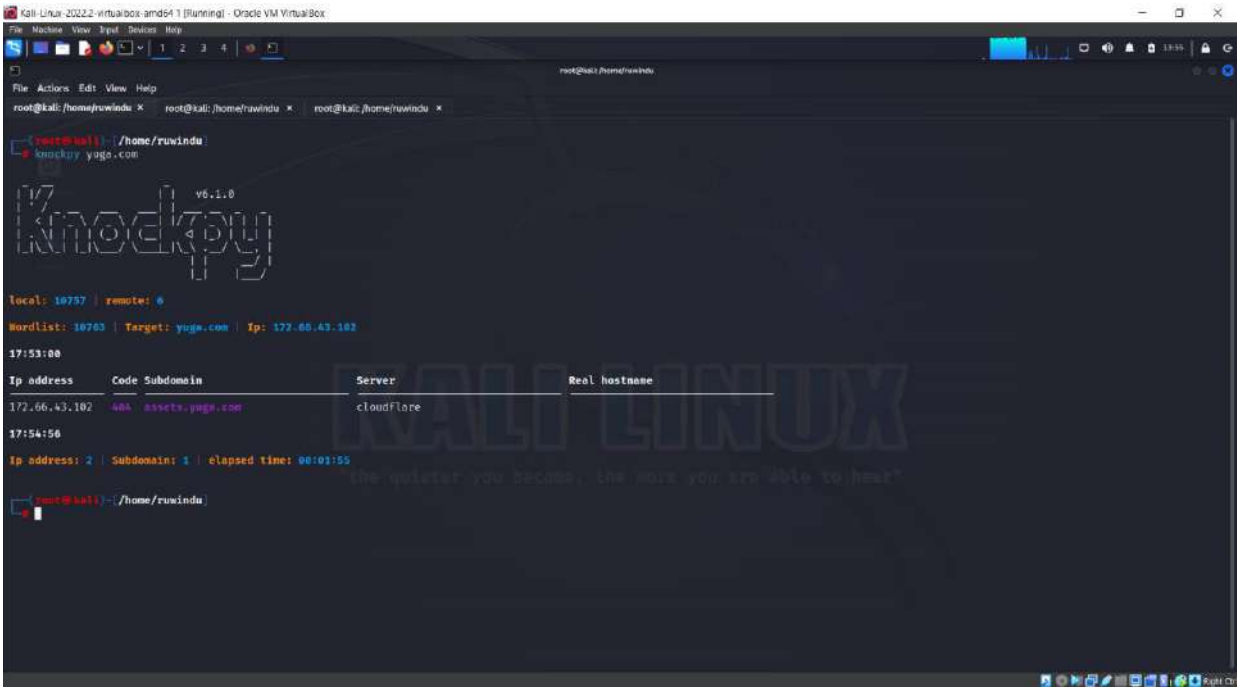
Let's have a look at the many options we have for gathering not just information about the technical capacities of https://www.yuga.com/, but also other crucial details. Many other options exist for how we may go about completing this assignment. Getting this done might be done in a number of ways, and we have access to them all. Since Netcraft is the only resource we have at the moment, let's go ahead and punch in our domain name and see what kind of information we can get by doing so. First, we'll type in our domain name and then investigate further with the help of the exclusive data provided by Netcraft. Since Netcraft is our only option at the moment, let's look into our network to see what kind of data we can get from it. If we do this, we can maximise the effectiveness of our time together. For the time being, Netcraft is the only tool we have, so let's take a look at what we can learn from it. This will help us stretch our limited funds farther. Since Netcraft is the only resource we currently have at our disposal, let's have a look at the data we can get with its help. Since Netcraft is all we have for the time being, let's have a look at what kind of data we can glean from it. Several applications and websites exist that are capable of doing this function; however, we will only be using Netcraft.


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Background
Site title
Site rank
Description
Date first seen
Netcraft Risk Rating
Primary language
Network
Site
Netblock Owner
Hosting company
Hosting country
IPv4 address
IPv4 autonomous systems
IPv6 address
IPv6 autonomous systems
Reverse DNS
Domain
Nameserver
Domain registrar
Nameserver organisation
Organisation
DNS admin
Top Level Domain
DNS Security Extensions
IP delegation
IPv4 address (172.66.40.154)
IP range
Country
Name
Description
Waiting for static.netcraft.com...


Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
NETCRAFT
Services
Solutions
News
Company
Resources
Discover More
Report Fraud
Site Technology (fetched today)
HTTP Accelerator
A web accelerator is a proxy server that reduces web site access times.
Technology
Description
Popular sites using this technology
Cloudflare
Client-Side
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).
JavaScript
Content Delivery Network
A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.
Character Encoding
Waiting for static.netcraft.com...

Using knockpy tool

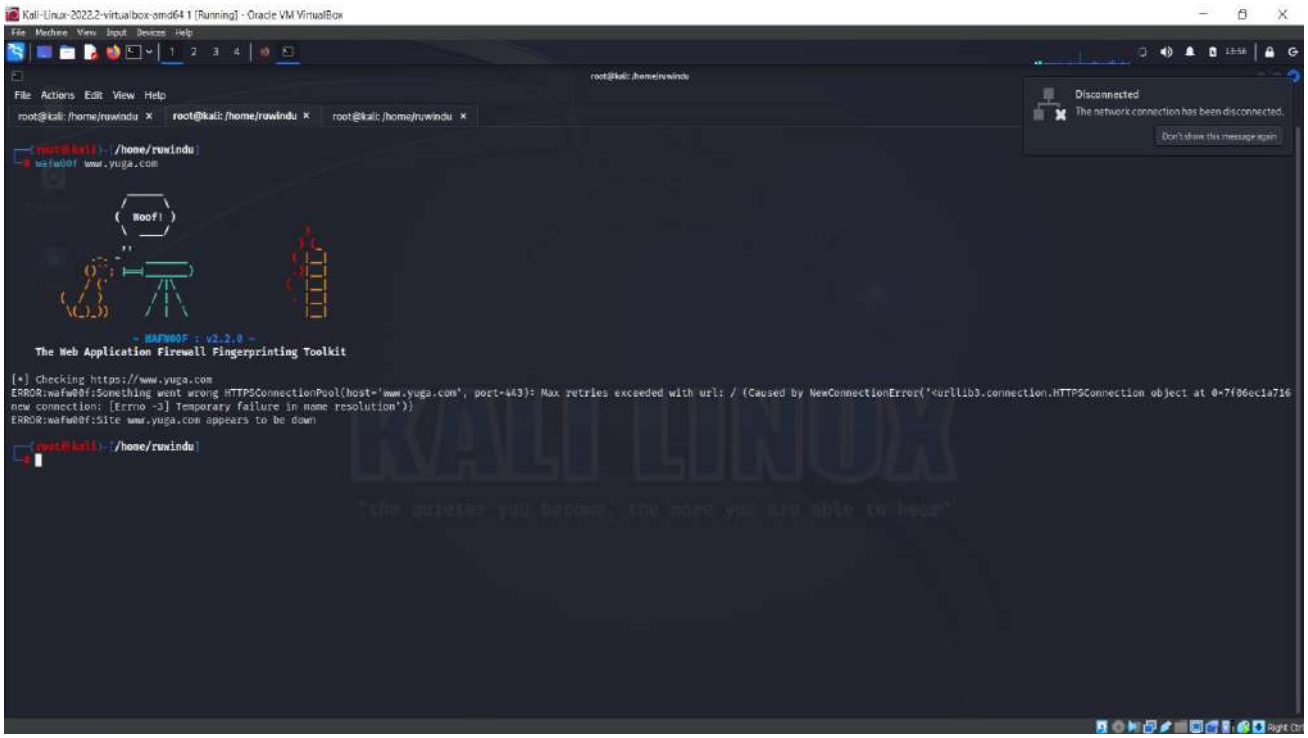
To find out what really happened here, we will need to do a subdomain scan using software that was made just for this kind of job. After that, and only then, will we be able to get answers to all of the questions we have now. After we're done running knockpy on both domains, we look at the data to see what kind of results it gave us. After this part of the action is done, we will move on to the first part of the process.



After finishing the process of enumerating subdomains, we are now in a position to explore the formatted versions of the subdomains that may be located at www.yuga.com. This is because we have finished the task of enumerating subdomains. These several iterations of the subdomains can be discovered on the website. This is because we have finished enumerating all of the procedure's subdomains, which is the reason for this result. It shouldn't come as a surprise to learn that the IP address and name server utilized by each and every subdomain that is contained inside the www.yuga.com domain are the same. Both of these resources are shared among the subdomains. This is the circumstance that prevails as a direct result of the fact that each of the subdomains is a part of the overall domain. You can find the information that you are looking for by going to the website that is located at www.yuga.com. This is demonstrated by the fact that the specific information at issue can be easily observed by a person using only their naked sight, which is proof that confirms this argument. This is a mobile application, which is the conclusion that we have reached, and the fact that the program's actual hostname is displayed lends more validity to the concept that it is a mobile application.

Using Wafw00f tool

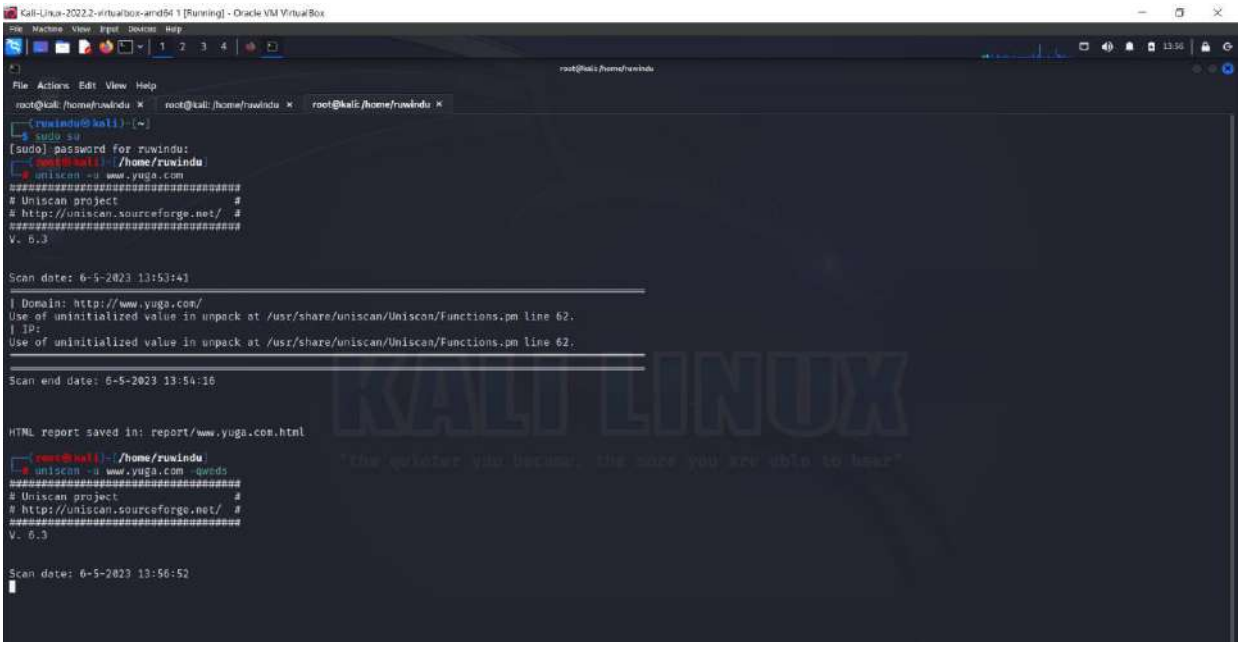
When we run the wafw00f scan with the URL that we are targeting, we are able to see that the website harvestapp.com seems to be protected by a web application firewall (WAF) or some other form of security solution. This is something that we are able to validate via our own direct experience. Because we had completed the scan, we were able to get this information and make the appropriate judgements.



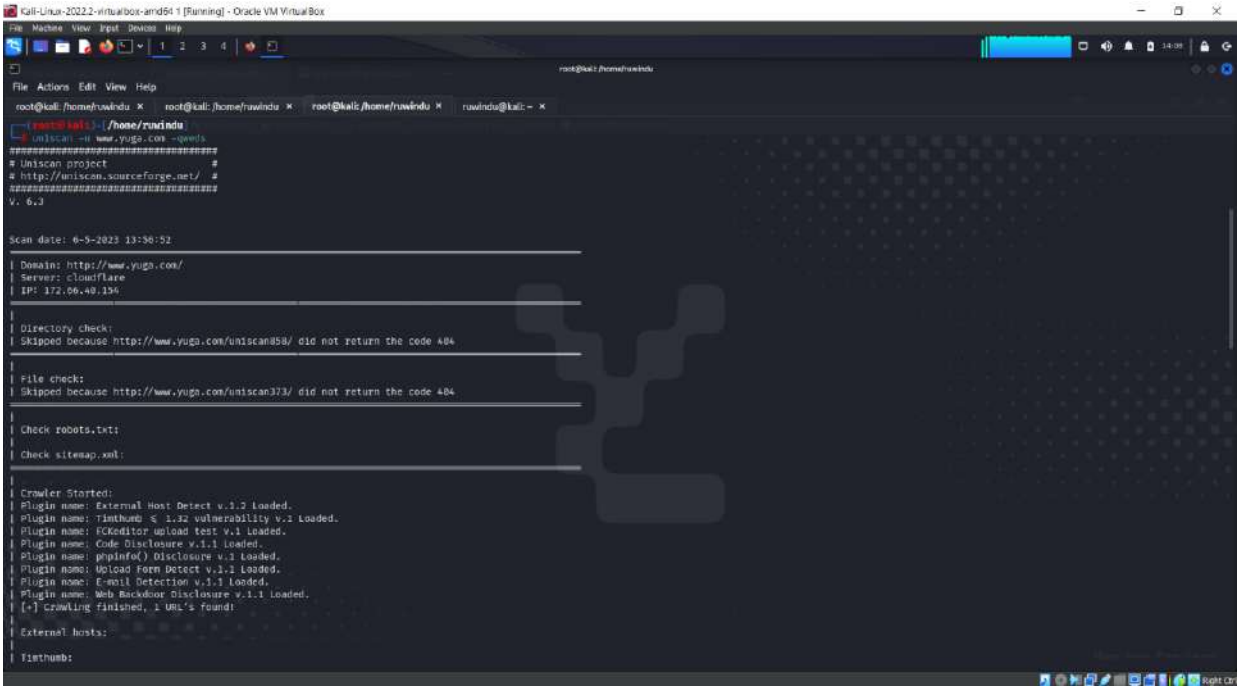
After doing the quick scan, we were able to locate and analyze the robust firewall that was a part of this domain

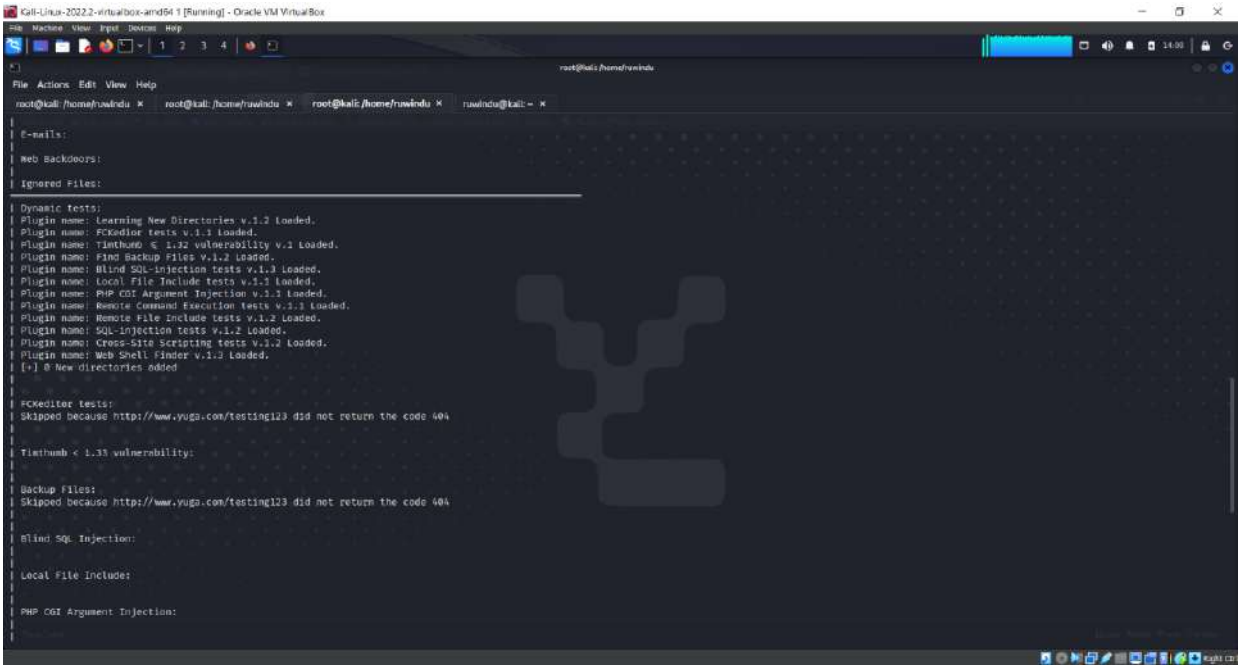
Using Uniscan tool

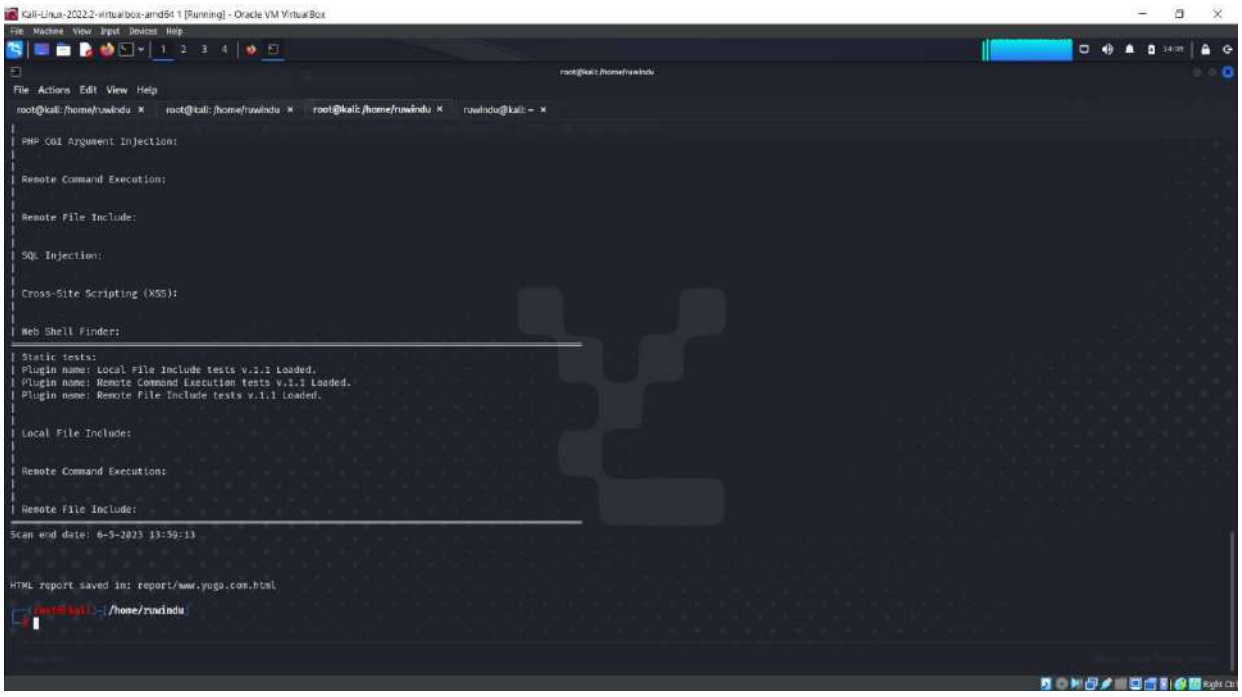
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



Following the execution of the uniscan –u www.semrush.com -qweds command:



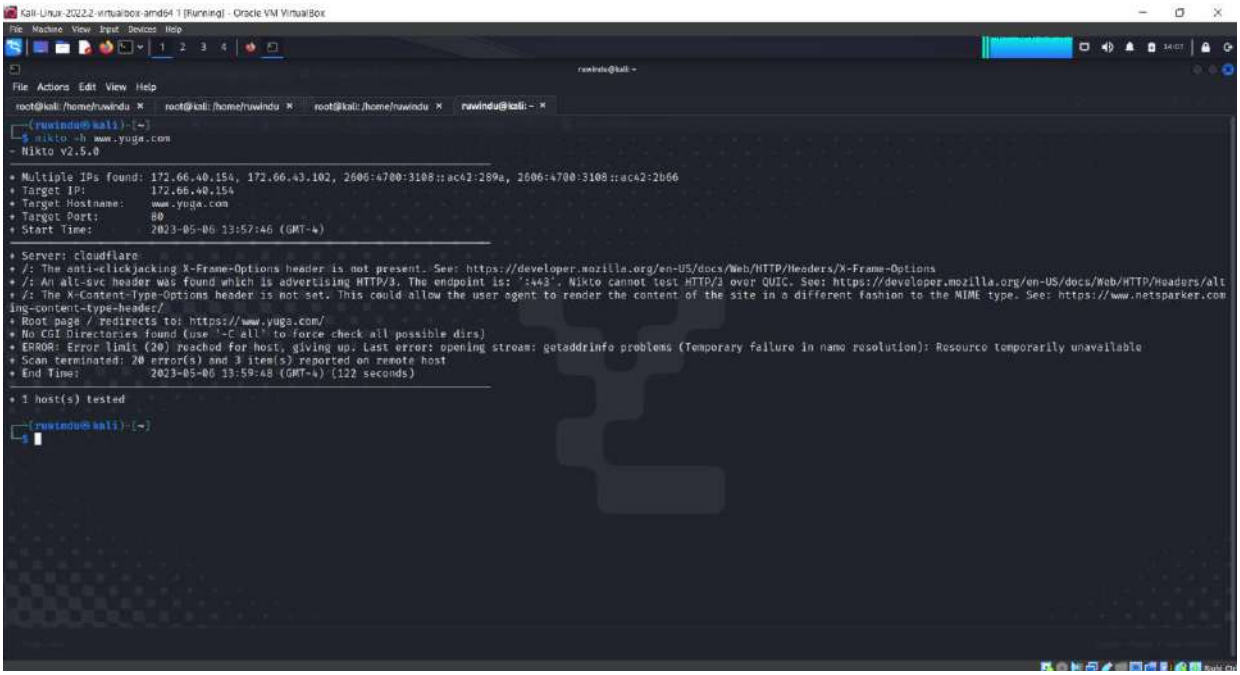




We were able to find some of the information that was housed by third parties by navigating to this region of the website, which is why it is referred to as the third-party sector of the website. In this specific investigation, web addresses, which are also often referred to as URLs, were found.

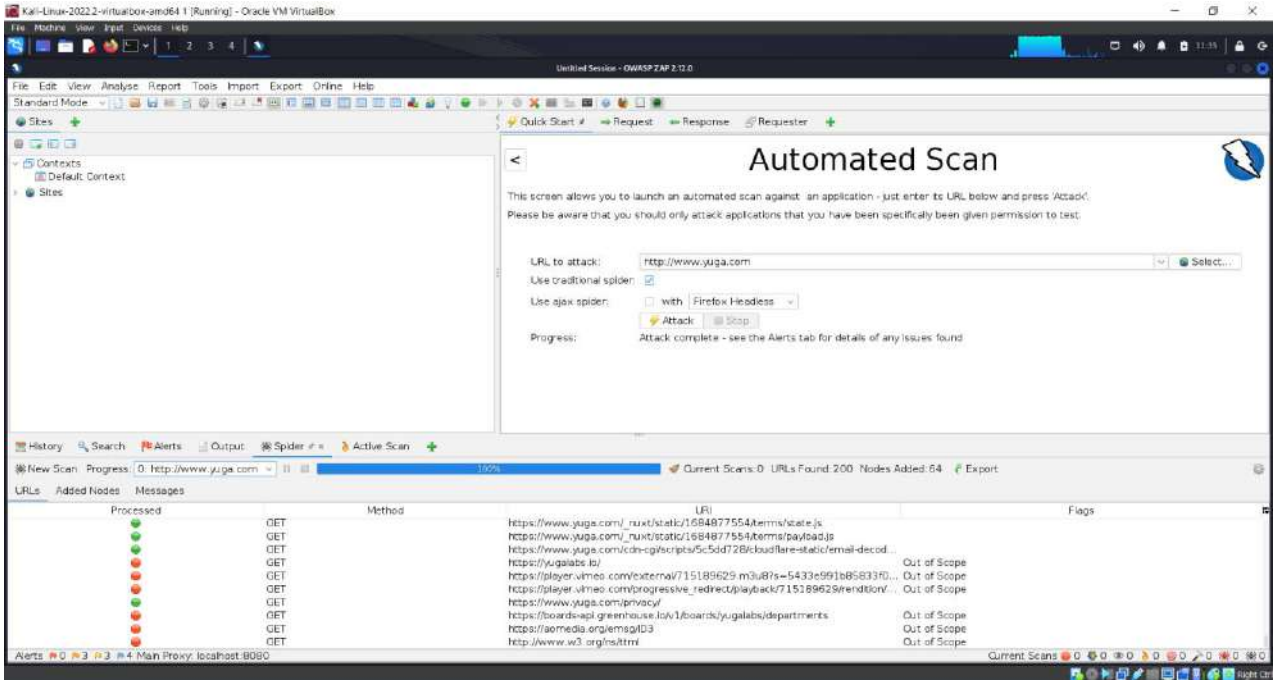
Using Nitko tool

We are provided with a greater number of high-level options and the nikto tool is utilised to cane the target domain when we run the command with the –h switch.

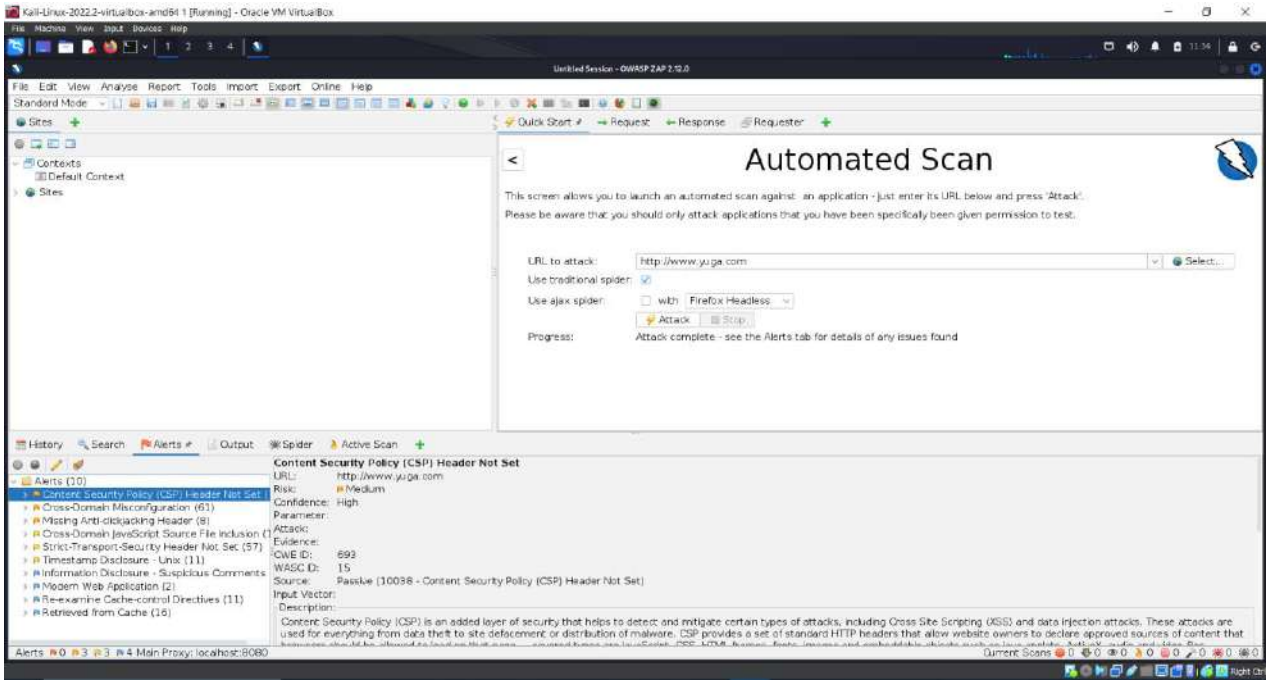


This scanner was not successful in discovering any vulnerabilities inside the system.

Using OWASP-ZAP tool



Found 200 Requests.

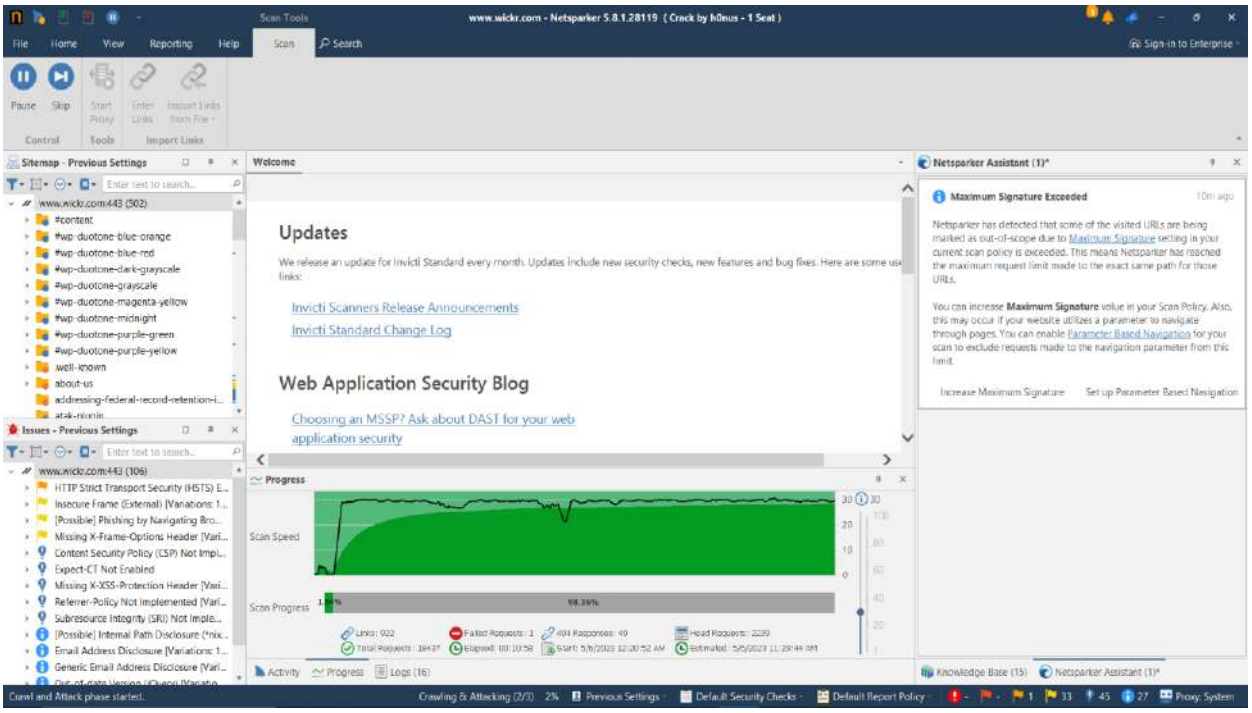


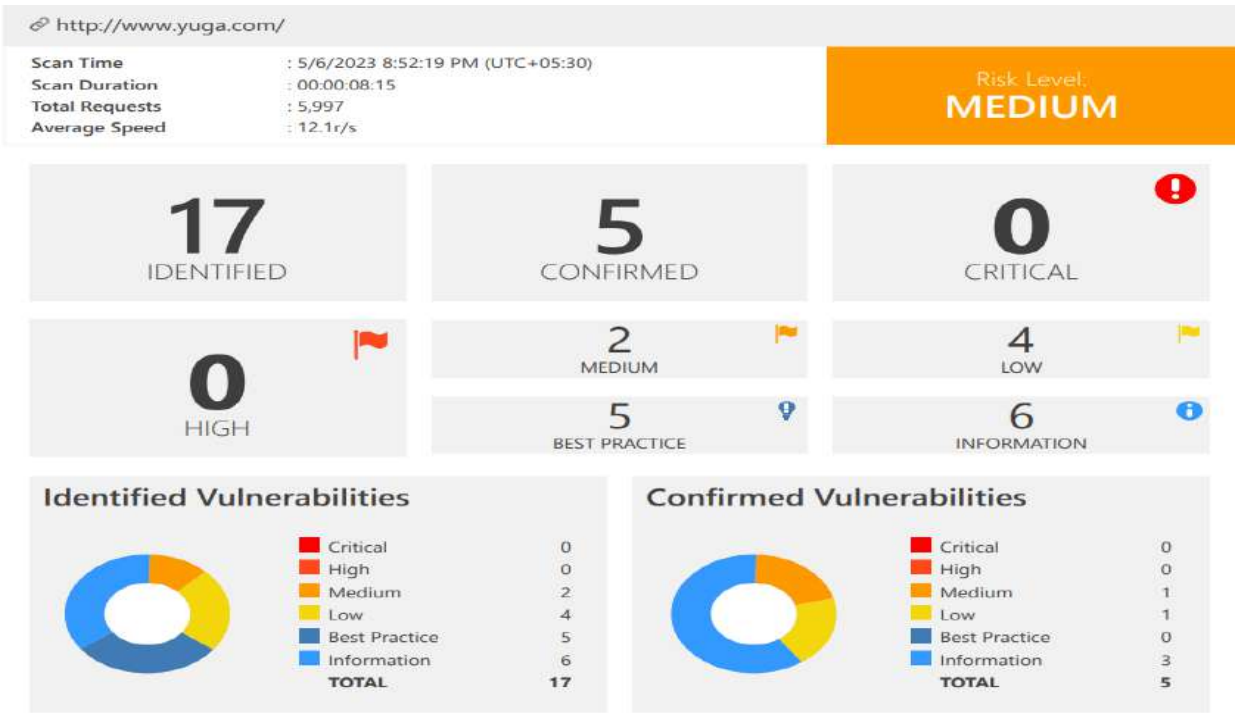
Found 10 Alerts.

Vulnerabilities found

Using Netsparker

In the course of my Audit, I performed a vulnerability check on harvestapp.com with the aid of Netsparker professional Edition (V), which proved to be of great service to me in my endeavor. For the purpose of this specific audit, the website was analyzed.





After doing a scan of the domain, I was able to identify a total of 17 vulnerabilities related to the domain, including vulnerabilities with a medium risk.

Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://www.yuga.com/	
	Weak Ciphers Enabled	GET	https://www.yuga.com/	
	[Possible] Phishing by Navigating Browser Tabs	GET	https://www.yuga.com/links/	
	Misconfigured Access-Control-Allow-Origin Header	GET	https://www.yuga.com/_nuxt/	
	Missing X-Frame-Options Header	GET	https://www.yuga.com/opensearch.xml	
	Insecure Frame (External)	GET	https://www.yuga.com/opensearch.xml	
	Content Security Policy (CSP) Not Implemented	GET	https://www.yuga.com/cdn-cgi/styles/	
	Expect-CT Not Enabled	GET	https://www.yuga.com/about	
	Missing X-XSS-Protection Header	GET	https://www.yuga.com/_nuxt/css/7a3f40f.css	
	Referrer-Policy Not Implemented	GET	https://www.yuga.com/cdn-cgi/styles/	
	Subresource Integrity (SRI) Not Implemented	GET	https://www.yuga.com/	
	Email Address Disclosure	GET	https://www.yuga.com/_nuxt/448f8f4.js	
	Generic Email Address Disclosure	GET	https://www.yuga.com/_nuxt/7db28fe.js	
	Sitemap Detected	GET	https://www.yuga.com/sitemap.xml	
	Cross-site Referrer Leakage through Referrer-Policy	GET	https://www.yuga.com/opensearch.xml	
	Forbidden Resource	GET	https://www.yuga.com/?%27%22--%3e%3c%2fstyle%3e%3c%2fscRipt%3e%3cscRipt%2Dsrc%3df%22%2f%2fiyeeyl.szhgib2zgzi1bnuuhyynjcuvkguz.z8ebq3m%26%2346%3bri87%26%2346%3bme%22%3e%3c%2fscRipt%3e	
	Robots.txt Detected	GET	https://www.yuga.com/robots.txt	

http://www.yuga.com has been found to have the following identified vulnerabilities:

Identified vulnerabilities in http://www.yuga.com

Vulnerability 10 - Misconfigured Access-Control-Allow-Origin Header

The resource's HTTP response contained a possible incorrectly configured Access-Control-Allow-Origin header, as discovered by Netsparker.

Cross-origin resource sharing, sometimes known as CORS, is a method that, when used in conjunction with XML Http Request, enables resources on a web page to be requested from locations outside of the domain.

The same-origin security policy requires that web browsers prohibit "cross-domain" queries of this nature unless the specified HTTP header is present in the request.

Impact

This is typically not deemed to be appropriate when putting into practice a security policy that is based on the same origin. When it comes to the implementation of the same-origin policy, the only time this should be done is when a website or API response is regarded to contain only information that is open to the general public and is meant to be made accessible to all users. In other words, the only time this should be done is when a website or API answer is deemed to be completely trustworthy.

Response

Response Time (ms) : 587.5664 Total Bytes Received : 5920 Body Length : 5134 Is Compressed : No

```
HTTP/1.1 404 Not Found
x-content-type-options: nosniff
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400
CF-Cache-Status: DYNAMIC
referrer-policy: strict-origin-when-cross-origin
Server: cloudflare
Connection: keep-alive
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=fa6%2Fvn0fBZecWZAnt1KMaGQ
x6lfefZxjbBN7BbNrkheIWenRilUtWIMCn5VPk5hqOW79BCtILrhC%2BNymmY1NbW5kd1kqC%2FefTKzv4bDJOuG92YpkC%2BX91e1v
212D6HE%2BcVINTKIMIrb%2FOvA%3D"}],"group":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Access-Control-Allow-Origin: *
CF-RAY: 7c323822aab90bad-AMS
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Sat, 06 May 2023 15:22:32 GMT

…
qOW79BCtILrhC%2BNymmY1NbW5kd1kqC%2FefTKzv4bDJOuG92YpkC%2BX91e1v212D6HE%2BcVINTKIMIrb%2FOvA%3D"}],"grou
p":"cf-nel","max_age":604800}
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Access-Control-Allow-Origin: *
CF-RAY: 7c323822aab90bad-AMS
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Content-Encoding:
Date: Sat, 06 May 2023 15:22:32 GMT
Vary: Accept-Encoding

<!doctype html>
<h
…
```

Solution

If it is the intention of this page that everyone should be able to access it, then you do not need to take any action. If that is not the case, please follow the instructions for the various architectures listed below in order to set this header and allow access from outside domains.

- If it is the intention of this page that everyone should be able to access it, then you do not need to take any action. If that is not the case, please follow the instructions for the various architectures listed below in order to set this header and allow access from outside domains.

```
Header set Access-Control-Allow-Origin "domain"
```

IIS6

1. Open Internet Information Service (IIS) Manager
2. Right click the site you want to enable CORS for and go to Properties
3. Change to the HTTP Headers tab
4. In the Custom HTTP headers section, click Add
5. Enter Access-Control-Allow-Origin as the header name
6. Enter domainas the header value

IIS7

- Merge the following xml into the web.config file at the root of your application or site:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <system.webserver>
    <httpprotocol>
      <customheaders>
        <add name="Access-Control-Allow-Origin" value="domain" />
      </customheaders>
    </httpprotocol>
  </system.webserver>
</configuration>
```

ASP.NET

- If you don't have access to configure IIS, you can still add the header through ASP.NET by adding the following line to your source pages:

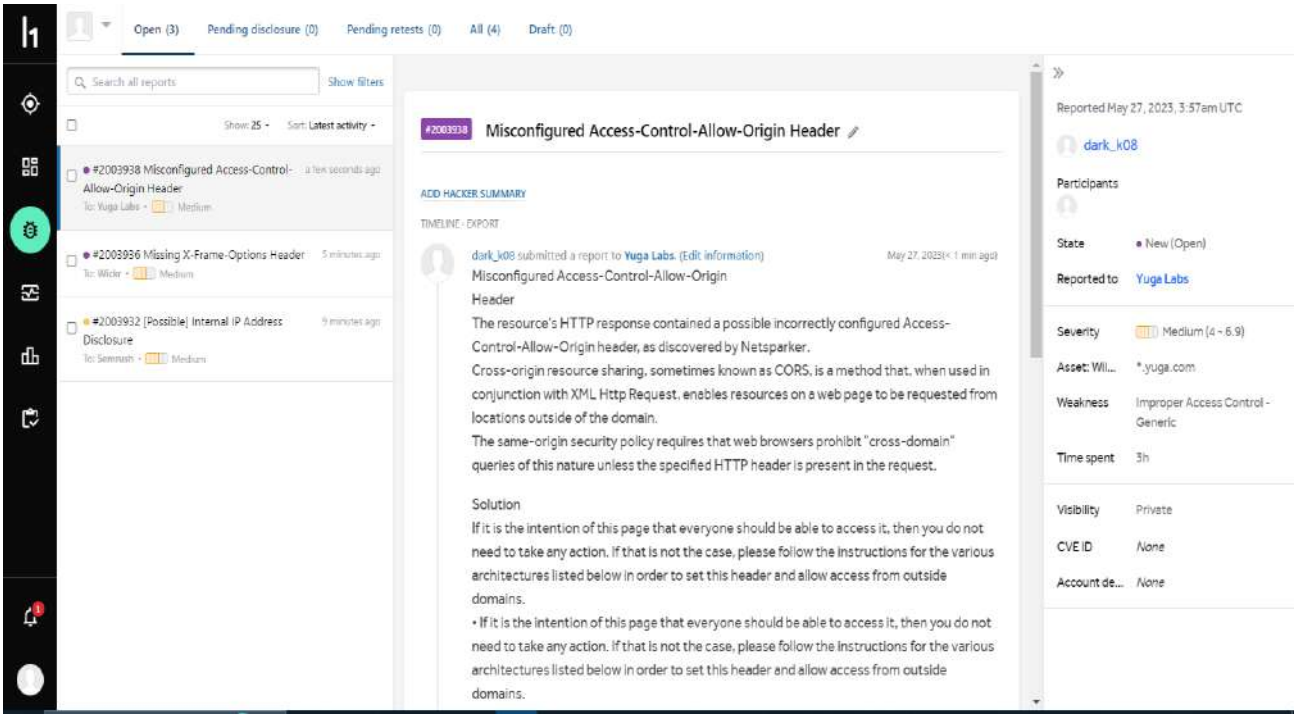
```
Response.AppendHeader("Access-Control-Allow-Origin", "domain");
```

Conclusion of the Report 10

We started with corporate history. This involved examining the company's operations and regulations. We started here. The presentation covered several topics. Before searching for bugs, we learn about our location. These include the name's technology and host's IP address. We migrate all subdomains to one machine. We discover each name uses the same IP address. Sometimes we need many tools to learn more and verify our knowledge. This is necessary to verify our data. After that, we used netcraft to check our domain diagram for files and instructions. We assumed such files and directives existed. We discovered that several files and directions don't exist. It altered the subject's overall clarity.

Next, identify system issues. We learned about the domain's weaknesses and how to utilise tools to detect them right then. Name issues were also discussed. We then utilise other websites to diagnose this online application's issue. After identifying the flaws, we tested one to prove it might damage. We proved it was unsafe. We were taught many intriguing things regarding the situation, even though we knew it wasn't a major matter. Despite our agreement, something transpired.

HackerOne Submitted Report Screenshot



Conclusion

We choose a HackerOne bug bounty programme to analyze for this report. The first discussion focused on the bug bounty programme itself, as well as its specifics (such as its rules and standards). From the list of available in-scope domains, we selected one and started our research. We collected data in various different areas, including technologies, subdomains, and files and folders. Next, we conducted a vulnerability assessment and learned that we can get a single alert of medium severity. The other notifications were all of low severity, so we went with the middle of the road option. In light of this, we discussed the meaning of vulnerability and its historical context.

In order to evaluate the safety of the online system, audit reports are crucial. A number of problems were identified by this investigation that need fixing immediately. The severity of the problems identified should determine the order in which the necessary fixes are implemented. This research makes use of the OWASP Top Ten list of common security flaws. Both human analysts and automatic systems were used in the threat detection process. I learned about potential problems and how to fix them by perusing the OWASP website and other popular resources including books and automated tools like Netsparker. There are references listed after each vulnerability explanation. All of the data obtained by the different instruments was combined and analyzed to produce an audit report.

References

[1] [Online]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain.

[2] [Online]. Available: https://www.techtarget.com/searchcio/feature/Top-9-blockchain-platforms-to-consider.

[3] [Online]. Available: https://www.simplilearn.com/blockchain-programming-languages-article.

[4] [Online]. Available: https://pixelplex.io/blog/smart-contract-vulnerabilities/.

[5] [Online]. Available: https://www.alchemy.com/best/smart-contract-tools.

[6] [Online]. Available: https://www.kali.org/tools/nikto/.

[7] [Online]. Available: https://nmap.org/.

[8] [Online]. Available: https://en.wikipedia.org/wiki/Vulnerability_assessment.

[9] [Online]. Available: https://kalilinuxtutorials.com/wafw00f/.

[10] [Online]. Available: https://www.invicti.com/blog/news/netsparker-is-now-invicti-signaling-a-new-era-for-modern-appsec/.

[11] [Online]. Available: https://hackerone.com/directory/programs.