

# 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 .....                               | 7  |
| 02.  | Objective .....                                     | 8  |
| 03.  | Introduction.....                                   | 9  |
| 04.  | Bug Bounty Reports.....                             | 11 |
| i.   | Report 01.....                                      | 11 |
|      | Target information: http://recordedfuture.com ..... | 11 |
|      | Information Gathering For Target Domain.....        | 14 |
|      | Using knockpy tool .....                            | 16 |
|      | Using Nitko tool.....                               | 17 |
|      | Using Uniscan tool.....                             | 19 |
|      | Using Wafw00f tool.....                             | 22 |
|      | Using pwnXss tool.....                              | 24 |
|      | Using Netsparker .....                              | 27 |
|      | Vulnerability 01 .....                              | 30 |
|      | Conclusion of the Report 01 .....                   | 32 |
|      | HackerOne Submitted Report Screenshot.....          | 32 |
| ii.  | Report 02.....                                      | 33 |
|      | Target information: api.recordedfuture.com.....     | 33 |
|      | Information Gathering For Target Domain.....        | 33 |
|      | Using knockpy tool .....                            | 35 |
|      | Using Uniscan tool.....                             | 36 |
|      | Using Wafw00f tool.....                             | 38 |
|      | Using OWASP-ZAP tool .....                          | 39 |
|      | Using Netsparker .....                              | 41 |
|      | Vulnerability 02 .....                              | 43 |
|      | Conclusion of the Report 02 .....                   | 45 |
|      | HackerOne Submitted Report Screenshot.....          | 45 |
| iii. | Report 03.....                                      | 46 |
|      | Target information: therecord.media .....           | 46 |
|      | Information Gathering For Target Domain.....        | 47 |
|      | Using knockpy tool .....                            | 49 |
|      | Using Uniscan tool.....                             | 50 |
|      | Using PwnXSS tool .....                             | 52 |
|      | Using OWASP-ZAP tool .....                          | 54 |
|      | Using Netsparker .....                              | 56 |
|      | Vulnerability 03 .....                              | 58 |
|      | Conclusion of the Report 03 .....                   | 60 |

|  |     |
|--|-----|
| HackerOne Submitted Report Screenshot.....           | 60  |
| iv. Report 04.....                                   | 61  |
| Target information: app.recordedfuture.com .....     | 61  |
| Information Gathering For Target Domain.....         | 61  |
| Using knockpy tool .....                             | 63  |
| Using Uniscan tool.....                              | 64  |
| Using Wafw00f tool.....                              | 66  |
| Using OWASP-ZAP tool.....                            | 67  |
| Using Netsparker .....                               | 69  |
| Vulnerability 04 .....                               | 72  |
| Conclusion of the Report 04 .....                    | 74  |
| HackerOne Submitted Report Screenshot.....           | 74  |
| v. Report 05.....                                    | 75  |
| Target information: https://www.getharvest.com ..... | 75  |
| Information Gathering For Target Domain.....         | 78  |
| Using knockpy tool .....                             | 80  |
| Using dotdotpwn tool.....                            | 81  |
| Using Nikto tool.....                                | 83  |
| Using Uniscan tool.....                              | 84  |
| Using wafw00f tool.....                              | 86  |
| Using OWASP-ZAP tool.....                            | 87  |
| Using Netsparker .....                               | 89  |
| Vulnerability 05 .....                               | 91  |
| Conclusion of the Report 05 .....                    | 93  |
| HackerOne Submitted Report Screenshot.....           | 93  |
| vi. Report 06.....                                   | 94  |
| Target information: http://harvestapp.com.....       | 94  |
| Information Gathering For Target Domain.....         | 94  |
| Using knockpy tool .....                             | 96  |
| Using Uniscan tool.....                              | 99  |
| Using Wafw00f tool.....                              | 101 |
| Using OWASP-ZAP tool.....                            | 102 |
| Using Netsparker .....                               | 103 |
| Vulnerability 06 .....                               | 105 |
| Conclusion of the Report 06 .....                    | 107 |
| HackerOne Submitted Report Screenshot.....           | 107 |
| vii. Report 07.....                                  | 108 |
| Target information: https://id.getharvest.com.....   | 108 |
| Information Gathering For Target Domain.....         | 108 |

|   |     |
|---|-----|
| Using knockpy tool .....  | 110 |
| Using Uniscan tool.....   | 111 |
| Using Wafw00f tool.....   | 113 |
| Using OWASP-ZAP tool.....   | 114 |
| Using Netsparker .....  | 115 |
| Vulnerability 07 .....  | 117 |
| Conclusion of the Report 07 .....   | 119 |
| HackerOne Submitted Report Screenshot.....  | 119 |
| viii. Report 08.....  | 120 |
| Target information: <a href="https://www.semrush.com/">https://www.semrush.com/</a> ..... | 120 |
| Information Gathering For Target Domain.....  | 123 |
| Using knockpy tool .....  | 125 |
| Using PwnXSS tool .....   | 127 |
| Using Uniscan tool.....   | 130 |
| Using Nitko tool.....   | 132 |
| Using OWASP-ZAP tool .....  | 133 |
| Using Netsparker .....  | 136 |
| Vulnerability 08 .....  | 138 |
| Conclusion of the Report 08 .....   | 140 |
| HackerOne Submitted Report Screenshot.....  | 140 |
| ix. Report 09.....  | 141 |
| Target information: <a href="https://www.wickr.com/">https://www.wickr.com/</a> .....     | 141 |
| Information Gathering For Target Domain.....  | 143 |
| Using knockpy tool .....  | 145 |
| Using Wafw00f tool.....   | 146 |
| Using Uniscan tool.....   | 147 |
| Using Nitko tool.....   | 149 |
| Using OWASP-ZAP tool .....  | 150 |
| Using Netsparker .....  | 151 |
| Vulnerability 09 .....  | 153 |
| Conclusion of the Report 09 .....   | 155 |
| HackerOne Submitted Report Screenshot.....  | 155 |
| x. Report 10.....   | 156 |
| Target information: <a href="https://www.yuga.com/">https://www.yuga.com/</a> .....       | 156 |
| Information Gathering For Target Domain.....  | 158 |
| Using knockpy tool .....  | 160 |
| Using Wafw00f tool.....   | 161 |
| Using Uniscan tool.....   | 162 |
| Using Nitko tool.....   | 164 |

|  |     |
|--|-----|
| Using OWASP-ZAP tool.....                  | 165 |
| Using Netsparker .....                     | 166 |
| Vulnerability 10 .....                     | 168 |
| Conclusion of the Report 10 .....          | 171 |
| HackerOne Submitted Report Screenshot..... | 171 |
| Conclusion .....                           | 172 |
| References.....                            | 173 |

## **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, Owasp 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.

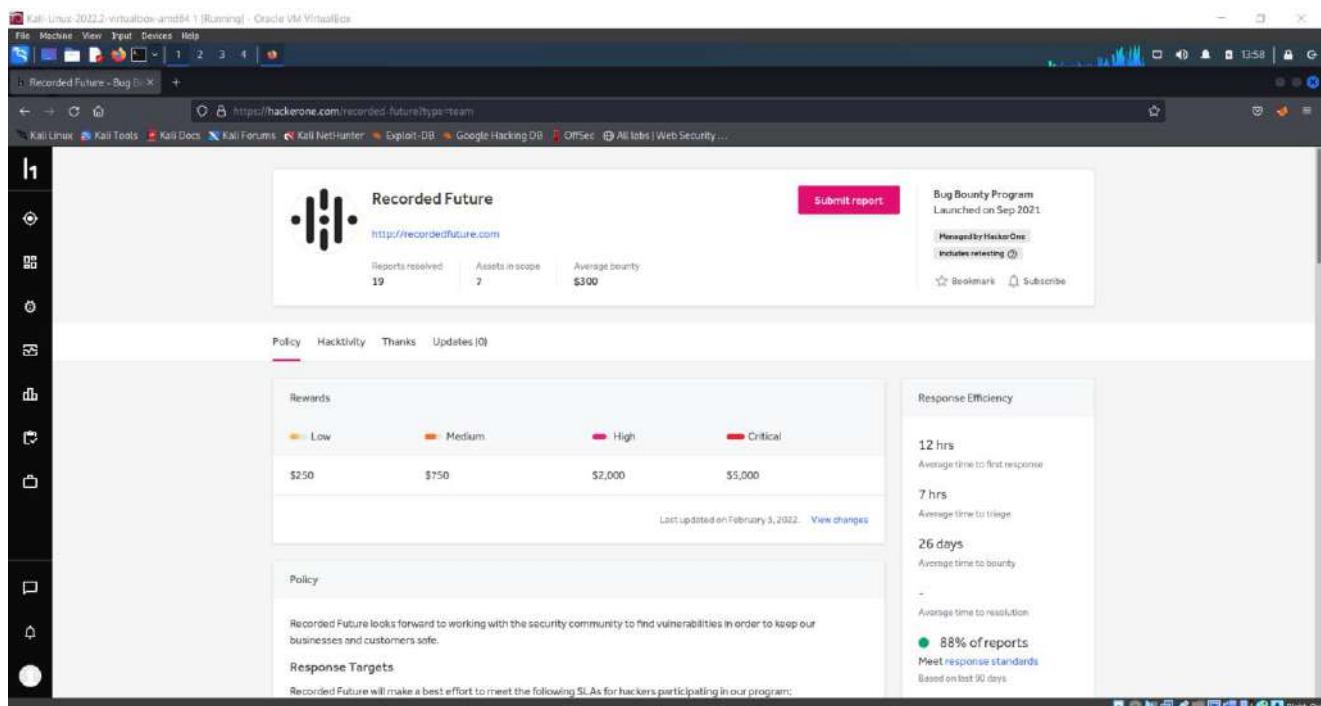
Is it true that an audit of an organization's information technology security may help enhance data security and reduce the likelihood of possible network security risks? This report on the examination will explain how and why an effective Web security audit is undertaken, in addition to addressing the 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](http://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>

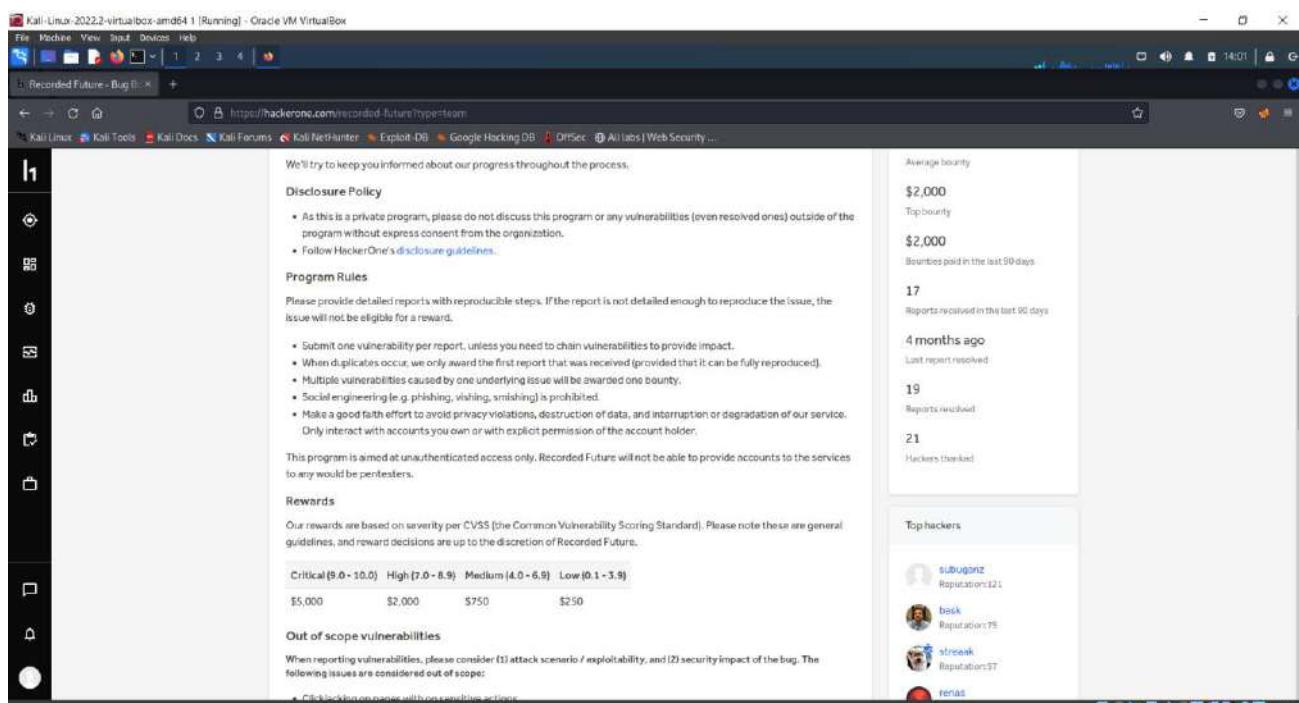
Finding vulnerabilities in the target domain (<http://recordedfuture.com>) and determining the risk level associated with such vulnerabilities is the purpose of this assessment. The aim of the assessment is to uncover vulnerabilities in the target domain.



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.

Critical (9.0 - 10.0) High (7.0 - 8.9) Medium (4.0 - 6.9) Low (0.1 - 3.9)

\$5,000 \$2,000 \$750 \$250

**Out of scope vulnerabilities**

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

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

Safe Harbor

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.

Scopes:

In Scope

| Domain                 | Services   | Risk Level | Status   |
|------------------------|--|------------|----------|
| www.recordedfuture.com | Cloudflare DDOS, Wordpress                           | Critical   | Eligible |
| api.recordedfuture.com | Amazon Web Services                                  | Critical   | Eligible |
| app.recordedfuture.com | Amazon Web Services, Cloudflare DDOS, Cloudflare WAF | Critical   | Eligible |
| id.recordedfuture.com  | Amazon Web Services, Cloudflare DDOS, Cloudflare WAF | Critical   | Eligible |
| therecord.media        | Cloudflare DDOS, Wordpress                           | Medium     | Eligible |
| iOS.ipa                | com.recordedfuture.mobile                            | Critical   | Eligible |
| Android.apk            | com.recordedfuture.mobile                            | Critical   | Eligible |

Download Surp Suite Project Configuration File (10 URLs) View changes Last updated on February 23, 2022.

## 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.

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The URL in the address bar is <http://siteReport.netcraft.com?url=http%3A%2F%2Frecordedfuture.com>. The page displays a detailed site report for the domain recordedfuture.com. The report is divided into sections: Background, Network, and Reverse DNS. The 'Background' section includes details like Site title (Recorded Future: Securing Our World With Intelligence), Date first seen (April 2009), and Netcraft Risk Rating (0/10). The 'Network' section provides information on the domain's infrastructure, including Netblock Owner (Cloudflare, Inc.), Name server (hugrns.cloudflare.com), Hosting company (Cloudflare), Domain registrar (name.com), Hosting country (US), Nameserver organisation (whois.cloudflare.com), IPv4 address (104.18.2.05), Organisation (Domain Protection Services, Inc., PO Box 1769, Denver, CO 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 (unknown), and Reverse DNS (unknown). A progress bar at the bottom indicates 'Transferring data from fonts.getstatic.com...'.

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

Recorded Future - Bug X Site report for http://recordedfuture.com

https://siteport.netcraft.com?url=http%3A%2F%2Frecordedfuture.com

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.

5 known trackers were identified.

**Companies**

|          |                  |                  |  |
|----------|------------------|------------------|--|
| Company  | Primary Category | Tracker          | Popular Sites with this Tracker                        |
| Facebook | Analytics        | FacebookPixel    | www.rutracker.org, www.infobar.com, www.avantipips.com |
| Google   | Advertising      | DoubleClick      | www.flightradar24.com, www.mrc.co.uk, www.marta.com    |
| Google   | Analytics        | GoogleAnalytics  | www.corriere.it, www.congegno.com, www.cnn.com         |
| Twitter  | Analytics        | TwitterAnalytics | www.algamadrich.com, www.rds.ca, www.chmeev.ca         |
| Twitter  | Tracker          | Twitter          | www.hbc.co.uk, mobile.twitter.com, online.hbc.co.uk    |

**Categories**

**Site Technology** (fetched 16 days ago)

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

Recorded Future - Bug X Site report for http://recordedfuture.com

https://siteport.netcraft.com?url=http%3A%2F%2Frecordedfuture.com

Services Solutions News Company Resources Discover More Report Fraud

### 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.eosta.org, www.lispq.qc.ca, chat.openai.com |
| Varnish    | An HTTP accelerator for web applications                            | www.zna.com, www.libc.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.robtex.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.

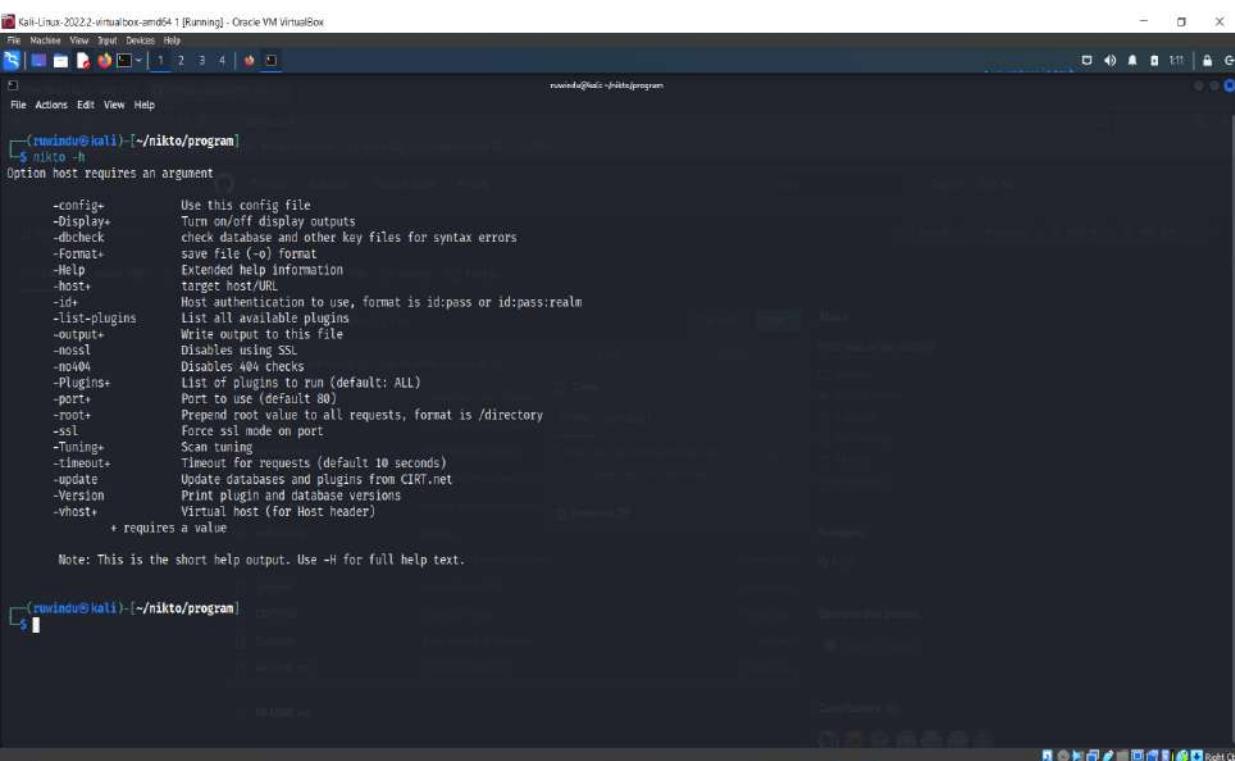
```
Kali-Linux-2022.2-virtualbox-64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
knockpy recordedfuture.com
v6.1.0
local: 18757 | connote: 0 py
W: /home/rwinda/.local/share/knockpy/knockpy.py:1: UserWarning: Using or importing the __builtin__ package is deprecated, and in future will be replaced by builtins.
  warnings.warn("Using or importing the __builtin__ package is deprecated, and in future will be replaced by builtins.", UserWarning)
W: /home/rwinda/.local/share/knockpy/knockpy.py:2: UserWarning: Using or importing the __builtin__ package is deprecated, and in future will be replaced by builtins.
  warnings.warn("Using or importing the __builtin__ package is deprecated, and in future will be replaced by builtins.", UserWarning)
root@kali:~# knockpy recordedfuture.com | tee -a knockpy.log
11:20:06
Ip address      Code Subdomain          Server           Real hostname
162.159.129.52  200 api.recordedfuture.com   cloudflare
184.18.6.86     304 api.recordedfuture.com   cloudflare
184.18.7.86     200 app.recordedfuture.com    cloudflare
184.18.7.86     200 ass.recordedfuture.com   cloudflare
184.18.7.86     200 blog.recordedfuture.com  cloudflare
184.18.7.86     200 call.recordedfuture.com  OSF
184.18.7.86     200 call_mobile.recordedfuture.com
184.18.7.86     200 cms.recordedfuture.com   cloudflare
151.181.130.216 200 cms.recordedfuture.com   cloudflare
184.18.7.86     200 files.recordedfuture.com  cloudflare
184.18.6.86     200 get.recordedfuture.com   cloudflare
199.68.193.2    304 go.recordedfuture.com   cloudflare
184.18.7.86     200 id.recordedfuture.com   cloudflare
18.233.118.192 304 index.recordedfuture.com
184.18.6.86     404 iisver1.recordedfuture.com
184.18.6.86     404 iisver2.recordedfuture.com
184.18.6.86     200 labs.recordedfuture.com
76.125.24.121   200 lyra.recordedfuture.com
184.18.6.86     200 partners.recordedfuture.com
184.18.6.86     200 press.recordedfuture.com
184.18.6.86     200 sales.recordedfuture.com
184.18.7.86     200 sandbox.recordedfuture.com
184.18.6.86     200 signups.recordedfuture.com
13.32.88.37    303 sso.recordedfuture.com
13.32.30.39    403 university.recordedfuture.com
184.18.7.86     304 ui.recordedfuture.com
184.18.6.86     500 www.recordedfuture.com
184.18.7.86     200 www.recordedfuture.com
11:42:07
Ip address: 21 | Subdomain: 34 | elapsed time: 00:12:04
[!] root@kali:~/home/rwinda
```

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.

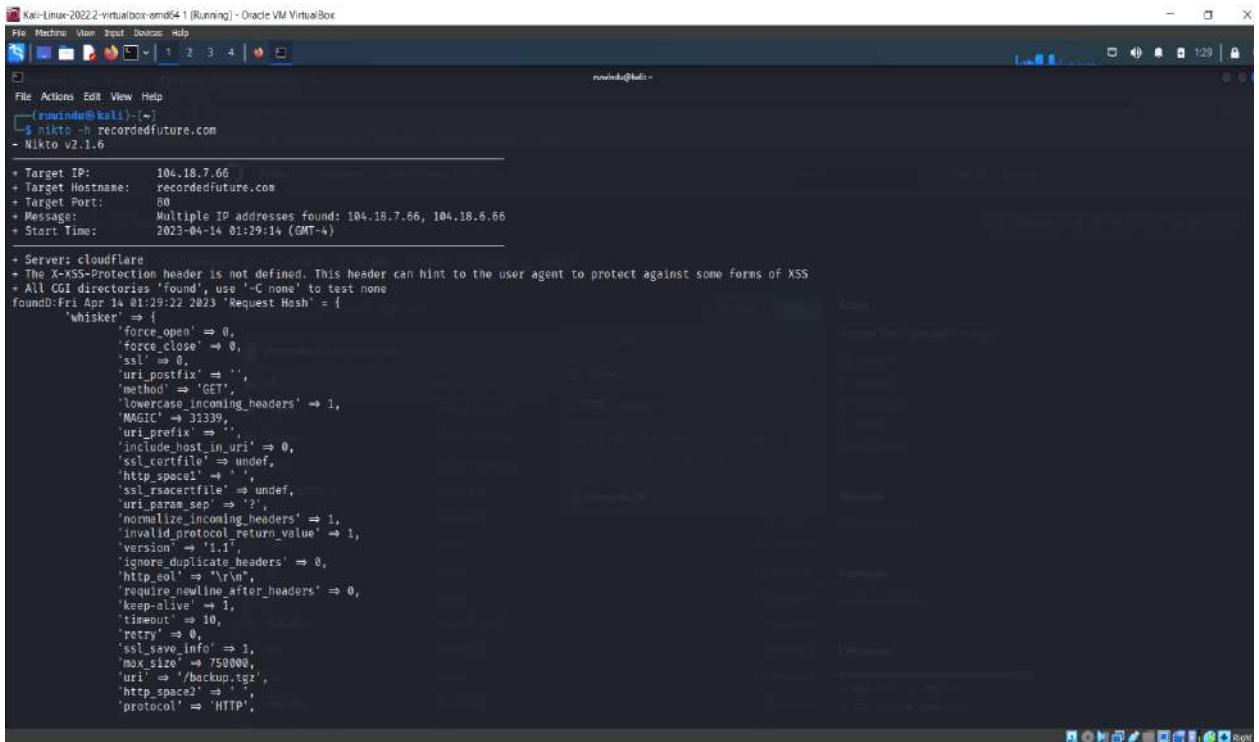


The screenshot shows a terminal window on a Kali Linux desktop environment. The window title is "Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox". The terminal prompt is "(root@kali:~/nikto/program)". The user has run the command "\$ nikto -h", which displays the help menu for the nikto tool. The help text provides detailed descriptions for various command-line options:

- config+ Use this config file
- Display+ Turn on/off display outputs
- dbcheck check database and other key files for syntax errors
- Format+ save file (-o) format
- Help Extended help information
- host+ target host/URL
- id+ Host authentication to use, format is id:pass or id:pass:realm
- list-plugins List all available plugins
- output+ Write output to this file
- nossl Disables SSL
- no404 Disables 404 checks
- Plugins+ List of plugins to run (default: ALL)
- port+ Port to use (default 80)
- root+ Prepend root value to all requests, format is /directory
- ssl Force SSL mode on port
- Tuning+ Scan tuning
- timeout+ Timeout for requests (default 10 seconds)
- update Update databases and plugins from CIRT.net
- Version Print plugin and database versions
- vhost+ Virtual host (for Host header)

A note at the bottom states: "+ requires a value. Note: This is the short help output. Use -H for full help text."

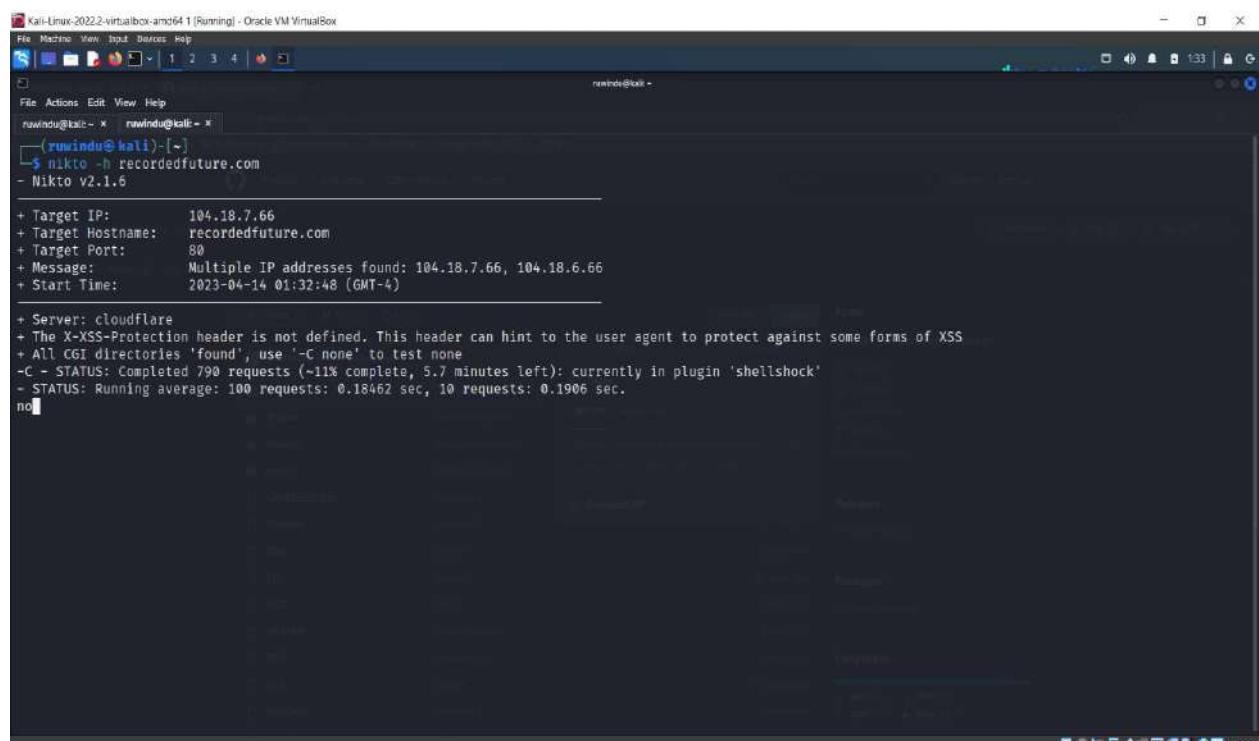
Scanned the target domain using nitko tool.



```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(ruwindu@kali)-[~]
└─$ nikto -h recordedfuture.com
- Nikto v2.1.6

+ Target IP:      104.18.7.66
+ Target Hostname: recordedfuture.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.18.7.66, 104.18.6.66
+ Start Time:    2023-04-14 01:29:14 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ All CGI directories 'found', use '-C none' to test none
Found@Fri Apr 14 01:29:22 2023 'Request Hash' = {
  'Whisker' => 1,
  'force_open' => 0,
  'force_close' => 0,
  'ssl' => 0,
  'uri_postfix' => '',
  'method' => 'GET',
  'lowercase_incoming_headers' => 1,
  'MAGIC' => 31339,
  'uri_prefix' => '',
  'include_host_in_uri' => 0,
  'ssl_certfile' => undef,
  'http_space1' => '',
  'ssl_rscacertfile' => undef,
  'uri_param_sep' => '?',
  'normalize_incoming_headers' => 1,
  'invalid_protocol_return_value' => 1,
  'version' => '1.1',
  'ignore_duplicate_headers' => 0,
  'http_eol' => '\r\n',
  'require_newline_after_headers' => 0,
  'keep-alive' => 1,
  'timeout' => 10,
  'retry' => 0,
  'ssl_save_info' => 1,
  'max_size' => 750000,
  'uri' => '/backup.tgz',
  'http_space2' => '',
  'protocol' => 'HTTP'.
```



```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
(ruwindu@kali)-[~]
└─$ nikto -h recordedfuture.com
- Nikto v2.1.6

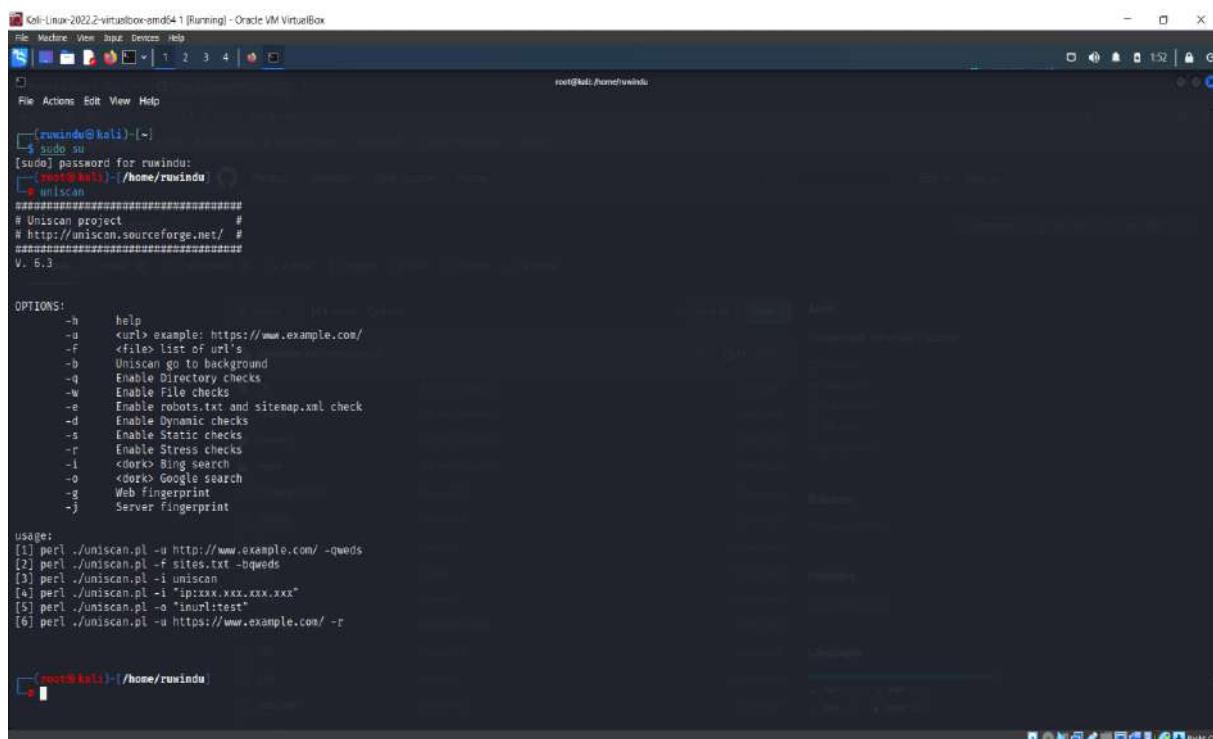
+ Target IP:      104.18.7.66
+ Target Hostname: recordedfuture.com
+ Target Port:    80
+ Message:        Multiple IP addresses found: 104.18.7.66, 104.18.6.66
+ Start Time:    2023-04-14 01:32:48 (GMT-4)

+ Server: cloudflare
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ All CGI directories 'found', use '-C none' to test none
-C - STATUS: Completed 790 requests (-1% complete, 5.7 minutes left): currently in plugin 'shellshock'
- STATUS: Running average: 100 requests: 0.18462 sec, 10 requests: 0.1906 sec.
no
```

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.



The screenshot shows a terminal window titled "Kali-Linux-2022.2-virtualbox-0md54 [Running] - Oracle VM VirtualBox". The terminal is running as root, indicated by the prompt "(root@kali:~)". The user is executing the Uniscan command:

```
$ uniscan
```

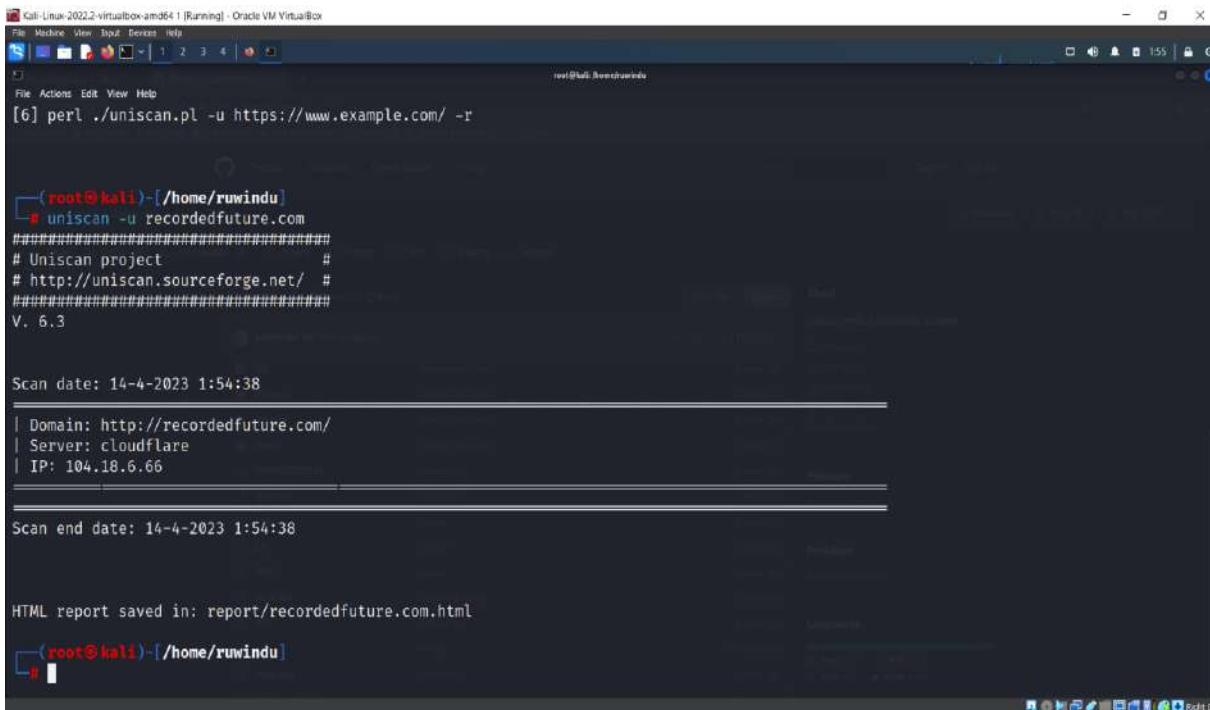
The output shows the Uniscan project details and usage instructions:

```
# Uniscan project
# http://uniscan.sourceforge.net/
# V. 6.3

OPTIONS:
-h      help
-u      <url> example: https://www.example.com/
-f      <file> list of url's
-b      Uniscan go to background
-q      Enable Directory checks
-w      Enable File checks
-e      Enable robots.txt and sitemap.xml check
-d      Enable Dynamic checks
-s      Enable Static checks
-r      Enable Stress checks
-i      <dork> Bing search
-o      <dork> Google search
-g      Web Fingerprint
-j      Server Fingerprint

usage:
[1] perl ./uniscan.pl -u http://www.example.com/ -qweds
[2] perl ./uniscan.pl -f sites.txt -bqweds
[3] perl ./uniscan.pl -i uniscan
[4] perl ./uniscan.pl -i "ip:xxx.xxx.xxx.xxx"
[5] perl ./uniscan.pl -o "inurl:test"
[6] perl ./uniscan.pl -u https://www.example.com/ -r
```

Quick scan by using the **-u** and enter the target domain.



```
[root@kali:~/home/ruwindu] [6] perl ./uniscan.pl -u https://www.example.com/ -r

[root@kali:~/home/ruwindu] # uniscan -u recordedfuture.com
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

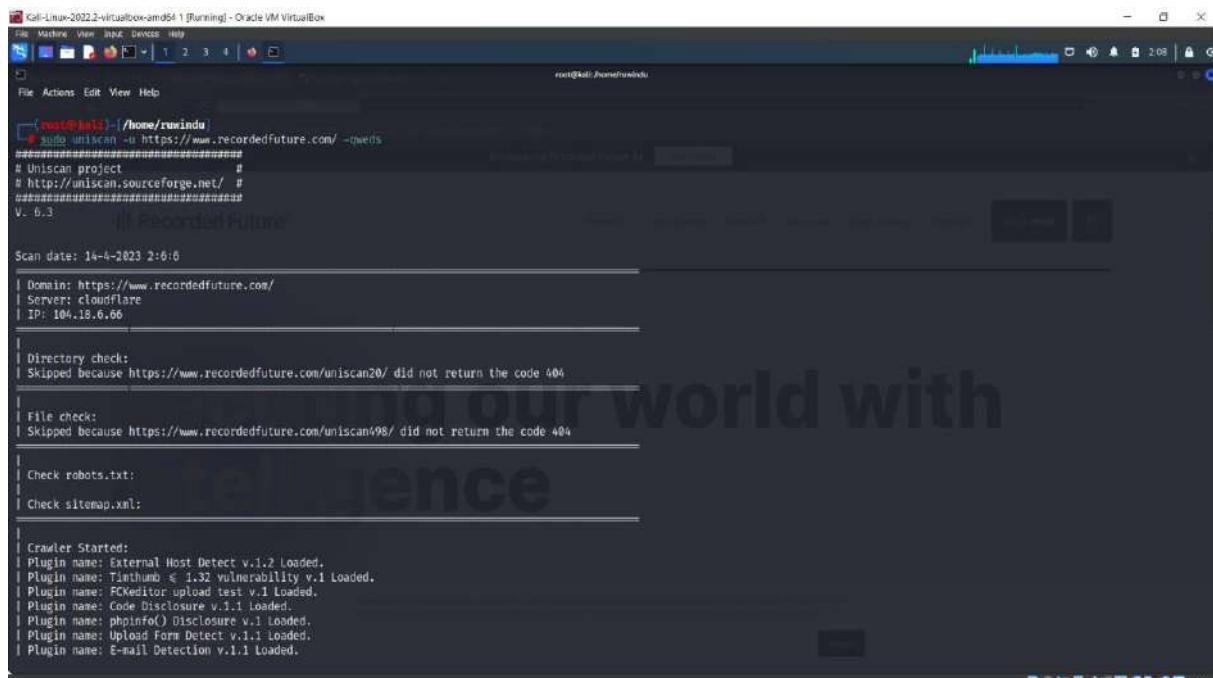
Scan date: 14-4-2023 1:54:38
#####
| Domain: http://recordedfuture.com/
| Server: cloudflare
| IP: 104.18.6.66
#####

Scan end date: 14-4-2023 1:54:38

HTML report saved in: report/recordedfuture.com.html

[root@kali:~/home/ruwindu]
```

And used the uniscan **-u recordedfuture.com -qweds**



```
[root@kali:~/home/ruwindu] [6] sudo uniscan -u https://www.recordedfuture.com/ -qweds

#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 14-4-2023 2:6:0
#####
| Domain: https://www.recordedfuture.com/
| Server: cloudflare
| IP: 104.18.6.66
#####

| Directory check:
| Skipped because https://www.recordedfuture.com/uniscan20/ did not return the code 404

| File check:
| Skipped because https://www.recordedfuture.com/uniscan498/ did not return the code 404

| Check robots.txt:
| Check sitemap.xml:

| Crawler Started:
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Tlenthumb < 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.
```

```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[+] Crawling Finished, 1 URL's found!
External hosts:
Timthumb:
FCKeditor File Upload:
Source Code Disclosure:
PHPIinfo() Disclosure:
File Upload Forms:
E-mails:
Web Backdoors:
Ignored Files:
Dynamic tests:
Plugin name: Learning New Directories v.1.2 Loaded.
Plugin name: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1.1 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 https://www.recordedfuture.com/testing123 did not return the code 404
```

```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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: 14-4-2023 2:8:33

HTML report saved in: report/www.recordedfuture.com.html
/home/runindu
```

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.

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

(ruwindu㉿kali)-[~]
$ wafw00f


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

Usage: wafw00f url1 [url2 [url3 ... ]]
example: wafw00f http://www.victim.org/

wafw00f: error: No test target specified.

(ruwindu㉿kali)-[~]
$
```

We are able to see that the website [www.recordedfuture.com](http://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

```
[root@kali:~/home/rwinda/PwnXSS]# python3 pwnxss.py -u https://www.recordedfuture.com/
[04:08:59] [INFO] Starting PwnXSS ...
*****
[04:08:59] [INFO] Checking connection to: https://www.recordedfuture.com/
[04:09:01] [INFO] Connection established 200
[04:09:01] [WARNING] Found link with query: mta_campaign=CaseStudy-Toshiba-Letter&mtm_kwds=toshiba&mtm_source=website Maybe a vuln XSS point
[04:09:01] [INFO] Query (GET) : https://go.recordedfuture.com/hubfs/case-studies/toshiba.pdf?mtm_campaign=<script>console.log(5000/3000)</script>
[04:09:01] [INFO] Query (GET) : https://go.recordedfuture.com/hubfs/case-studies/toshiba.pdf?mtm_campaign=%3Cscript%3Econsole.log%25000%2F3000%29%3Ch2fscript%3Cscript%3Econsole%3C2fscript%3Ealert%25000%2F3000%29%3Ch2fscript%3E
[04:09:01] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:09:01] [INFO] Checking connection to: https://www.recordedfuture.com/careers
[04:09:02] [INFO] Connection established 200
*****
[04:09:02] [INFO] Checking connection to: https://www.recordedfuture.com/jobs
[04:09:03] [INFO] Connection established 200
*****
[04:09:03] [INFO] Checking connection to: https://www.recordedfuture.com/cdn-cgi/l/email-protection
[04:09:03] [INFO] Connection established 200
[04:09:03] [WARNING] Found link with query: utm_source=email_protection Maybe a vuln XSS point
[04:09:03] [INFO] Query (GET) : https://www.cloudflare.com/sign-up?utm_source=<script>alert(6000/3000)</script>
[04:09:03] [INFO] Query (GET) : https://www.cloudflare.com/sign-up?utm_source=%3Cscript%3Ealert%256000%2F3000%29%3Ch2fscript%3E
[04:09:03] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:09:03] [INFO] Checking connection to: https://www.recordedfuture.com/contact
[04:09:04] [INFO] Connection established 200
*****
[04:09:04] [INFO] Checking connection to: https://www.recordedfuture.com/careers/
[04:09:06] [INFO] Connection established 200
*****
[04:09:06] [INFO] Checking connection to: https://www.recordedfuture.com/
[04:09:06] [INFO] Connection established 200
```

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/>.

```
[root@kali:~/home/rwinda/PwnXSS]# python3 pwnxss.py -u https://www.recordedfuture.com/
[04:09:06] [INFO] Connection established 200
*****
[04:09:06] [INFO] Checking connection to: https://www.recordedfuture.com/
[04:09:06] [INFO] Connection established 200
[04:09:06] [WARNING] Found link with query: mta_campaign=CaseStudy-Toshiba-Letter&mtm_kwds=toshiba&mtm_source=website Maybe a vuln XSS point
[04:09:06] [INFO] Query (GET) : https://go.recordedfuture.com/hubfs/case-studies/toshiba.pdf?mtm_campaign=<script>alert(6000/3000)</script>
[04:09:06] [INFO] Query (GET) : https://go.recordedfuture.com/hubfs/case-studies/toshiba.pdf?mtm_campaign=%3Cscript%3Ealert%256000%2F3000%29%3Ch2fscript%3E
[04:09:06] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:09:07] [INFO] Checking connection to: https://www.recordedfuture.com/platform
[04:09:08] [INFO] Connection established 200
*****
[04:09:08] [INFO] Checking connection to: https://www.recordedfuture.com/platform/brand-intelligence
[04:09:09] [INFO] Connection established 200
[04:09:09] [WARNING] Found link with query: mta_campaign=CaseStudy-Toshiba-Letter&mtm_kwds=toshiba&mtm_source=website Maybe a vuln XSS point
[04:09:09] [INFO] Query (GET) : https://go.recordedfuture.com/hubfs/case-studies/toshiba.pdf?mtm_campaign=<script>alert(6000/3000)</script>
[04:09:09] [INFO] Query (GET) : https://go.recordedfuture.com/hubfs/case-studies/toshiba.pdf?mtm_campaign=%3Cscript%3Ealert%256000%2F3000%29%3Ch2fscript%3E
[04:09:09] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:09:10] [INFO] Checking connection to: https://www.recordedfuture.com/press-releases/20210202
[04:09:11] [INFO] Connection established 200
*****
[04:09:11] [INFO] Checking connection to: https://www.recordedfuture.com/platform/secops-intelligence
[04:09:12] [INFO] Connection established 200
*****
[04:09:12] [INFO] Checking connection to: https://www.recordedfuture.com/press-releases/20210413
[04:09:13] [INFO] Connection established 200
*****
[04:09:13] [INFO] Checking connection to: https://www.recordedfuture.com/platform/threat-intelligence
[04:09:14] [INFO] Connection established 200
[04:09:14] [WARNING] Found link with query: v=REZZEDASxM1Y Maybe a vuln XSS point
[04:09:14] [INFO] Query (GET) : https://www.youtube.com/watch?v=<script>alert(6000/3000)</script>
[04:09:14] [INFO] Query (GET) : https://www.youtube.com/watch?v=%3Cscript%3Ealert%256000%2F3000%29%3Ch2fscript%3E
[04:09:14] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:09:15] [INFO] Checking connection to: https://www.recordedfuture.com/threats/dark-web-monitoring
[04:09:16] [INFO] Connection established 200
*****
[04:09:16] [INFO] Checking connection to: https://www.recordedfuture.com/platform/vulnerability-intelligence
[04:09:17] [INFO] Connection established 200
```

```
Kali-USB-2022.2-virtualbox-and64[1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5
root@kali: /home/nminds/PwnBoss
File Actions Edit View Help
*****
[04:09:30] [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-fje_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=k3Cscript%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=a1-blog-demo&mtm_source=a1-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=k3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[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/061123
[04:09:43] [INFO] Connection established 200
*****
[04:09:43] [INFO] Checking connection to: https://www.recordedfuture.com/cdn-eg1//email-protection#d1F72a0e7b5caf7F2a0e7c4e0f7f2a0e7e5caef7f2a0e7e0ea7f72a0e5c1caef7f2e0e0e5eaf
[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=k3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:09:43] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:09:42] [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
*****
[04:09:49] [INFO] Checking connection to: https://www.recordedfuture.com/integrations
[04:09:50] [INFO] Connection established 200
*****
[04:09:50] [INFO] Checking connection to: https://www.recordedfuture.com/integrations/splunk
```

```

Kali-Linux-2022.2-virtualbox-arm64_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[04:09:54] [INFO] Connection established 200
*****
[04:09:54] [INFO] Checking connection to: https://www.recordedfuture.com/integrations/splunk-siem
[04:09:55] [INFO] Connection established 200
[04:09:55] [WARNING] Found link with query: __hstc=209570217_de388a55bb79f0eb36278a059a7852f_1643293880635_1652462081859_16527191640138__hsfp-312135231
[04:09:55] [INFO] Query (GET) : https://go.recordedfuture.com/splunk-integration-trial?__hstc=<script>alert(6000/3000)</script>
[04:09:55] [INFO] Query (GET) : https://go.recordedfuture.com/splunk-integration-trial?__hstc=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E__hsfp=%3Cscript%3Ealert%286000%2F3000%29%3C
[04:09:56] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:09:56] [INFO] Checking connection to: https://www.recordedfuture.com/threats/ransomware
[04:09:57] [INFO] Connection established 200
[04:09:57] [WARNING] Found link with query: utm_source=brighttalk-portalutm_medium=web&utm_campaign=channel-feed Maybe a vuln XSS point
[04:09:57] [INFO] Query (GET) : https://www.brighttalk.com/webcast/13713/475345?utm_source=<script>alert(6000/3000)</script>
[04:09:58] [INFO] Query (GET) : https://www.brighttalk.com/webcast/13713/475345?utm_source=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:00] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:10:00] [INFO] Checking connection to: https://www.recordedfuture.com/training
[04:10:01] [INFO] Connection established 200
*****
[04:10:01] [INFO] Checking connection to: https://www.recordedfuture.com/training/getting-started
[04:10:02] [INFO] Connection established 200
*****
[04:10:02] [INFO] Checking connection to: https://www.recordedfuture.com/cdn-cgi/l/email-protection#7a0e083b1344311d3a081f1915081ef1fc0f0e0f0801f54391517
[04:10:02] [INFO] Connection established 200
[04:10:02] [WARNING] Found link with query: utm_source=email_protection Maybe a vuln XSS point
[04:10:02] [INFO] Query (GET) : https://www.cloudflare.com/sign-up?utm_source=<script>alert(6000/3000)</script>
[04:10:02] [INFO] Query (GET) : https://www.cloudflare.com/sign-up?utm_source=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:02] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:10:02] [INFO] Checking connection to: https://www.recordedfuture.com/training/certified-analyst
[04:10:03] [INFO] Connection established 200
*****
[04:10:03] [INFO] Checking connection to: https://www.recordedfuture.com/training/experts-corner
[04:10:04] [INFO] Connection established 200
*****
[04:10:04] [INFO] Checking connection to: https://www.recordedfuture.com/cdn-cgi/l/email-protection#176365787e797c79705765727478a57372737162636265723974787a
[04:10:04] [INFO] Connection established 200
[04:10:05] [WARNING] Found link with query: utm_source=email_protection Maybe a vuln XSS point
[04:10:05] [INFO] Query (GET) : https://www.cloudflare.com/sign-up?utm_source=<script>alert(6000/3000)</script>

```

```

Kali-Linux-2022.2-virtualbox-arm64_1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[04:10:18] [INFO] Query (GET) : https://www.privacyshield.gov/article?id=N3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:19] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:10:19] [INFO] Checking connection to: https://www.recordedfuture.com/privacy-policy/1
[04:10:20] [INFO] Connection established 200
[04:10:20] [WARNING] Found link with query: id=ANNEX-I-introduction Maybe a vuln XSS point
[04:10:20] [INFO] Query (GET) : https://www.privacyshield.gov/article?id=<script>alert(6000/3000)</script>
[04:10:20] [INFO] Query (GET) : https://www.privacyshield.gov/article?id=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:20] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:10:20] [INFO] Checking connection to: https://www.recordedfuture.com/privacy-policy/3-0/cookies
[04:10:21] [INFO] Connection established 200
*****
[04:10:21] [INFO] Checking connection to: https://www.recordedfuture.com/privacy-policy
[04:10:22] [INFO] Connection established 200
[04:10:22] [WARNING] Found link with query: id=ANNEX-I-introduction Maybe a vuln XSS point
[04:10:22] [INFO] Query (GET) : https://www.privacyshield.gov/article?id=<script>alert(6000/3000)</script>
[04:10:22] [INFO] Query (GET) : https://www.privacyshield.gov/article?id=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:22] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:10:22] [INFO] Checking connection to: https://www.recordedfuture.com/terms-of-use
[04:10:23] [INFO] Connection established 200
*****
[04:10:23] [INFO] Checking connection to: https://www.recordedfuture.com/terms-of-use/7-0
[04:10:24] [INFO] Connection established 200
[04:10:24] [WARNING] Found link with query: id=ANNEX-I-introduction Maybe a vuln XSS point
[04:10:24] [INFO] Query (GET) : https://www.privacyshield.gov/article?id=<script>alert(6000/3000)</script>
[04:10:24] [INFO] Query (GET) : https://www.privacyshield.gov/article?id=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:24] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:10:24] [INFO] Checking connection to: https://www.recordedfuture.com/terms-of-use/7-0
[04:10:25] [INFO] Connection established 200
[04:10:25] [WARNING] Found link with query: q=https://www.recordedfuture.com/support/automated-indicator-sharing/osa=0$source=editors&ust=16591049821448290usg=A0vVan3a1uX5QyUKY021wBphuZ2A_M
[04:10:25] [INFO] Query (GET) : https://www.google.com/url?q=<script>alert(6000/3000)</script>
[04:10:25] [INFO] Query (GET) : https://www.google.com/url?o=3$script%3Ealert%286000%2F3000%29%3C%2Fscript%3E&source=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:25] [INFO] Parameter page using (GET) payloads but not 100% yet ...
*****
[04:10:25] [INFO] Checking connection to: https://www.recordedfuture.com/terms-of-use/7-0
[04:10:26] [INFO] Connection established 200
[04:10:26] [WARNING] Found link with query: q=https://www.recordedfuture.com/support/automated-indicator-sharing/osa=0$source=editors&ust=16591049821448290usg=A0vVan3a1uX5QyUKY021wBphuZ2A_N
[04:10:26] [INFO] Query (GET) : https://www.google.com/url?o=3$script%3Ealert%286000%2F3000%29%3C%2Fscript%3E&source=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:26] [INFO] Query (GET) : https://www.google.com/url?o=3$script%3Ealert%286000%2F3000%29%3C%2Fscript%3E&source=%3Cscript%3Ealert%286000%2F3000%29%3C%2Fscript%3E
[04:10:26] [INFO] Parameter page using (GET) payloads but not 100% yet ...

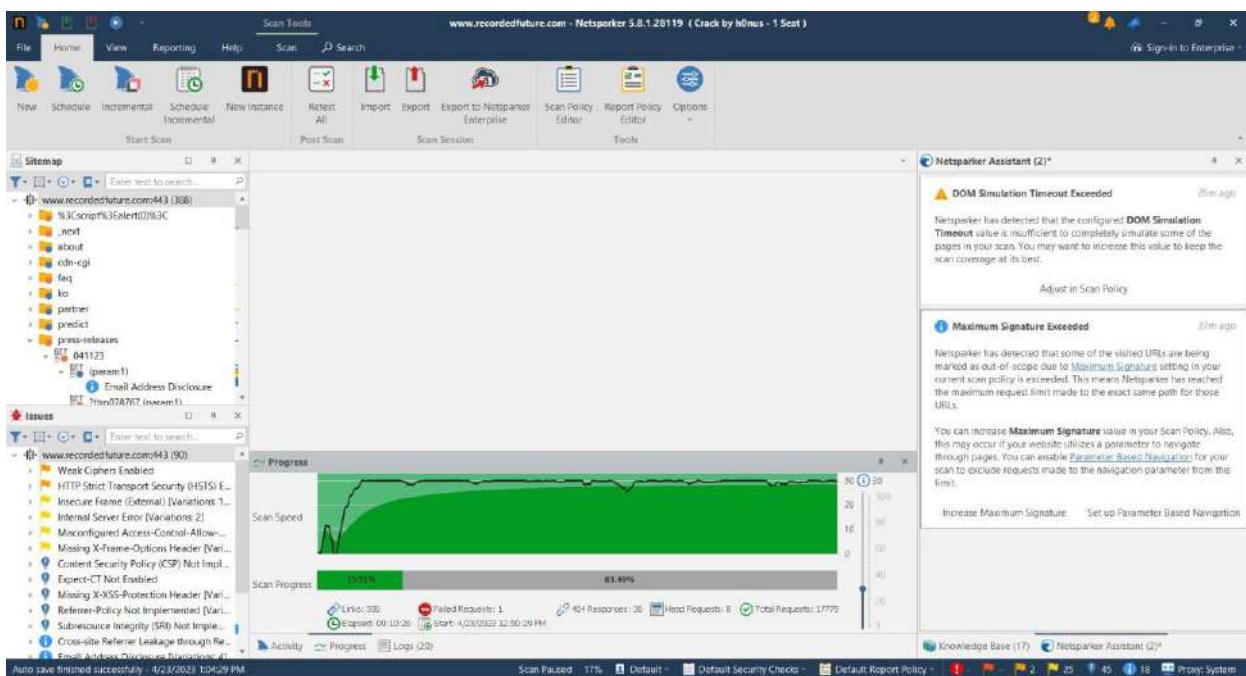
```

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 |
|---------|---|---------|---|-----------|
| !       | <a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a> | GET     | https://www.recordedfuture.com/   |           |
| !       | <a href="#">Weak Ciphers Enabled</a>                                      | GET     | https://www.recordedfuture.com/   |           |
| !       | <a href="#">Misconfigured Access-Control-Allow-Origin Header</a>          | GET     | https://www.recordedfuture.com/feed/  |           |
| !       | <a href="#">Missing X-Frame-Options Header</a>                            | GET     | https://www.recordedfuture.com/   |           |
| !       | <a href="#">Insecure Frame (External)</a>                                 | GET     | https://www.recordedfuture.com/   |           |
| !       | <a href="#">Internal Server Error</a>                                     | GET     | https://www.recordedfuture.com/%22%26%20ping%20-n%205%20127.0.0.1%20%26?%2f%2fr87?com%2f%3f |           |
| !       | <a href="#">Windows Short Filename</a>                                    | OPTIONS | https://www.recordedfuture.com/_next/static/*~1%5ca.aspx?asperrorpath=/                     |           |

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

| CONFIRM | VULNERABILITY | METHOD  | URL | PARAMETER  |
|---------|---------------|---|-----|--|
|         |               | <a href="#">Generic Email Address Disclosure</a>  | GET | https://www.recordedfuture.com/support/two-factor-authentication |
|         |               | <a href="#">Sitemap Detected</a>                  | GET | https://www.recordedfuture.com/sitemap.xml                       |
|         |               | <a href="#">Web Application Firewall Detected</a> | GET | https://www.recordedfuture.com/%3Cscript%3Ealert(0)%3Cscript%3E  |
|         |               | <a href="#">Forbidden Resource</a>                | GET | https://www.recordedfuture.com/.svn/wc.db                        |
|         |               | <a href="#">Robots.txt Detected</a>               | 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.

### Vulnerabilities

2.1. <https://www.recordedfuture.com/>

**CONFIRMED**

#### List of Supported Weak Ciphers

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)

### Request

[NETSPARKER] SSL Connection

### Response

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

[NETSPARKER] SSL Connection

#### 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 regedit32 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
```



|              |                          |
|--------------|--------------------------|
| PCI DSS v3.2 | <a href="#">6.5.4</a>    |
| OWASP 2013   | <a href="#">A6</a>       |
| OWASP 2017   | <a href="#">A3</a>       |
| SANS Top 25  | <a href="#">327</a>      |
| CAPEC        | <a href="#">217</a>      |
| WASC         | <a href="#">4</a>        |
| ISO27001     | <a href="#">A.14.1.3</a> |

## 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.

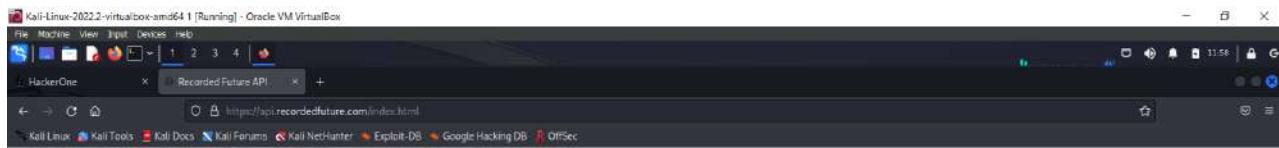
## HackerOne Submitted Report Screenshot

The screenshot shows the HackerOne interface. On the left is a sidebar with navigation links: Opportunities, Dashboard, **Inbox** (highlighted in green), Hacktivity, Leaderboard, and Directory. The main content area displays a report titled '#2002404 Weak Ciphers Enabled (Medium)'. The report details a finding from Netsparker: 'Weak Ciphers Enabled (Medium)' with a note: 'During a secure communication session (also known as SSL), Netsparker found that the ciphers being utilized were not very safe. Your web server needs to solely support powerful ciphers in order to guarantee the confidentiality and safety of any communication that takes place with visitors of your website.' Below this are sections for Solution, Impact, and a detailed description of the issue. To the right, there's a sidebar with participant information, state (New (Open)), reported to Recorded Future (Managed), severity (Medium), asset (Domain www.recordedfuture.com), weakness (Use of a Broken or Risky Cryptographic Algorithm), time spent (3h), visibility (Private), CVE ID (None), and account details (None).

## ii. Report 02

### Target information: [api.recordedfuture.com](https://api.recordedfuture.com)

The purpose of this research is to determine whether or not there are vulnerabilities in the target domain ([api.recordedfuture.com](https://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.



#### Recorded Future APIs

For information on how to use the API, visit the [Recorded Future API Documentation](#).  
An active API subscription and a valid API token are required to make live, real-time API requests.

| API   | Description  |
|---|--|
| <a href="#">Connect API</a>                 | The Connect API is the main API, providing intelligence about many types of indicators.  |
| <a href="#">Detection Rule API</a>          | The detection rules API is used to search for and download detection rules used to hunt for malwares. Sigma, Yara and Snort rules are available. |
| <a href="#">Detection Rule Relation API</a> | The Detection Rule API is supported by this API which can provide entities usable when filtering the response from the Detection Rule API.       |
| <a href="#">Entity Match API</a>            | This API can be used to find the entity id of any entity.  |
| <a href="#">Identity API</a>                | API to lookup identity leaks data  |
| <a href="#">Links API</a>                   | An API to retrieve verified links between entities.  |
| <a href="#">List API</a>                    | List API for reading and writing user lists  |
| <a href="#">Playbook Alert API</a>          | API for Recorded Future Playbook Alerts.   |
| <a href="#">Threat API</a>                  | API for Recorded Future Threat Data.   |
| <a href="#">Collective Insights API</a>     | API for sending data to the Recorded Future Intelligence Cloud.  |



### 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](https://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... +

https://site.report.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      |
|-------------|---------------------|----------------------|
| Site rank   | 54905               | Netcraft Risk Rating |
| Description | Not Present         | Primary language     |

**Network**

| Site                    | http://api.recordedfuture.com | Domain                   | recordedfuture.com  |
|-------------------------|-------------------------------|--------------------------|---|
| Netblock Owner          | Cloudflare, Inc.              | Namenserver              | hughes.cloudflare.com   |
| Hosting company         | Cloudflare                    | Domain registrar         | name.com  |
| Hosting country         | US                            | Namenserver organisation | whois.cloudflare.com  |
| IPv4 address            | 162.159.129.62                | Organisation             | Domain Protection Services, Inc., PO Box 1768, Denver, 80201, United States |
| IPv4 autonomous systems | AS13335                       | DNS admin                | dns@cloudflare.com  |
| IPv6 address            | 2006:4700:7::0:ca29:8198      | 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... +

https://site.report.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**

**Categories**

| Company | Primary Category | Tracker   | Popular Sites with this Tracker                         |
|---------|------------------|-----------|---|
| Google  | CDN              | Googlecdn | www.caosemables.com, www.inspq.qc.ca, www.nexusmeds.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...

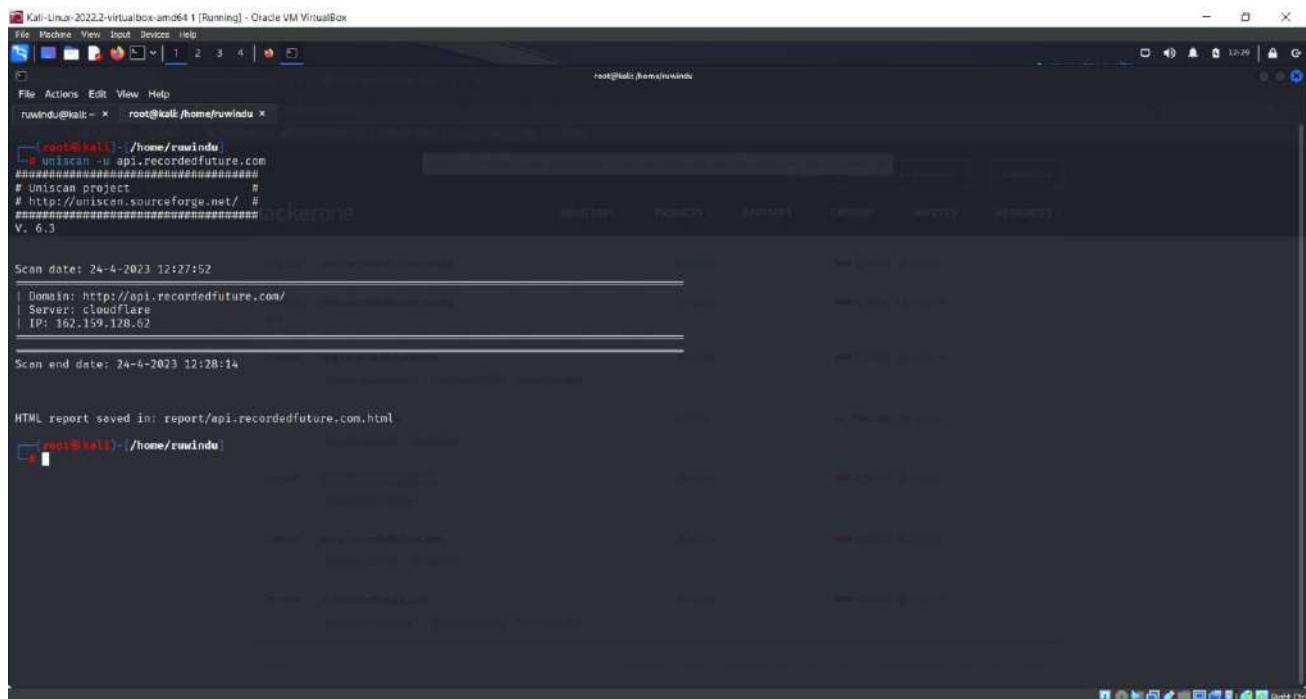
## Using knockpy tool

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.



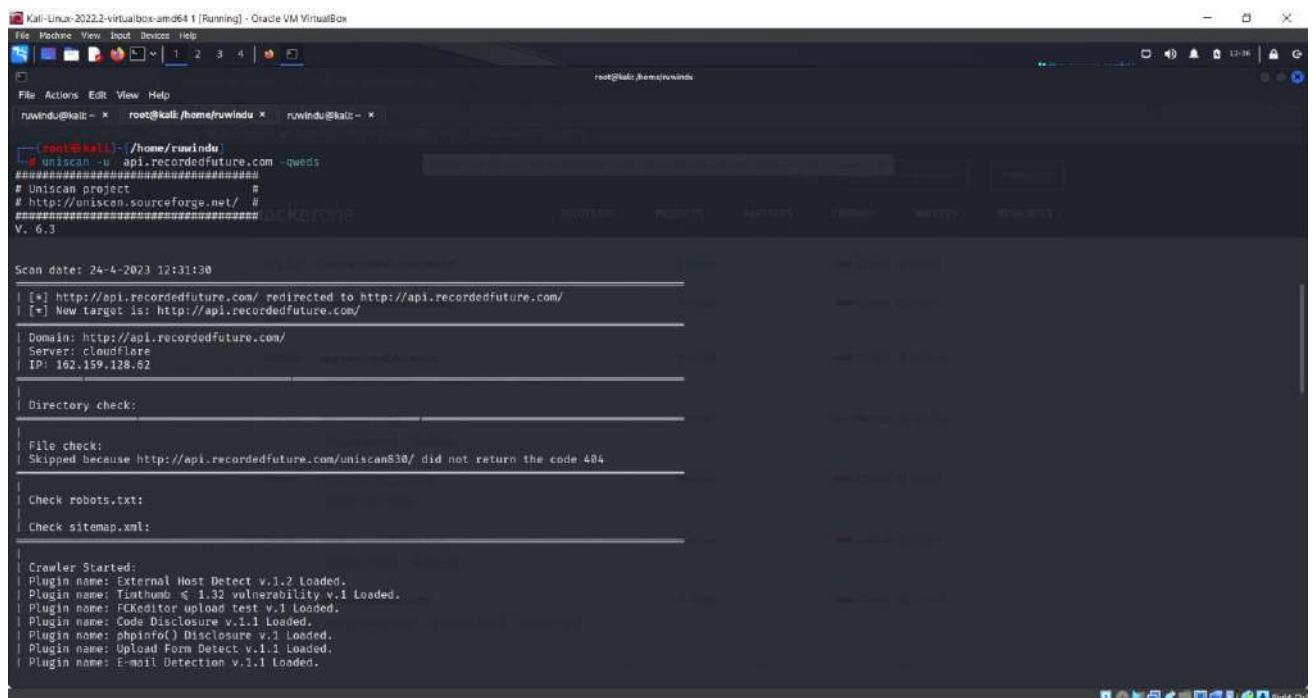
```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# uniscan -u api.recordedfuture.com
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 24-4-2023 12:27:52
Domain: http://api.recordedfuture.com/
Server: cloudflare
IP: 162.159.128.62

Scan end date: 24-4-2023 12:28:14

HTML report saved in: report/api.recordedfuture.com.html
root@kali:~#
```

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



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# uniscan -u api.recordedfuture.com -qweds
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 24-4-2023 12:31:30
[*] http://api.recordedfuture.com/ redirected to http://api.recordedfuture.com/
[*] New target is: http://api.recordedfuture.com/
Domain: http://api.recordedfuture.com/
Server: cloudflare
IP: 162.159.128.62

Directory check:
File check:
Skipped because http://api.recordedfuture.com/uniscan830/ did not return the code 404

Check robots.txt:
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: phpinfol() Disclosure v.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
```

```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# ./rwindsu -X
root@kali:/home/rwindsu# ./rwindsu@kali -X
[+] 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: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb's 1.32 vulnerability v.1 loaded.
Plugin name: File 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
```

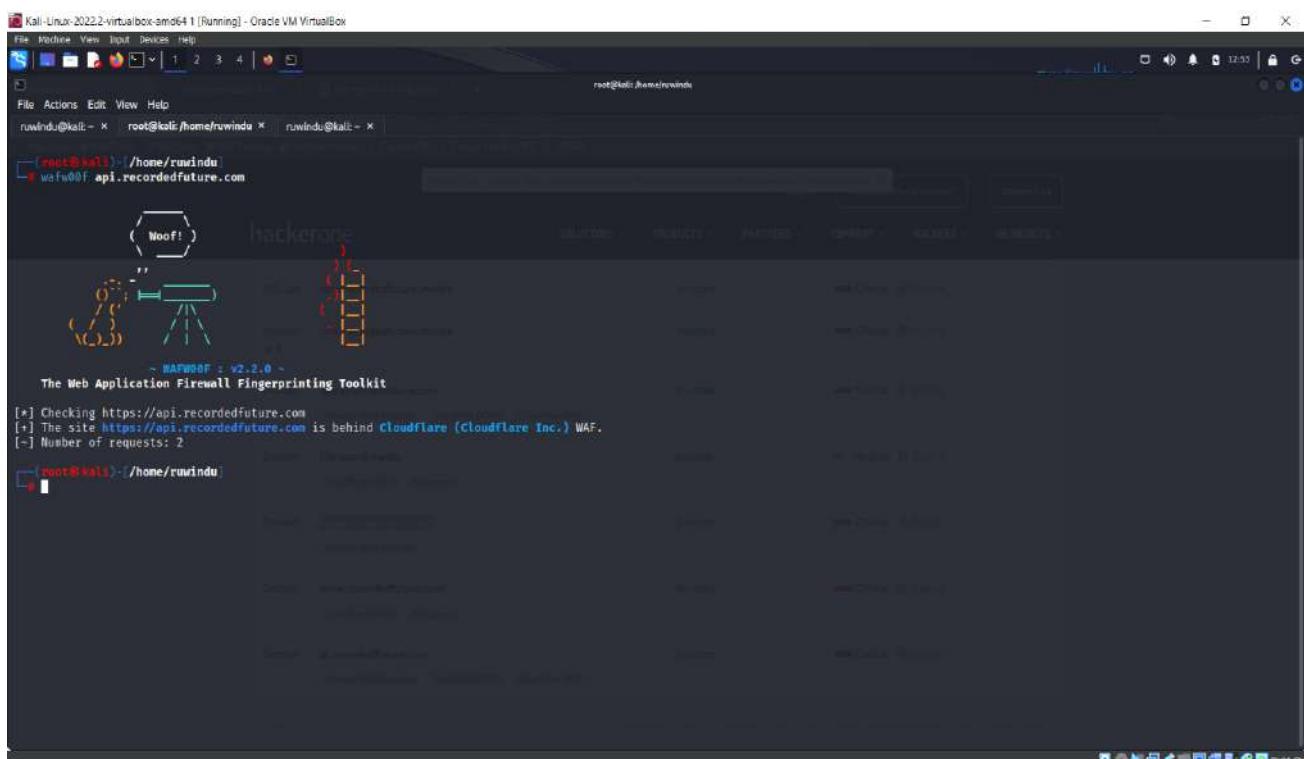
```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# ./rwindsu -X
root@kali:/home/rwindsu# ./rwindsu@kali -X
Local File Include:
PHP CGI Argument Injection:
Remote Command Execution:
Remote File Include:
SQL Injection:
Cross-Site 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.



```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Medhee View Input Devices Help
File Actions Edit View Help
root@kali: ~ | root@kali:/home/rwindu | root@kali: ~ |
[root@kali: ~] ./home/rwindu
[+] wafw00f api.recordedfuture.com
[!] Noof! hackerone
[!] WAFW00F v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://api.recordedfuture.com
[+] The site https://api.recordedfuture.com is behind Cloudflare (CloudFlare Inc.) WAF.
[-] Number of requests: 2
[root@kali: ~] ./home/rwindu
```

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

## Using OWASP-ZAP tool

The screenshot shows the OWASP-ZAP interface. In the top right, there's a status bar with "Current Scans: 0 Num Requests: 160 New Alerts: 28". Below it, the main window has tabs for History, Search, Alerts, Output, Spider, and Active Scan. The Alerts tab is selected, showing 28 new alerts. One alert is expanded, detailing an "Absence of Anti-CSRF Tokens" (WASC ID: 9) with a severity of "Passive (10202 - Absence of Anti-CSRF Tokens)". The alert description notes that CSRF attacks are effective in various situations, such as when the victim has an active session or is authenticated via HTTP auth. The solution section suggests using a vetted library or framework that does not allow this weakness to occur or provides constructs that make it easier to avoid.

Found 160 Requests.

This screenshot shows the OWASP-ZAP interface with the Alerts tab selected, displaying 15 new alerts. One specific alert is expanded: "Absence of Anti-CSRF Tokens" (WASC ID: 9). The alert details a "Passive (10202 - Absence of Anti-CSRF Tokens)" issue. It describes CSRF attacks and suggests using a vetted library or framework to avoid this weakness. The interface includes standard ZAP navigation and analysis tools.

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

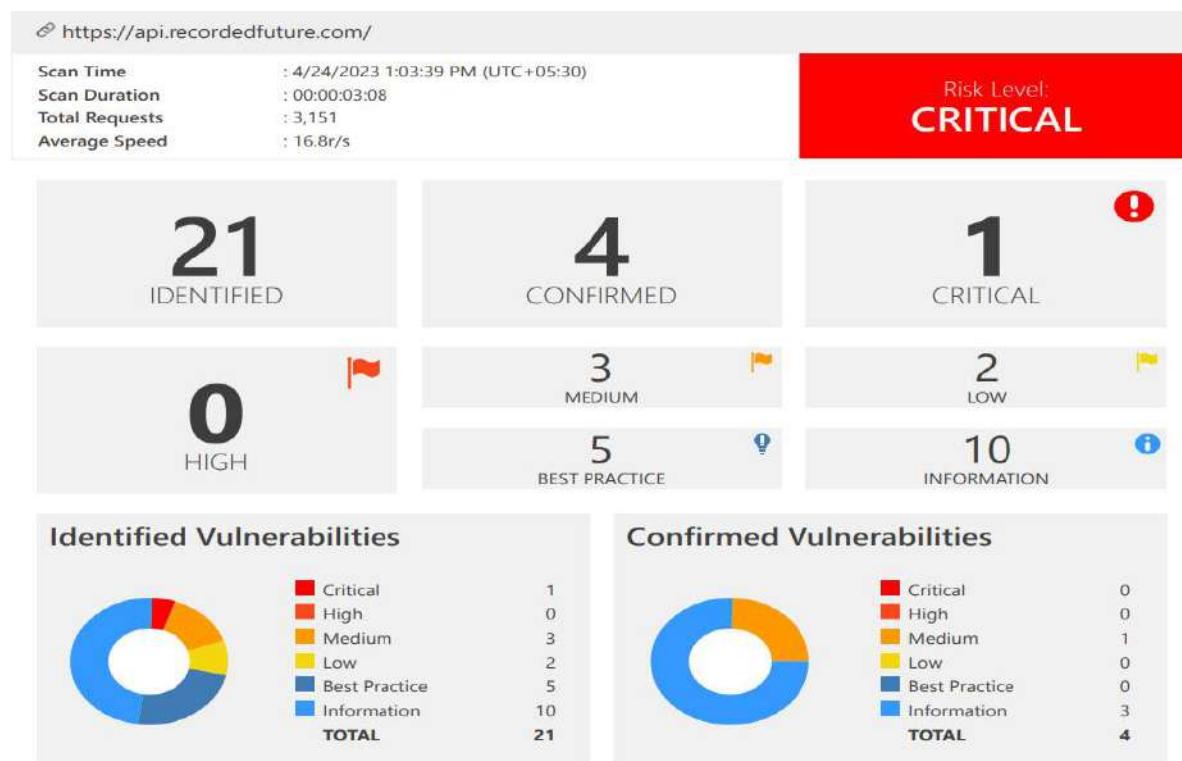
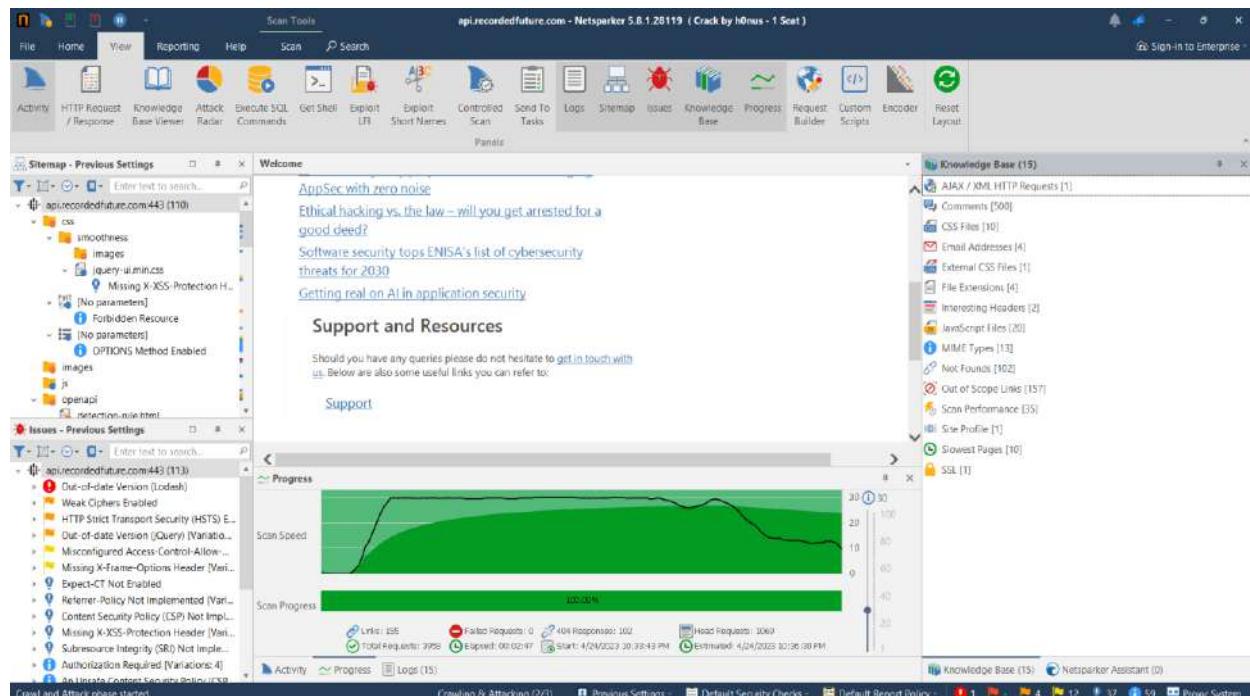
Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

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 |
|---------|---|--------|--|-----------|
| !       | <a href="#">Out-of-date Version (Lodash)</a>                              | GET    | https://api.recordedfuture.com/v2/   |           |
| !       | <a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a> | GET    | https://api.recordedfuture.com/  |           |
| !       | <a href="#">Out-of-date Version (jQuery)</a>                              | GET    | https://api.recordedfuture.com/v2/lib/jquery-1.8.0.min.js                              |           |
| !       | <a href="#">Weak Ciphers Enabled</a>                                      | GET    | https://api.recordedfuture.com/  |           |
| !       | <a href="#">Misconfigured Access Control-Allow-Origin Header</a>          | GET    | https://api.recordedfuture.com/v2/api-docs/swagger.json                                | URI-BASED |
| !       | <a href="#">Missing X-Frame-Options Header</a>                            | GET    | https://api.recordedfuture.com/v2/lib/   |           |
| !       | <a href="#">Content Security Policy (CSP) Not Implemented</a>             | GET    | https://api.recordedfuture.com/links   |           |
| !       | <a href="#">Expect-CT Not Enabled</a>                                     | GET    | https://api.recordedfuture.com/  |           |
| !       | <a href="#">Missing X-XSS-Protection Header</a>                           | GET    | https://api.recordedfuture.com/css/smoothness/jquery-ui.min.css                        |           |
| !       | <a href="#">Referrer-Policy Not Implemented</a>                           | GET    | https://api.recordedfuture.com/v2/lib/   |           |
| !       | <a href="#">Subresource Integrity (SRI) Not Implemented</a>               | GET    | https://api.recordedfuture.com/index.html?insext-%20d%20and%3Aanetsparka056650763dvuh. | INJECT    |
| !       | <a href="#">An Unsafe Content Security Policy (CSP) Directive In Use</a>  | GET    | https://api.recordedfuture.com/v2/lib/   |           |
| !       | <a href="#">data Used in a Content Security Policy (CSP) Directive</a>    | GET    | https://api.recordedfuture.com/v2/lib/   |           |
| !       | <a href="#">default-src Used in Content Security Policy (CSP)</a>         | 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

### Vulnerability 02 - 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

#### Vulnerabilities

1.1. <https://api.recordedfuture.com/v2/>

##### Identified Version

- 3.10.1

##### Latest Version

- 4.17.21 (in this branch)

##### Vulnerability Database

- Result is based on 04/18/2023 20:30:00 vulnerability database content.

#### Certainty



#### 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): 385.3754 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' 'unsafe-inline' 'unsafe-eval' cdn.jsdelivr.net; style-src 'self' 'unsafe-inline' fonts.googleapis.com cdn.jsdelivr.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: 7bcc91e8bfa7f11-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/highlight.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-polyfill.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/javascript'>
```

## 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

The screenshot shows the HackerOne interface with a list of reports on the left and a detailed view of a specific report on the right.

**Left Panel (Report List):**

- Open (3)
- Pending disclosure (0)
- Pending retests (0)
- All (4)
- Draft (0)

Search bar: Search all reports

Show filters

Recent reports:

- #1984171 Out-of-date Version (Lodash) - Recorded Future - Critical (Submitted May 11, 2023)
- #1984167 Cross-site Request Forgery - Recorded Future - Medium (Submitted May 11, 2023)
- #1984163 Phishing by Navigating Browser Tabs - Harvard - Medium (Submitted May 11, 2023)

**Right Panel (Report Detail):**

**Report Summary:** #1984171 Out-of-date Version (Lodash)

**Timeline:** darkkiller08 submitted a report to Recorded Future. [Edit Information] May 11th (1 min ago)

**Description:** 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.

**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.

**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

**Report Details (Right Side):**

- Reported May 11, 2023 9:43pm +0530
- darkkiller08
- Participants: 1
- State: New (Open)
- Reported to: Recorded Future
- Severity: Critical (9 ~ 10)
- Asset: Dom... api.recordedfuture.com
- Weakness: Out-of-bounds Read
- Time spent: None
- Visibility: Private
- CVE ID: None
- Account de... None

### **iii. Report 03**

#### **Target information: therecord.media**

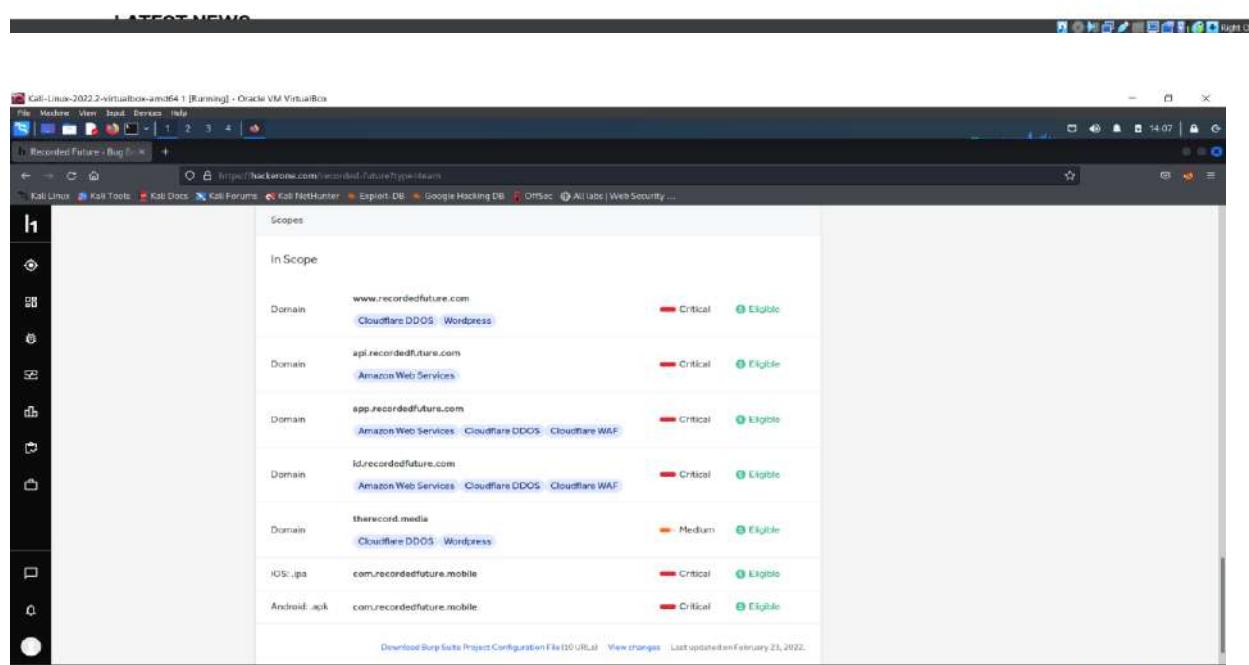
The purpose of this study is to determine whether vulnerabilities exist in the target domain (therecord.media) and the amount of risk that is associated with each of those vulnerabilities. The primary purpose of the evaluation is to identify any areas of the target domain that need improvement.



**Acting US National Cyber Director:**  
**'We're allowing the adversary to set our agenda'**

**Chinese-language threat group targeted a dozen South Korean institutions**

**Bipartisan legislation aims to 'arm Taiwan to the teeth in the cyber domain'**



| Scopes       | In Scope   | Risk Level | Status   |
|--------------|--|------------|----------|
| Domain       | www.recordedfuture.com<br>Cloudflare DDOS - Wordpress                            | Critical   | Eligible |
| Domain       | api.recordedfuture.com<br>Amazon Web Services                                    | Critical   | Eligible |
| Domain       | app.recordedfuture.com<br>Amazon Web Services - Cloudflare DDOS - Cloudflare WAF | Critical   | Eligible |
| Domain       | ld.recordedfuture.com<br>Amazon Web Services - Cloudflare DDOS - Cloudflare WAF  | Critical   | Eligible |
| Domain       | therecord.media<br>Cloudflare DDOS - Wordpress                                   | Medium     | Eligible |
| iOS:.ipa     | com.recordedfuture.mobile  | Critical   | Eligible |
| Android:.apk | com.recordedfuture.mobile  | Critical   | Eligible |

## 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.

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The address bar displays the URL <https://site-report.netcraft.com/?url=https://therecord.media>. The browser title bar reads "Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox". The Netcraft site report page is visible, containing detailed information about the domain `therecord.media`.

**Background**

| Site title  | Therecord from Recorded Future News   | Date first seen      | September 2020 |
|-------------|---|----------------------|----------------|
| Site rank   | 10408   | Netcraft Risk Rating | 8/10           |
| Description | The Record from Recorded Future News gives exclusive, behind-the-scenes access to leaders, policymakers, researchers, and the shadows of the cyber underground. | Primary language     | English        |

**Network**

| Site                    | https://therecord.media      | Domain                  | therecord.media   |
|-------------------------|------------------------------|-------------------------|---|
| Netblock Owner          | Fastly, Inc.                 | Nameserver              | hugh.no.cloudflare.com  |
| Hosting company         | Fastly                       | Domain registrar        | domain.ca   |
| Hosting country         | US                           | Nameserver organisation | whois.cloudflare.com  |
| IPv4 address            | 151.101.130.216 (reverse IP) | Organisation            | Domain Protection Services, Inc., Redacted For Privacy, REDACTED FOR PRIVACY, United States |
| IPv4 autonomous systems | AS58113                      | DNS admin               | dnscloudflare.com   |
| IPv6 address            | Not Present                  | Top Level Domain        | Media (.media)  |
| IPv6 autonomous systems | Not Present                  | DNS Security Extensions | Unknown   |
| Reverse DNS             | unknown                      |                         |   |

**IP delegation**

| IPv4 address (151.101.130.216) |  |
|--------------------------------|--|
|                                |  |

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

HackerOne R, The Record from Records Site report for https://the... +

https://sitereport.netcraft.com?url=https://thercord.media

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.

1 known tracker was identified.

**Companies**

**Categories**

| Company | Primary Category | Tracker          | Popular Sites with this Tracker            |
|---------|------------------|------------------|--|
| Google  | Analytics        | GoogleTagManager | www.nation.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.comiere.it |

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

HackerOne R, The Record from Records Site report for https://the... +

https://sitereport.netcraft.com?url=https://thercord.media

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

Google Analytics GoogleTagManager www.nation.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.comiere.it |

#### 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

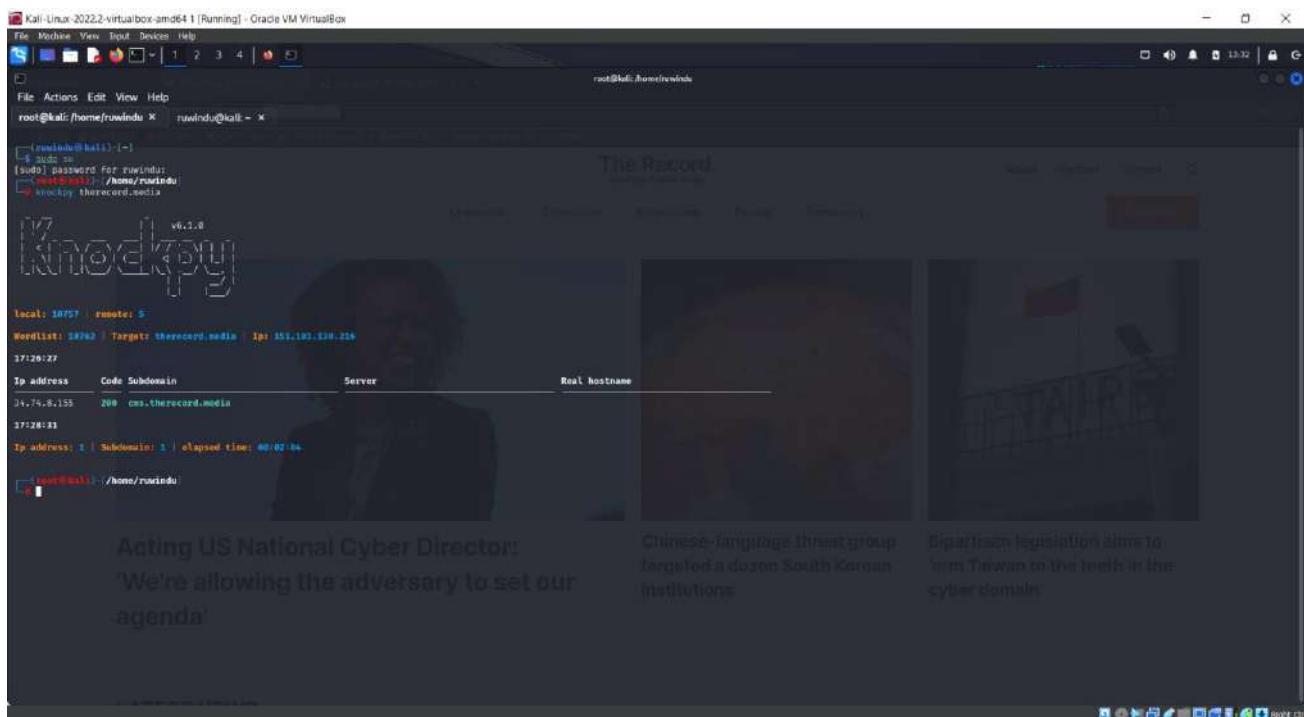
Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

| Technology | Description  | Popular sites using this technology              |
|------------|--|--|
| 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.

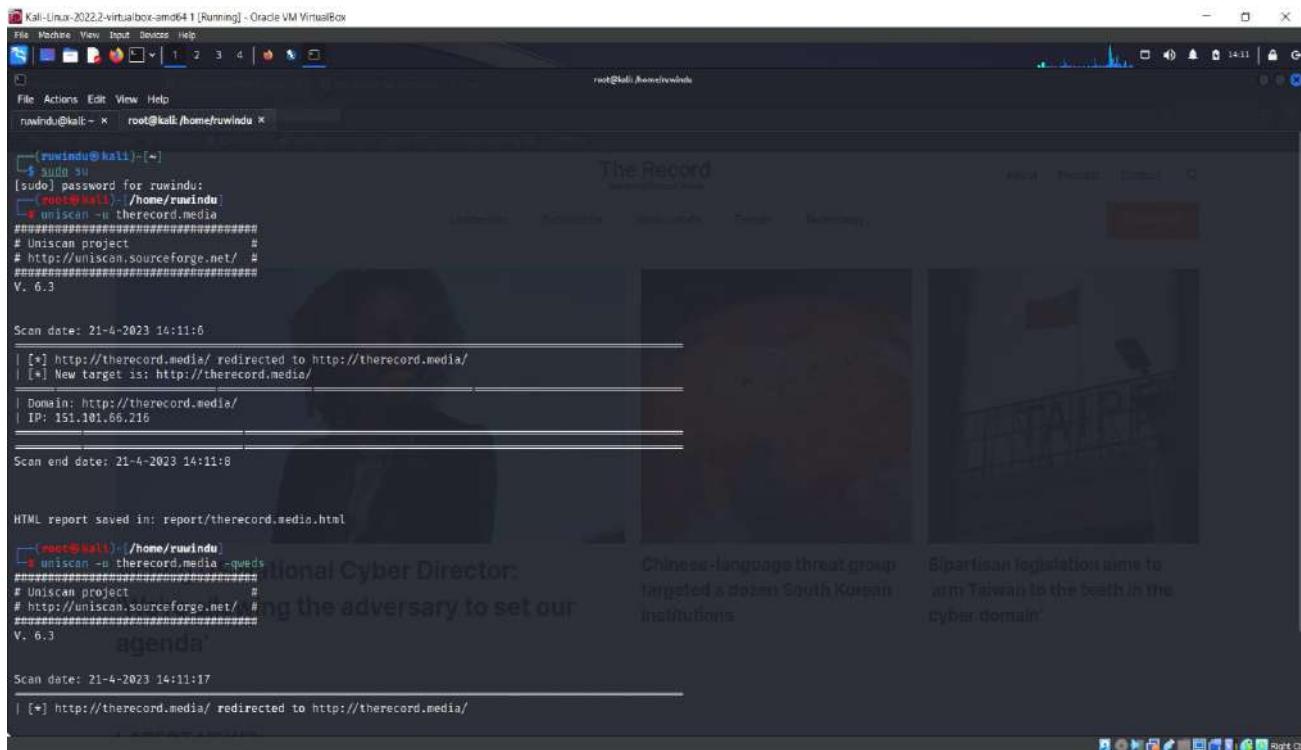


```
[root@kali: /home/rwindu] -> knockpy therecord.media
[sudo] password for rwindu:
[root@kali: /home/rwindu] -> knockpy therecord.media
[!] v6.1.0
[!] Local: 10757 Remote: 0
[!] Wordlist: 58962 Target: therecord.media | ips: 151.191.130.216
[!] 17:26:27
[!] Ip address      Code Subdomain           Server          Real hostname
[!] 34.74.8.155     200  cms.therecord.media
[!] 27:28:33
[!] Ip address      Subdomain      elapsed time: 00:02:04
[!] [root@kali: /home/rwindu]
```

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.



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
ruwindu@kali: ~ root@kali:/home/ruwindu ~

[ruwindu@kali:~]# sudo su
[sudo] password for ruwindu:
[ruwindu@kali: /home/ruwindu]
# uniscan -u therecord.media
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3

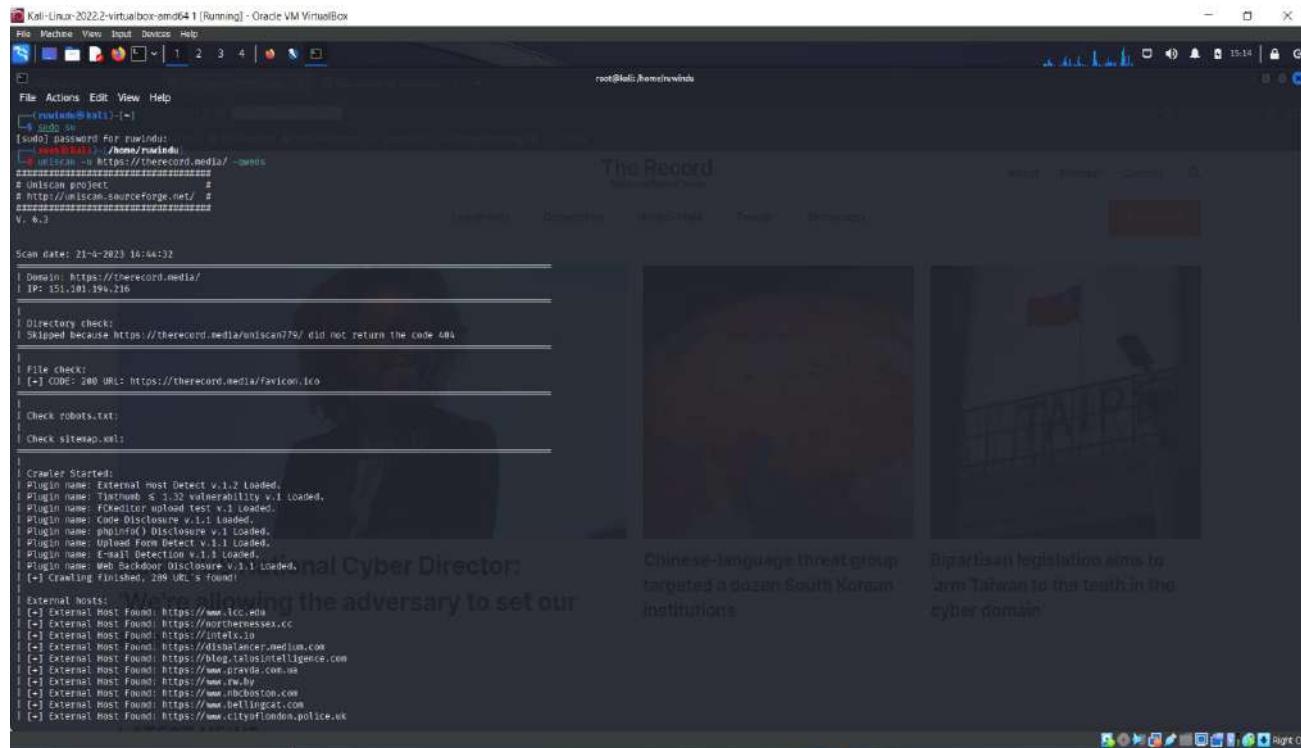
Scan date: 21-4-2023 14:11:0
[+] http://therecord.media/ redirected to http://therecord.media/
[+] New target is: http://therecord.media/
| Domain: http://therecord.media/
| IP: 151.101.66.216

Scan end date: 21-4-2023 14:11:8

HTML report saved in: report/therecord.media.html
[ruwindu@kali: /home/ruwindu]
# uniscan -u therecord.media -qweds
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3

Scan date: 21-4-2023 14:11:17
| [*] http://therecord.media/ redirected to http://therecord.media/
```

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



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
ruwindu@kali: ~ root@kali:/home/ruwindu ~

[ruwindu@kali:~]# sudo su
[sudo] password for ruwindu:
[ruwindu@kali: /home/ruwindu]
# uniscan -u https://www.semrush.com/ -qweds
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V. 6.3

Scan date: 21-4-2023 14:44:32
| Domain: https://www.semrush.com/
| IP: 151.101.194.216

| Directory check:
| Skipped because https://www.semrush.com/uniscan779/ did not return the code 404

| File check:
| (+) CODE: 200 URL: https://www.semrush.com/favicon.ico

| Check robots.txt:
| Check sitemap.xml:

| Crawler Started:
| Plugin name: External Host Detect v.1.2 loaded.
| Plugin name: Thumbn s 1.32 Vulnerability v.1 loaded.
| Plugin name: FOXeditor upload test v.1 loaded.
| Plugin name: Code Disclosure v.1.1 loaded.
| Plugin name: Exploit Finder v.1.1 loaded.
| Plugin name: Upload Form Detect v.1.1 loaded.
| Plugin name: Email Detection v.1.1 loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 loaded.
| (+) Crawling finished, 209 URLs found!

External Hosts:
[+] External Host Found: https://www.tcc.edu
[+] External Host Found: https://northernesssex.cc
[+] External Host Found: https://intelc10
[+] External Host Found: https://disbalancer.medium.co
[+] External Host Found: https://blog.tslosintelligence.com
[+] External Host Found: https://www.safesurfing.com.us
[+] External Host Found: https://www.rv.hv
[+] External Host Found: https://www.nbcBoston.com
[+] External Host Found: https://www.bellingcat.com
[+] External Host Found: https://www.cityoflondon.police.uk
```

A screenshot of a Kali Linux terminal window titled "root@kali:~" running on Oracle VM VirtualBox. The terminal displays a penetration test report from "The Record". The report lists findings such as PHPinfo() disclosure, file upload forms, emails, and various web-based vulnerabilities. In the background, there are several news articles visible, including one about the US National Cyber Director, another about a Chinese-language threat group targeting South Korean institutions, and a third about bipartisan legislation for Taiwan.

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

Kali-Linux-2022-2-virtualbox-smd64 1 [Running] - Oracle VM VirtualBox

File Medie View Input Devices Help

root@kali:~/home/rwlinu/PwnXSS

PWNXSS (rw's visual) https://github.com/pwnies/PwnXSS

<<<< STARTING >>>>

```
[15:25:06] [INFO] Starting PwnXSS ...
*****
[15:25:06] [INFO] Checking connection to: https://therecord.media/
[15:26:00] [INFO] Internal error: HTTPSConnectionPool(host='therecord.media', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f2ab2b10e0>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution'))
[15:26:00] [INFO] Connection established 200
*****
[15:26:07] [INFO] Checking connection to: https://therecord.media/news/leadership
[15:26:07] [INFO] Connection established 200
*****
[15:26:07] [INFO] Checking connection to: https://therecord.media/news/cybercrime
[15:26:08] [INFO] Connection established 200
*****
[15:26:08] [INFO] Checking connection to: https://therecord.media/news/nation-state
[15:26:08] [INFO] Connection established 200
*****
[15:26:09] [INFO] Checking connection to: https://therecord.media/news/people
[15:26:09] [INFO] Connection established 200
*****
[15:26:10] [INFO] Checking connection to: https://therecord.media/news/technology
[15:26:10] [INFO] Connection established 200
*****
[15:26:10] [INFO] Checking connection to: https://therecord.media/about
[15:26:11] [INFO] Connection established 200
*****
[15:26:11] [INFO] Checking connection to: https://therecord.media/author/aden-janefsky
[15:26:11] [INFO] Connection established 200
*****
[15:26:12] [INFO] Checking connection to: https://therecord.media/author/martin-metashok
[15:26:12] [INFO] Connection established 200
*****
[15:26:12] [INFO] Checking connection to: https://therecord.media/author/jonathan-gregg
[15:26:13] [INFO] Connection established 200
*****
[15:26:13] [INFO] Checking connection to: https://therecord.media/author/joe-worlinsky
[15:26:14] [INFO] Connection established 200
*****
[15:26:14] [INFO] Checking connection to: https://therecord.media/author/alexander-martin
[15:26:15] [INFO] Connection established 200
*****
```

The Record. The International News Source

Chinese-language threat group targeted A dozen South Korean institutions

Bipartisan legislation aims to arm Taiwan to the teeth in the cyber domain

```
Kali-Linux-2022.2-virtualbox-smd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] 15:33 | root@kali:~/Desktop/vmX5

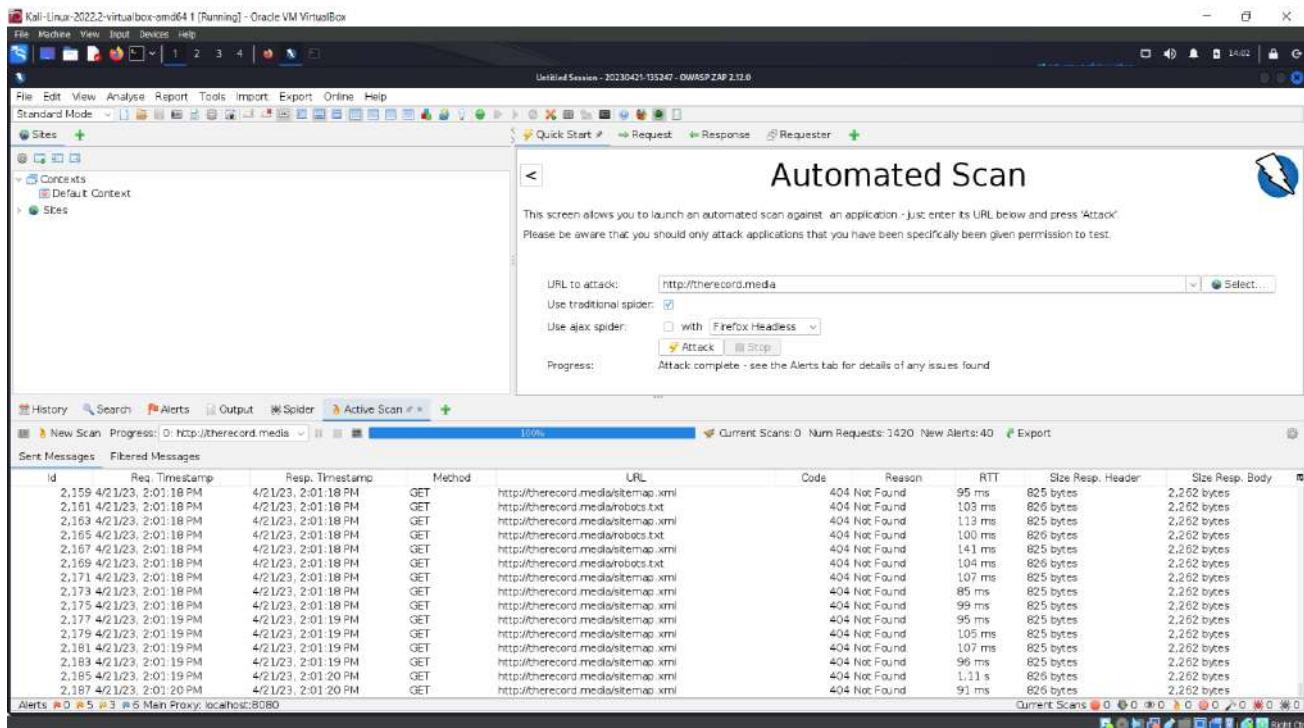
File Actions Edit View Help
[15:26:13] [INFO] Connection established 200
[15:26:13] [INFO] Checking connection to: https://therecord.media/author/adam-jane-feky
[15:26:13] [INFO] Connection established 200
*****
[15:26:12] [INFO] Checking connection to: https://therecord.media/author/martin-matishok
[15:26:12] [INFO] Connection established 200
*****
[15:26:12] [INFO] Checking connection to: https://therecord.media/author/jonathan-gregg
[15:26:12] [INFO] Connection established 200
*****
[15:26:12] [INFO] Checking connection to: https://therecord.media/author/joe-wormsky
[15:26:12] [INFO] Connection established 200
*****
[15:26:12] [INFO] Checking connection to: https://therecord.media/author/alexander-martin
[15:26:12] [INFO] Connection established 200
*****
[15:26:12] [INFO] Checking connection to: https://therecord.media/author/dina-temple-raston
[15:26:12] [INFO] Connection established 200
*****
[15:26:15] [INFO] Checking connection to: https://therecord.media/author/sean-powers
[15:26:15] [INFO] Connection established 200
*****
[15:26:16] [INFO] Checking connection to: https://therecord.media/author/will-jarvis
[15:26:16] [INFO] Connection established 200
*****
[15:26:17] [INFO] Checking connection to: https://therecord.media/podcast
[15:26:17] [INFO] Connection established 200
*****
[15:26:17] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-clear-the-runway-ukraines-model-pilots/id1225077306?i=<script>prompt(5000/200)</script>
[15:26:21] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:21] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-clear-the-runway-ukraines-model-pilots/id1225077306?i=<3script%3Eprompt%285000%2F200%29%3C%2Fscript%3E
[15:26:21] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:21] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-what-the-cyber-war-in-ukraine-is-teaching-us/id1225077306?i=<script>prompt(5000/200)</script>
[15:26:21] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:22] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-enemy-of-the-state-part-2-quebec-drone-whisperers-who/iid1225077306?i=<script>prompt(5000/200)</script>
[15:26:22] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:22] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-enemy-of-the-state-part-2-quebec-drone-whisperers-who/iid1225077306?i=<3script%3Eprompt%285000%2F200%29%3C%2Fscript%3E
[15:26:22] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:23] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-enemy-of-the-state-part-1-mexico-spyware/iid1225077306?i=<script>prompt(5000/200)</script>
[15:26:23] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:23] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-enemy-of-the-state-part-1-mexico-spyware/iid1225077306?i=<3script%3Eprompt%285000%2F200%29%3C%2Fscript%3E
[15:26:23] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:24] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-ukraines-drone-whisperers-what-the-weapons-are/iid1225077306?i=<script>prompt(5000/200)</script>
[15:26:24] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:24] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-ukraines-drone-whisperers-what-the-weapons-are/iid1225077306?i=<3script%3Eprompt%285000%2F200%29%3C%2Fscript%3E
[15:26:24] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=1800040593196# Maybe a vuln XSS point
[15:26:25] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/55-eyes-over-twenty-six-words-get-them-day-in/iid1225077206?i=<script>prompt(5000/200)</script>
[15:26:25] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=18000559492024# Maybe a vuln XSS point
[15:26:25] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/55-eyes-over-twenty-six-words-get-them-day-in/iid1225077206?i=<3script%3Eprompt%285000%2F200%29%3C%2Fscript%3E
[15:26:25] [INFO] Parameter page using (GET) payloads but not 100% yet ...
[WARNING] Found link with query: i=18000559492024# Maybe a vuln XSS point
```

```
Kali-Linux-2022.2-virtualbox-amd64-1 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
root@kali:~# ./pwnXSS
[15:26:23] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:23] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:23] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/57-why-the-state-part-1-mexico-spyware/id122507730671<script>prompt(5000/200)</script>
[15:26:25] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/57-why-the-state-part-1-mexico-spyware/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:27] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:27] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:27] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/56-ukraine-drone-whisperers-what-the-weapons-are/id122507730671<script>prompt(5000/200)</script>
[15:26:27] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/56-ukraine-drone-whisperers-what-the-weapons-are/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:29] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:29] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:29] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/55-oyez-oyez-twenty-six-words-get-their-day-in/id122507730671<script>prompt(5000/200)</script>
[15:26:29] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/55-oyez-oyez-twenty-six-words-get-their-day-in/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:30] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:30] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:30] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/54-its-a-little-bit-of-a-tale-with-hearts-and-the-money-notes/id122507730671<script>prompt(5000/200)</script>
[15:26:30] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/54-its-a-little-bit-of-a-tale-with-hearts-and-the-money-notes/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:32] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:32] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:32] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/53-x-is-brave-new-world/id122507730671<script>prompt(5000/200)</script>
[15:26:32] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/53-x-is-brave-new-world/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:33] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:33] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:34] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/52-special-feature-shoot-the-messenger-espionage/id122507730671<script>prompt(5000/200)</script>
[15:26:34] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/52-special-feature-shoot-the-messenger-espionage/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:36] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:36] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:36] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/51-x-is-still-wants-to-put-taser-drones-in-your-kids-school/id122507730671<script>prompt(5000/200)</script>
[15:26:36] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/51-x-is-still-wants-to-put-taser-drones-in-your-kids-school/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:38] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:38] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:38] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-lock-it-diaries-a-researchers-year-undercover/id122507730671<script>prompt(5000/200)</script>
[15:26:38] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/50-lock-it-diaries-a-researchers-year-undercover/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:40] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:40] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:40] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/49-encore-geshin-impacts-balances-nass-apocali-with/id122507730671<script>prompt(5000/200)</script>
[15:26:40] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/49-encore-geshin-impacts-balances-nass-apocali-with/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:42] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:42] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:42] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/48-call-me-cryptic-curious/id122507730671<script>prompt(5000/200)</script>
[15:26:42] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/48-call-me-cryptic-curious/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:43] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:43] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:43] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/47-special-feature-summer-in-caputh-from-exile/id122507730671<script>prompt(5000/200)</script>
[15:26:43] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/47-special-feature-summer-in-caputh-from-exile/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:45] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:45] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:45] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/46-encore-the-musicians-who-came-in-from-the-cold/id122507730671<script>prompt(5000/200)</script>
[15:26:45] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/46-encore-the-musicians-who-came-in-from-the-cold/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:47] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:47] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:47] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/44-encore-throwing-bricks-for-$$$-violence-as-a/id122507730671<script>prompt(5000/200)</script>
[15:26:47] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/44-encore-throwing-bricks-for-$$$-violence-as-a/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:49] [INFO] Parameter page using (GET) payloads but not 100% yet...
```

```
Kali-Linux-2022.2-virtualbox-amd64-1 [Running] - Oracle VM VirtualBox
File Actions Edit View Help
root@kali:~# ./pwnXSS
[15:26:57] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:57] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:57] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/39-the-supreme-court-case-that-could-change-the-internet/id122507730671<script>prompt(5000/200)</script>
[15:26:57] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/39-the-supreme-court-case-that-could-change-the-internet/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:26:59] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:26:59] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:26:59] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/38-prince-matters-nakasone-and-eastern-ukraine/id122507730671<script>prompt(5000/200)</script>
[15:26:59] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/38-prince-matters-nakasone-and-eastern-ukraine/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:01] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:01] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:01] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/37-the-hijab-will-never-be-the-same/id122507730671<script>prompt(5000/200)</script>
[15:27:01] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/37-the-hijab-will-never-be-the-same/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:03] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:03] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:03] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/35-encore-reality-winner-and-the-handling/id122507730671<script>prompt(5000/200)</script>
[15:27:03] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/35-encore-reality-winner-and-the-handling/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:04] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:04] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:04] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/34-encore-matters-nakasone-and-eastern-ukraine/id122507730671<script>prompt(5000/200)</script>
[15:27:04] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/34-encore-matters-nakasone-and-eastern-ukraine/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:06] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:06] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:06] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/33-throwing-bricks-for-$$$-violence-as-a-service-comics-of-age/id122507730671<script>prompt(5000/200)</script>
[15:27:06] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/33-throwing-bricks-for-$$$-violence-as-a-service-comics-of-age/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:08] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:08] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:08] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/32-the-great-tractor-jailbreak/id122507730671<script>prompt(5000/200)</script>
[15:27:08] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/32-the-great-tractor-jailbreak/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:10] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:10] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:10] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/31-seagulls-in-the-park/id122507730671<script>prompt(5000/200)</script>
[15:27:10] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/31-seagulls-in-the-park/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:12] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:12] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:12] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/30-the-scariest-piece-of-malware-since-stuxnet/id122507730671<script>prompt(5000/200)</script>
[15:27:12] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/30-the-scariest-piece-of-malware-since-stuxnet/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:14] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:14] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:14] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/29-the-musicians-who-came-in-from-the-cold/id122507730671<script>prompt(5000/200)</script>
[15:27:14] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/29-the-musicians-who-came-in-from-the-cold/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:16] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:16] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:16] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/28-a-return-to-stansluv/id122507730671<script>prompt(5000/200)</script>
[15:27:16] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/28-a-return-to-stansluv/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:18] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:18] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:18] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/27-exclusive-north-koreas-monster-fake-out/id122507730671<script>prompt(5000/200)</script>
[15:27:18] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/27-exclusive-north-koreas-monster-fake-out/id122507730671<3>script<3>prompt2850002f2000293c2fscriptk3e
[15:27:20] [INFO] Parameter page using (GET) payloads but not 100% yet...
[15:27:20] [WARNING] Found link with query: i=1000500210755 Maybe a vuln XSS point
[15:27:20] [INFO] Query (GET) : https://podcasts.apple.com/us/podcast/26-a-return-to-stansluv/id122507730671<script>prompt(5000/200)</script>
```

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.

The screenshot shows the OWASP ZAP interface. At the top, a browser window displays a page from 'theRecord.media/news/leadership' with various HTTP headers and a portion of the page source code. Below the browser is a navigation bar with tabs like File, Edit, View, Analyse, Report, Tools, Import, Export, Online, Help, and Standard Mode. The main pane is titled 'Alerts' and lists 23 alerts. One alert is expanded, showing detailed information about 'Re-examine Cache-control Directives'. The alert includes fields for URL (https://thercord.media/news/leadership), Risk (Informational), Confidence (Low), Parameter (Cache-Control), Attack, Evidence (s-maxage=60, stale-while-revalidate), CWE ID (525), WASC ID (13), Source (Passiva (10015 - Re-examine Cache-control Directives)), Input Vector, Description (The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.), and Other Info. At the bottom of the alert pane, there are buttons for 'Current Scans' and other tool icons.

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.

## Vulnerability Summary

| CONFIRM | VULNERABILITY   | METHOD | URL  | PARAMETER |
|---------|---|--------|--|-----------|
| 1       | <a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a> | GET    | <code>https://thererecord.media/</code>        |           |
| 1       | <a href="#">Weak Ciphers Enabled</a>                                      | GET    | <code>https://thererecord.media/</code>        |           |
| 1       | <a href="#">[Possible] Phishing by Navigating Browser Tabs</a>            | GET    | <code>https://thererecord.media/podcast</code> |           |
| 1       | <a href="#">Missing X-Frame-Options Header</a>                            | GET    | <code>https://thererecord.media/</code>        |           |
| 1       | <a href="#">Cookie Not Marked as HttpOnly</a>                             | GET    | <code>https://thererecord.media/</code>        |           |
| 1       | <a href="#">Cookie Not Marked as Secure</a>                               | GET    | <code>https://thererecord.media/</code>        |           |
| 1       | <a href="#">Insecure Frame (External)</a>                                 | GET    | <code>https://thererecord.media/</code>        |           |
| 1       | <a href="#">Content Security Policy (CSP) Not Implemented</a>             | GET    | <code>https://thererecord.media/</code>        |           |

|   |  |     |   |
|---|--|-----|---|
| 1 | Weak Ciphers Enabled                           | GET | https://therecord.media/  |
| 1 | [Possible] Phishing by Navigating Browser Tabs | GET | https://therecord.media/podcast   |
| 1 | Missing X-Frame-Options Header                 | GET | https://therecord.media/  |
| 1 | Cookie Not Marked as HttpOnly                  | GET | https://therecord.media/  |
| 1 | Cookie Not Marked as Secure                    | GET | https://therecord.media/  |
| 1 | Insecure Frame (External)                      | GET | https://therecord.media/  |
| 1 | Content Security Policy (CSP) Not Implemented  | GET | https://therecord.media/  |
| 1 | Expect-CT Not Enabled                          | GET | https://therecord.media/  |
| 1 | Missing X-XSS-Protection Header                | GET | https://therecord.media/  |
| 1 | Referrer-Policy Not Implemented                | GET | https://therecord.media/  |
| 1 | Subresource Integrity (SRI) Not Implemented    | GET | https://therecord.media/sudan-internet-shut-down-amid-fightin<br>g      |
| 1 | Email Address Disclosure                       | GET | https://therecord.media/_next/static/chunks/735-7645aca2d7173<br>1dd.js |
| 1 | Generic Email Address Disclosure               | GET | https://therecord.media/_next/static/chunks/735-7645aca2d7173<br>1dd.js |
| 1 | Forbidden Resource                             | GET | https://therecord.media/?nsextt=%0d%0ans%3anetsparker05665<br>0%3dvuln  |

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.

**Vulnerabilities**

3.1. <https://therecord.media/?s=>

| Method | Parameter | Value |
|--------|-----------|-------|
| GET    | s         |       |

**Form Action(s)**

- /?s=&\_cf\_chl\_f\_tk=XVxvvLf9KF444YydLsI3.KqC9G31qmxcY7r0ihWtgZ4-1683222157-0-gaNycGzNCDs

**Certainty**

**Request**

```
GET /?s= HTTP/1.1
Host: therecord.media
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://therecord.media/
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) : 97.6691 Total Bytes Received : 7666 Body Length : 6724 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Cross-Origin-Embedder-Policy: require-corp
Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
CF-RAY: 7c228a96afb2b2f9-CMB
Strict-Transport-Security: max-age=31536000; includeSubDomains
Transfer-Encoding: chunked
Server: cloudflare
Connection: close
Cross-Origin-Resource-Policy: same-origin
Expires: Thu, 01 Jan 1970 00:00:01 GMT
X-Frame-Options: SAMEORIGIN
Vary: Accept-Encoding
Referrer-Policy: same-origin
cf-mitigated: challenge
Content-Type: text/html; charset=UTF-8
Cross-Origin-Opener-Policy: same-origin
Permissions-Policy: accelerometer=(),autoplay=(),camera=(),clipboard-read=(),clipboard-write=(),fullscreen=(),geolocation=(),gyroscope=(),hid=(),interest-cohort=(),magnetometer=(),microphone=(),payment=(),publickey-credentials-get=(),screen-wake-lock=(),serial=(),sync-xhr=(),usb=()
Date: Thu, 04 May 2023 17:42:37 GMT
Content-Encoding:

<!DOCTYPE html>
<html lang="en-US">
<head>
<title>Just a moment...</title>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=Edge">
<meta name="robots" content="noindex,nofollow">
<meta name="viewport" content="width=device-width,initial-scale=1">
<link href="/cdn-cgi/styles/challenges.css" rel="stylesheet">
<meta http-equiv="refresh" content="35">

</head>
<body class="no-js">
<div class="main-wrapper" role="main">
<div class="main-content">
<noscript>
<div id="challenge-error-title">
<div class="h2">
<span class="icon-wrapper">
<div class="heading-icon warning-icon"></div>
</span>
<span id="challenge-error-text">
Enable JavaScript and cookies to continue
</span>
</div>
```

## 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 XMLHttpRequest.

## 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

The screenshot shows the HackerOne interface with a sidebar on the left containing navigation links: Opportunities, Dashboard, Inbox (highlighted in green), Hacktivity, Leaderboard, Directory, Job Board, Nav Feedback, Notifications (with 1 notification), and Profile. The main content area displays a report for a "Cross-site Request Forgery" vulnerability. The report details include:

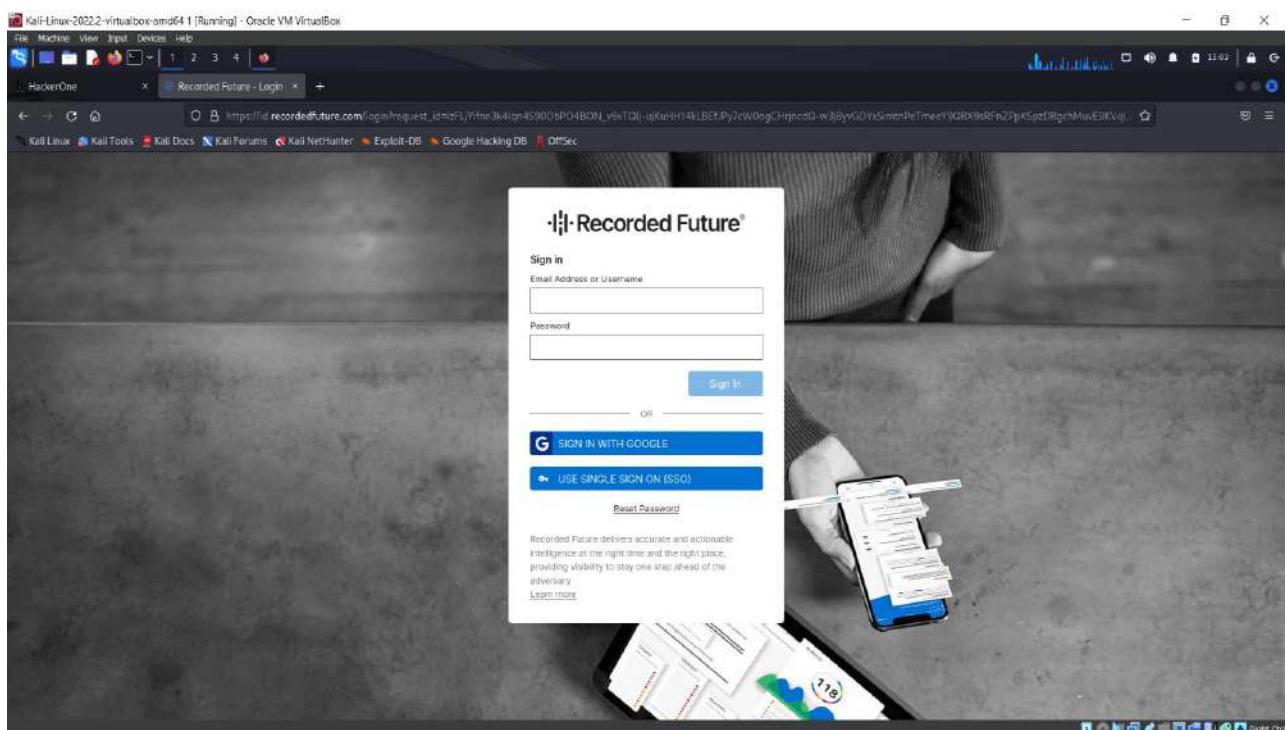
- Reported:** May 11, 2023 9:38pm +0530
- Reporter:** darkkiller08
- Participants:** darkkiller08
- State:** New (Open)
- Reported to:** Recorded Future (Managed)
- Severity:** Medium (4 - 6.9)
- Asset:** Dom... therecord.media
- Weakness:** Cross-Site Request Forgery (CSRF)
- Time spent:** 3h
- Visibility:** Private
- CVE ID:** None
- Account de...:** None

The report itself contains sections for ADD HACKER SUMMARY, TIMELINE - EXPORT, Solution, Impact, and a detailed description of the vulnerability found by Netsparker.

## **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 | Running - Oracle VM VirtualBox

HackerOne Site report for http://app.recordedfuture.com

<https://site.report.netcraft.com/?url=http://app.recordedfuture.com>

NETCRAFT

**Background**

|             |                         |                      |          |
|-------------|-------------------------|----------------------|----------|
| Site title  | Recorded Future - Login | Date first seen      | May 2017 |
| Site rank   | 4821                    | Netcraft Risk Rating | 0.10     |
| Description | Not Present             | Primary language     | English  |

**Network**

|                         |                               |                         |  |
|-------------------------|-------------------------------|-------------------------|--|
| Site                    | http://app.recordedfuture.com | Domain                  | recordedfuture.com   |
| Netblock Owner          | Cloudflare, Inc.              | Nameserver              | hugh.us.cloudflare.com   |
| Hosting company         | Cloudflare                    | Domain registrar        | name.com   |
| Hosting country         | US                            | Nameserver organisation | whois.cloudflare.com   |
| IPv4 address            | 104.18.7.66 (located in US)   | Organisation            | Domain Protector Services, Inc., PO Box 1769, Denver, 80201, United States |
| IPv4 autonomous systems | AS32339                       | 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                         |
| 104.18.7.66/24             | 104.18.7.0/24 | United States | IANA IPv4 MAPPED ADDRESS | Internet Assigned Numbers Authority |

Read static.netcraft.com

Kali-Linux-2022.2-virtualbox-amd64 | Running - Oracle VM VirtualBox

HackerOne Site report for http://app.recordedfuture.com

<https://site.report.netcraft.com/?url=http://app.recordedfuture.com>

NETCRAFT

**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 Script | A server-side Java programming language class | www.tutorialspoint.com, www.aliexpress.com, jp2catholicpowerschool.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.

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Edit View Input Devices Help

(rwindu㉿kali):~\$

8 sudo su  
(sudo) password for rwindu:  
root@kali: /home/rwindu  
# ./enum4linux app.recordedfuture.com

v6.3.0

local: 10757 | remote: 1

Wordlist: 38758 | Target: app.recordedfuture.com | Ip: 104.18.6.66

37:28:54

| Ip address  | Code Subdomain | Server | Real hostname |
|---|----------------|--------|---------------|
| 17:38:26  |                |        |               |
| Ip address: #   Subdomain: #   elapsed time: 00:03:31 |                |        |               |
| (root㉿kali):/home/rwindu\$                            |                |        |               |

Running 1000 threads - 1000 ports - 1000 services

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.

```
Kali-Linux-2022.2-virtualbox-amd64.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[ 1 2 3 4 ] 🌐 🔍
root@kali:~# uniscan -u app.recordedfuture.com
[sudo] password for ruwindu:
(root@kali) [~]
$ sudo su
[uniscan] password for ruwindu:
(root@kali) [/home/ruwindu]
# uniscan -u app.recordedfuture.com
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 25-4-2023 13:36:54
| Domain: http://app.recordedfuture.com/
| Server: cloudflare
| IP: 104.18.6.66

Scan end date: 25-4-2023 13:36:54

HTML report saved in: report/app.recordedfuture.com.html

(root@kali) [/home/ruwindu]
# uniscan -u app.recordedfuture.com -qweds
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
```

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

```
Kali-Linux-2022.2-virtualbox-amd64.1 [Running] - Grade VM VirtualBox
File Machine View Input Devices Help
root@Kali:~# uniscan -u app.recordedfuture.com -qweds
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 25-4-2023 13:37:27

| Domain: http://app.recordedfuture.com/
| Server: cloudflare
| IP: 104.18.7.66

| Directory check:
| Skipped because http://app.recordedfuture.com/uniscan810/ did not return the code 404

| File check:
| Skipped because http://app.recordedfuture.com/uniscan895/ did not return the code 404

| Check robots.txt:
| 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.
```

```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
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: FCKeditor tests v.1.1 Loaded.
Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
Plugin name: Ffm 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
```

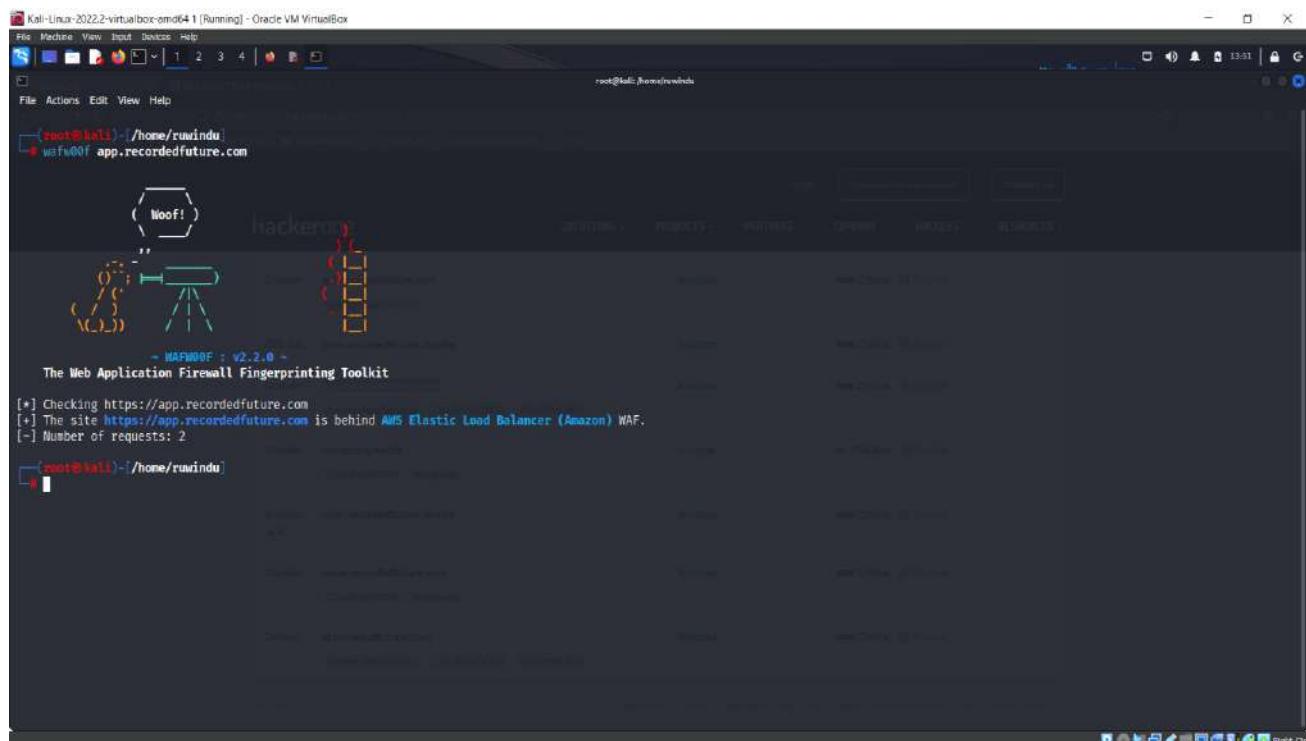
```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
Remote Command Execution:
Remote File Include:
SQL Injection:
Cross-Site Scripting (XSS):
Web Shell Finder:
Static tests:
Plugin name: Local File Include tests v.1.1 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 13:39:6

HTML report saved in: report/app.recordedfuture.com.html
[root@kali ~]# /home/rwinda
```

## 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.



```
Kali-Linux-2022.2-virtualbox-omg64-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
[root@kali:~]# ./wafw00f app.recordedfuture.com
[!] Checking https://app.recordedfuture.com
[+] The site https://app.recordedfuture.com is behind AWS Elastic Load Balancer (Amazon) WAF.
[-] Number of requests: 2
[root@kali:~]
```

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

The screenshot shows the OWASP-ZAP 2.12.0 interface. In the center, the 'Automated Scan' dialog is open, prompting the user to enter a URL to attack. The URL 'http://app.recordedfuture.com' is already entered. Below the dialog, the 'Output' tab is active, displaying a table of 100 requests. The table includes columns for Id, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Header, and Size Resp. Body. The 'Alerts' tab is also visible at the bottom.

Found 100 Requests.

The screenshot shows the OWASP-ZAP 2.12.0 interface with the 'Alerts' tab selected. A specific alert for Content Security Policy (CSP) is highlighted. The 'Description' section explains that Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. It states that 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. The 'Other Info' section notes that 'style-src' includes 'unsafe-inline'. The 'Solution' section advises ensuring that the web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header. The 'Reference' section provides a link to the Mozilla CSP specification.

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.

| Parameter: Content-Security-Policy |   |
|------------------------------------|---|
| Attack:                            | default-src 'self' blob; style-src 'self' 'unsafe-inline' *.googleapis.com; script-src 'self' blob; 'nonce-d5bc67fb-7612-4d8a-baea-e8e9271d6d2f' maps.googleapis.com googleapis.com profservice.s.recordedfuture.com www.recordedfuture.com app.recordedfuture.com; font-src 'self' data: *.gstatic.com; img-src 'self' *.googleapis.com *.google.com googleapis.com *.googleusercontent.com *.ggph.com data: d3ts35pk9eeaj.cloudfront.net *.gstatic.com profservices.recordedfuture.com www.firebaseio.com https://s3.walkmeusercontent.com; connect-src 'self' rmainitenance.s3-website-us-east-1.amazonaws.com googleapis.com *.googleapis.com *.google.com https://*.gstatic.com data: blob: https://ase.recordedfuture.com; object-src 'none'; frame-src 'self' blob: maps.google.com www.google.com; report-uri /rf/kobradata/csp_report/?disposition=enforce |
| Evidence:                          | .com *.ggph.com data: d3ts35pk9eeaj.cloudfront.net *.gstatic.com profservices.recordedfuture.com www.firebaseio.com https://s3.walkmeusercontent.com; connect-src 'self' rmainitenance.s3-website-us-east-1.amazonaws.com googleapis.com *.googleapis.com *.google.com https://*.gstatic.com data: blob: https://ase.recordedfuture.com; object-src 'none'; frame-src 'self' blob: maps.google.com www.google.com; report-uri /rf/kobradata/csp_report/?disposition=enforce   |
| CWE ID:                            | 693   |
| WASCID:                            | 15  |
| Source:                            | Passive (10055 - CSP)   |

## Solution

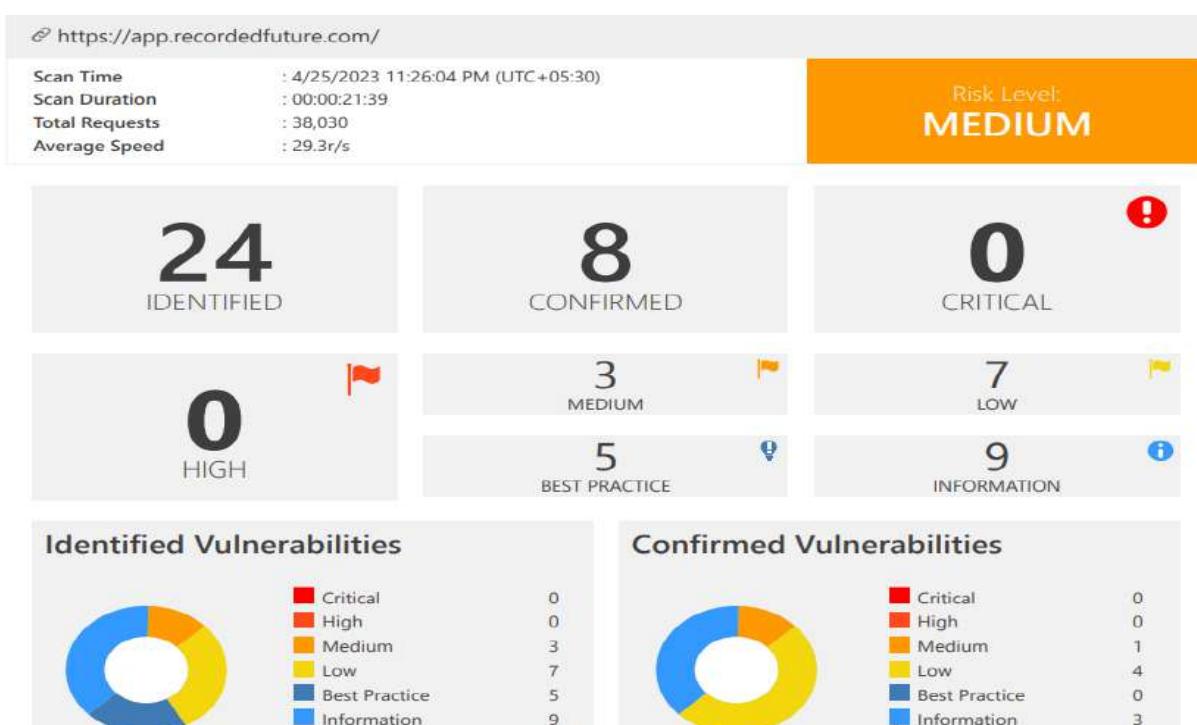
Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.

| Alert Tags:    |   |
|----------------|---|
| Key            | Value   |
| OWASP_2021_A05 | <a href="https://owasp.org/Top10/A05_2021-Security_Misconfiguration/">https://owasp.org/Top10/A05_2021-Security_Misconfiguration/</a>   |
| OWASP_2017_A06 | <a href="https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html">https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html</a> |

## 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.

The screenshot shows the Netsparker interface with a scan in progress. The main window displays a tree view of the website's structure under 'Sitemap - Previous Settings'. A central panel shows 'Updates' with links to scanner announcements and change logs. Below it is the 'Web Application Security Blog' section. On the right, a 'Knowledge Base' sidebar lists various security topics with counts. At the bottom, a 'Progress' bar indicates the scan is at 99% completion. The status bar at the bottom shows 'Report successfully exported' and various system metrics.



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

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

## Response

Response Time (ms) : 29.8966 Total Bytes Received : 198 Body Length : 0 Is Compressed : No

HTTP/1.1 404 Not Found  
Server: cloudflare  
X-Content-Type-Options: nosniff  
Connection: keep-alive  
CF-RAY: 7c224287bcc77f23-CMB  
Transfer-Encoding: chunked  
Date: Thu, 04 May 2023 16:53:26 GMT

## 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.

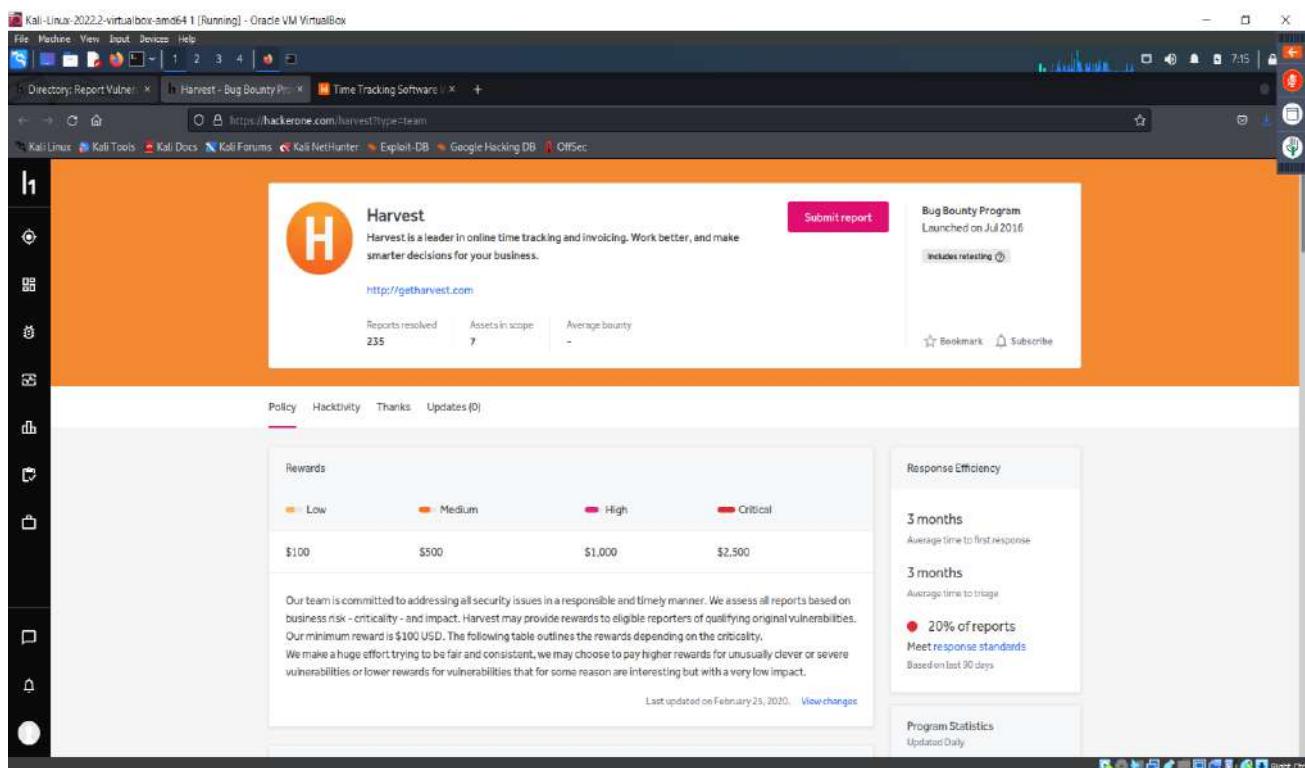
## HackerOne Submitted Report Screenshot

The screenshot shows the HackerOne interface. On the left is a sidebar with navigation links: Opportunities, Dashboard (selected), Inbox (highlighted in green), Hacktivity, Leaderboard, Directory, Job Board, Nav Feedback, Notifications, and Profile. The main content area displays a report for issue #1984175 titled "Missing X-XSS-Protection Header". The report details a finding from "darkkiller08" submitted on May 11th. It describes a potential XSS attack due to the absence of the X-XSS-Protection header. A "Solution" section suggests adding the header with a value of "1; mode=block". The "Impact" section notes no immediate implications. On the right, the report's metadata is shown, including the reporter's name, state (New Open), reported to (Recorded Future), severity (Medium), asset (app.recordedfuture.com), weakness (Cross-site Scripting (XSS) - DOM), time spent (3h), visibility (Private), CVE ID (None), and account details (None). There is also a note about an attachment: "F2347661: app.recordedfuture.com\_Bug\_Bounty\_Report.pdf".

## 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.

The screenshot shows a web browser window titled "Kali-Linux-2022.2-virtualbox-amd64 1 (Running) - Oracle VM VirtualBox". The URL is https://hackerone.com/harvest/type-team. The page content includes:

- A legend for vulnerability criticality: Low (\$100), Medium (\$500), High (\$1,000), and Critical (\$2,500).
- A statement: "Our team is committed to addressing all security issues in a responsible and timely manner. We assess all reports based on business risk - criticality - and impact. Harvest may provide rewards to eligible reporters of qualifying original vulnerabilities. Our minimum reward is \$100 USD. The following table outlines the rewards depending on the criticality." (Note: The table above the statement is identical to the one in the previous text block.)
- A note: "We make a huge effort trying to be fair and consistent, we may choose to pay higher rewards for unusually clever or severe vulnerabilities or lower rewards for vulnerabilities that for some reason are interesting but with a very low impact."
- A timestamp: "Last updated on February 25, 2020. View changes"
- A "Policy" section:
  - At Harvest security is very important, our customers trust us with their data and we take this trust extremely seriously.
  - With this security bounty system, we aim to reward the work of security researchers who find issues with Harvest's suite of applications. Our team is committed to addressing all security issues in a responsible and timely manner.
- A "Rules for reporting" section:
  - If you find a security issue let us know and we will make every effort to resolve the issue as soon as possible. Please do not publicly disclose any details until Harvest has confirmed the bug has been fixed. If you provide us a reasonable amount of time to resolve it, we promise to get back to you quickly at each step of the resolution process.
- A "All bug reports should include" section:
  - A detailed step-by-step explanation of how to replicate the issue.
  - An Attack Scenario to demonstrate the risk.
- A "Rules for testing security Issues on Harvest" section:
  - Use test accounts. Please add +hackerone to your email address before the @, e.g. researcher+hackerone@example.com
- Program Statistics:
  - 3 months Average time to first response
  - 3 months Average time to triage
  - 20% of reports Meet response standards Based on last 90 days
  - \$38,950 Total bounties paid
  - \$500 - \$2,000 Top bounty range
  - \$0 Bounties paid in the last 20 days
  - 9 Reports received in the last 90 days
  - 9 months ago Last report resolved
  - 235 Reports resolved

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 screenshot shows the Burp Suite interface with a list of domains categorized as 'Out of Scope'. A red box highlights this section.

| Out of Scope |                         |          |          |
|--------------|-------------------------|----------|----------|
| Domain       | harveststatus.com       | Critical | Eligible |
| Domain       | help.getharvest.com     | Critical | Eligible |
| Domain       | getharvest.com/contact  | Critical | Eligible |
| Domain       | support.forecastapp.com | Critical | Eligible |

Download Burp Suite Project Configuration File (16 URLs) View changes Last updated on February 25, 2020.

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.

The screenshot shows the Burp Suite interface with a list of domains categorized as 'In Scope'. A red box highlights this section.

| In Scope            |   |          |          |
|---------------------|---|----------|----------|
| Domain              | harvestapp.com  | Critical | Eligible |
| Domain              | forecastapp.com   | Critical | Eligible |
| Domain              | id.getharvest.com   | Critical | Eligible |
| Domain              | getharvest.com  | Critical | Eligible |
| Other               | getharvest.com/mac<br>https://www.getharvest.com/mac                                  | Critical | Eligible |
| Android: Play Store | com.harvestapp<br>https://play.google.com/store/apps/details?id=com.harvestapp        | Critical | Eligible |
| iOS: App Store      | 355395846<br>https://itunes.apple.com/us/app/harvest-time-expense-tracker/id355395846 | Critical | Eligible |

## 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.

The screenshot shows a Kali Linux desktop environment within Oracle VM VirtualBox. The browser window displays the Netcraft Site Report for <https://www.getharvest.com>. The report includes sections for Background, Network, and Whois. The Network section provides details such as the site's IP address (199.60.103.225), hosting company (HubSpot, Inc.), and DNS admin (AS2199242). The Whois section shows the domain name as getharvest.com and the registrar as name.com.

| Background  | Network   | Whois  |
|---|---|--|
| Site title: Time Tracking Software With Invoicing   Harvest   Date first seen: November 2010  | Site IP: 199.60.103.225   Hosting Company: HubSpot, Inc.   DNS Admin: AS2199242 | Domain: getharvest.com   Registrar: name.com |
| Site rank: 47014   Netcraft Risk Rating: 0/10   | Hosting Country: US   Nameserver Organisation: whois.pr.org                     |  |
| Description: Time tracking and management software with powerful easy reporting and streamlined online invoicing. Loved by 75,000 businesses. Get started for free. | Organisation: Harvest, 16 W 22nd St, 8th Floor, New York, 10010, United States  |  |

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

Recorded Future - Bug Bounty X Recorded Future - Security X Harvest - Bug Bounty Pro X Time Tracking Software X Site report for https://www.getharvest.com X

https://sitereport.netcraft.com?url=https://www.getharvest.com

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.

| Company    | Primary Category | Tracker          | Popular Sites with this Tracker  |
|------------|------------------|------------------|--|
| Google     | Advertising      | Google AdSense   | <a href="http://www.arco.co.uk">www.arco.co.uk</a> , <a href="http://www.duolingo.com">www.duolingo.com</a> , <a href="http://www.walmart.com">www.walmart.com</a>     |
| Google     | Analytics        | GoogleTagManager | <a href="http://www.corriere.it">www.corriere.it</a> , <a href="http://www.coingecko.com">www.coingecko.com</a> , <a href="http://www.chess.com">www.chess.com</a>     |
| Optimizely | Analytics        | Optimizely       | <a href="http://www.imperva.com">www.imperva.com</a> , <a href="http://www.fexbusiness.com">www.fexbusiness.com</a> , <a href="http://www.aanda.com">www.aanda.com</a> |

## Site Technology

(fetched today)

### HTTP Accelerator

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

Recorded Future - Bug Bounty X Recorded Future - Security X Harvest - Bug Bounty Pro X Time Tracking Software X Site report for https://www.getharvest.com X

https://sitereport.netcraft.com?url=https://www.getharvest.com

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 | <a href="http://www.chess.com">www.chess.com</a> , <a href="http://www.coingecko.com">www.coingecko.com</a> , <a href="http://www.ecosia.org">www.ecosia.org</a> |

## 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  | <a href="http://www.microsoft.com">www.microsoft.com</a> , <a href="http://www.roblox.com">www.roblox.com</a> , <a href="http://www.qwant.com">www.qwant.com</a> |
| JavaScript              | Widely-supported programming language commonly used to power client-side dynamic content on websites. |  |

## Using knockpy tool

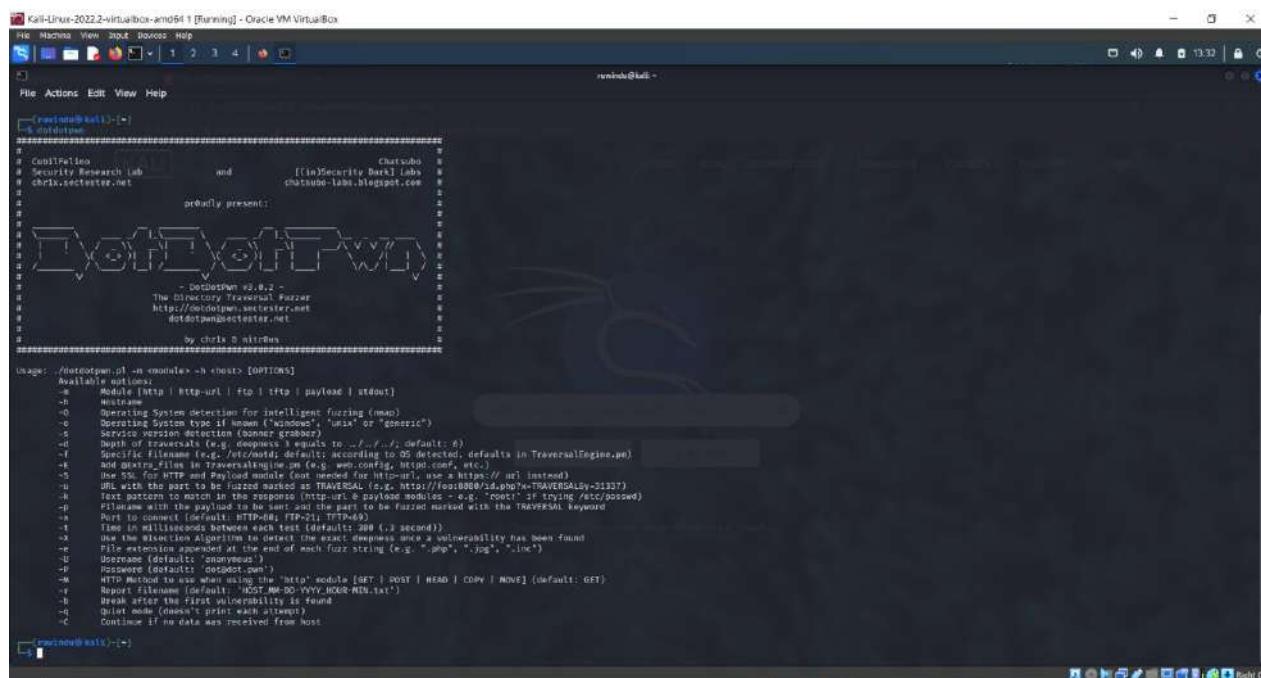
In order for us to get to the bottom of what has really taken place here, we are going to need to do a subdomain scanning using software that is created specifically for that purpose. Only then will we be able to get all of the questions we have answered. First, we give knockpy a go on both domains, 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.

A screenshot of a Kali Linux terminal window titled "root@kali:~#". The terminal shows two main sections of output. The top section is a knockipy exploit command with its results: "knockipy.getharvest.com folder not exists or not writable: knockipy\_report". The bottom section is a getharvest scan with a banner: "More than time tracking". It lists various IP addresses, codes, subdomains, servers, and real hostnames. A progress bar at the bottom indicates the scan is 100% complete.

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](https://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

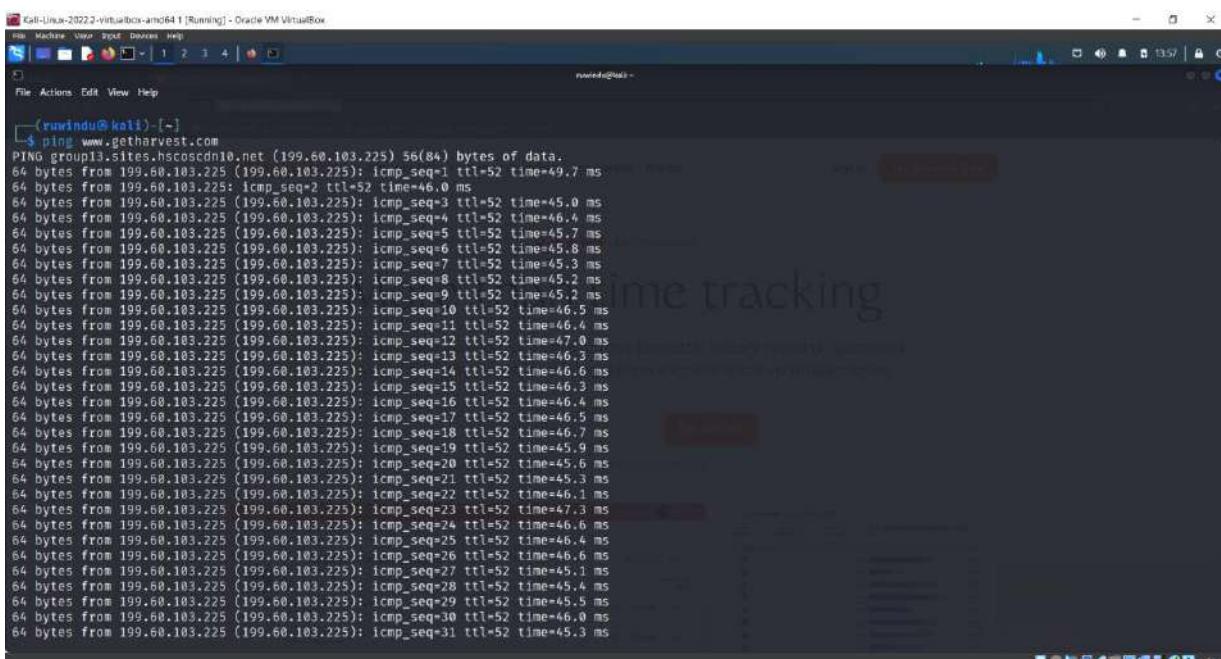
Users are able to find vulnerabilities in a wide number of protocols, servers, and apps with the help of DotDotPwn, which is a tool for doing penetration testing. DotDotPwn is open-source. Throughout the whole of its operation, the malware makes use of several methods, such as directory traversal and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



The screenshot shows a terminal window on Kali Linux with the title 'Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The command entered is 'dotdotpwn --help'. The output displays the usage information for the dotdotpwn tool, including options for module selection, host configuration, and various attack parameters. The terminal window is part of a desktop environment with icons visible at the bottom.

```
usage: ./dotdotpwn.pl [-n modules] -h host [OPTIONS]
  -m Module [http | http-url | ftp | rtsp | payload | stdio]
  -h Hostname
  -O Operating System detection for intelligent fuzzing (man)
  -S Specified OS (e.g. "Ubuntu" or "generic")
  -s Service version detection (banner grabber)
  -d Depth of traversals (e.g. depthness ) equals to ..../../. default: 6
  -f Specific filename (e.g. /etc/passwd) default: according to OS detected, defaults in TraversalEngine.php
  -a Attack mode (GET, POST, HEAD, COPY, MOVE, PUT, DELETE, PATCH, PUT-MD5, VVVV-HOUR-MIN.txt)
  -u URL with the part to be fuzzed marked as TRAVERSAL (e.g. http://foo:8080/id.php?%s=1)
  -r Text pattern to match in the response (http-url & payload modules - e.g. "root" if trying /etc/passwd)
  -p Path to connect (default: HTTP=80, FTP=21, TFTP=69)
  -t Time in milliseconds between each test (200 0.1 second)
  -x Use the Selection Algorithm to detect the exact depthness once a vulnerability has been found
  -y Path to save the results of each fuzz string (e.g. "tmp", "log", ".txt")
  -U Username (default: anonymous)
  -P Password (default: dotdotpwn)
  -M HTTP Method to use when using the "http" module [GET | POST | HEAD | COPY | MOVE] (default: GET)
  -A Path to a file containing a list of attack modules [GET | POST | HEAD | COPY | MOVE]
  -B Break after the first vulnerability is found
  -q Quiet mode (doesn't print each attempt)
  -c Continue if no data was received from host
```

Use ping command and fid the IP address



The screenshot shows a terminal window on Kali Linux with the title 'Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The command entered is 'ping www.getharvest.com'. The output shows the ping results to the website, with many ICMP echo requests being sent and their responses being received. The terminal window is part of a desktop environment with icons visible at the bottom.

```
PING www.getharvest.com (199.68.103.225) 56(84) bytes of data.
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=1 ttl=52 time=49.7 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=2 ttl=52 time=46.0 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=3 ttl=52 time=45.0 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=4 ttl=52 time=46.4 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=5 ttl=52 time=45.7 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=6 ttl=52 time=45.8 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=7 ttl=52 time=45.3 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=8 ttl=52 time=45.2 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=9 ttl=52 time=45.2 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=10 ttl=52 time=46.5 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=11 ttl=52 time=46.4 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=12 ttl=52 time=47.0 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=13 ttl=52 time=46.3 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=14 ttl=52 time=46.6 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=15 ttl=52 time=46.3 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=16 ttl=52 time=46.4 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=17 ttl=52 time=46.5 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=18 ttl=52 time=46.7 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=19 ttl=52 time=45.9 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=20 ttl=52 time=45.6 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=21 ttl=52 time=45.3 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=22 ttl=52 time=46.1 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=23 ttl=52 time=47.3 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=24 ttl=52 time=46.6 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=25 ttl=52 time=46.4 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=26 ttl=52 time=46.6 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=27 ttl=52 time=45.1 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=28 ttl=52 time=45.4 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=29 ttl=52 time=45.5 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=30 ttl=52 time=46.0 ms
64 bytes from 199.68.103.225 (199.68.103.225): icmp_seq=31 ttl=52 time=45.3 ms
```

Get the IP address and use the dotdotpwn tool

```
[root@kali: ~]# ./dotdotopen -r http://199.68.183.225
[+] Starting the dotdotopen engine...
[+] Target IP: 199.68.183.225
[+] Port: 80
[+] Protocol: http
[+] Traversal Engine: /tmp/dotdotopen_traversals/
[+] Testing Results: /tmp/dotdotopen_traversals/testing_results/
[+] Exploit: /tmp/dotdotopen_traversals/exploit/
[+] Exploit File: /tmp/dotdotopen_traversals/exploit/exploit.py

[+] Creating Traversal patterns (mix of dots and slashes)
[+] Multiplying 4 times the traversal patterns (-d switch)
[+] Creating the Special Traversal patterns
[+] Translating backslashes in the filenames
[+] Adapting the filenames according to the OS type detected (unix)
[+] Including Special suffixes
[+] Traversal Engine DONE ! - Total traversal tests created: 13028

[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)
```

## Using Nikto tool

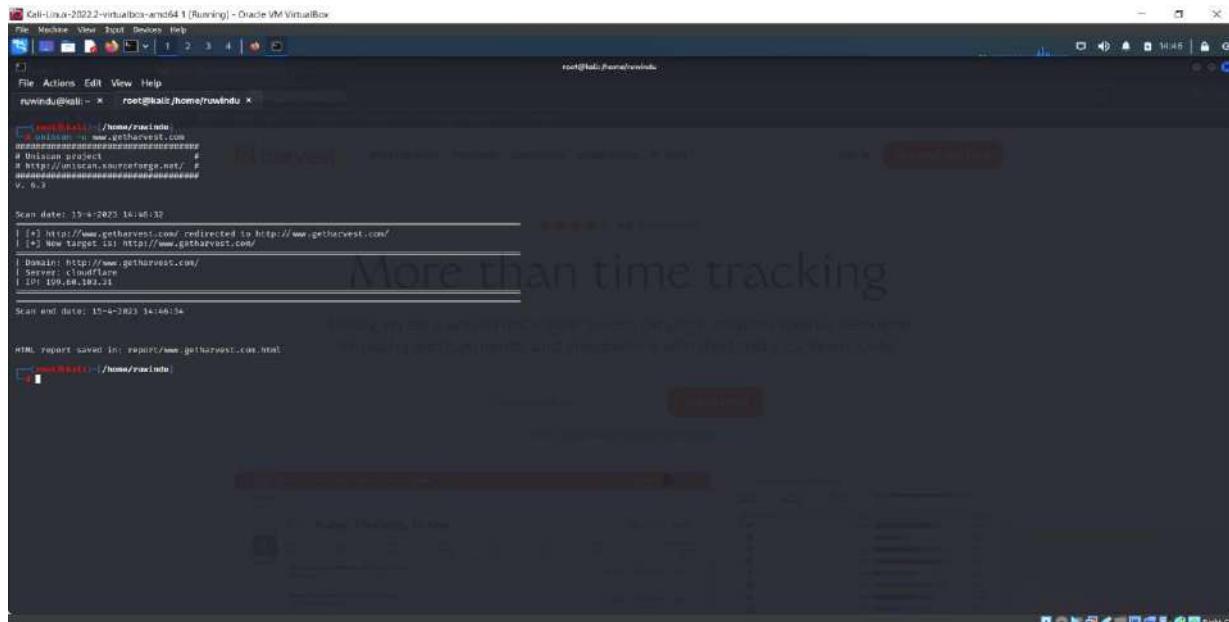
The first scan did not make any mention of the available options, rather, it was only a routine scan of the targeted website.

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.

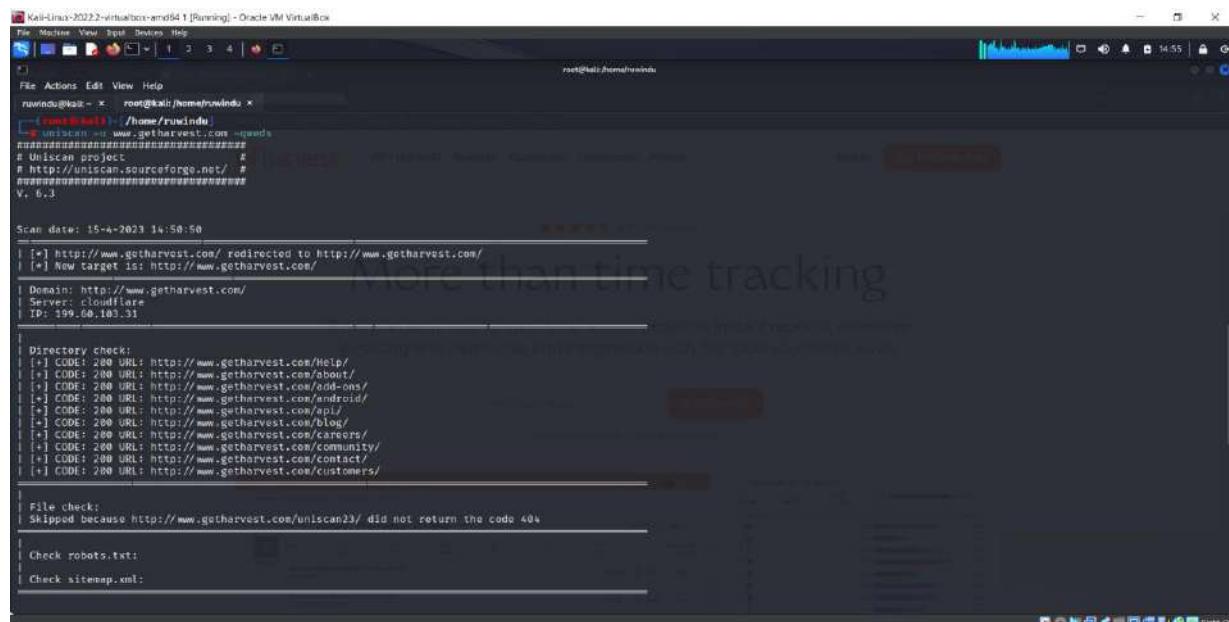
## Using Uniscan tool

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



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
root@kali:~# uniscan -u www.getharvest.com  
[+] Uniscan v6.3  
[+] Domain: http://www.getharvest.com  
[+] Server: cloudflare  
[+] IP: 109.66.183.31  
V. 6.3  
  
Scan date: 15-4-2023 14:46:32  
[+] http://www.getharvest.com/ redirected to http://www.getharvest.com/  
[+] Now target is: http://www.getharvest.com/  
[+] Domain: http://www.getharvest.com/  
[+] Server: cloudflare  
[+] IP: 109.66.183.31  
  
Scan end date: 15-4-2023 14:46:34  
  
HTML report saved in: report/www.getharvest.com.html  
[+] root@kali:~# /home/root/uniscan
```

After the command used uniscan –u [www.getharvest.com](http://www.getharvest.com) -qweds



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
root@kali:~# uniscan -u www.getharvest.com -qweds  
[+] Uniscan project  
[+] http://uniscan.sourceforge.net/ #  
V. 6.3  
  
Scan date: 15-4-2023 14:50:50  
[+] http://www.getharvest.com/ redirected to http://www.getharvest.com/  
[+] Now target is: http://www.getharvest.com/  
[+] Domain: http://www.getharvest.com/  
[+] Server: cloudflare  
[+] IP: 109.66.183.31  
  
Directory check:  
[+] CODE: 200 URL: http://www.getharvest.com/Help/  
[+] CODE: 200 URL: http://www.getharvest.com/about/  
[+] CODE: 200 URL: http://www.getharvest.com/add-ons/  
[+] CODE: 200 URL: http://www.getharvest.com/android/  
[+] CODE: 200 URL: http://www.getharvest.com/api/  
[+] CODE: 200 URL: http://www.getharvest.com/blog/  
[+] CODE: 200 URL: http://www.getharvest.com/careers/  
[+] CODE: 200 URL: http://www.getharvest.com/community/  
[+] CODE: 200 URL: http://www.getharvest.com/contact/  
[+] CODE: 200 URL: http://www.getharvest.com/customers/  
  
File check:  
Skipped because http://www.getharvest.com/uniscan23/ did not return the code 404  
  
Check robots.txt:  
Check sitemap.xml:
```

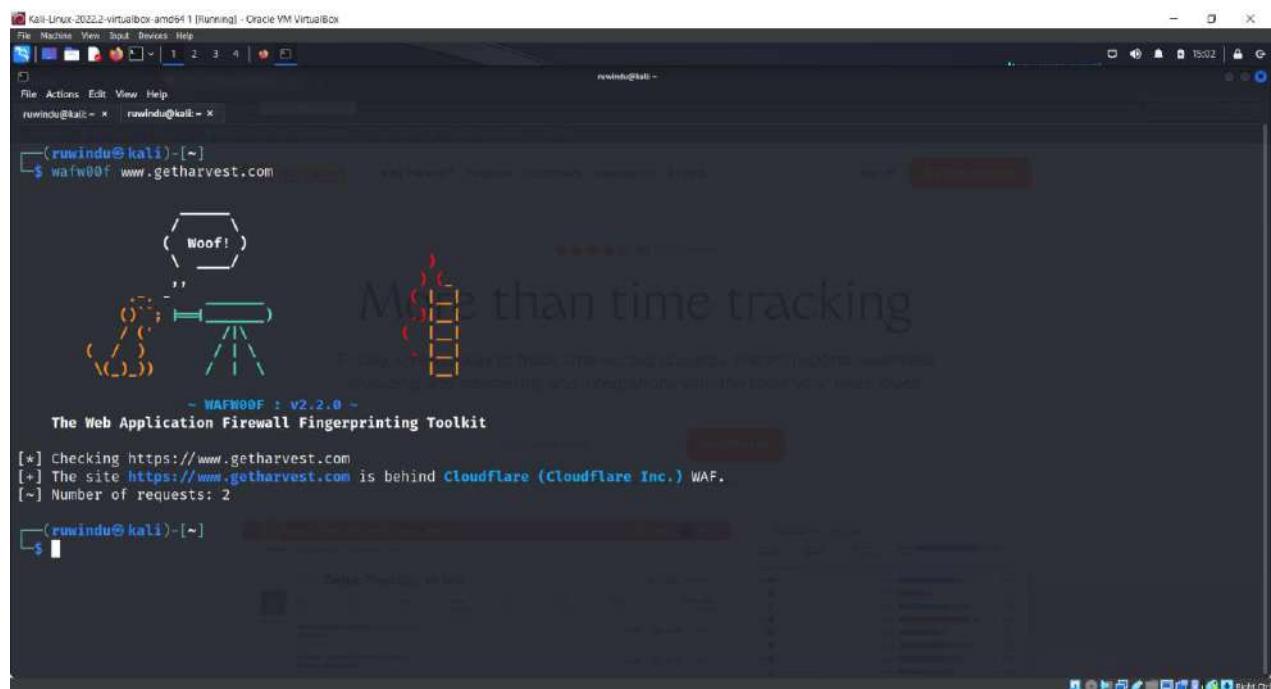
```
| File check:  
| Skipped because http://www.getharvest.com/uniscan23/ did not return the code 404  
|  
| Check robots.txt:  
| Check sitemap.xml:  
|  
| Crawler Started:  
| Plugin name: External Host Detect v.1.2 Loaded.  
| Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.  
| Plugin name: FCKeditor upload test v.1.1 Loaded.  
| Plugin name: Code Disclosure v.1.1 Loaded.  
| Plugin name: phpinfo() Disclosure v.1.1 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:
```

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.

```
| File Actions Edit View Help  
root@kali:~> root@kali:/home/rwwindu >  
| Web Backdoors:  
| Ignored Files:  
|  
| Dynamic tests:  
| Plugin name: Learning New Directories v.1.2 Loaded.  
| Plugin name: FCKeditor 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.1.3 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://www.getharvest.com/testing123 did not return the code 404  
|  
| Timthumb < 1.33 vulnerability:  
|  
| Backup Files:  
|  
| Blind SQL Injection:  
|  
| Local File Include:  
|  
| PHP CGI Argument Injection:  
|  
| Remote Command Execution:
```

## Using wafw00f tool

The website [www.getharvest.com](http://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.



Kali-Linux-2022.2-virtualbox-amd64.1 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
File Actions Edit View Help  
rwwindu@kali: ~ rwwindu@kali: ~  
(rwwindu@kali)-[~]\$ wafw00f www.getharvest.com  
  
Woof! Woof! Woof!  
More than time tracking  
The Web Application Firewall Fingerprinting Toolkit  
~ WAFW00F : v2.2.0 ~  
The Web Application Firewall Fingerprinting Toolkit  
[\*] Checking https://www.getharvest.com  
[+] The site <https://www.getharvest.com> is behind Cloudflare (Cloudflare Inc.) WAF.  
[~] Number of requests: 2  
(rwwindu@kali)-[~]\$

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

## Using OWASP-ZAP tool

The screenshot shows the OWASP ZAP 2.12.0 interface. The main window displays a list of 103 requests made to the URL <http://www.getharvest.com>. The requests are listed in a table with columns: Id, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Header, and Size Resp. Body. Most requests are GET methods to various URLs, with status codes 403 or 200 OK. The RTT (Round Trip Time) varies from 64 ms to 214 ms. The size of the response header and body is also listed.

Found 103 Requests.

The screenshot shows the OWASP ZAP 2.12.0 interface with the 'Alerts' tab selected. It displays a list of 26 alerts found during the scan. One specific alert is expanded, showing details about a 'Cross-Domain Misconfiguration'. The alert information includes:

- URL: <https://www.getharvest.com/hubs/favicon-h-1.ico>
- Risk: Medium
- Confidence: Medium
- Parameter:
- Attack:
- Evidence: Access-Control-Allow-Origin: \*
- CWE ID: 264
- WASC ID: 14
- Source: Passive (10098 - Cross-Domain Misconfiguration)
- Input Vector:
- Description: Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.

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

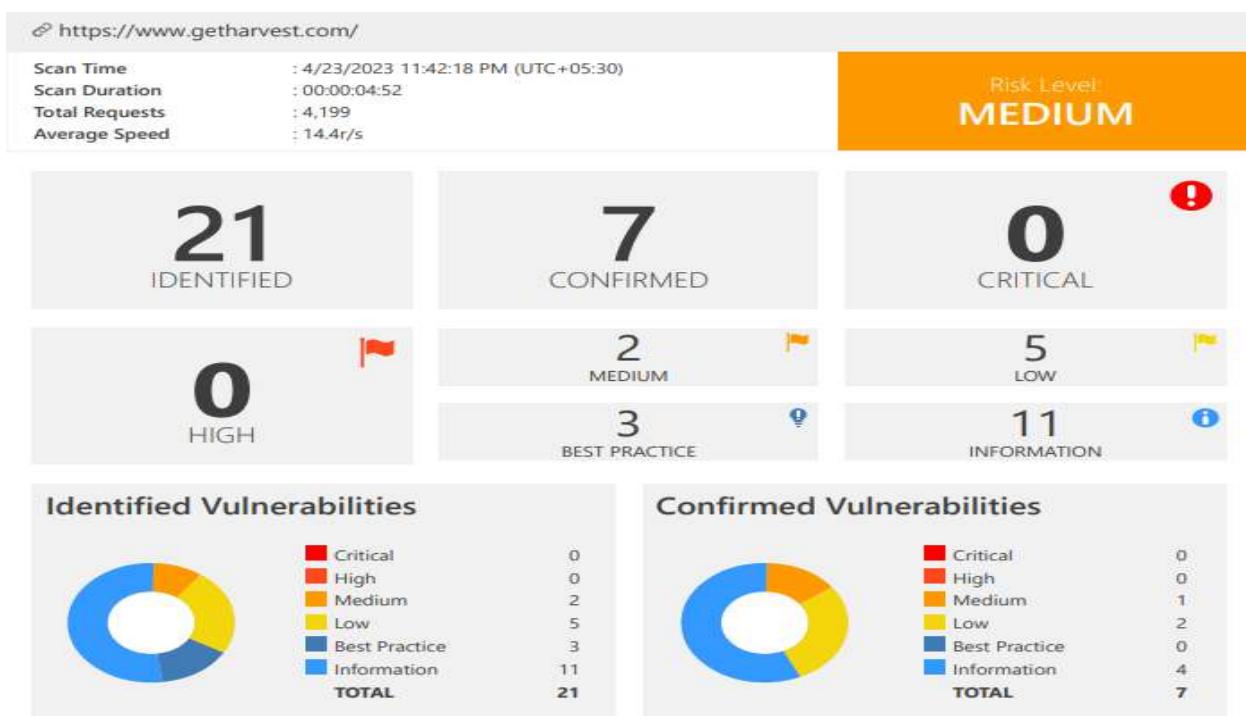
#### Solution

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](https://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.

## Vulnerability Summary

| CONFIRM | VULNERABILITY   | METHOD | URL   | PARAMETER |
|---------|---|--------|---|-----------|
| +       | <a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a> | GET    | <a href="https://www.getharvest.com/">https://www.getharvest.com/</a>                         |           |
| +       | <a href="#">Weak Ciphers Enabled</a>                                      | GET    | <a href="https://www.getharvest.com/">https://www.getharvest.com/</a>                         |           |
| +       | <a href="#">[Possible] Phishing by Navigating Browser Tabs</a>            | GET    | <a href="https://www.getharvest.com/careers">https://www.getharvest.com/careers</a>           |           |
| +       | <a href="#">Misconfigured Access-Control-Allow-Origin Header</a>          | GET    | <a href="https://www.getharvest.com/hs/hsstatic/">https://www.getharvest.com/hs/hsstatic/</a> | URI-BASED |
| +       | <a href="#">Missing X-Frame-Options Header</a>                            | GET    | <a href="https://www.getharvest.com/">https://www.getharvest.com/</a>                         |           |
| +       | <a href="#">Autocomplete is Enabled</a>                                   | GET    | <a href="https://www.getharvest.com/signup">https://www.getharvest.com/signup</a>             |           |
| +       | <a href="#">Insecure Frame (External)</a>                                 | GET    | <a href="https://www.getharvest.com/">https://www.getharvest.com/</a>                         |           |

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

| CONFIRM | VULNERABILITY | METHOD  | URL     | PARAMETER   |
|---------|---------------|---|---------|---|
|         |               | <a href="#">Web Application Firewall Detected</a>                   | GET     | https://www.getharvest.com/%3Cscript%3Ealert(0)%3C/script%3E <span style="border: 1px solid #ccc; padding: 2px;">URI-BASED</span> |
|         |               | <a href="#">Cross-site Referrer Leakage through Referrer-Policy</a> | GET     | https://www.getharvest.com/   |
|         |               | <a href="#">File Upload Functionality Detected</a>                  | GET     | https://www.getharvest.com/contact  |
|         |               | <a href="#">Forbidden Resource</a>                                  | POST    | https://www.getharvest.com/   |
|         |               | <a href="#">OPTIONS Method Enabled</a>                              | OPTIONS | https://www.getharvest.com/   |

[www.getharvest.com](http://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-AZ6VlpaHP5tCT1vc383hS0sFSR3J0f
Jxn2dRpP+X1jKGDPgVMXFPIJztAls9CvRP8k10dAaPrs30QKBfvN8mg40=; __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

### Solution

Add `rel=noopener` to the links to prevent pages from abusing `window.opener`. This ensures that the page cannot access the `window.opener` property in Chrome and Opera browsers. For older browsers and in Firefox, you can add `rel=noreferrer` which 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

The screenshot shows the HackerOne interface for a submitted report. The top navigation bar includes 'Open (1)', 'Pending disclosure (0)', 'Pending retests (0)', 'All (2)', and 'Draft (0)'. A search bar and filter options are also present. The main content area displays a report titled '#1984163 Phishing by Navigating Browser Tabs' submitted by 'darkkiller08' on May 11th. The report details a vulnerability where Netsparker was able to discover possible phishing by cycling through the tabs of the browser, but was unable to verify that the vulnerability existed. It describes how 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. The solution involves adding rel=noopener to the links to prevent pages from abusing window.opener. The impact is described as follows:

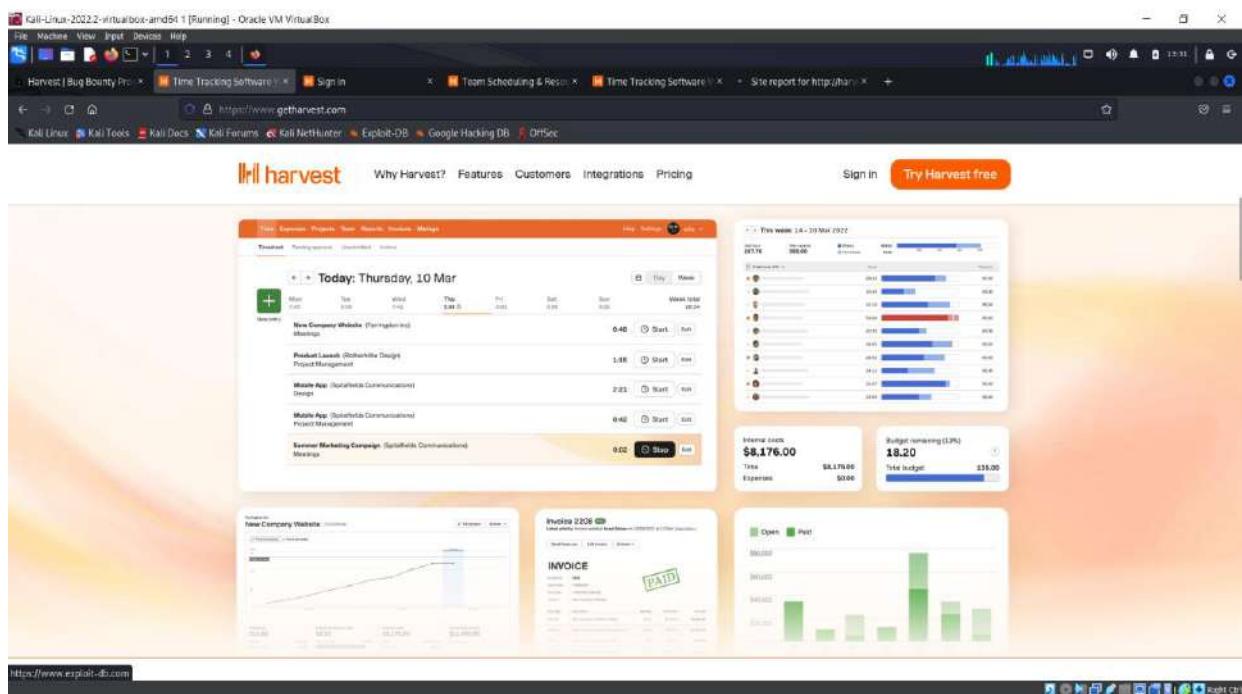
**Impact**  
Although this vulnerability does not make it possible to execute scripts, it does make it possible to conduct phishing attacks in which the parent tab is silently replaced. In the event that the links do not have the rel="noopener noreferrer" tag, a third-party website is able to alter the URL of the source tab by utilizing the window.opener.location.assign property. users may be duped into believing that they

Reported May 11, 2023 9:31pm +0530  
darkkiller08  
Participants  
State: New (Open)  
Reported to: Harvest  
Severity: Medium (4 ~ 6.9)  
Asset: Dom... getharvest.com  
Weakness: Phishing  
Time spent: 3h  
Visibility: Private  
CVE ID: None  
Account de... None

## 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

File Machine View Input Devices Help

Harvest | Bug Bounty Pro | Time Tracking Software | Sign in | Team Scheduling & Res. | Time Tracking Software | Site report for http://harvestapp.com | +

https://site-report.netcraft.com/alive/http://harvestapp.com

Kali Linux Kali Tools Kali Docs Kali Forum Kali NetHunter Exploit-DB Google Hacking DB OffSec

 NETCRAFT

Services Solutions News Company Resources Discover More Report Fraud

## Background

|             |   |                      |            |
|-------------|---|----------------------|------------|
| Site title  | Time Tracking Software Web Inviting   Harvest   | Date first seen      | April 2006 |
| Site rank   | Not Present   | Netcraft Risk Rating | 0/10       |
| Description | Time tracking and management software with powerful easy reporting and streamlined online invoicing. Used by 73,000 businesses. Get started for free. | Primary language     | English    |

## Network

|                         |   |                         |  |
|-------------------------|---|-------------------------|--|
| Site                    | <a href="http://harvestapp.com">http://harvestapp.com</a> | Domain                  | harvestapp.com   |
| Notable Owner           | Google LLC  | Nameserver              | ns-2024.sakura-ip.co.uk  |
| Hosting company         | Google  | Domain registrar        | name.com   |
| Hosting country         | US  | Nameserver organisation | whois.rak  |
| IPv4 address            | 34.107.228.235  | Organisation            | Harvest, 16 W 22nd St, 8th Floor, New York, 10010, United States |
| IPv4 autonomous systems | AS29982   | DNS admin               | as29982-hostmaster@amazon.com                                    |
| IPv6 address            | 2000:1001:0:1771::0:0:0                                   | Top Level Domain        | Commercial entities (.com)                                       |
| IPv6 autonomous systems | A315169   | DNS Security Extensions | Unknown  |
| Reverse DNS             | 235.228.107.34.ip-peopleusercontent.com                   |                         |  |

## IP delegation

|                               |         |      |             |
|-------------------------------|---------|------|-------------|
| IPv4 address (34.107.228.235) | Country | Name | Description |
|-------------------------------|---------|------|-------------|

Gall-Unto-20222-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

Harvest | Bug Bounty Pro ✎ Time Tracking Software ✎ Sign in ✎ Team Scheduling & Res. ✎ Time Tracking Software ✎ Site report for http://harvestapp.com ✎ +

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**NETCRAFT**

Services Solutions News Company Resources Q 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   | <a href="http://www.avito.ru">www.avito.ru</a> , <a href="http://www.arco.co.uk">www.arco.co.uk</a> , <a href="http://www.walmart.com">www.walmart.com</a> |
|         | Analytics        | GoogleTagManager | <a href="http://www.cengizci.com">www.cengizci.com</a> , <a href="http://www.norden.se">www.norden.se</a> , <a href="http://www.cnbc.com">www.cnbc.com</a> |

Kali-Linux-2022.2-virtualbox-amd64.1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Harvest | Bug Bounty Pro X Time Tracking Software X Sign in X Team Scheduling & Review X Time Tracking Software X SiteReport for http://harvestapp.com X

Exit Linux Kali Tools Kali Devs Kali Forums Kali Nethunter Export DB Google Hacking DB OffSec

**NETCRAFT**

Services Solutions News Company Resources Discover Index Report Abuse

**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  |
|-----------------------|---|--|
| Google Compute Engine | Google's cloud platform for large scale computing workloads | <a href="http://www.freepik.com">www.freepik.com</a> , <a href="http://www.babbel.net">www.babbel.net</a> , <a href="http://www.flashescore.com">www.flashescore.com</a> |

**Network**

Any network related service or technology.

| Technology                     | Description                                   | Popular sites using this technology |
|--------------------------------|---|-------------------------------------|
| Akamai Web Services - Route 53 | Cross-Signed Domain Name System (DNS) Service |                                     |

**HTTP Accelerator**

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

| Technology                | Description   | Popular sites using this technology  |
|---------------------------|---|--|
| Google HTTP Load Balancer | Google's external HTTPS load balancer                               | <a href="http://www.mozilla.org">www.mozilla.org</a> , <a href="http://www.spring.io">www.spring.io</a>  |
| Cloudflare                | Content delivery network and distributed domain name server service | <a href="http://www.cloudflare.org">www.cloudflare.org</a> , <a href="http://www.cloudflare.com">www.cloudflare.com</a> , <a href="http://www.mapillary.com">www.mapillary.com</a> |

**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 Window View Input Devices Help
root@kali:~# nmap -sT -O -p 22-443 192.168.22.235
Starting Nmap 7.8.0 ( https://nmap.org ) at 2023-07-10 15:57 CEST
Nmap scan report for 192.168.22.235
Host is up (0.000s latency).
OS: Linux 5.10.0 - 5.15.0 [great confidence]
Nmap done: 1 IP address (1 host up) scanned in 1.00 seconds

root@kali:~# curl -s http://192.168.22.235
<!DOCTYPE html>
<html>
<head>
<title>Harvest App</title>
</head>
<body>
<h1>Harvest App</h1>
<h2>Welcome to the Harvest App!</h2>
<ul>
<li>Logout</li>

```

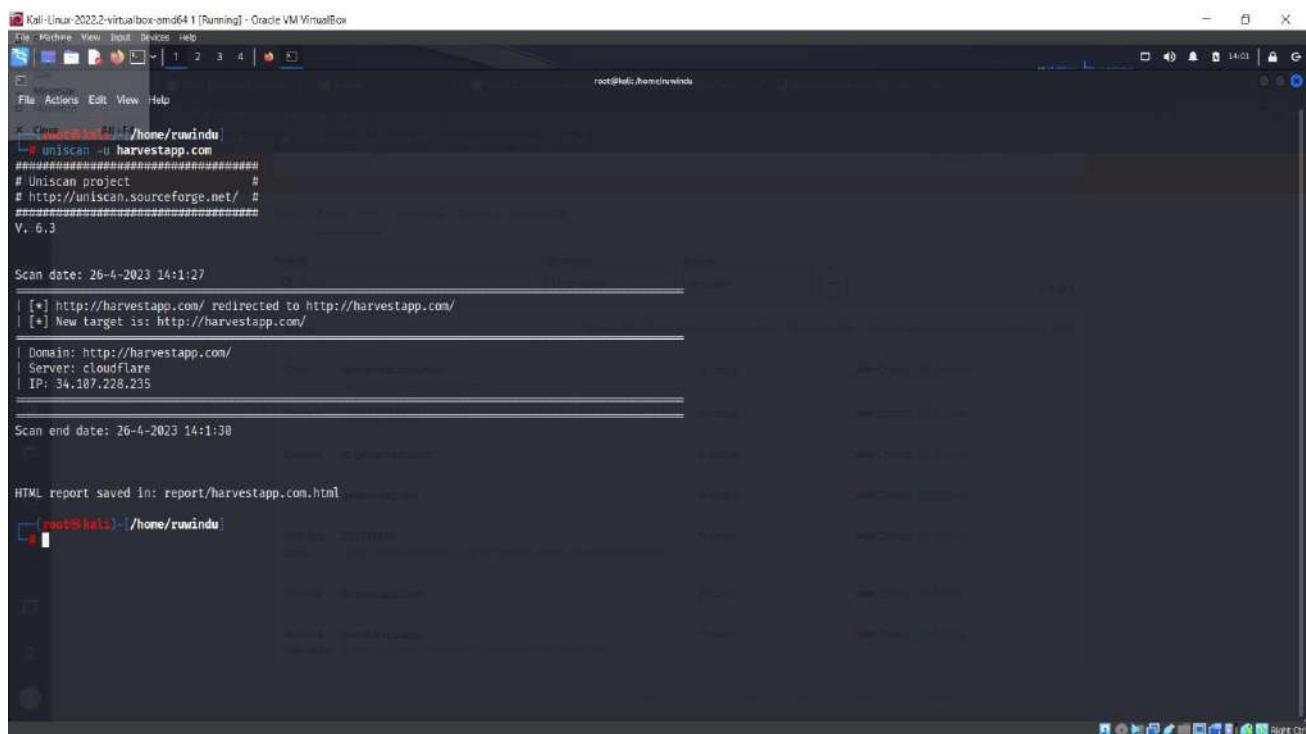
The screenshot shows a terminal window on a Kali Linux VM. The user has run a Nmap scan against the IP 192.168.22.235, which is identified as a Linux host running version 5.10.0 to 5.15.0. The scan results show a single host up. The user then runs a curl command on the same IP, which returns the homepage of the Harvest App. The page title is "Harvest App" and it includes a welcome message and a "Logout" link.



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.



```
Kali-Linux-2022.2-virtualbox-omd64 1 [Running] - Oracle VM VirtualBox
File Archive View Input Devices Help
File Actions Edit View Help
root@kali:/home/ruwindu
└─$ uniscan -u harvestapp.com
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

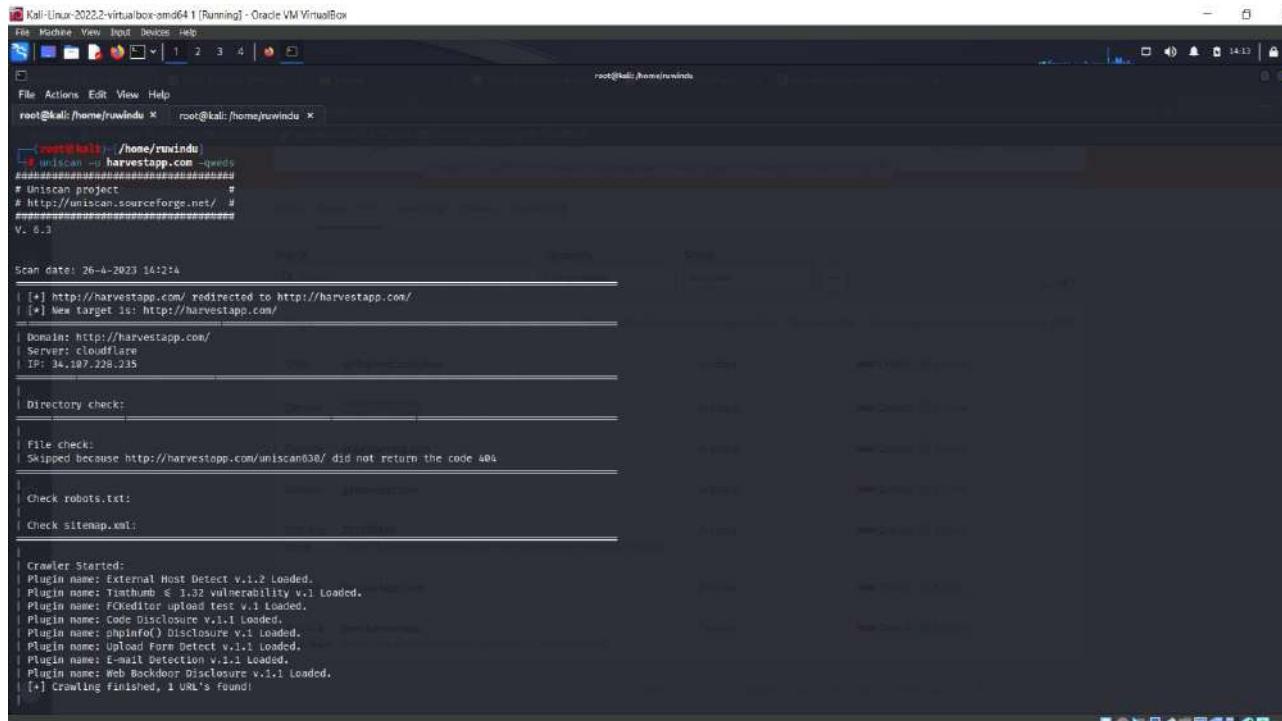
Scan date: 26-4-2023 14:1:27
[+] http://harvestapp.com/ redirected to http://harvestapp.com/
[+] New target is: http://harvestapp.com/

Domain: http://harvestapp.com/
Server: cloudflare
IP: 34.107.228.235

Scan end date: 26-4-2023 14:1:30

HTML report saved in: report/harvestapp.com.html
root@kali:/home/ruwindu
└─$
```

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



```
Kali-Linux-2022.2-virtualbox-omd64 1 [Running] - Oracle VM VirtualBox
File Archive View Input Devices Help
File Actions Edit View Help
root@kali:/home/ruwindu × root@kali:/home/ruwindu ×
root@kali:/home/ruwindu ×
└─$ uniscan -u harvestapp.com -qweds
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 26-4-2023 14:12:14
[+] http://harvestapp.com/ redirected to http://harvestapp.com/
[+] New target is: http://harvestapp.com/

Domain: http://harvestapp.com/
Server: cloudflare
IP: 34.107.228.235

Directory check:
File check:
Skipped because http://harvestapp.com/uniscan030/ did not return the code 404

Check robots.txt:
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: FQEditor upload test v.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: phpInfo() Disclosure v.1.1 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:
```

```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Device Help
root@kali:/home/rwwindu x  root@kali:/home/rwwindu x
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: FCKeditor 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 Device Help
root@kali:/home/rwwindu x  root@kali:/home/rwwindu x
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 14:9:27

HTML report saved in: report/harvestapp.com.html
[root@kali ~]#
```

## 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.

Kali-Linux-2022.2-virtualbox-amd64\_1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

root@kali:~# WAFW00F -v2.2.0.1 - The Web Application Firewall Fingerprinting Toolkit

[+] Checking https://harvestapp.com

[+] the site https://harvestapp.com is behind CloudFlare (CloudFlare Inc.) WAF.

[+] Number of requests: 2

root@kali:~#

The terminal window shows the WAFW00F tool version 2.2.0.1 being used to check the website https://harvestapp.com. The output indicates that the site is behind a CloudFlare WAF and shows two requests made during the process.

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

The screenshot shows the OWASP-ZAP interface. In the center, the 'Automated Scan' dialog is open with the URL 'http://harvestapp.com' entered. Below it, the 'Sent Messages' tab is selected, showing a table of 103 requests. The table includes columns for Id, Req. Timestamp, Resp. Timestamp, Method, URL, Code, Reason, RTT, Size Resp. Header, and Size Resp. Body. The requests are mostly GETs to various URLs like /sitemap.xml and /robots.txt. At the bottom of the interface, the status bar shows 'Current Scans: 0' and 'Progress: 100%'.

Found 103 Requests.

The screenshot shows the OWASP-ZAP interface with the 'Alerts' tab selected. It displays 26 alerts. One alert is expanded: 'Missing Anti-clickjacking Header' for the URL http://harvestapp.com. The alert details are: Risk: Medium, Confidence: Medium, Parameter: X-Frame-Options, Attack: Clickjacking, CWE ID: 1021, WASC ID: 15, Source: Passive (10020 - Anti-clickjacking Header), and Input Vector: Content-Security-Policy. The description states: 'The response does not include either Content-Security-Policy with "frame-ancestors" directive or X-Frame-Options to protect against "Clickjacking" attacks.'

Found 26 Alerts.

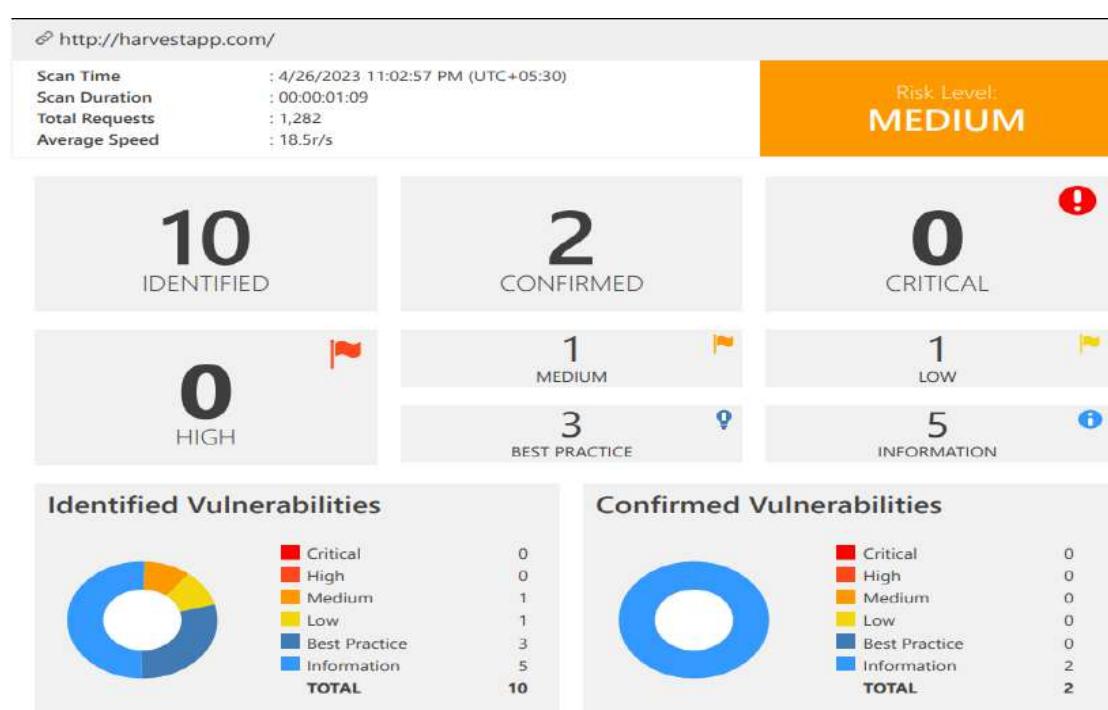
## Vulnerabilities found

## 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.

The screenshot shows the Netsparker interface with the following details:

- Top Navigation Bar:** File, Home, View, Reporting, Help, Search.
- Left Sidebar:** New report template, Detailed Scan Report, Executive Summary Report, SANS Top 25 Report, PCI DSS Compliance Report, OWASP Top Ten 2017 Report, HIPAA Compliance Report, ISO 27001 Compliance Report, Knowledge Base Report, Comparison Report, ModSecurity WAF Rules, F5 BIG-IP ASM Rules, Vulnerabilities List (XML), Vulnerabilities List (JSON), Vulnerabilities List (CSV), Scanned URLs List (XML), Scanned URLs List (JSON), Scanned URLs List (CSV).
- Central Area:**
  - Welcome:** Updates section with links to Invicti Scanners Release Announcements and Invicti Standard Change Log.
  - Web Application Security Blog:** Scanning by the numbers: New Invicti report shows more testing means less risk.
  - Progress:** Scan Speed graph and Scan Progress bar (100%).
  - Logs:** Activity, Progress, Logs (22).
- Bottom Status Bar:** Report successfully exported, Scan Finished, Previous Settings, Default Security Checks, Default Report Policy, Proxy System.



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

<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.

#### **Vulnerabilities**

##### **10.1. <https://harvestapp.com/robots.txt>**

**CONFIRMED**

#### **Interesting Robots.txt Entries**

- disallow: /

#### **Request**

```
GET /robots.txt HTTP/1.1
Host: harvestapp.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) : 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

The screenshot shows the HackerOne interface for a submitted report. The left sidebar has icons for Open (2), Pending disclosure (0), Pending retests (0), All (6), and Draft (0). A search bar at the top says "Search all reports". The main area shows a timeline of events:

- #1988225 Robots.txt Detected (Submitted by darkkiller08 to Harvest, Medium, 1 min ago)
- #1984163 Phishing by Navigating Browser Tabs (Submitted by darkkiller08 to Harvest, Medium, 4 days ago)

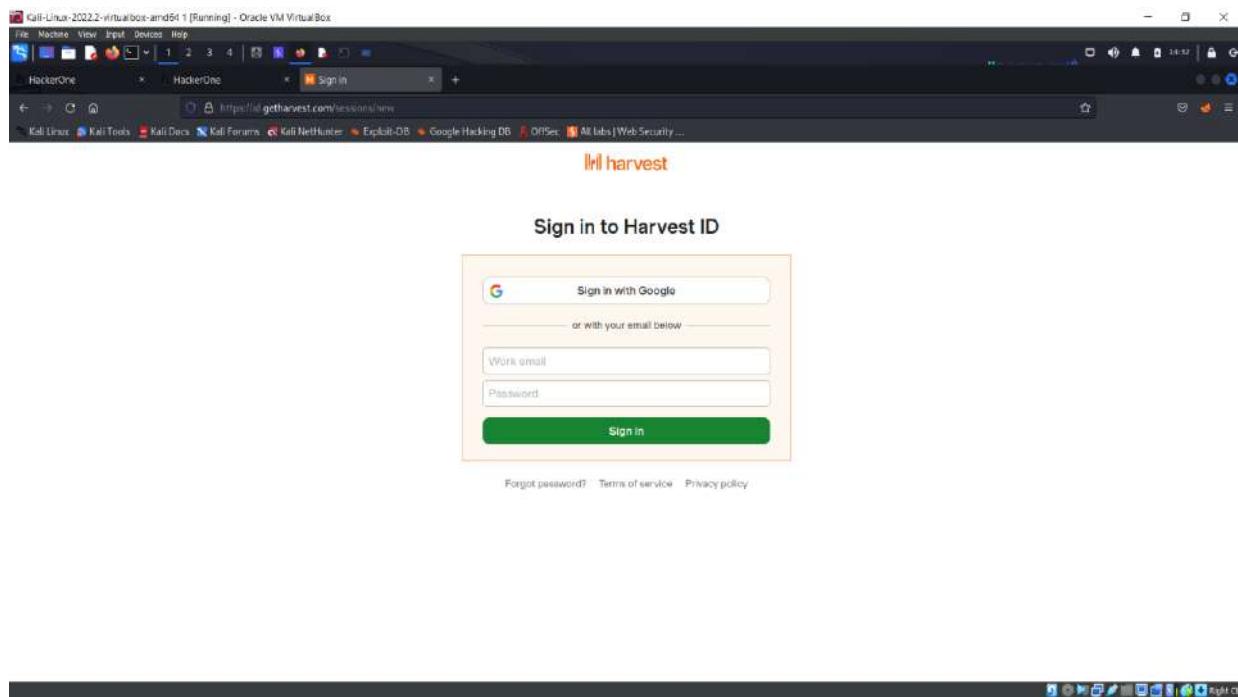
The detailed view for the first report includes:

- ADD HACKER SUMMARY**
- TIMELINE - EXPORT**
- darkkiller08 submitted a report to Harvest. (Edit information)** May 15th (< 1 min ago)  
Robots.txt Detected
- 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.
- Impact**
- 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.
- Participants**
- State**: New (Open)
- Reported to**: Harvest
- Severity**: Medium (4 ~ 6.9)
- Asset Domains**: harvestapp.com
- Weakness**: Insecure Direct Object Reference (IDOR)
- Time spent**: 3h
- Visibility**: Private
- CVE ID**: None
- Account details**: None

## 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 [Running] - Oracle VM VirtualBox

HackerOne HackerOne Sign In Site report for https://id.getharvest.com

<https://site-report.netcraft.com/?url=https://id.getharvest.com>

Site report for https://id.getharvest.com

NETCRAFT

Background

Site title: getharvest.com | Sign in | Date first seen: April 2014

Site rank: 31083 | Network Risk Rating: 0/10 | Net Present: Primary language: English

Network

Site: https://getharvest.com | Domain: getharvest.com

Registrant: Google LLC | Name server: ns.1333.awards-38.org

Hosting company: Google | Domain registrar: names.com

Hosting country: United States | Nameserver organisation: whois.pr.org

IPv4 address: 34.187.175.177 | Organization: Harvest, 10 W 22nd St, 10th Floor, New York, 10010, United States

IPv4 autonomous systems: AS299982 | DNS alias: awsdns-hochzettel.amazon.com

IPv6 address: 2600:1901:95fe::10:0 | Top Level Domain: Commercial entities (.com)

IPv6 autonomous systems: AS65160 | DNS Security Extensions: unKnown

Reverse DNS: 177.15.107.34 (c.googleusercontent.com)

IP delegation

IPv4 address (34.187.175.177)

| IP range   | Country       | Name                     | Description                         |
|------------|---------------|--------------------------|-------------------------------------|
| 1.1.1.1/32 | United States | IANA/IPv4-MAPPED-ADDRESS | Internet Assigned Numbers Authority |

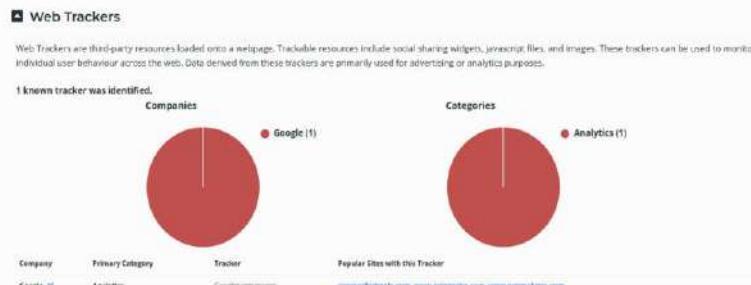
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

HackerOne HackerOne Sign In Site report for https://id.getharvest.com

<https://site-report.netcraft.com/?url=https://id.getharvest.com>

Site report for https://id.getharvest.com

NETCRAFT



### 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.

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

HackerOne HackerOne Sign In Site report for https://id.getharvest.com

<https://site-report.netcraft.com/?url=https://id.getharvest.com>

Site report for https://id.getharvest.com

NETCRAFT

### 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                  |
|-----------------------|--|--|
| Google Compute Engine | Google's cloud platform for large-scale computing services | www freepik com, www zeroedge com, pointofheyday net |

#### 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 HTTPS load balancer | www flickr com, www meetup org, www batnet net |

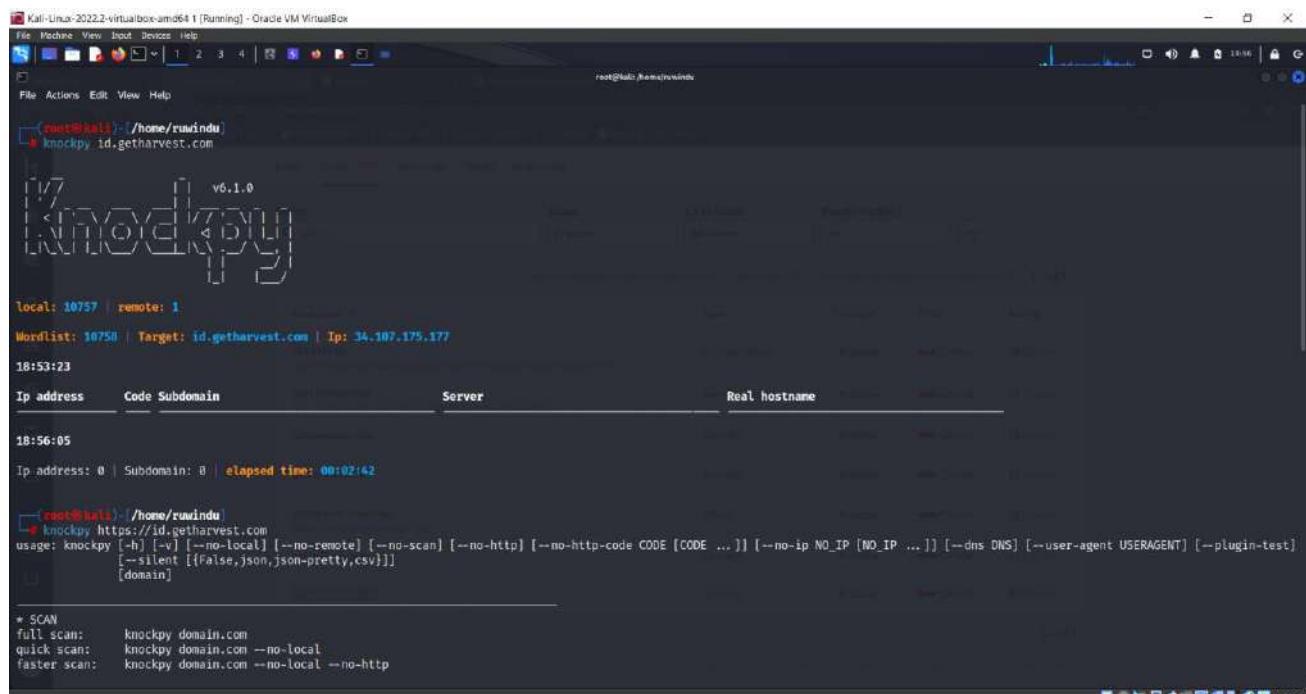
#### Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

| Technology | Description  | Popular sites using this technology                   |
|------------|--|---|
| Rails      | Web application framework built on the Ruby programming language | www codesamples com, www zedlheads com, www reverb io |

## 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.



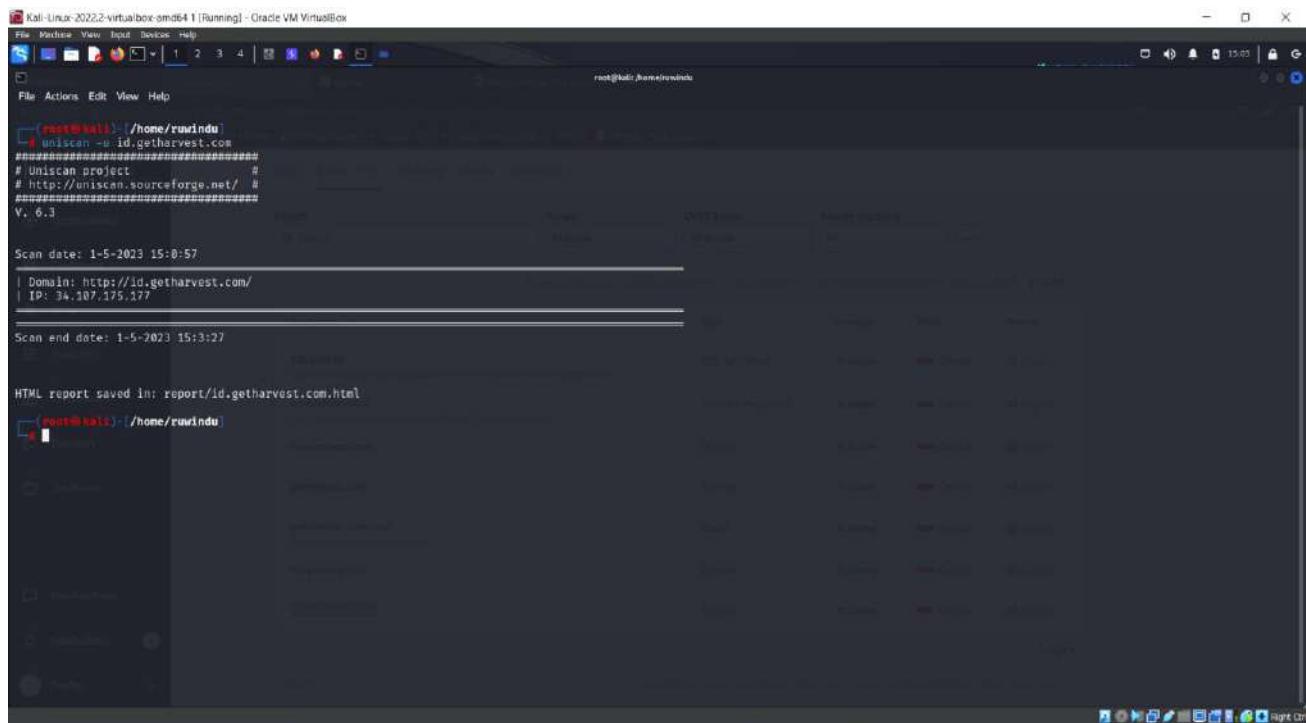
The screenshot shows a terminal window on a Kali Linux system. The title bar reads "Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox". The terminal prompt is "root@kali:~#". The user has run the command "knockpy id.getharvest.com". The output shows the tool's progress, including the IP address (3A.107.175.177), target (id.getharvest.com), and the number of subdomains found (1). The tool version is v6.1.0. A table is displayed with columns for Ip address, Code, Subdomain, Server, and Real hostname. The table shows one entry where the IP address is 0, the code is 0, and the subdomain is 0. The elapsed time is 00:02:42. Below the table, the usage information for the knockpy command is shown, including options for scan type (full, quick, faster) and various output formats (JSON, CSV, etc.).

```
v6.1.0
local: 10757  remote: 1
Wordlist: 10758 | Target: id.getharvest.com | Ip: 3A.107.175.177
18:53:23
18:56:05
Ip address      Code Subdomain      Server      Real hostname
18:56:05
Ip address: 0 | Subdomain: 0 | elapsed time: 00:02:42
[root@kali:~# knockpy https://id.getharvest.com
usage: knockpy [-h] [-v] [--no-local] [--no-remote] [--no-scan] [--no-http] [--no-http-code CODE [CODE ...]] [--no-ip NO_IP [NO_IP ...]] [--dns DNS] [--user-agent USERAGENT] [--plugin-test]
               [-silent [False,JSON,JSON-Pretty,Csv]] [--domain]
* SCAN
full scan:      knockpy domain.com
quick scan:     knockpy domain.com --no-local
faster scan:    knockpy domain.com --no-local --no-http
```

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

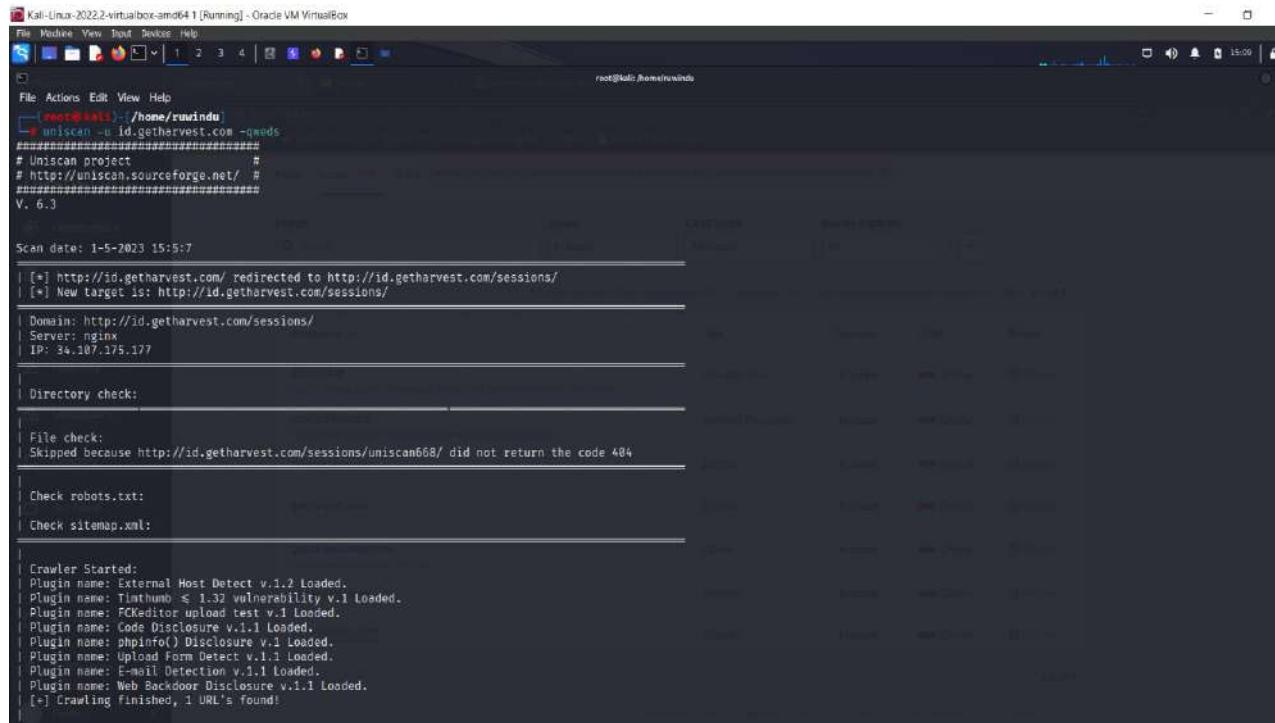
Perform a quick scan by using the -u switch, and then enter the domain you want to search.



```
[root@kali:~/home/rwwindu]
└─# uniscan -u id.getharvest.com
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 1-5-2023 15:0:57
| Domain: http://id.getharvest.com/
| IP: 34.107.175.177
| Scan end date: 1-5-2023 15:3:27
| HTML report saved in: report/id.getharvest.com.html
[root@kali:~/home/rwwindu]
```

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



```
[root@kali:~/home/rwwindu]
└─# uniscan -u id.getharvest.com -qweds
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 1-5-2023 15:5:7
| [*] http://id.getharvest.com/ redirected to http://id.getharvest.com/sessions/
| [*] New target is: http://id.getharvest.com/sessions/
| Domain: http://id.getharvest.com/sessions/
| Server: nginx
| IP: 34.107.175.177
| Directory check:
| File check:
| Skipped because http://id.getharvest.com/sessions/uniscan668/ did not return the code 404
| Check robots.txt:
| 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: phpinf() 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!
```

```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#nmap -sC -sV --script=sitemap.xml
root@kali:~# 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.1.1 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: FCKeditor 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.

root@kali:~#
```

```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#nmap -sC -sV --script=sitemap.xml
root@kali:~# Check sitemap.xml:

FCKeditor testing:
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.

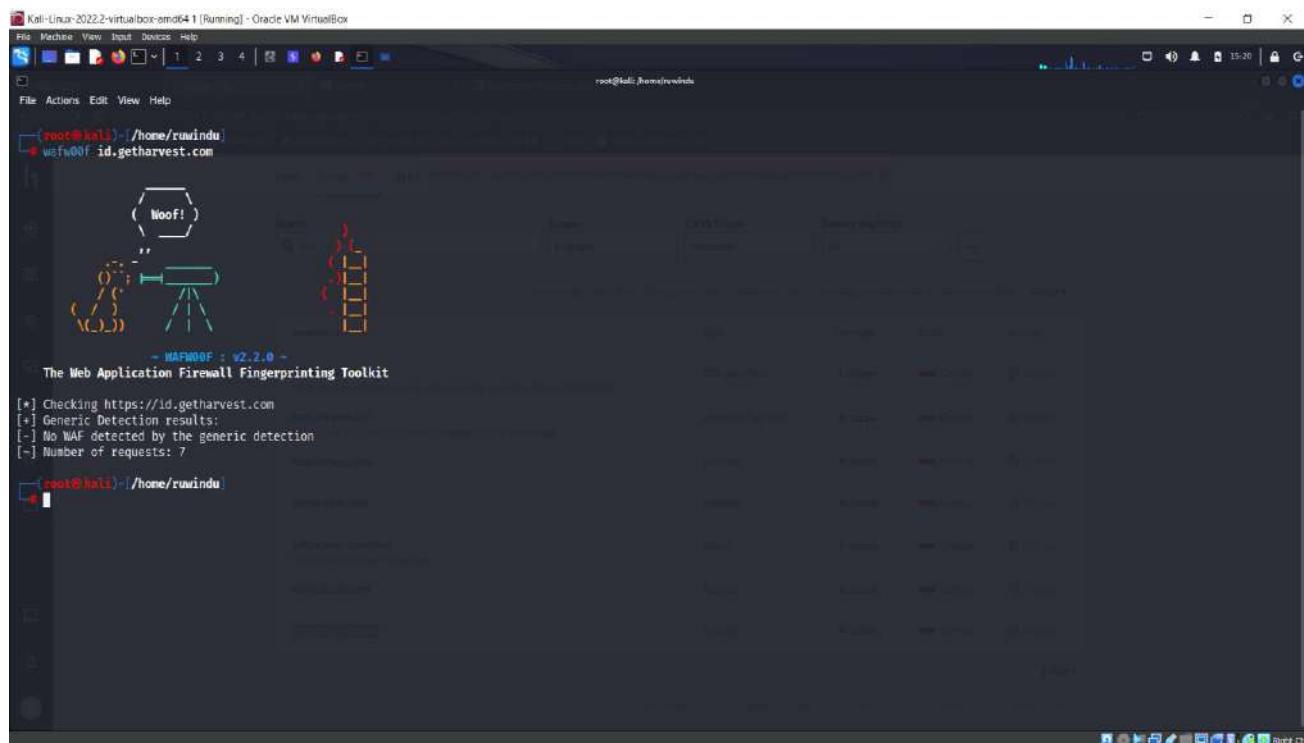
Blind SQL Injection:
Local File Include:
PHP CGI Argument Injection:
Remote Command Execution:
Remote File Include:
SQL Injection:
Cross-Site Scripting (XSS):
Web Shell Finder:
Static tests:
Plugin name: Local File Include tests v.1.1 Loaded.
Plugin name: Remote Command Execution tests v.1.1 Loaded.
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 15:08:26

HTML report saved in: report/id.getharvest.com.html
[+] http://id.getharvest.com/
```

## 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.



The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal title is 'Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox'. The command entered is 'wafw00f id.getharvest.com'. The output shows the version of the tool (WAFW00F : v2.2.0), followed by a generic detection result indicating no WAF was detected. The terminal prompt returns to the user's directory: '/home/rwwindu'.

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

```

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

Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://id.getharvest.com

Attack complete - see the Alerts tab for details of any issues found

| ID  | Req. Timestamp      | Resp. Timestamp     | Method | URL                                    | Code | Reason    | RTT   | Size Resp. Header | Size Resp. Body |
|-----|---------------------|---------------------|--------|--|------|-----------|-------|-------------------|-----------------|
| 362 | 5/24/23, 9:46:03 AM | 5/24/23, 9:46:03 AM | CET    | http://id.getharvest.com               | 200  | OK        | 39 ms | 1,311 bytes       | 5,124 bytes     |
| 364 | 5/24/23, 9:46:04 AM | 5/24/23, 9:46:04 AM | CET    | http://id.getharvest.com/systemmap.xml | 404  | Not Found | 42 ms | 288 bytes         | 119 bytes       |
| 266 | 5/24/23, 9:46:04 AM | 5/24/23, 9:46:04 AM | GET    | http://id.getharvest.com/systemmap.xml | 404  | Not Found | 40 ms | 288 bytes         | 119 bytes       |
| 268 | 5/24/23, 9:46:04 AM | 5/24/23, 9:46:04 AM | GET    | http://id.getharvest.com/systemmap.xml | 404  | Not Found | 45 ms | 288 bytes         | 119 bytes       |
| 370 | 5/24/23, 9:46:04 AM | 5/24/23, 9:46:04 AM | GET    | http://id.getharvest.com               | 200  | OK        | 46 ms | 1,315 bytes       | 5,124 bytes     |
| 372 | 5/24/23, 9:46:05 AM | 5/24/23, 9:46:05 AM | GET    | http://id.getharvest.com/systemmap.xml | 404  | Not Found | 45 ms | 288 bytes         | 119 bytes       |
| 374 | 5/24/23, 9:46:05 AM | 5/24/23, 9:46:05 AM | GET    | http://id.getharvest.com/systemmap.xml | 404  | Not Found | 46 ms | 288 bytes         | 119 bytes       |
| 376 | 5/24/23, 9:46:05 AM | 5/24/23, 9:46:05 AM | CET    | http://id.getharvest.com               | 200  | OK        | 42 ms | 1,319 bytes       | 5,124 bytes     |
| 378 | 5/24/23, 9:46:06 AM | 5/24/23, 9:46:06 AM | CET    | http://id.getharvest.com               | 200  | OK        | 41 ms | 1,303 bytes       | 5,124 bytes     |
| 380 | 5/24/23, 9:46:07 AM | 5/24/23, 9:46:07 AM | CET    | http://id.getharvest.com               | 200  | OK        | 47 ms | 1,309 bytes       | 5,124 bytes     |

Found 290 Requests.

X-Content-Type-Options Header Missing (7)

URL: https://id.getharvest.com/robots.txt

Risk: Low

Confidence: Medium

Parameter: X-Content-Type-Options

Attack:

Evidence:

CWE ID: 693

WASC ID: 15

Source: Passive (10021 - X-Content-Type-Options Header Missing)

Input Vector:

Description:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (Content-Type), either than performing MIME-sniffing.

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.

The screenshot shows the Netsparker interface with the following details:

- Top Bar:** File, Home, View, Reporting, Help, Search.
- Left Sidebar:** New Report Template, Detailed Scan Report, Executive Summary Report, SANS Top 25 Report, PCI DSS Compliance Report, OWASP Top Ten 2013 Report, OWASP Top Ten 2017 Report, HIPAA Compliance Report, ISO 27001 Compliance Report, Knowledge Base Report, Comparison Report, ModSecurity WAF Rules, F5 BIG-IP ASM Rules, Vulnerabilities List (XML), Vulnerabilities List (JSON), Vulnerabilities List (CSV), Scanned URLs List (XML), Scanned URLs List (JSON), Scanned URLs List (CSV).
- Central Area:**
  - Updates:** We release an update for Invicti Standard every month. Updates include new security checks, new features and bug fixes. Here are some useful links:
    - [Invicti Scanners Release Announcements](#)
    - [Invicti Standard Change Log](#)
  - Web Application Security Blog:** Invicti Insights: Squashing AppSec urban myths and legends.
  - Progress:** Scan Speed graph showing activity over time, Scan Progress bar, and a summary table:

|                   |                             |                    |                    |                       |
|-------------------|-----------------------------|--------------------|--------------------|-----------------------|
| Links: 207        | Failed Requests: 0          | 404 Responses: 217 | Head Requests: 482 | Total Requests: 29120 |
| Elapsed: 00:18:44 | Start: 5/2/2023 12:23:27 AM |                    |                    |                       |
  - Logs:** Activity, Progress, Logs (24).
- Right Panel:** Netsparker Assistant (2\*)
  - Scan Policy Optimized:** Assistant has optimized your scan policy for the current scan and saved as Default Security Checks (Optimized by Assistant). Would you like to switch to the optimized policy?
  - Warning:** It is strongly advised to restart your scan to keep your scan coverage of its best after the scan policy is switched.
  - Switch to Optimized Policy**
  - Maximum Signature Exceeded:** Netsparker has detected that some of the visited URLs are being marked as out-of-scope due to Maximum Signature setting in your current scan policy is exceeded. This means Netsparker has reached the maximum request limit made to the exact same path for those URLs.
  - Action:** Increase Maximum Signature | Set up Parameter Based Navigation

The report summary for <http://id.getharvest.com/> is as follows:

- Risk Level:** MEDIUM
- Scan Time:** 5/2/2023 12:23:27 AM (UTC+05:30)
- Scan Duration:** 00:00:18:44
- Total Requests:** 25,129
- Average Speed:** 22.3r/s

**Vulnerability Breakdown:**

| Type          | Count     |
|---------------|-----------|
| Critical      | 0         |
| High          | 0         |
| Medium        | 2         |
| Low           | 4         |
| Best Practice | 5         |
| Information   | 9         |
| <b>TOTAL</b>  | <b>20</b> |

**Identified Vulnerabilities:**

| Severity      | Count     |
|---------------|-----------|
| Critical      | 0         |
| High          | 0         |
| Medium        | 2         |
| Low           | 4         |
| Best Practice | 5         |
| Information   | 9         |
| <b>TOTAL</b>  | <b>20</b> |

**Confirmed Vulnerabilities:**

| Severity      | Count    |
|---------------|----------|
| Critical      | 0        |
| High          | 0        |
| Medium        | 0        |
| Low           | 2        |
| Best Practice | 0        |
| Information   | 4        |
| <b>TOTAL</b>  | <b>6</b> |

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            |
|---------|---|--------|--|----------------------|
| !       | <a href="#">[Possible] BREACH Attack Detected</a>                         | POST   | https://id.getharvest.com/sessions                                 |                      |
| !       | <a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a> | GET    | https://id.getharvest.com/   |                      |
| !       | <a href="#">[Possible] Phishing by Navigating Browser Tabs</a>            | POST   | https://id.getharvest.com/sessions/                                |                      |
| !       | <a href="#">Missing X-Frame-Options Header</a>                            | POST   | https://id.getharvest.com/sessions                                 |                      |
| !       | <a href="#">Insecure Frame (External)</a>                                 | GET    | https://id.getharvest.com/sessions/new                             |                      |
| !       | <a href="#">Internal Server Error</a>                                     | POST   | https://id.getharvest.com/password_reset                           |                      |
| !       | <a href="#">Content Security Policy (CSP) Not Implemented</a>             | GET    | https://id.getharvest.com/sessions/new                             |                      |
| !       | <a href="#">Expect-CT Not Enabled</a>                                     | GET    | https://id.getharvest.com/opensearch.xml                           |                      |
| !       | <a href="#">Missing X-XSS-Protection Header</a>                           | GET    | https://id.getharvest.com/opensearch.xml                           |                      |
| !       | <a href="#">Referrer-Policy Not Implemented</a>                           | POST   | https://id.getharvest.com/sessions                                 |                      |
| !       | <a href="#">Subresource Integrity (SRI) Not Implemented</a>               | GET    | https://id.getharvest.com/svn/wc/db                                |                      |
| !       | <a href="#">CDN Detected (Google Cloud CDN)</a>                           | GET    | https://id.getharvest.com/opensearch.xml                           |                      |
| !       | <a href="#">Disabled X-XSS-Protection Header</a>                          | GET    | https://id.getharvest.com/google/auth2/new?state%5Bintent%5D=%2527 | state%5Bint%5D=%2527 |
| !       | <a href="#">Email Address Disclosure</a>                                  | POST   | https://id.getharvest.com/sessions/                                |                      |
| !       | <a href="#">Generic Email Address Disclosure</a>                          | POST   | https://id.getharvest.com/sessions/                                |                      |
| !       | <a href="#">Nginx Web Server Identified</a>                               | 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.

**Vulnerabilities**

5.1. [https://id.getharvest.com/password\\_reset](https://id.getharvest.com/password_reset)  
**CONFIRMED**

| Method | Parameter          | Value  |
|--------|--------------------|--|
| POST   | Accept             | .../.../.../.../.../.../.../.../.../etc/passwd{{                                       |
| POST   | authenticity_token | xyjVvK&gnNjBb4H85X94c-eH4XtIc4uIRwQknfsKinV4q7rh0iIMTe7zIm1SPzLEXF7kaNrhro8FPcDYbOKShA |
| POST   | email              |  |
| POST   | commit             | Send link  |
| POST   | continue_to        |  |

#### Request

```
POST /password_reset HTTP/1.1
Host: id.getharvest.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
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=sFLuxURd94VcFX73GtCFrYD06iVouZ25WgU6smhM2RaXqSjEsZ5sZzmnTzEw%2B8zH9Yc
iLMkFhJ8IIiU2a2bsxi%2B50UgkZ16Sm3YS3BREt0ojHJp5YA62B7R3r%2FPdLU5Dh3QZBrNPGhC93tS0zt272G1JtusVqXhbX72vF33
1%2BBWwOU8xi%2FuyH6gd%2BkKIjPPji%2FdF8SBTIBqi07qG%2BixbcNsDg9XnzbbeHFI8SV01UOYzXFpBX%2Fh1oK4T2B9UL9N1%2F
EuHFYQrvxC50KazMvkFc5WXY2fC8LeXmEBbd6SyJk2wKmtT4odpxX23j%2FnvOTOhxNNv85TM8XhKPm0scV9QE6soKh%2B9NexXg%3
D%3D--%2FIs8RN05JPMj5oeA--S@Tvr23CQ6fxVJAgK6czkA%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=xyjVvK6gnNjBbHHB5X04c-eH4XtIc4uIRwQknfsKinV4q7rh0iIMTe7zImISPzLEXF7kaNrhr08FPcDYbOKShA&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

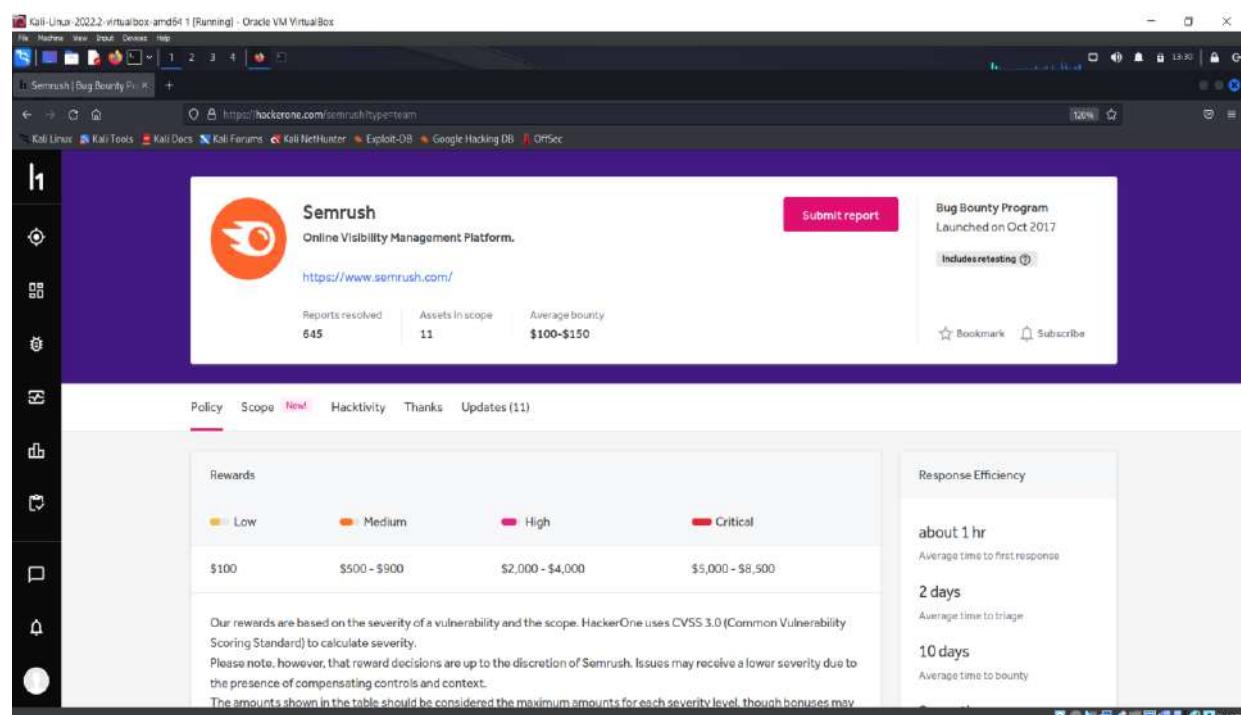
The screenshot shows the HackerOne interface. On the left is a dark sidebar with navigation links: Opportunities, Dashboard, **Inbox** (highlighted in green), Hacktivity, Leaderboard, Directory, Job Board, Notifications (0), and Profile. The main area displays a report card for an 'Internal Server Error'. At the top right of the card are buttons for 'Pending disclosure (0)', 'Pending retests (0)', 'All (7)', and 'Draft (0)'. Below these are filters for 'Show 25+' and 'Sort: Latest activity'. The report itself has a purple header '#1988235 Internal Server Error'. It includes sections for 'ADD HACKER SUMMARY', 'TIMELINE - EXPORT', and detailed descriptions of the issue, solution, impact, and a summary table on the right. The summary table contains the following data:

|               |   |
|---------------|---|
| Reported      | May 15, 2023 8:00pm +0530                     |
| By            | darkkiller08                                  |
| Participants  |   |
| State         | New (Open)                                    |
| Reported to   | Harvest                                       |
| Severity      | Medium (4 - 6.9)                              |
| Asset: Dom... | id.getharvest.com                             |
| Weakness      | Information Exposure Through an Error Message |
| Time spent    | 3h  |
| Visibility    | Private                                       |
| CVE ID        | None  |
| Account de... | None  |

## 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.



A screenshot of a Kali Linux desktop environment (version 2022.2) running in Oracle VM VirtualBox. The window title is "Kali-Uinx-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox". The URL in the browser is <https://hackerone.com/semrush/hyperteam>. The page displays the Semrush Bug Bounty Program, which was launched on October 2017. It shows statistics: 645 reports resolved, 11 assets in scope, and an average bounty of \$100-\$150. A legend indicates reward levels: Low (yellow), Medium (orange), High (pink), and Critical (red). Below this, a table shows maximum reward amounts: \$100 for Low, \$500-\$900 for Medium, \$2,000-\$4,000 for High, and \$5,000-\$8,500 for Critical. A note states rewards are based on severity and scope, using CVSS 3.0. A sidebar on the right shows response efficiency metrics: about 1hr average time to first response, 2 days average time to triage, and 10 days average time to bounty. The interface includes a sidebar with various icons and navigation links like Policy, Scope, New!, Hacktivity, Thanks, and Updates (11).

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 became 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.

The screenshot shows a Kali Linux desktop environment with a web browser window open to the Semrush Bug Bounty Program page. The browser title bar reads "Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox". The page content includes a table for reward amounts by severity level, a list of scopes and their severities, and a sidebar with program statistics.

| Scope  | Critical    | High        | Medium    | Low   |
|--------|-------------|-------------|-----------|-------|
| Main   | \$3000-8500 | \$2000-4000 | \$500-900 | \$100 |
| Second | \$2000-5500 | \$1000-2000 | \$300-500 | \$50  |

| Main Scope      | Severity |
|-----------------|----------|
| * semrush.com   | Critical |
| * semrush.net   | High     |
| Second Scope    | Severity |
| * semrush.com   | Critical |
| * myinsights.io | High     |
| * swoopake.com  | Medium   |
| * sellzone.com  | Medium   |
| * aseob.io      | Low      |
| * seotrac.io    | Low      |

| Ineligible for bounty | Severity |
|-----------------------|----------|
| * prosely.com         | Critical |
| workflows.semrush.com | Medium   |
| investors.semrush.com | Medium   |
| ... (truncated)       | Medium   |

**Program Statistics**  
Updated Daily

| Range           | Count |
|-----------------|-------|
| >\$250,000      | 1     |
| \$100 - \$150   | 1     |
| \$700 - \$6,000 | 1     |
| \$5,000         | 1     |
| 55              | 1     |
| 14 days ago     | 1     |
| 645             | 1     |

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.

The screenshot shows a web browser window titled "Kali-Linux-2022-2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox". The URL is [https://hackerone.com/semrush/policy\\_scope?typ=team](https://hackerone.com/semrush/policy_scope?typ=team). The page displays the Semrush Online Visibility Management Platform logo and navigation links like "Submit report", "Bug Bounty Program", and "Ineligible reporting". Below this, it shows statistics: "Reports received: 645", "Assets in scope: 11", and "Averaged bounty: \$100-\$150". A red box highlights the "Scope" section where two domains are listed as "Out of scope": "advocates.semrush.com" and "email.semrush.com", both marked as "None" and "Ineligible".

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.

The screenshot shows the same web browser window and URL as the previous one. The "Scope" section now lists multiple domains as "In scope": "http://\*.semrush.com", "http://\*.acotec.de", "investors.semrush.com", "http://\*.defline.com", "http://\*.benih.com", "http://\*.semrush.net", "http://\*.growly.com", "http://\*.seosquare.com", "workflow.semrush.com", "https://\*.seowekz.de", and "http://\*.myheights.it". Each entry includes a red "Critical" or green "Exploit" badge, indicating the severity and exploitability of the bugs found.

## 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.

The screenshot shows a Kali Linux 2022.2 virtual machine running in Oracle VM VirtualBox. The Firefox browser window is open, displaying the Netcraft site report for [www.semrush.com](https://www.semrush.com). The page includes sections for 'Background' and 'Network', providing detailed technical information about the domain.

**Background**

| Site title  | Semrush - Online Marketing Can Be Easy  | Date first seen      | December 2008 |
|-------------|---|----------------------|---------------|
| Site rank   | 1287  | Netcraft Risk Rating | 0/10          |
| Description | Turn the algorithm into a friend. Make your business visible online with 55+ tools for SEO, PPC, content, social media, competitive research, and more. | Primary language     | English       |

**Network**

| Site                    | Domain                     | semrush.com             |
|-------------------------|----------------------------|-------------------------|
| Netblock Owner          | Google LLC                 | Nameserver              |
| Hosting company         | Google                     | Domain registrar        |
| Hosting country         | US                         | Nameserver organisation |
| IPv4 address            | 34.120.45.191 (VirusTotal) | Organisation            |
| IPv4 autonomous systems | AS396982                   | DNS admin               |
| IPv6 address            | Not Present                | Top Level Domain        |
| IPv6 autonomous systems | Not Present                | DNS Security Extensions |

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

HackerOne Semrush - Online Market X Site report for https://www.sem.com

https://site-report.netcraft.com/?url=https%3A%2F%2Fwww.sem.com

Services Solutions News Company Resources Q Report Privacy

### 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**

| Company  | Primary Category | Tracker          | Popular Sites with this Tracker   |
|----------|------------------|------------------|---|
| Facebook | Widget           | Facebook         | www.behance.net, www.gazeta.pl, www.ilmeteo.it                            |
|          | Advertising      | DixeClick        | www.vito.ru, www.artco.co.uk, www.corriere.it                             |
| Google   | Analytics        | GoogleAnalytics  | www.flightadar24.com, www.researchgate.net, www.infobae.com               |
|          | CDN              | GoogleCloud      | www.nextcloud.com, www.of.mencomptiaformation.gov.fr, www.tesamuelles.com |
|          | Analytics        | TwitterAnalytics | www.janiper.net, www.ctanews.ca, www.evernote.com                         |
| Twitter  | Tracker          | Tidoco           | www.tid.co.uk, www.sigmaldrich.com, mobile.twitter.com                    |

[Read static.netcraft.com](#)

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

HackerOne Semrush - Online Market X Site report for https://www.sem.com

https://site-report.netcraft.com/?url=https%3A%2F%2Fwww.sem.com

Services Solutions News Company Resources Q Report Privacy

### 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.getepic.com, www.hubspot.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/TLS    | 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](http://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](http://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](http://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

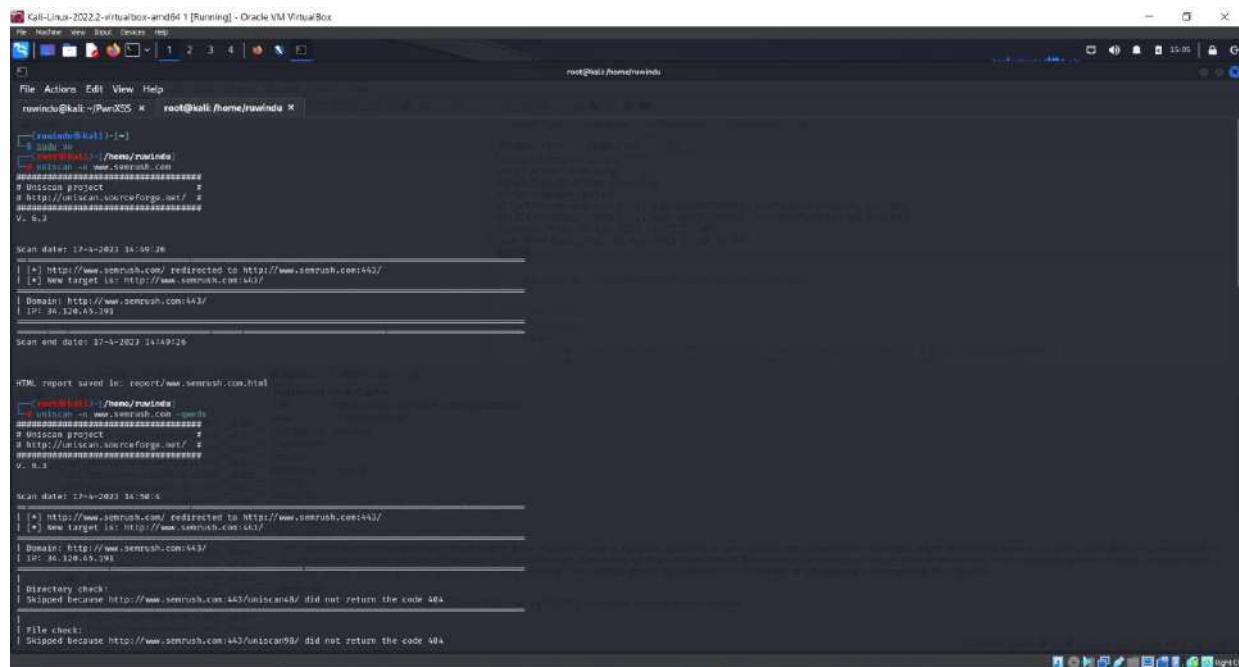


The findings of the scans that are presented both above and below were acquired with the assistance of the PwnXss scanner. As a direct consequence of these results, a number of previously unidentified XSS vulnerabilities that were found to exist on the website located at <https://www.semrush.com> have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



```
Kali-Linux-2022.2-virtualbox-amd64-1 [Running] - Oracle VM VirtualBox
File Actions View Help Devices Help
root@kali:~# ./uniscan -u www.semrush.com -qweds
[+] Starting [www.semrush.com] -qweds
[+] Uniscan -> www.semrush.com -qweds
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V.. 6.3

Scan date: 17-4-2023 14:50:26
[*] http://www.semrush.com/ redirected to http://www.semrush.com:443/
[*] New target is: http://www.semrush.com:443/
Domain: http://www.semrush.com:443/
IP: 36.128.45.193

Scan end date: 17-4-2023 14:50:26

HTML report saved in: report/www.semrush.com.html
[+] Uniscan -> www.semrush.com -qweds
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V.. 6.3

Scan date: 17-4-2023 14:50:45
[*] http://www.semrush.com/ redirected to http://www.semrush.com:443/
[*] New target is: http://www.semrush.com:443/
Domain: http://www.semrush.com:443/
IP: 36.128.45.193

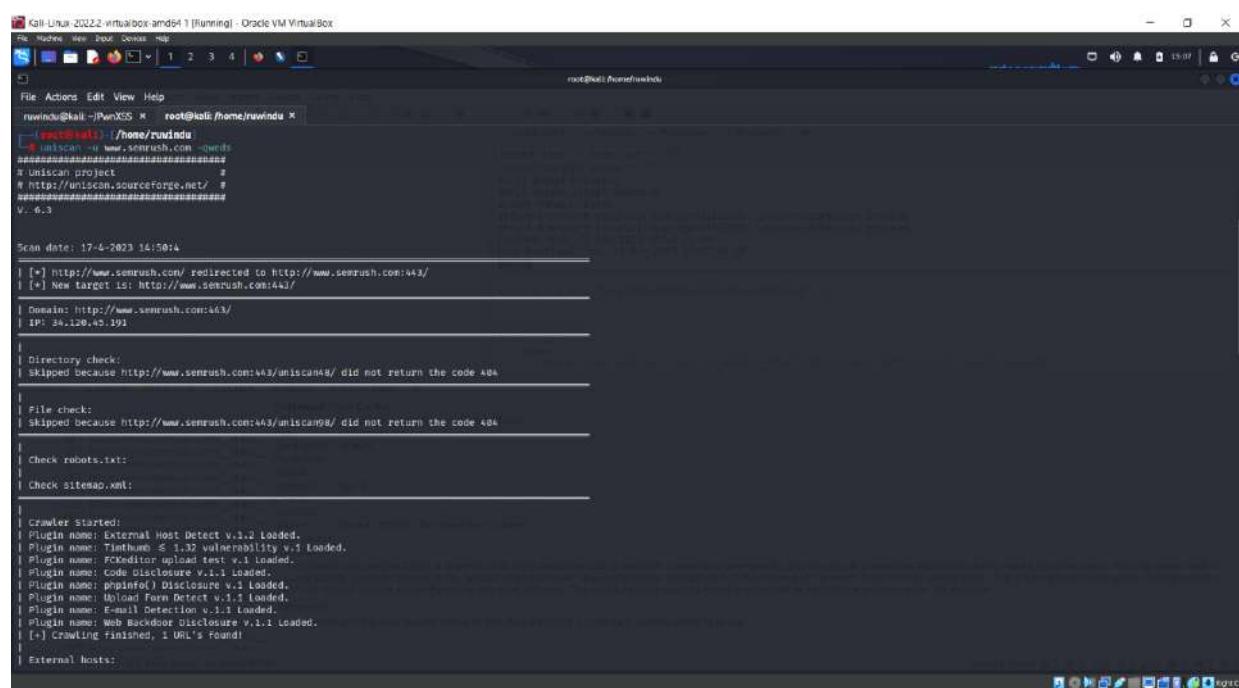
[!] Directory check:
Skipped because http://www.semrush.com:443/uniscan48/ did not return the code 404

[!] File check:
Skipped because http://www.semrush.com:443/uniscan98/ did not return the code 404

[!] Check robots.txt:
[!] Check sitemap.xml:

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: Tinhthanh 8.1.32 vulnerability v.1 Loaded.
Plugin name: FCXeditor upload test v.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: Clickjacking v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backup Disclosure v.1.1 Loaded.
[+/-] Crawling Finished, 1 URL's Found!
External hosts:
```

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



```
Kali-Linux-2022.2-virtualbox-amd64-1 [Running] - Oracle VM VirtualBox
File Actions View Help Devices Help
root@kali:~# ./uniscan -u www.semrush.com -qweds
[+] Starting [www.semrush.com] -qweds
[+] Uniscan -> www.semrush.com -qweds
#####
# Uniscan project
# http://uniscan.sourceforge.net/
#####
V.. 6.3

Scan date: 17-4-2023 14:50:44
[*] http://www.semrush.com/ redirected to http://www.semrush.com:443/
[*] New target is: http://www.semrush.com:443/
Domain: http://www.semrush.com:443/
IP: 36.128.45.193

[!] Directory check:
Skipped because http://www.semrush.com:443/uniscan48/ did not return the code 404

[!] File check:
Skipped because http://www.semrush.com:443/uniscan98/ did not return the code 404

[!] Check robots.txt:
[!] Check sitemap.xml:

Crawler Started:
Plugin name: External Host Detect v.1.2 Loaded.
Plugin name: Tinhthanh 8.1.32 vulnerability v.1 Loaded.
Plugin name: FCXeditor upload test v.1 Loaded.
Plugin name: Code Disclosure v.1.1 Loaded.
Plugin name: Clickjacking v.1.1 Loaded.
Plugin name: Upload Form Detect v.1.1 Loaded.
Plugin name: E-mail Detection v.1.1 Loaded.
Plugin name: Web Backup Disclosure v.1.1 Loaded.
[+/-] Crawling Finished, 1 URL's Found!
External hosts:
```

```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Bookmarks Help
root@kali:~# ./PanXSS
root@kali:~# ./PanXSS
root@kali:~/PanXSS x  root@kali:~/home/rwinda x
[+] Crawler Started:
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Timthumb < 1.32 vulnerability v.1 Loaded.
| Plugin name: FCKeditor File Upload test v.1.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: PHPinfo() Disclosure v.1.1 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: FCKeditor 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: RarArchive Exploit tests v.1.1 Loaded.
| Plugin name: RarCommand 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.
```

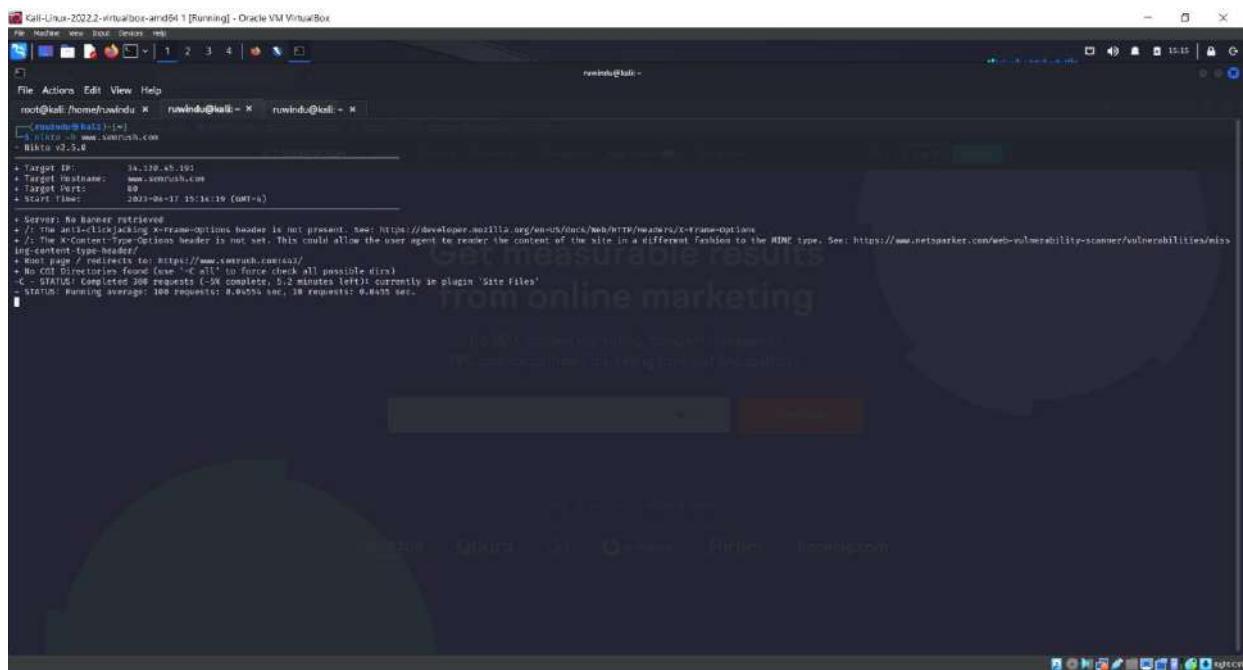
```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Bookmarks Help
root@kali:~# ./PanXSS
root@kali:~# ./PanXSS
root@kali:~/PanXSS x  root@kali:~/home/rwinda x
[+] PHP OGI Argument Injection:
[+] Remote Command Execution:
[+] Remote file Include:
[+] SQL Injection:
[+] 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: 17-6-2023 10:51:33

HTML report saved in: report/www.semrush.com.html
[+] root@kali:~/home/rwinda
```

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.

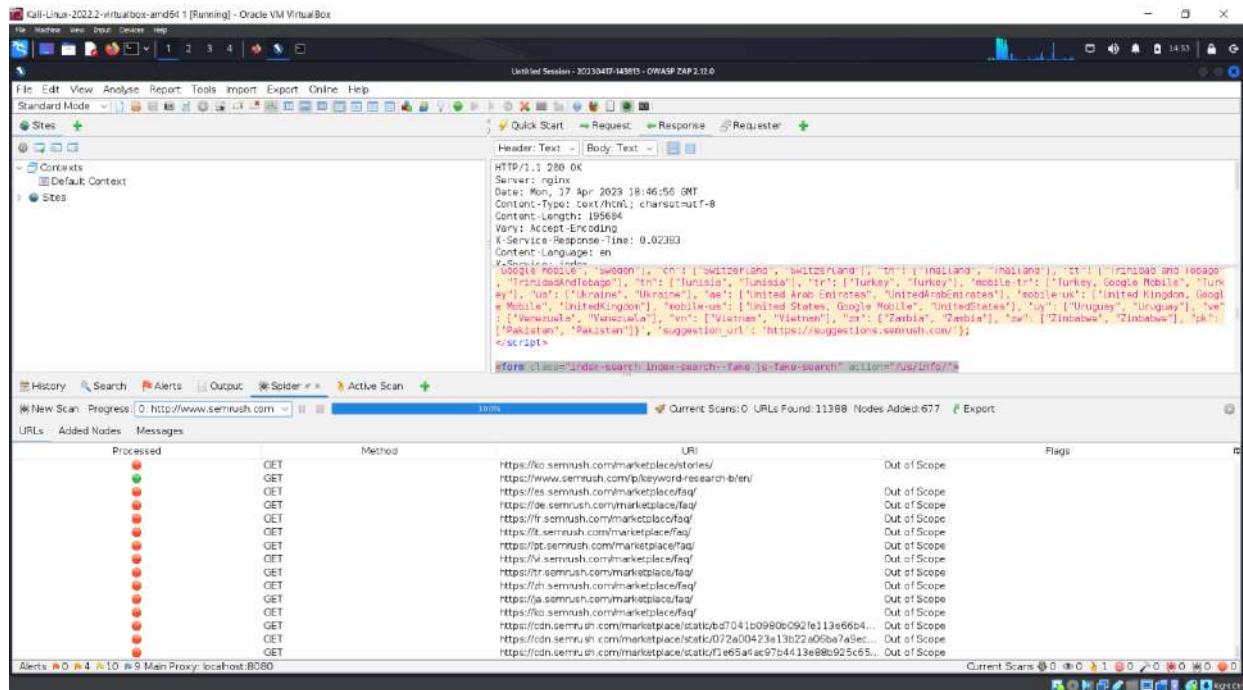


The screenshot shows a terminal window titled 'Call-Linux-2022.2-virtualbox-amd64.1 [Running] - Oracle VM VirtualBox'. The terminal session is running as root ('root@kali') and shows the command 'nikto -h www.xenrush.com' being executed. The output of the command is displayed below:

```
+ Target IP: 34.120.45.192
+ Target Port: 80
+ Start Time: 2023-04-17 15:14:19 (GMT+0)
+ Server: No banner retrieved
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content in a different fashion to the MIME type. See: https://www.netspark.net/web-vulnerability-scanner/vulnerabilities/mis
+ img-content-type-warning: set https://www.xenrush.com/404/
+ No CTF Directories Found (use '-C' to Force check ALL possible dirs)
- CTF/404: Completed 300 requests (-3% complete), 0.2 minutes left! (currently in plugin 'Site Files')
- Status: Running average: 100 requests: 0.0055 sec, 30 requests: 0.0455 sec.
```

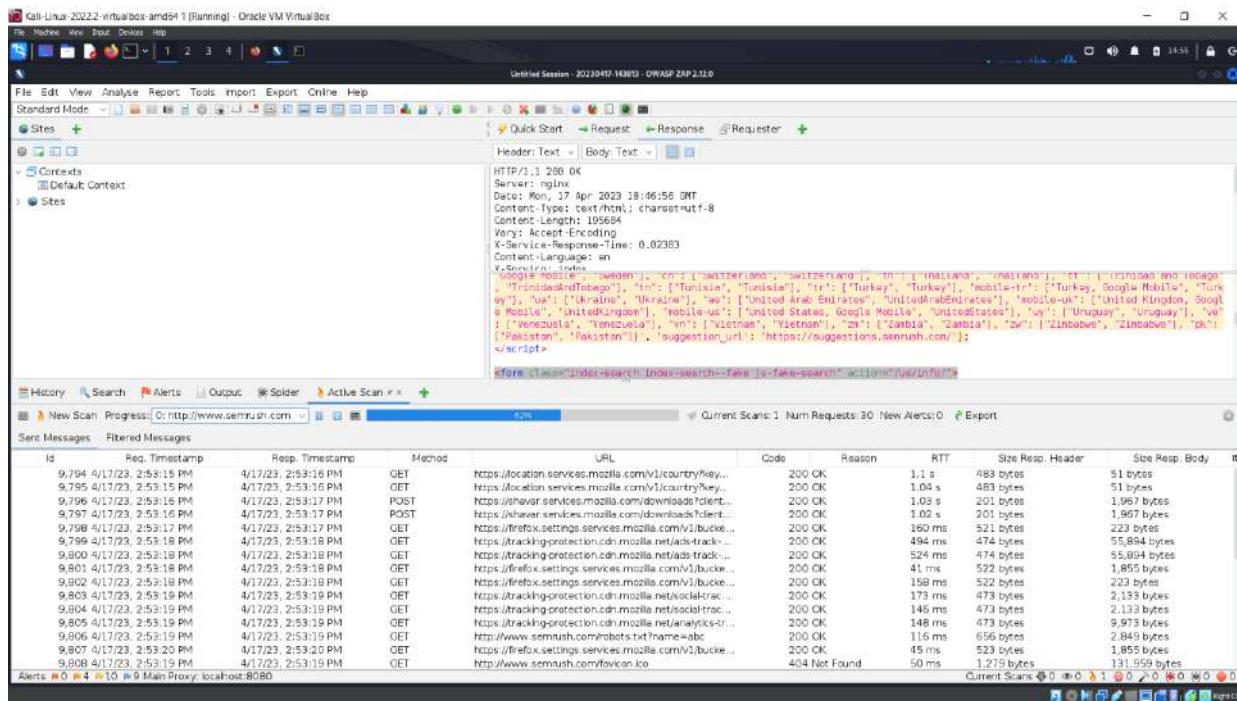
This scanner was not successful in discovering any vulnerabilities inside the system.

## Using OWASP-ZAP tool



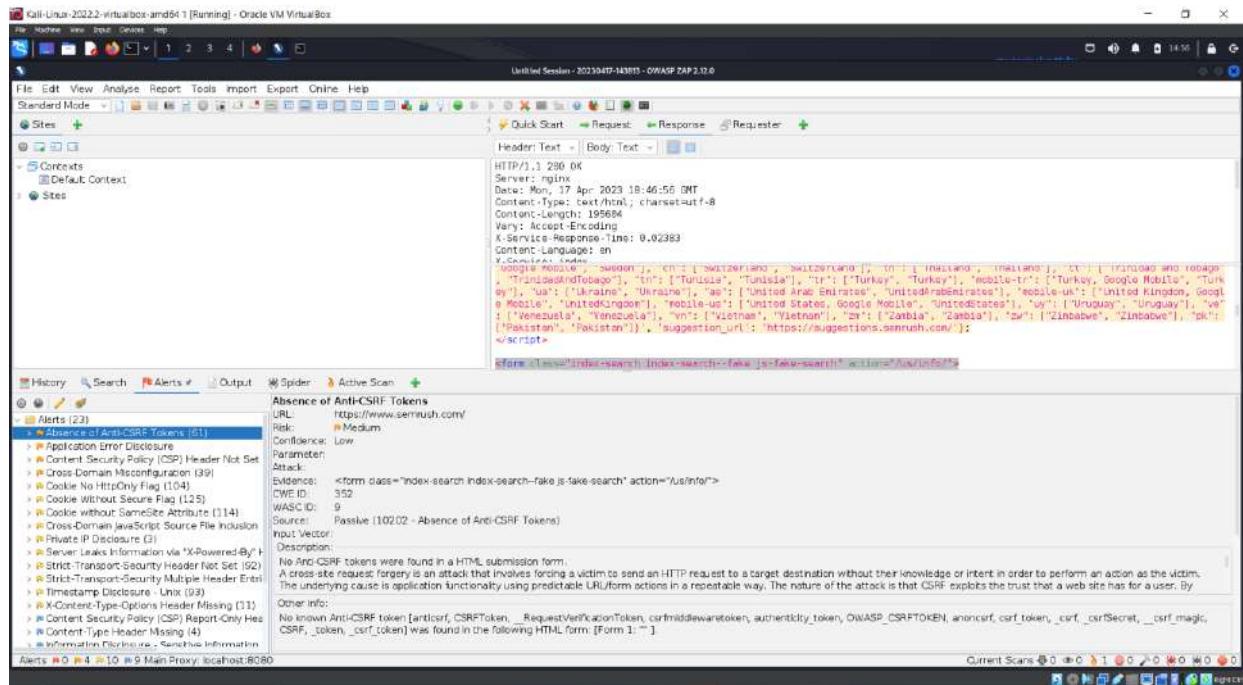
Found 11388 URLs.

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.

The screenshot shows the Netsparker interface with a scan in progress. The main window displays a tree view of the scanned website's structure under 'Sitemap - Previous Settings'. A 'Updates' section provides links to Invicti Scanners Release Announcements and Invicti Standard Change Log. Below this is a 'Web Application Security Blog' section with a link to Invicti Insights: Squashing AppSec urban myths and legends. A 'Progress' chart shows 'Scan Speed' over time, with a current progress of 97.70%. The bottom status bar indicates 'Scan Paused' at 2%, with various request counts: 1464 URLs, 2 Failed Requests, 324 404 Responses, 800 Head Requests, and a total of 1000 Requests. The 'Netsparker Assistant' sidebar on the right lists several alerts: 'Max Parameters to Attack Reached' (with a note about increasing the 'Maximum Number of Parameters to Attack on a Single Page' value), 'DOM Simulation Timeout Exceeded' (with a note about increasing the 'DOM Simulation Timeout' value), and 'Skip Threshold Reached' (with a note about increasing the 'Skip Threshold' value or using 'Exclude by CSS selector'). There is also a note about 'Scan Policy Optimized'.



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 |
|---------|--|--------|---|-----------|
| 1       | Weak Ciphers Enabled                             | GET    | https://www.semrush.com/  |           |
| 1       | [Possible] Internal IP Address Disclosure        | GET    | https://www.semrush.com/marketplace/?nsextt=%2522%252bnet sparker(0x004278)%252b%2522 | nsextt    |
| 1       | [Possible] Phishing by Navigating Browser Tabs   | GET    | https://www.semrush.com/kb/?nsextt=%60ans%3anetsparkers056650%3dvuln                  | nsextt    |
| 1       | Misconfigured Access-Control-Allow-Origin Header | GET    | https://www.semrush.com/splitsignal/  |           |
| 1       | Cookie Not Marked as HttpOnly                    | POST   | https://www.semrush.com/i18n/set_language/  |           |
| 1       | Cookie Not Marked as Secure                      | GET    | https://www.semrush.com/  |           |
| 1       | Insecure Frame (External)                        | GET    | https://www.semrush.com/webinars/   |           |
| 1       | Internal Server Error                            | GET    | https://www.semrush.com/news/categories/WS_FTP.log                                    | URI-BASED |
| 1       | Content Security Policy (CSP) Not Implemented    | GET    | https://www.semrush.com/  |           |
| 1       | Expect-CT Not Enabled                            | GET    | https://www.semrush.com/  |           |
| 1       | Referrer-Policy Not Implemented                  | GET    | https://www.semrush.com/  |           |
| 1       | SameSite Cookie Not Implemented                  | GET    | https://www.semrush.com/  |           |
| 1       | Subresource Integrity (SRI) Not Implemented      | GET    | https://www.semrush.com/  |           |
| 1       | CDN Detected (Google Cloud CDN)                  | GET    | https://www.semrush.com/  |           |
| 1       | Email Address Disclosure                         | GET    | https://www.semrush.com/  |           |
| 1       | ExpressJS Identified                             | GET    | https://www.semrush.com/agencies/?HTTP://rB7.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.

#### **Vulnerabilities**

2.1. [https://www.semrush.com/marketplace/?nsextt=%2522%252bnetsparker\(0x004278\)%252b%2522](https://www.semrush.com/marketplace/?nsextt=%2522%252bnetsparker(0x004278)%252b%2522)

| Method | Parameter | Value                            |
|--------|-----------|----------------------------------|
| GET    | nsextt    | %22%2bnetsparker(0x004278)%2b%22 |
| GET    | param1    | marketplace                      |

#### **Extracted IP Address(es)**

- 10.8.5.5

#### **Certainty**



### 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=CN2RtpWFyrXeoAE; PHPSESSID=8ae51cda77ff18c1dbe889989f0e27a8; SSO-JWT=eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJqdGkiOiI4YWU1MWNkYTc3ZmYxOGMxZGJlODg50Tg5ZjB1MjdhOCIsImlhCI6MTY4Mjk2OTYxNyviaXNzIjoic3NvIn0.RtusJabvCSmeuD5i-Q4D7W_ud3149480aLzi13s6QTxBgI_JrbclpLBXNZKL4jz-mzAXDvVXvlatkqOctiNIRg; app_center_csrf_token=142239eac0cf4dcbb4dafd048b94a5f6; site_csrftoken=e9QzgUKHQ42xWalPEMdifwtoi5Ih55SubyiZYDSEK0sXw08rJUxBs0nfxE2dU9hsI; localization=%78%22locale%22%3A%22en%22%7D; XSRF-TOKEN=eyJpdiI6InJWSGtQQ3lsR0UrS05ESUpabjUxY0E9PSISInZhbHVlIjoIZSsxUm5nM3VBTUhIU1BsR2VISGpVS0dhNGZGb0dGV1dnSExqRjf1STN1eVNaWG5hQ1R1a3hjd3NvVzdzTEtcLzYilCjtYWMiOiiwNTRhOT1lNWU4ZjV1ZGEExMmUzMDYxMjM0ZjY1MzE4YWY2MTJiZDhhZjkxYjM1YzU0YjcyZDM2ODNkYzVmN2M1In0%3D; webinars_session=nJDKdUjk5Gqh1dRd7x1arb70z0WEit18Y3D8nn1Q; csrftoken=fF84v2UDzYZoJBqq3PizXuuVU3bvDfGKY8dM1vgFDC3k3z1XhFSNUyiQuQhLZC1c
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
00-3.2-2.61-1.6 2.6zm-10 16110.8-19a13.5 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 23.8117.7 41.8h-1.11-17.6-4
...
```

## 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

The screenshot shows the HackerOne interface with a report details page. The report is titled "[Possible] Internal IP Address Disclosure" and was submitted by user #2003932 [dark\_k08]. The report is marked as "Pre-submission (Open)". Key details include:

- Participants:** dark\_k08
- State:** Pre-submission (Open)
- Reported to:** Semrush
- Severity:** No Rating (---)
- Asset:** \*.semrush.com
- Weakness:** Information Disclosure
- Time spent:** 3h
- Visibility:** Private
- CVE ID:** None
- Account de...:** None

The report content includes:

- Timeline - Export:** Shows the submission timestamp: May 27, 2023, 3:48am UTC.
- Summary:** dark\_k08 submitted a report to Semrush.
- Description:** 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.
- 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.
- 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

## **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.

A screenshot of a web browser window showing the Wickr Bug Bounty Program on the hackerone.com platform. The page displays various metrics and reward levels for the bounty program.

| Rewards   | Low     | Medium   | High     | Critical  |
|---|---------|----------|----------|-----------|
| Wickr Pro/Wickr Me (all related technical components) (up to) | \$1,000 | \$10,000 | \$25,000 | \$100,000 |

Metrics shown on the right side:

- Bug Bounty Program Launched on Nov 2021
- Managed by HackerOne
- Includes rebasing
- 4 hrs Average time to first response
- 22 hrs Average time to triage
- Average time to bounty
- Average time to resolution
- 100% of reports

A screenshot of the Wickr homepage. The main headline reads "DATA RETENTION WITHOUT COMPROMISE". Below it, a sub-headline says "Protect all of your communications — from video conferences to group messaging and file sharing — with Wickr." There are two calls-to-action: "Download Wickr" and "Contact Sales".

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

File Machine View Input Device Help

Wicker | Bug Bounty Proj... AWS Wicker | Secure Comm...

In Scope

|    | Domain   | Critical       | Eligible |          |
|----|--|----------------|----------|----------|
| 1  | admin.wicker.com   | Critical       | Eligible |          |
| 2  | Wicker Pro Wicker Metal related technical component tool | Critical       | Eligible |          |
| 3  | Wicker Pro Android                                       | Critical       | Eligible |          |
| 4  | Wicker Pro iOS   | Critical       | Eligible |          |
| 5  | Wicker Pro Linux   | Critical       | Eligible |          |
| 6  | Wicker Me iOS  | Critical       | Eligible |          |
| 7  | Wicker Me Android  | Critical       | Eligible |          |
| 8  | Wicker Me Linux  | Critical       | Eligible |          |
| 9  | Wicker Me OS X   | Critical       | Eligible |          |
| 10 | Wicker Pro OS X  | Critical       | Eligible |          |
| 11 | Wicker Pro Windows                                       | Critical       | Eligible |          |
| 12 | Wicker Me Windows  | Critical       | Eligible |          |
| 13 | Domain   | www.wicker.com | Critical | Eligible |

Out of Scope

|   | Domain             | Critical | Eligible |
|---|--------------------|----------|----------|
| 1 | support.wicker.com | Critical | Eligible |

Scopes

Opportunities Security Underload Big Data Support Dictionary Guidelines News Privacy Terms

Download Burp Suite Project Configuration File (SURL) View Changes Last updated on November 10, 2022.

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

File Machine View Input Device Help

Wicker | Bug Bounty Proj... AWS Wicker | Secure Comm...

In Scope

|    | Domain             | Critical       | Eligible |          |
|----|--------------------|----------------|----------|----------|
| 1  | Wicker Pro Android | Critical       | Eligible |          |
| 2  | Wicker Pro iOS     | Critical       | Eligible |          |
| 3  | Wicker Pro Linux   | Critical       | Eligible |          |
| 4  | Wicker Me iOS      | Critical       | Eligible |          |
| 5  | Wicker Me Android  | Critical       | Eligible |          |
| 6  | Wicker Me Linux    | Critical       | Eligible |          |
| 7  | Wicker Me OS X     | Critical       | Eligible |          |
| 8  | Wicker Pro OS X    | Critical       | Eligible |          |
| 9  | Wicker Pro Windows | Critical       | Eligible |          |
| 10 | Wicker Me Windows  | Critical       | Eligible |          |
| 11 | Domain             | www.wicker.com | Critical | Eligible |

Out of Scope

|   | Domain             | Critical | Eligible |
|---|--------------------|----------|----------|
| 1 | support.wicker.com | Critical | Eligible |

Scopes

Opportunities Security Underload Big Data Support Dictionary Guidelines News Privacy Terms

Download Burp Suite Project Configuration File (SURL) View Changes Last updated on November 10, 2022.

## 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.

The screenshot shows a Kali Linux desktop environment with a browser window open to the Netcraft website. The URL in the address bar is <https://site-report.netcraft.com/www.wickr.com>. The page displays detailed information about the domain, including its background, network details, and IP delegation. Key findings include:

- Background:** Site ID: 312002, Last seen: September 2014, Netcraft Risk Rating: 6/10.
- Network:** Hosted by Amazon.com, Inc., using AWS Lambda. IP address 13.224.68.66 is associated with Amazon Technologies, Inc. (US).
- IP delegation:** The IP range 13.224.68.66-13.224.68.99 is delegated to Internet Assigned Number Authority (IANA) and American Registry for Internet Numbers (ARIN).

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wicker | Bug Bounty Prog... AWS Wicker | Secure Cons... Site report for https://www.wicker.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All Labs Web Security ...

**NETCRAFT**

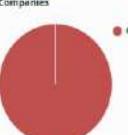
Services Solutions News Company Resources Discover More Report Fraud

**Web Trackers**

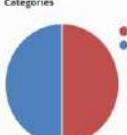
Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics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

2 known trackers were identified.

**Companies**



**Categories**



| Company    | Primary Category | Tracker          | Popular sites with this Tracker                           |
|------------|------------------|------------------|---|
| Google [2] | Analytics        | GoogleTagManager | www.risingweb.com, www.cnn.com, www.netcraft.com          |
|            | CDN              | GoogleCDN        | www.netflix.com, www.netflix.ca, www.banquecanadienne.com |

**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 [4] | Amazon Content Delivery Network                | www.tdc.com, www.mapillary.com, www.amazon.ca |
| Amazon Web Services - S3 [4]         | Cloud storage service (Simple Storage Service) | www.netflix.com, www.netflix.ca, www.tdc.ca   |

Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Wicker | Bug Bounty Prog... AWS Wicker | Secure Cons... Site report for https://www.wicker.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All Labs Web Security ...

**NETCRAFT**

Services Solutions News Company Resources Discover More Report Fraud

**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 [4] | Amazon Content Delivery Network                | www.tdc.com, www.mapillary.com, www.amazon.ca |
| Amazon Web Services - S3 [4]         | Cloud storage service (Simple Storage Service) | www.netflix.com, www.netflix.ca, www.tdc.ca   |

**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 [5] | Mostly-supported programming language commonly used to power client-side dynamic content on websites. | http://www.esri.com/arcgis/demand.com |

**Client-side Scripting Frameworks**

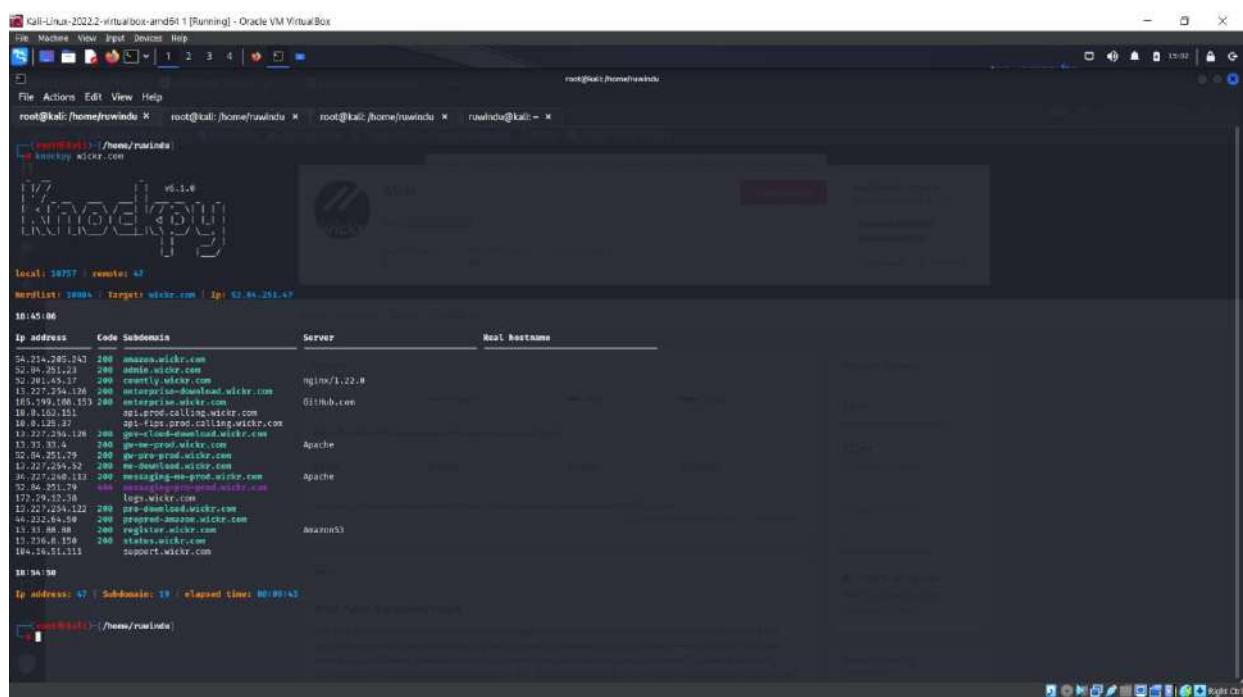
Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

| Technology             | Description  | Popular sites using this technology            |
|------------------------|--|--|
| Google Tag Manager [4] | No description   | www.esri.com, www.w3schools.com, www.chess.com |
| jQuery [4]             | A JavaScript library used to simplify the client-side scripting of HTML. | www.esri.com, www.amazon.tv, www.amazon.com    |

**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.



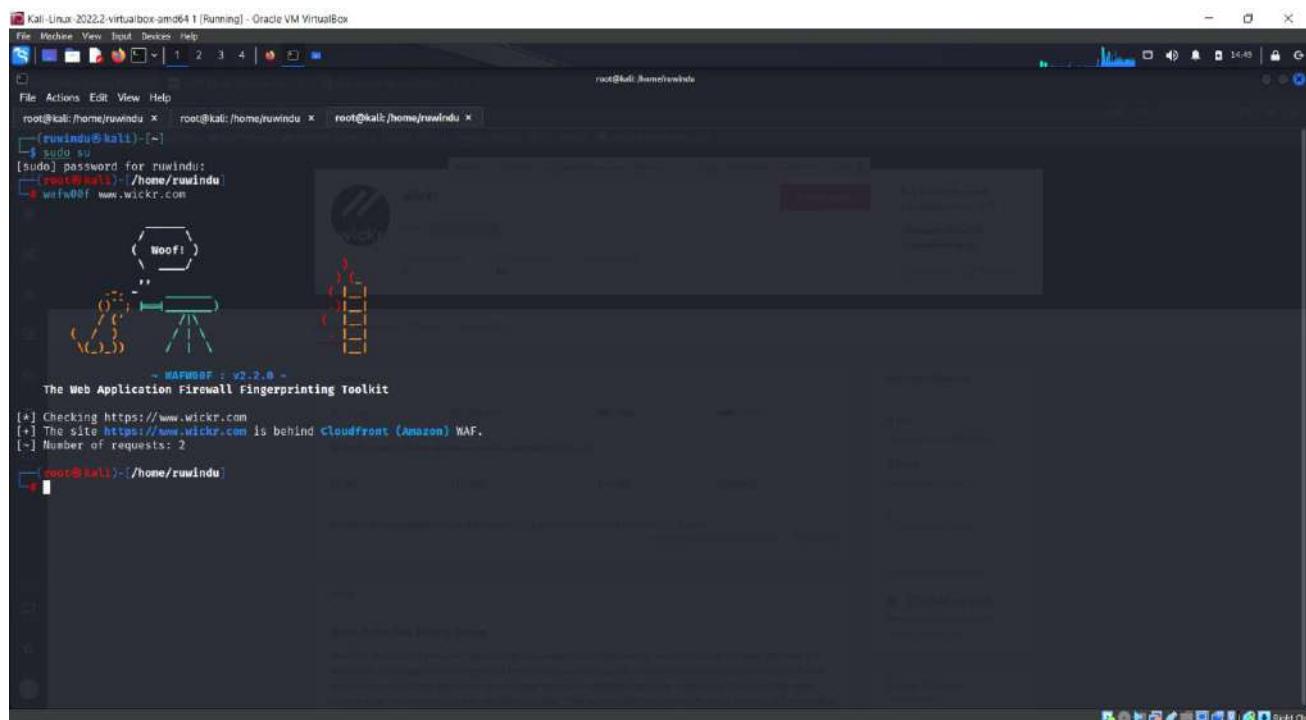
The screenshot shows a Kali Linux terminal window with several tabs open. The current tab displays the output of the knockpy tool. The output lists numerous subdomains of the target domain wickr.com, along with their IP addresses, port numbers (mostly 200), and server types (nginx, Apache, or NginxS3). A preview of a website page is visible in the background of the terminal window.

| IP address     | Code | Subdomain                       | Server       | Real hostname |
|----------------|------|---------------------------------|--------------|---------------|
| 54.234.205.243 | 200  | amazon.wickr.com                |              |               |
| 52.04.25.23    | 200  | admin.wickr.com                 |              |               |
| 52.201.45.37   | 200  | covertly.wickr.com              | nginx/1.22.0 |               |
| 13.227.159.176 | 200  | enterprise-download.wickr.com   |              |               |
| 100.99.103.03  | 200  | fileprod.wickr.com              |              |               |
| 10.0.103.151   | 200  | fileprod.calling.wickr.com      | GithHub.com  |               |
| 10.0.128.37    | 200  | opt-fips.prod.calling.wickr.com |              |               |
| 13.227.230.128 | 200  | geo-cloud-download.wickr.com    |              |               |
| 13.227.230.129 | 200  | geo-cloud.wickr.com             | Apache       |               |
| 50.24.251.79   | 200  | gv-pre-prod.wickr.com           |              |               |
| 13.227.234.52  | 200  | gv-download.wickr.com           |              |               |
| 36.227.124.113 | 200  | message-ing-prod.wickr.com      | Apache       |               |
| 52.23.125.100  | 200  | msg-ing-prod.wickr.com          |              |               |
| 173.29.12.38   | 200  | log.wickr.com                   |              |               |
| 13.227.234.122 | 200  | pre-download.wickr.com          |              |               |
| 46.222.64.58   | 200  | prepared-ingress.wickr.com      |              |               |
| 13.227.234.58  | 200  | register.wickr.com              | NginxS3      |               |
| 13.236.4.58    | 200  | storage.wickr.com               |              |               |
| 104.19.51.111  | 200  | support.wickr.com               |              |               |

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.

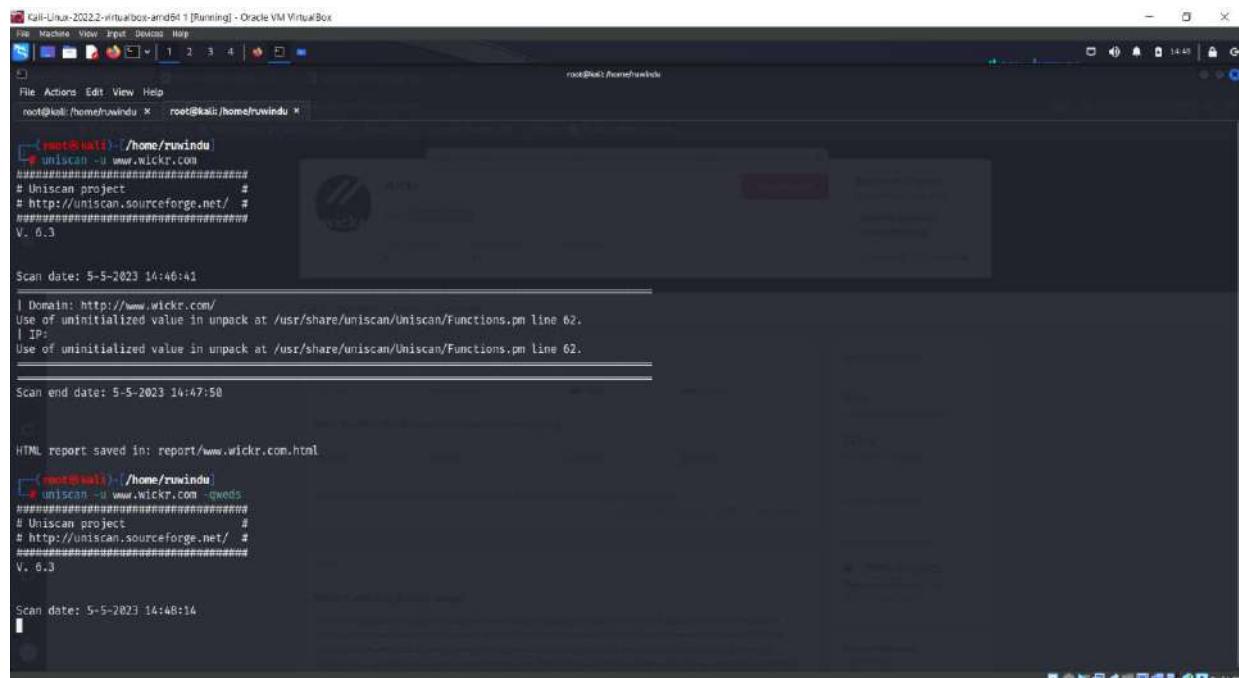


```
Kali-Linux-2022.2-virtualbox-amd64.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# su
[sudo] password for ruwindu:
[root@kali:~# /home/ruwindu/wafw00f www.wickr.com
[*] Checking https://www.wickr.com
[+] The site https://www.wickr.com is behind CloudFront (Amazon) WAF.
[-] Number of requests: 2
[root@kali:~#
```

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.



```
Kali-Linux-2022.2-virtualbox-amd64-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/rwinda ~ root@kali:/home/rwinda ~
root@kali:~/home/rwinda ~ root@kali:/home/rwinda ~
root@kali:~/home/rwinda ~ uniscan -u www.wickr.com
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

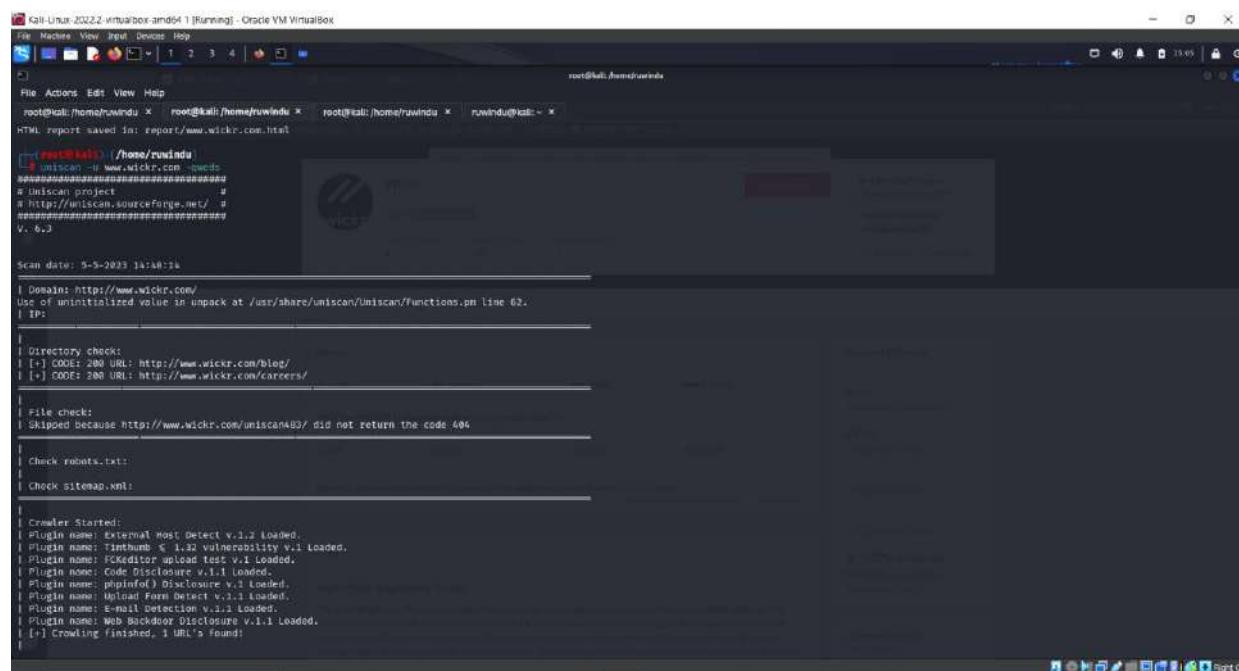
Scan date: 5-5-2023 14:46:42
| Domain: http://www.wickr.com/
| Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
| Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.

Scan end date: 5-5-2023 14:47:50

HTML report saved in: report/www.wickr.com.html
root@kali:~/home/rwinda ~ uniscan -u www.wickr.com -qweds
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 5-5-2023 14:48:14
```

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



```
Kali-Urux-2022.2-virtualbox-amd64-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:/home/rwinda ~ root@kali:/home/rwinda ~ root@kali:/home/rwinda ~ rwinda@kali:~ 
root@kali:~/home/rwinda ~ uniscan -u www.wickr.com -qweds
#####
# Uniscan project      #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 5-5-2023 14:48:34
| Domain: http://www.wickr.com/
| Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
| Directory check:
| (+) CODE: 200 URL: http://www.wickr.com/blog/
| (+) CODE: 200 URL: http://www.wickr.com/careers/
| File check:
| Skipped because http://www.wickr.com/uniscan403/ did not return the code 404
| Check robots.txt:
| Check sitemap.xml:
| Crawling Started:
| Plugin name: External Host Detect v.1.2 Loaded.
| Plugin name: Tintthumb < 1.32 vulnerability v.1 Loaded.
| Plugin name: FCKeditor upload test v.1 Loaded.
| Plugin name: Code Disclosure v.1.1 Loaded.
| Plugin name: Clickjacking v.1.1 Loaded.
| Plugin name: Upload Form Detect v.1.1 Loaded.
| Plugin name: E-mail Detection v.1.3 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| (+) Crawling finished, 1 URL's Found!
```

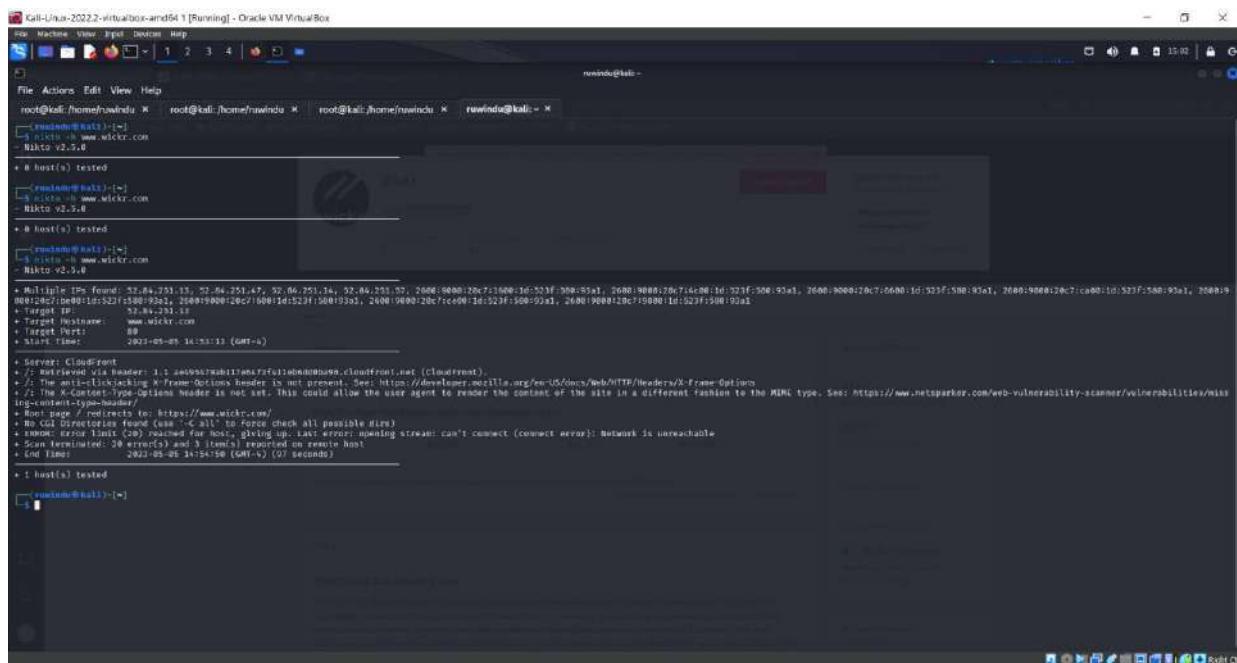
```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
root@kali:/home/rwindsu x root@kali:/home/rwindsu x rwindsu@kali: ~  
External hosts:  
Tiuthmb:  
FCKeditor File Upload:  
Source Code Disclosure:  
PHPInfo() Disclosure:  
File Upload Forms:  
E-mails:  
Web Backdoors:  
Ignored Files:  
Dynamic tests:  
Plugin name: learning New Directories v.1.2 loaded.  
Plugin name: FCKeditor tests v.1.1 loaded.  
Plugin name: Tiuthmb < 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 v.1.1 loaded.  
Plugin name: Remote File Include tests v.1.1 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.  
(-) 8 New directories added  
  
FCKeditor tests:  
Skipped because http://www.wickr.com/testing22 did not return the code 404  
  
Tiuthmb < 1.33-vulnerability:  
  
Backup Files:
```

```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
root@kali:/home/rwindsu x root@kali:/home/rwindsu x rwindsu@kali: ~  
Local File Include:  
PHP CGI Argument Injection:  
Remote Command Execution:  
Remote File Include:  
SQL Injection:  
Cross-Site Scripting (XSS):  
Web Shell #lndert:  
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: 5-5-2023 14:35:10  
  
HTML report saved in: report/www.wickr.com.html  
www.wickr.com/home/rwindsu
```

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

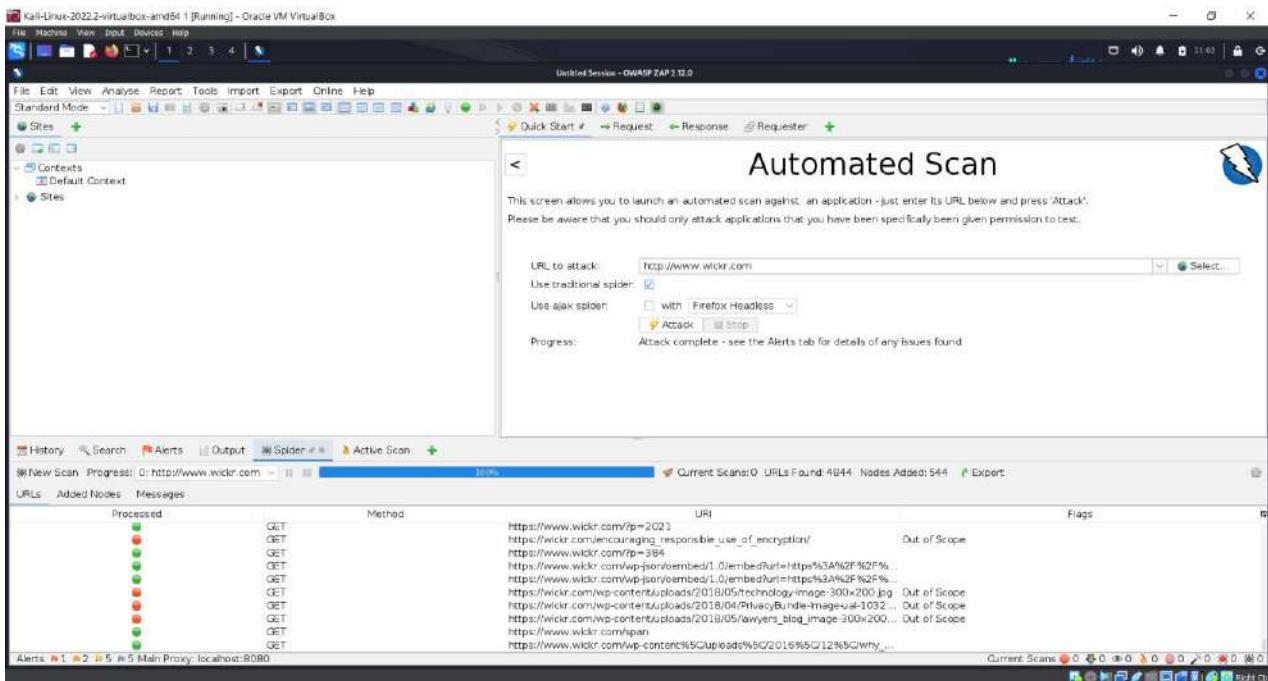
We are provided with a greater number of high-level options and the nikto tool is utilised to cane the target domain when we run the command with the –h switch.



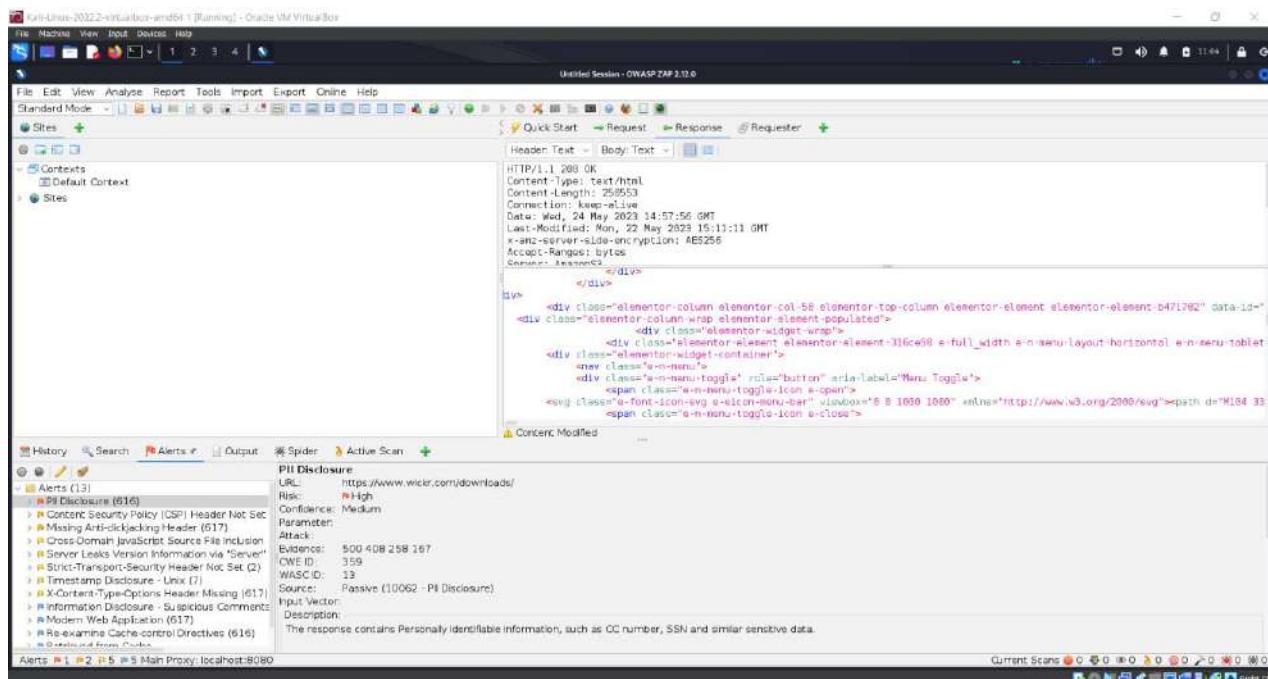
```
Kali-Linux-2022.2-virtualbox-amd64 1 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
root@kali:~# nikto -h www.wicker.com  
nikto v2.5.0  
+ # hosts(1) tested  
+ root@kali:~# nikto -h www.wicker.com  
nikto v2.5.0  
+ # hosts(1) tested  
+ root@kali:~# nikto -h www.wicker.com  
nikto v2.5.0  
+ Multiple IP Found: 52.84.231.15, 52.84.251.47, 52.84.251.14, 52.84.231.57, 2608:9080:20c7:52f:508:93a1, 2608:9080:20c7:52f:508:93a1, 2608:9080:20c7:52f:508:93a1, 2608:9080:20c7:52f:508:93a1, 2608:9080:20c7:52f:508:93a1  
+ Target IP: 52.84.231.15  
+ Target Portname: www.wicker.com  
+ Threads: 4  
+ Start Timer: 2023-05-05 14:53:13 (GMT+4)  
+ Servers: CloudFront  
+ CloudFront Via Header: 1.1 aewssstwttt7ehfrfutibebanuse.cloudfront.net (CloudFront)  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netparker.com/web-vulnerability-scanner/vulnerabilities/misconfigurations-xcontent-type-options  
+ Root page redirects to: https://www.wicker.com  
+ No CGI Directories found (use '-C' to force check all possible dirs)  
+ Known error limit: 20 errors and 3 times requery on remote host  
+ End Timer: 2023-05-05 14:54:06 (GMT+4) (07 seconds)  
+ 1 hosts(1) tested  
root@kali:~#
```

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.

The screenshot shows the Netsparker application window. At the top, there's a toolbar with icons for Pause, Skip, Start, Proxy, Import Links, Scan, and Search. Below the toolbar is a menu bar with File, Home, View, Reporting, Help, and Scan Tools. The main area is titled "Welcome" and shows a "Sitemap - Previous Settings" tree view on the left. The central part displays "Updates" information, "Web Application Security Blog", and a "Choosing an MSSP? Ask about DAST for your web application security" section. On the right, there's a "Netsparker Assistant (1)" panel with a message about "Maximum Signature Exceeded". At the bottom, there's a "Progress" bar showing "Scan Progress: 100%", "Links: 922", "Failed Requests: 1", "Total Requests: 18437", "Elapsed: 00:00:59", "Start: 5/6/2023 12:20:52 AM", and "Estimated: 5/6/2023 11:29:44 AM". A status bar at the bottom includes "Crawling & Attack phase started.", "Knowledge Base (15)", and "Netsparker Assistant (1)".

This screenshot shows the detailed report for the scan of www.wickr.com. At the top, it displays the URL, Scan Time (5/6/2023 12:20:52 AM), Scan Duration (00:00:11:29), Total Requests (19,443), and Average Speed (28.2r/s). To the right, it shows the Risk Level: MEDIUM. Below this, there are three large boxes: one for IDENTIFIED vulnerabilities (14), one for CONFIRMED vulnerabilities (1), and one for CRITICAL vulnerabilities (0). The CRITICAL box has a red exclamation mark icon. Further down, there are two more boxes: one for HIGH vulnerabilities (0) and one for BEST PRACTICE (5). The report also includes sections for Identified Vulnerabilities (with a donut chart showing counts for Critical, High, Medium, Low, Best Practice, and Information) and Confirmed Vulnerabilities (with a yellow donut chart showing counts for Critical, High, Medium, Low, Best Practice, and Information). Both sections have their own risk level legends.

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 |
|---------|---|--------|--|-----------|
| !       | <a href="#">HTTP Strict Transport Security (HSTS) Errors and Warnings</a> | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">[Possible] Phishing by Navigating Browser Tabs</a>            | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Missing X-Frame-Options Header</a>                            | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Insecure Frame (External)</a>                                 | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Content Security Policy (CSP) Not Implemented</a>             | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Expect-CT Not Enabled</a>                                     | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Missing X-XSS-Protection Header</a>                           | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Referrer-Policy Not Implemented</a>                           | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Subresource Integrity (SRI) Not Implemented</a>               | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">[Possible] Internal Path Disclosure (*nix)</a>                | GET    | https://www.wickr.com/aws-wickr-a-secure-end-to-end-encrypte<br>d-communication-service-for-enterprises-with-auditing-and-reg<br>ulatory-requirements/ |           |
| !       | <a href="#">Email Address Disclosure</a>                                  | GET    | https://www.wickr.com/ramp/  |           |
| !       | <a href="#">Generic Email Address Disclosure</a>                          | GET    | https://www.wickr.com/terms/?hTtp://rB7.com/n  |           |
| !       | <a href="#">Out-of-date Version (jQuery)</a>                              | GET    | https://www.wickr.com/   |           |
| !       | <a href="#">Sitemap Detected</a>  | 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 : 201811 Body Length : 201183 Is Compressed : No

```
HTTP/1.1 200 OK
X-Amz-CF-Pop: SINS-CI
Server: AmazonS3
X-Cache: Miss from cloudfront
Connection: keep-alive
Via: 1.1 b4eebf047952c39ed1b8a9637b729e04.cloudFront.net (CloudFront)
Content-Encoding:
Last-Modified: Wed, 19 Apr 2023 16:05:12 GMT
Strict-Transport-Security: max-age=31536000; includeSubDomains
ETag: W/"h89ew533a289172422a4dh88d6679e03"
Content-Type: text/html
Transfer-Encoding: chunked
X-Amz-CF-Id: WcQgu0sGDLnahLSSKa2mN7Cn27ACKtgCP55W0Kq4o9TdE7TinOMl0w==
x-amz-server-side-encryption: AES256
Date: Fri, 06 May 2023 18:58:58 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/se/
-->
<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

The screenshot shows the HackerOne interface. On the left is a dark sidebar with navigation links: Opportunities, Dashboard, Inbox (highlighted in green), Hacktivity, Leaderboard, Directory, Notifications (with 1 notification), and Profile. The main content area shows a report titled '#2003936 Missing X-Frame-Options Header' submitted by 'dark\_k08' to 'Wickr'. The report details a clickjacking vulnerability due to the absence of an X-Frame-Options header. It includes a timeline entry from 'dark\_k08' and a detailed description of the X-Frame-Options header's purpose and potential defenses. To the right, there is a sidebar with report metadata: Reported May 27, 2023, 3:52am UTC; Participants (dark\_k08); State (New (Open)); Reported to (Wickr Managed); Severity (Medium (4 ~ 6.9)); Asset: Dom... (www.wickr.com); Weakness (Improper Neutralization of HTTP Headers for Scripting Syntax); Time spent (3h); Visibility (Private); CVE ID (None); and Account de... (None).

## x. Report 10

**Target information:** <https://www.yuga.com/>

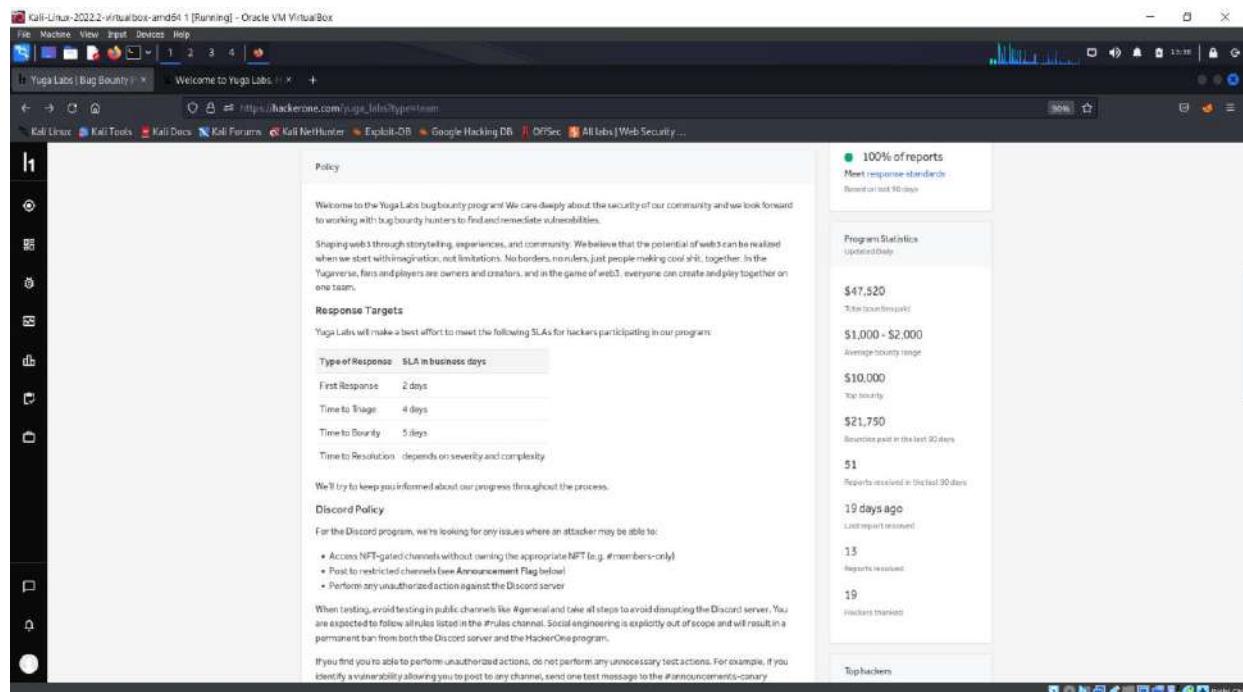
This evaluation aims to establish the risk associated with the target domain's (<https://www.yuga.com/>) possible vulnerabilities. The study also identifies target domain vulnerabilities. By identifying target domain vulnerabilities, we can attain these goals. To put it another way, this evaluation seeks 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.

The screenshot shows a web browser window titled "Yuga Labs Bug Bounty" on a Kali Linux desktop. The page displays the Yuga Labs logo and a brief description: "Yuga Labs is shaping web3 through storytelling, experiences, and community." It features a "Submit report" button and a "Bug Bounty Program" section stating "Launched on Dec 2022". Below this are statistics: "Reports resolved: 13", "Alerts in scope: 13", and "Average bounty: \$1k-\$2k". A sidebar on the left contains various icons. The main content area includes sections for "Rewards" (Low, Medium, High, Critical levels) and "Response Efficiency" (3 hrs, 4 hrs, 10 hrs, 2 days). At the bottom, there are links for "Policy", "Scope", "New", "Hacktivity", "Thanks", and "Updates (0)". The status bar at the bottom right shows "Last updated on July 18, 2022" and "View changes".

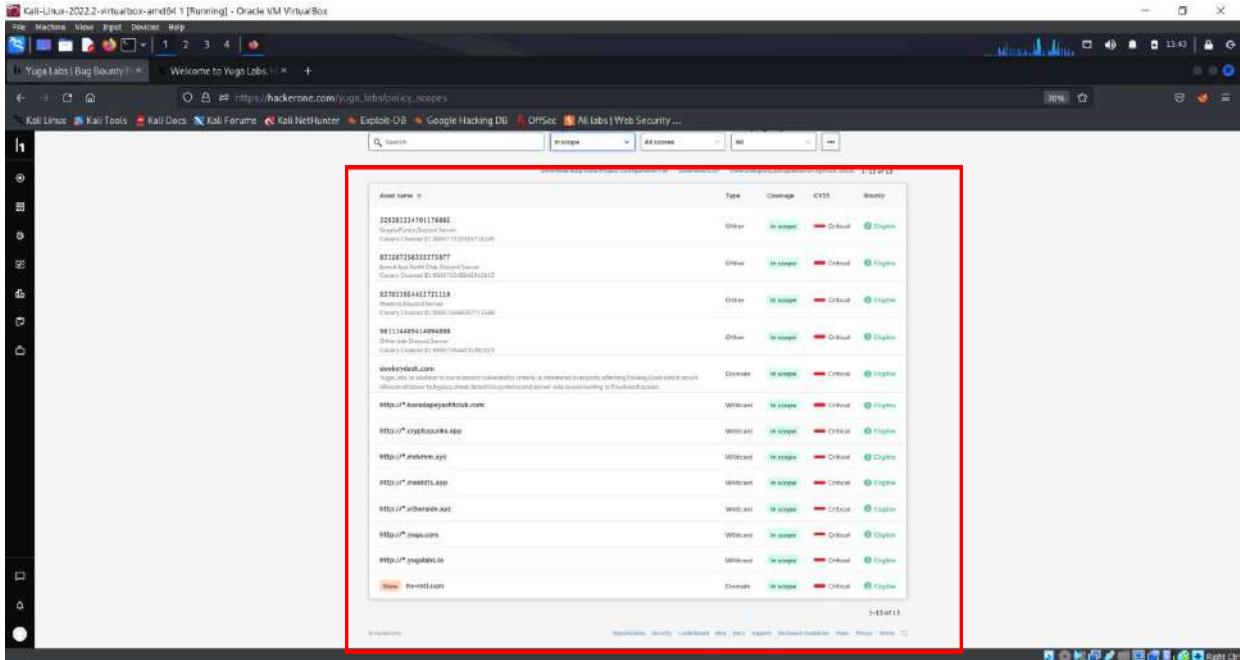
The screenshot shows a web browser window titled "Welcome to Yuga Labs, Inc." on a Kali Linux desktop. The page has a black background with a white abstract geometric pattern of dots and squares. At the top, it says "Welcome to Yuga Labs, Inc." and "Your place for decentralized web3 projects". Below this is a large "Join our team" button. The footer contains the Yuga Labs logo and links for "Home", "About", "Press", and "Careers". The status bar at the bottom right shows "Last updated on July 18, 2022" and "View changes".

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

File Machine View Input Devices Help

Yuga Labs | Bug Bounty Welcome to Yuga Labs Site report for https://www.yuga.com +

https://sitereports.netcraft.com/?url=https://www.yuga.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All Jobs Web Security ...

**NETCRAFT**

Services Solutions News Company Resources Discover More Report Fraud

**Background**

Site title: Welcome to Yuga Labs, Home of BAYC, MAYC, OtherSide, Cryptopunks, and Meetups Date first seen: March 2016

Site rank: 212948 Netcraft Risk Rating: 1/10

Description: Not Present Primary language: English

**Network**

| Site                    | https://www.yuga.com       | ICP                     | Domains   | yuga.com |
|-------------------------|----------------------------|-------------------------|---|----------|
| Netblock Owner          | Cloudflare, Inc.           | Nameserver              | poppy.m.cloudflare.com  |          |
| Hosting company         | Cloudflare                 | Domain registrar        | google.com  |          |
| Hosting country         | US                         | Nameserver organization | whois.cloudflare.com  |          |
| IPv4 address            | 172.66.40.154              | reverse ip              | Contact Privacy Inc. Customer 2151971251, 96 Merton Ave, Toronto, M4R 3K1, Canada |          |
| IPv4 autonomous systems | AS13335                    | IP                      | dnsadmin.cloudflare.com   |          |
| IPv6 address            | 2606:4700:3101:612::42:289 | Top Level Domain        | commercialentities.com  |          |
| IPv6 autonomous systems | AS13335                    | IP                      | DNS Security Extensions   |          |
| Reverse DNS             | unknown                    |                         | Enabled   |          |

**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

File Machine View Input Devices Help

Yuga Labs | Bug Bounty Welcome to Yuga Labs Site report for https://www.yuga.com +

https://sitereports.netcraft.com/?url=https://www.yuga.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec All Jobs Web Security ...

**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 | Content delivery network and distributed domain name server service | www.chess.com, www.camra.com, www.ilovepdf.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 | reg20053.sso.creandemand.com, twitter.com |

**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.

| Technology | Description   | Popular sites using this technology               |
|------------|---|---|
| Cloudflare | Content delivery network and distributed domain name server service | www.econia.org, www.udemy.com, www.wappalyzer.com |

**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.

```
v6.1.0
[!] KNOCKPY [!]
[!] v6.1.0

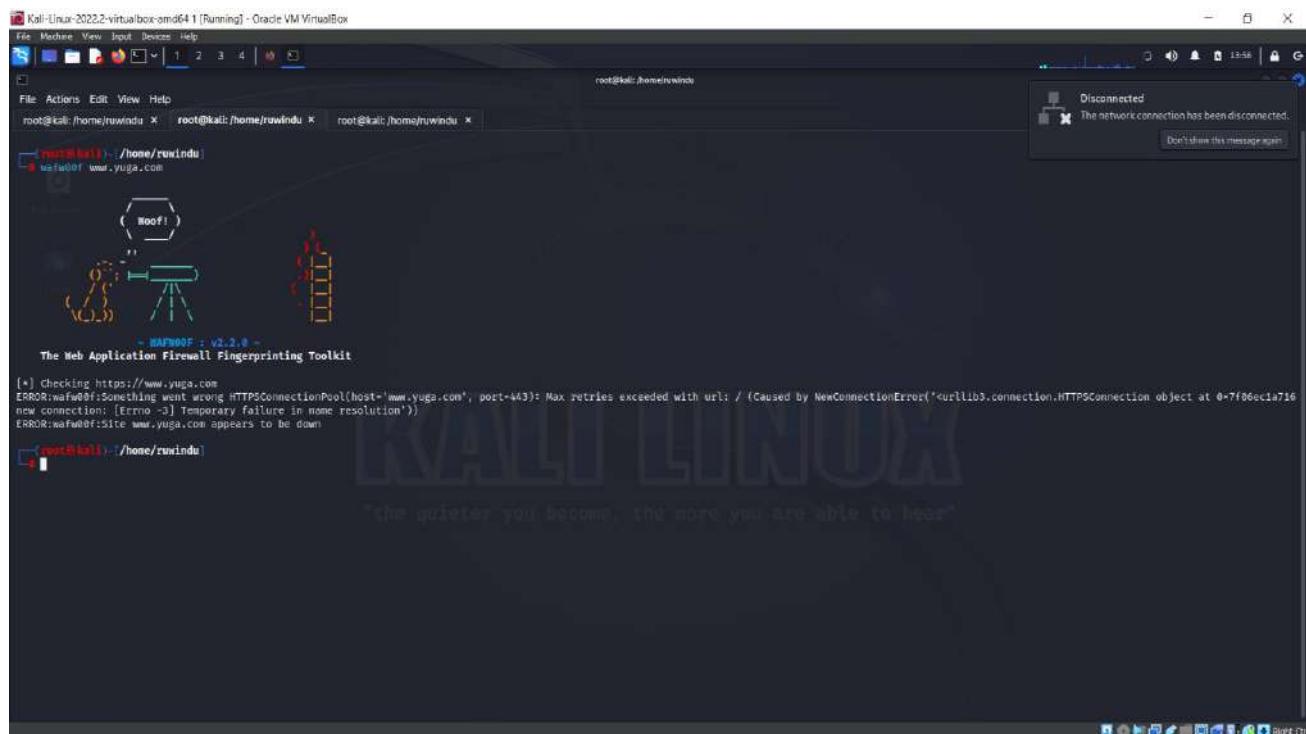
local: 10737 | remote: 6
Wordlist: 10763 | Target: yuga.com | Ip: 172.68.43.102
17:53:08
Ip address      Code Subdomain          Server           Real hostname
172.68.43.102   404 assets.yuga.com       cloudflare
17:54:56
Ip address: 2 | Subdomain: 1 | elapsed time: 00:01:55

[root@kali ~]#
```

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.

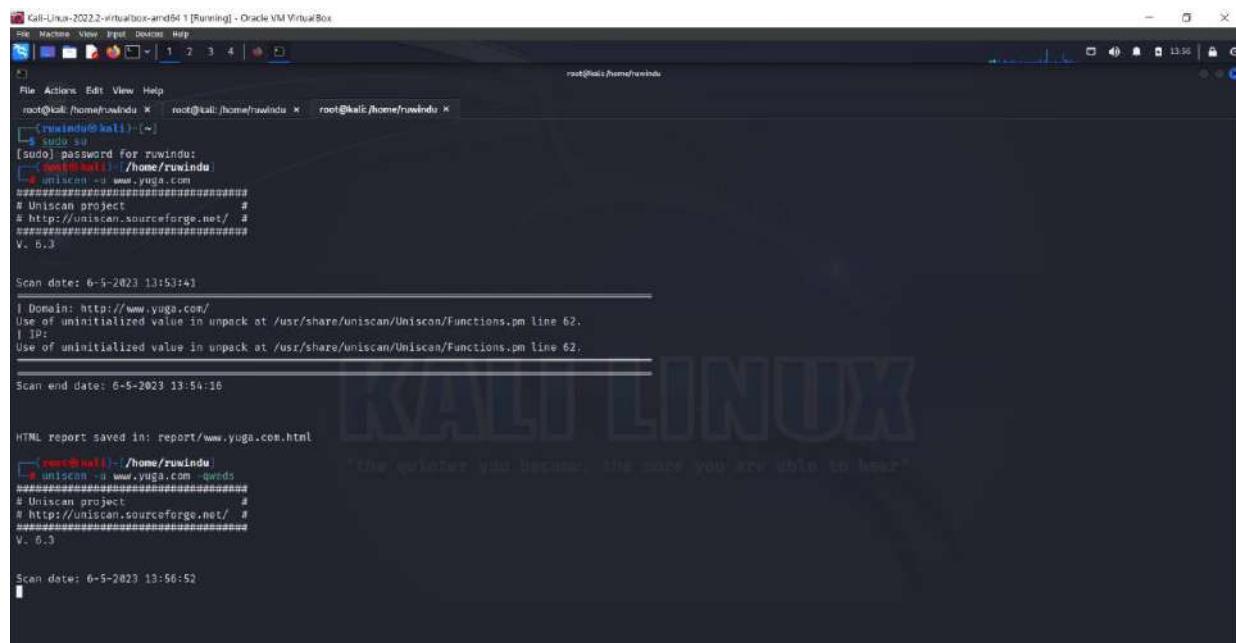


```
Kali-Linux-2022.2-virtualbox-ova64.1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# ./wafw00f -v www.yuga.com
[*] Checking https://www.yuga.com
ERROR:wafw00f[Something went wrong HTTPSConnectionPool(host='www.yuga.com', port=443): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPSConnection object at 0x7f06ec1a7160>'))
new connection: [Errno -3] Temporary failure in name resolution']
ERROR:wafw00f[Site www.yuga.com appears to be down]
root@kali:~#
```

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.



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# uniscan -u www.yuga.com -qweds
[sudo] password for ruwindu:
[uniscan@kali] ~
[uniscan] www.yuga.com
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

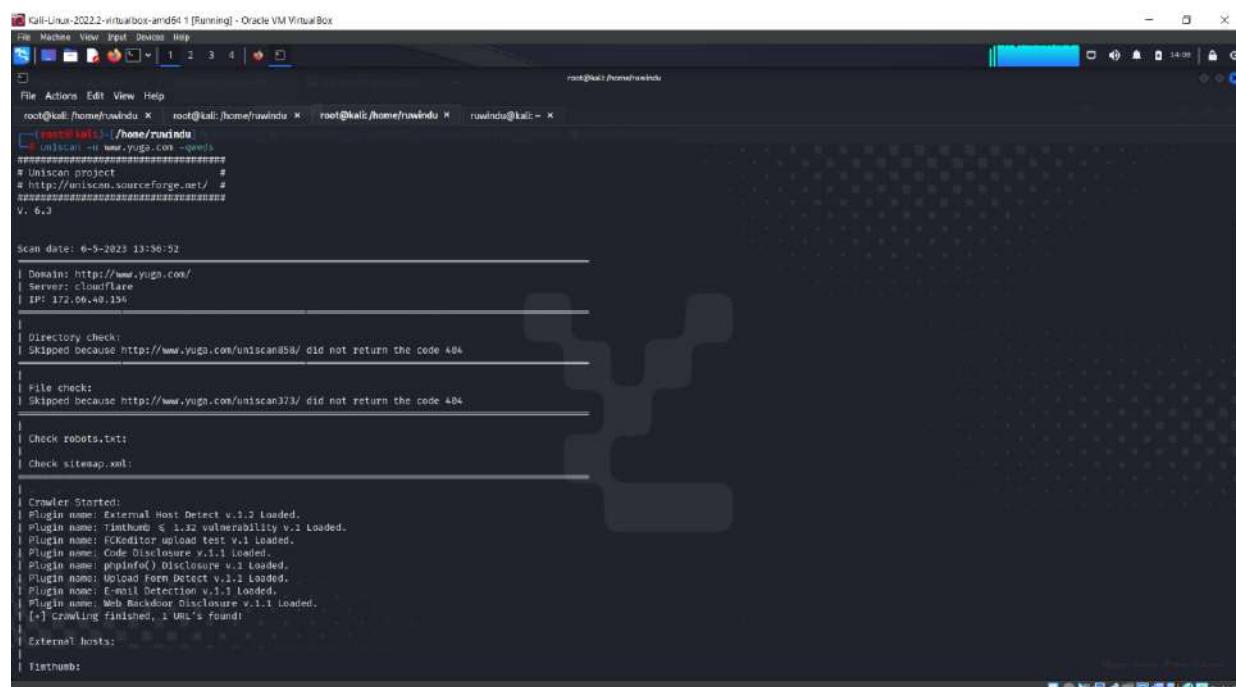
Scan date: 6-5-2023 13:53:41
| Domain: http://www.yuga.com/
| Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.
| IP:
| Use of uninitialized value in unpack at /usr/share/uniscan/Uniscan/Functions.pm line 62.

Scan end date: 6-5-2023 13:54:16

HTML report saved in: report/www.yuga.com.html
[uniscan@kali] ~
[uniscan] www.yuga.com -qweds
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 6-5-2023 13:56:52
```

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



```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~# uniscan -u www.yuga.com -qweds
[sudo] password for ruwindu:
[uniscan@kali] ~
[uniscan] www.yuga.com
#####
# Uniscan project          #
# http://uniscan.sourceforge.net/ #
#####
V. 6.3

Scan date: 6-5-2023 13:58:52
| Domain: http://www.yuga.com/
| Server: Cloudflare
| IP: 92.206.40.134

|
| Directory check:
| Skipped because http://www.yuga.com/uniscan58/ did not return the code 404

|
| File check:
| Skipped because http://www.yuga.com/uniscan373/ did not return the code 404

|
| Check robots.txt
|
| Check sitemap.xml:
|
| Crawler Started:
| Plugin name: External Host Detect v.1.3 Loaded.
| Plugin name: LinkedIn S Links 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: Email Detection v.1.1 Loaded.
| Plugin name: Web Backdoor Disclosure v.1.1 Loaded.
| (+) crawling finished, 1 URL's found!
|
| External hosts:
|
| Favicon:
```

```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Device Help
root@kali:/home/rwwindu ~ root@kali:/home/rwwindu ~ root@kali:/home/rwwindu ~ rwwindu@kali: ~
| E-mails:
| web Backdoors:
| Ignored Files:
| Dynamic tests:
| Plugin name: Learning New Directories v.1.2 loaded.
| Plugin name: FCKeditor tests v.1.1 loaded.
| Plugin name: TiNthumU < 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 v.1.1 loaded.
| Plugin name: PHP CGT Argument Injection v.1.3 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: Web Shell Finder v.1.3 loaded.
| (+) 0 New directories added

| FCKeditor tests:
| Skipped because http://www.yuga.com/testing123 did not return the code 404

| TiNthumU < 1.31 vulnerability:
| Backup files:
| Skipped because http://www.yuga.com/testing123 did not return the code 404

| Blind SQL Injection:
| Local File Include:
| PHP CGT Argument Injection:
|
```

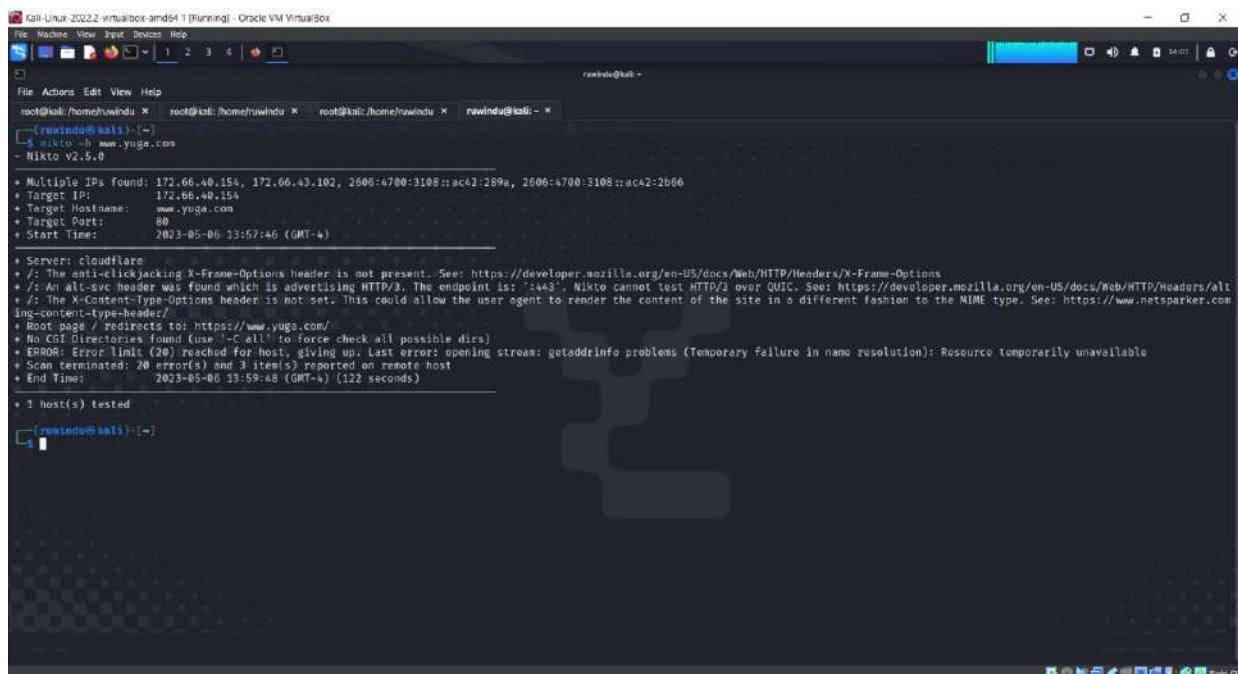
```
Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Device Help
root@kali:/home/rwwindu ~ root@kali:/home/rwwindu ~ root@kali:/home/rwwindu ~ rwwindu@kali: ~
| PHP CGT Argument Injection:
| Remote Command Execution:
| Remote File Include:
| SQL Injection:
| 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: 6-5-2023 13:59:13

HTML report saved in: report/www.yuga.com.html
└── report[www.yuga.com.html]
└── rwwindu@kali: /home/rwwindu
```

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.



```
Kali-Linux-2022.2-virtualbox-amd64-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~/.windu ~ root@kali:~/.windu ~ root@kali:~/.windu ~ rawindu@kali:~ 
(rawindu@kali:~) $ nikto -h www.yuga.com
- Nikto v2.5.0

* Multiple IPs found: 172.66.40.154, 172.66.43.102, 2606:4700:3108::ac42:189a, 2606:4700:3108::ac42:2866
* Target IP: 172.66.40.154
* Target Hostname: www.yuga.com
* Target Port: 80
* Start Time: 2023-05-06 13:57:46 (GMT-4)

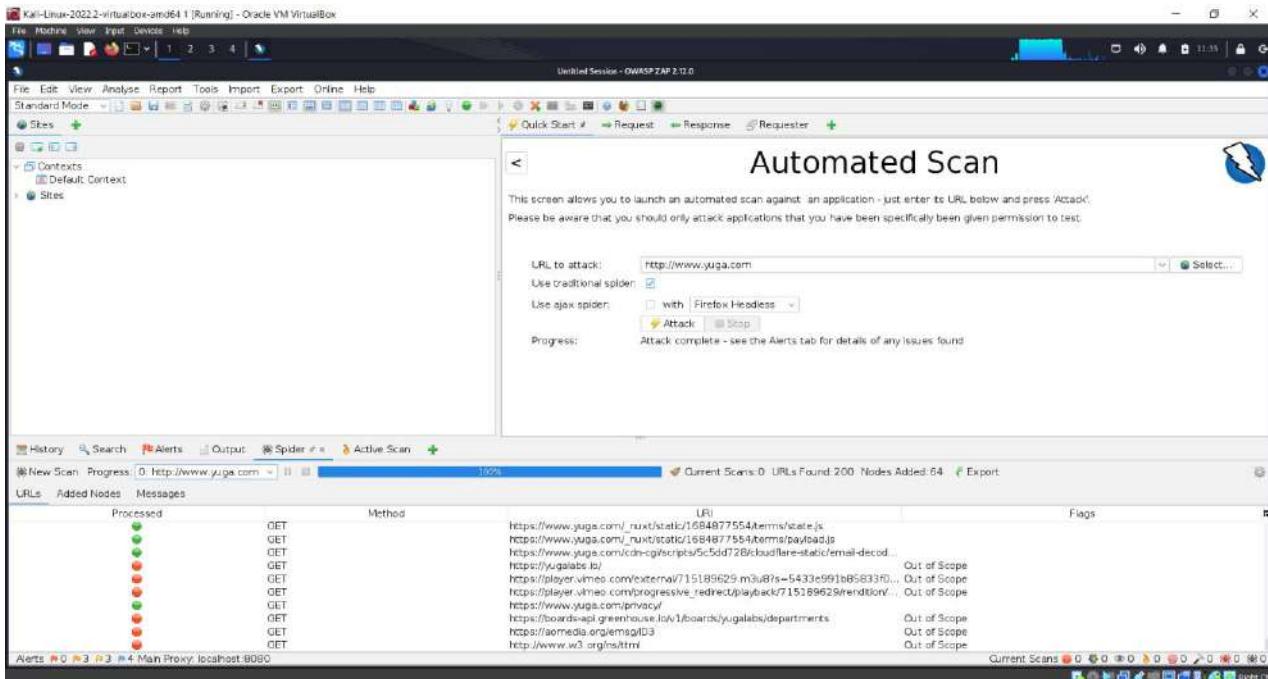
* Server: cloudflare
* /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
* /: An alt-svc header was found which is advertising HTTP/3. The endpoint is ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
* /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/img-content-type-header/
* Root page / redirects to: https://www.yuga.com/
* No CGI Directories found (use '-C all' to force check all possible dirs)
* ERROR: Error limit (20) reached for host, giving up. Last error: opening stream: getaddrinfo problems (Temporary failure in name resolution): Resource temporarily unavailable
* Scan terminated: 20 error(s) and 3 item(s) reported on remote host
* End Time: 2023-05-06 13:59:48 (GMT-4) (122 seconds)

* 1 host(s) tested

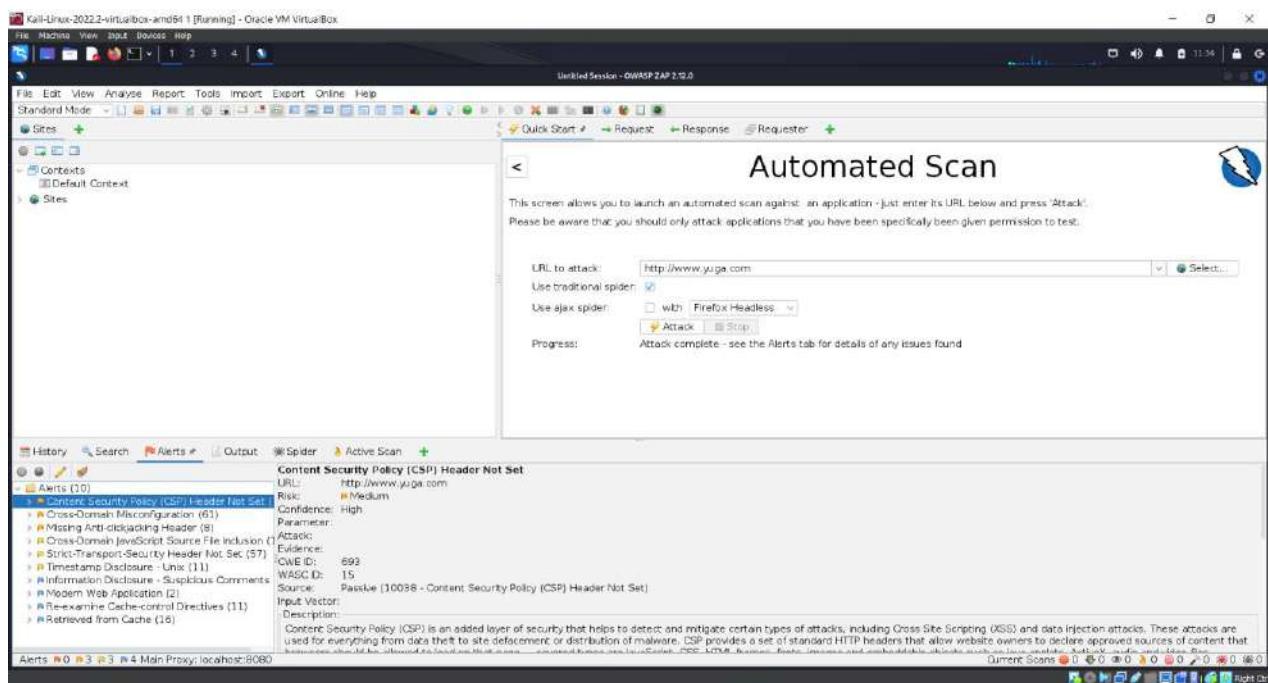
(rawindu@kali:~) $
```

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.

The screenshot shows the Netsparker interface with a scan in progress on the website [www.wickr.com](http://www.wickr.com). The main window displays the 'Updates' section, which includes links to 'Invicti Scanners Release Announcements' and 'Invicti Standard Change Log'. Below this is the 'Web Application Security Blog' section. The 'Issues' tab is selected, showing a list of vulnerabilities found, such as 'HTTP Strict Transport Security (HSTS) ...', 'Insecure Frame (External) (Variations: 1...)', and 'Content Security Policy (CSP) Not Impl...'. The 'Progress' tab shows a graph of the scan speed and statistics: 'Scan Progress: 100%', 'Links: 922', 'Failed Requests: 1', '404 Responses: 40', 'Total Requests: 18437', 'Elapsed: 00:00:59', 'Start: 5/6/2023 12:20:52 AM', and 'Estimated: 5/6/2023 11:29:44 AM'. A message in the top right corner states 'Maximum Signature Exceeded' with a note about increasing the 'Maximum Signature' value. The bottom of the interface includes tabs for 'Activity', 'Progress', and 'Logs (16)'.

The screenshot shows the Netsparker report for the website [www.yuga.com](http://www.yuga.com). The report summary indicates a 'Risk Level: MEDIUM'. Key findings include 17 identified vulnerabilities, 5 confirmed, 0 critical, 2 medium, 4 low, 5 best practice, and 6 information. The report is divided into two main sections: 'Identified Vulnerabilities' and 'Confirmed Vulnerabilities', each with a pie chart and a detailed table of counts for different severity levels (Critical, High, Medium, Low, Best Practice, Information).

| Vulnerability Type | Critical | High | Medium | Low | Best Practice | Information | Total |
|--------------------|----------|------|--------|-----|---------------|-------------|-------|
| Identified         | 0        | 0    | 2      | 4   | 5             | 6           | 17    |
| Confirmed          | 0        | 0    | 1      | 1   | 0             | 3           | 5     |

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 |
|---------|--|--------|--|-----------|
| !       | <a href="#">HTTP Strict Transport Security (HSTS) Policy Not Enabled</a> | GET    | https://www.yuga.com/  |           |
| !       | <a href="#">Weak Ciphers Enabled</a>                                     | GET    | https://www.yuga.com/  |           |
| !       | <a href="#">[Possible] Phishing by Navigating Browser Tabs</a>           | GET    | https://www.yuga.com/links/  |           |
| !       | <a href="#">Misconfigured Access-Control-Allow-Origin Header</a>         | GET    | https://www.yuga.com/_nuxt/  |           |
| !       | <a href="#">Missing X-Frame-Options Header</a>                           | GET    | https://www.yuga.com/opensearch.xml  |           |
| !       | <a href="#">Insecure Frame (External)</a>                                | GET    | https://www.yuga.com/opensearch.xml  |           |
| !       | <a href="#">Content Security Policy (CSP) Not Implemented</a>            | GET    | https://www.yuga.com/cdn-cgi/styles/   |           |
| !       | <a href="#">Expect-CT Not Enabled</a>                                    | GET    | https://www.yuga.com/about   |           |
| !       | <a href="#">Missing X-XSS-Protection Header</a>                          | GET    | https://www.yuga.com/_nuxt/css/7a3f40f.css   |           |
| !       | <a href="#">Referrer-Policy Not Implemented</a>                          | GET    | https://www.yuga.com/cdn-cgi/styles/   |           |
| !       | <a href="#">Subresource Integrity (SRI) Not Implemented</a>              | GET    | https://www.yuga.com/  |           |
| !       | <a href="#">Email Address Disclosure</a>                                 | GET    | https://www.yuga.com/_nuxt/448fbf4.js  |           |
| !       | <a href="#">Generic Email Address Disclosure</a>                         | GET    | https://www.yuga.com/_nuxt/7db28fe.js  |           |
| !       | <a href="#">Sitemap Detected</a>   | GET    | https://www.yuga.com/sitemap.xml   |           |
| !       | <a href="#">Cross-site Referrer Leakage through Referrer-Policy</a>      | GET    | https://www.yuga.com/opensearch.xml  |           |
| !       | <a href="#">Forbidden Resource</a>                                       | GET    | https://www.yuga.com/0%27%22--%3e%3c%2fstyle%3e%3c%2fscript%3e%3c%2fscript%20src%3d%22%2f%2fryveyl_szhgzbzgzb1bm_uuhyyrijcuukguz_z8ebq3m%26%2346%3br87%26%2346%3bme%22%3e%3c%2fscript%3e |           |
| !       | <a href="#">Robots.txt Detected</a>                                      | 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.

**Vulnerabilities**

5.1. [https://www.yuga.com/\\_nuxt/](https://www.yuga.com/_nuxt/)

**Access-Control-Allow-Origin**

- \*

**Certainty**

**Request**

```
GET /_nuxt/ HTTP/1.1
Host: www.yuga.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) : 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.net.cloudflare.com/report/v3?s=fa6%2Fvn0fBZecWZAnt1KMaGQx61fefZxjbBN78bNrkheIwenR1lUtWIMCn5VPk5hqQw79BCtILrhC%2BNymmY1NbW5kd1kqC%2FeFTKzv4bOJ0uG92YpkC%2BX9le1v212D6HE%2BcVINTKIMIrB%2FOvA%3D"}], "group": "cf-net", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-net", "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  
  
-  
q0W79BCtILrhC%2BNymmY1NbW5kd1kqC%2FeFTKzv4bOJ0uG92YpkC%2BX9le1v212D6HE%2BcVINTKIMIrB%2FOvA%3D"}], "group": "cf-net", "max\_age": 604800}  
NEL: {"success\_fraction": 0, "report\_to": "cf-net", "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>  
ch  
-

## 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 domain as 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

The screenshot shows the HackerOne interface. On the left is a sidebar with icons for reports, users, and settings. The main area has a header with navigation links: Open (3), Pending disclosure (0), Pending retests (0), All (4), and Draft (0). Below this is a search bar labeled "Search all reports". A list of reports is displayed on the left, with the first item being "#2003938 Misconfigured Access-Control-Allow-Origin Header" reported by "dark\_k08". The main content area shows the details of this report. At the top right of the report card, it says "Reported May 27, 2023, 3:57am UTC" and "dark\_k08". To the right of the report card is a sidebar with participant information, state ("New (Open)"), reported to ("Yuga Labs"), severity ("Medium (4 ~ 6.9)"), asset ("\*.yuga.com"), weakness ("Improper Access Control - Generic"), time spent ("3h"), visibility ("Private"), CVE ID ("None"), and account details ("None"). The report card itself has sections for "ADD HACKER SUMMARY", "TIMELINE - EXPORT", and "Solution". The "Solution" section contains two bullet points explaining the issue and how to fix it.

#2003938 Misconfigured Access-Control-Allow-Origin Header

dark\_k08 submitted a report to Yuga Labs. (Edit information)

Misconfigured Access-Control-Allow-Origin Header

May 27, 2023 (1 min ago)

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.

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.

## **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](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>.