

Sri Lanka Institute of Information Technology



# Journal Book

Bug Bounty

Web Security - IE2062

B.Sc. (Hons) in Information Technology Specializing in Cyber Security

Submitted by:

Student ID	Student Name
IT21301322	C.D.ALuthge

Date of Submission :

**27/05/2023**

## **Introduction**

This is my bug bounty diary, where I write about my fascinating foray into the world of bug reward schemes. Through the discovery and

disclosure of vulnerabilities in different firms' systems and apps, bug bounty programs provide a special chance for ethical hackers like myself.

I will talk about a variety of topics related to my bug bounty adventure in my weblog. I start by introducing the bug bounty concept and describing the methodical process I used to find, exploit, and disclose vulnerabilities. This technique provided the framework for my work and guaranteed a methodical and effective approach to my bug bounty projects.

I next go into the various stages I ran across when engaging in bug bounty operations. Each stage of my journey, from reconnaissance and vulnerability identification through exploitation and reporting, was essential. I go through the approaches and strategies used in each stage to increase my chances of success.

I used a variety of tools to help with my bug bounty operations. My process was expedited and I was able to successfully identify possible security problems thanks to these technologies, which included vulnerability scanners, attack frameworks, and reconnaissance and information collecting tools. I discuss the tools utilized and how they affected my bug bounty experience.

In the course of my bug bounty assignments, I investigated numerous weaknesses. I go into depth about these flaws, addressing their

significance, exploitability, and their repercussions. I include details on the apps or systems impacted and the procedures used to verify and recreate these flaws.

I then go about the challenges I had along the way of my bug bounty quest and how I overcame them. I demonstrate my problem-solving skills by providing ideas, workarounds, and lessons gained from each obstacle. Finally, I consider the overall learnings from my bug bounty efforts and discuss the most important lessons I learned. I go through the important knowledge gained, the abilities obtained, and the personal development realized as a result of taking part in bug bounty programs.

I want to encourage other people who are interested in cybersecurity, support the bug bounty community, and further my personal development as a skilled ethical hacker by jotting down my experiences and sharing them in my diary.

## **1) Introduction to Bug bounty methodology.**

### **1.i) What is Bug Bounty**

Companies and organizations that host bug bounty programs ask security researchers, ethical hackers, and enthusiasts about cybersecurity to identify and disclose security flaws in their websites, software, or

other systems. These initiatives aim to strengthen the organization's security posture by utilizing outside specialists' capabilities to find vulnerabilities that could go unnoticed in routine security audits.

Program participants, often known as "Bug Bounty Hunters" or "Researchers," are compensated for finding and appropriately reporting security vulnerabilities. These prizes are usually monetary, although they can also include recognition or other advantages. Bug Bounties are designed to promote responsible disclosure, ethical hacking techniques, and cooperation between corporations and security experts.

Because they enable companies to crowdsource security testing efforts, access a variety of skill sets, and find vulnerabilities before malevolent actors can exploit them, bug bounty programs are seen as an important part of cybersecurity tactics. A successful bug bounty program can lead to major security enhancements, a rise in customer confidence, and good ties with the cybersecurity community.

## **Introduction to Bug bounty methodology.**

### **I. Describe a bug bounty.**

Businesses use independent security researchers to uncover and report security vulnerabilities in their software, websites, and apps as part of a practice known as bug bounties. Businesses can detect security flaws

with this approach and address them before adversaries take advantage of them.

## II. The bug bounty phases?

Bug bounty schemes frequently involve a phased, comprehensive, and methodical assessment of the security posture of the system.

### 1. Phase 01

During the first step of scoping, the organization identifies the target systems, applications, and vulnerabilities that are included in the program's scope. This is important because it helps to focus the efforts of security researchers and ensures that the company can successfully address any vulnerabilities discovered.

### 2. Phase 02

The second step is testing, in which researchers use a range of tools and techniques to look for vulnerabilities in the target systems and applications. This process may also make use of automated scanning, manual testing, and other specialized technologies to identify specific vulnerabilities. Technologies like Burp Suite, OWASP ZAP, Nmap, and Metasploit are frequently used in bug bounty schemes.

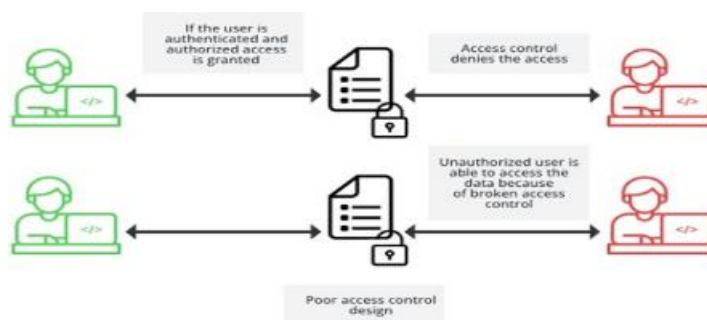
### 3. Phase 03

Reporting is the third phase of vulnerability detection, in which the researcher provides a detailed report on the vulnerability to the organization. This report should describe the vulnerability, an analysis of its potential impacts, and any remedial recommendations. Following examination of the report, the business affirms the susceptibility

## Introduction to OWASP top 10 vulnerabilities.

- Broken Access Control

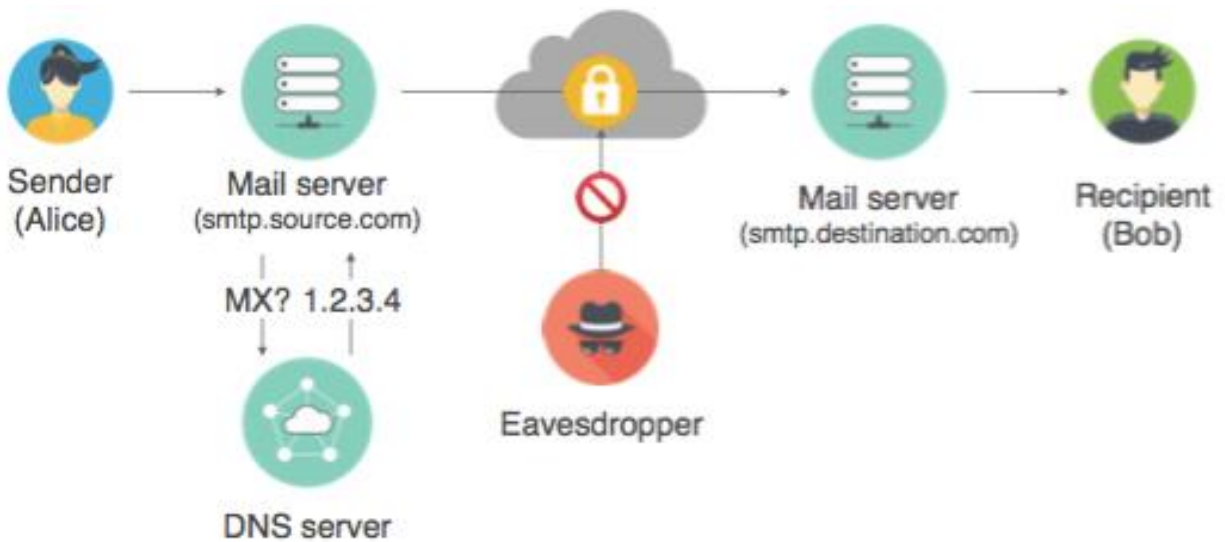
When users are unable to adequately impose limitations on what they can access or do within a system, this is known as broken access control. This vulnerability makes it possible for unauthorized individuals to access private data or carry out tasks that shouldn't be permitted. Insecure references to objects, improperly configured permissions, and a lack of authentication checks are the causes of it. Because it can result in illegal data exposure, manipulation, or system penetration, it's a major problem.



- Cryptographic Failures

Cryptographic collapses are the result of poor algorithms, incorrect implementations, or improper management of encryption keys, which compromise the security of information encrypted via encryption techniques. Undermining security safeguards and perhaps leading in data breaches, this can lead to unauthorized access to or exposure of sensitive data.

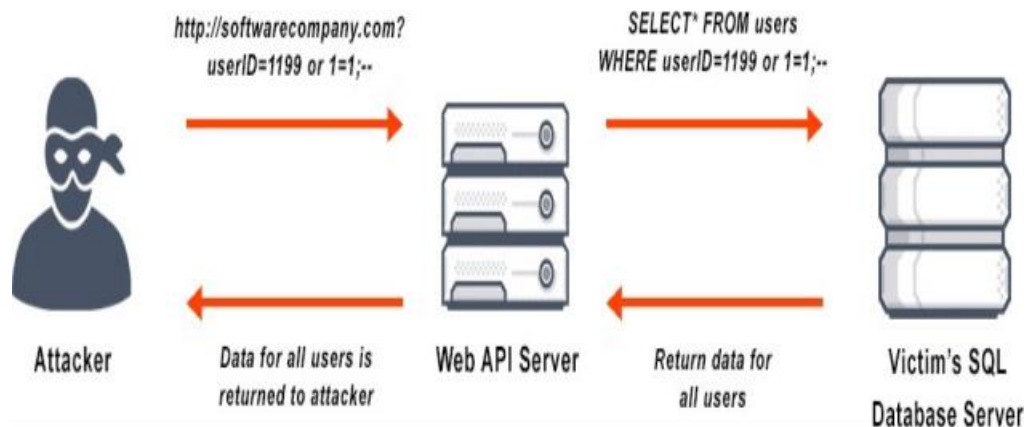




- Injection

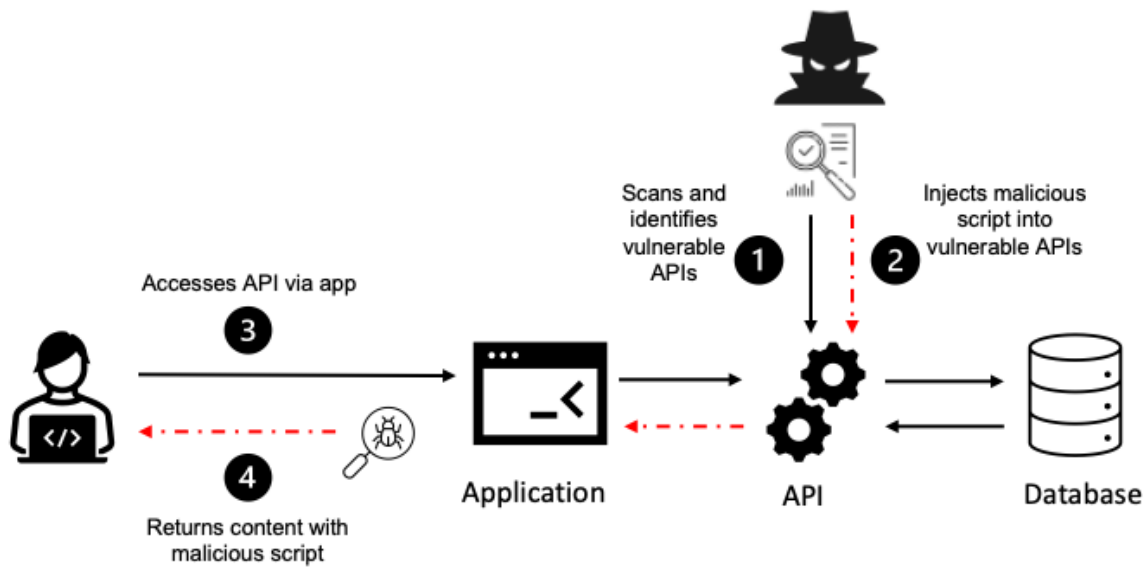
Injection: it is a type of security vulnerability in which untrusted data is sent to an interpreter as part of a command or query. Most often, attackers use this to inject malicious code into input fields, for example, login forms or search boxes. The interpreter then executes this code, which can give the attacker unauthorized access to data, alter the application's behavior, or gain full control over the system. There are many types of injections,

such as SQL injection, where the attackers manipulate database queries, or cross-site scripting, where the malicious script is injected into a web page that other users view.



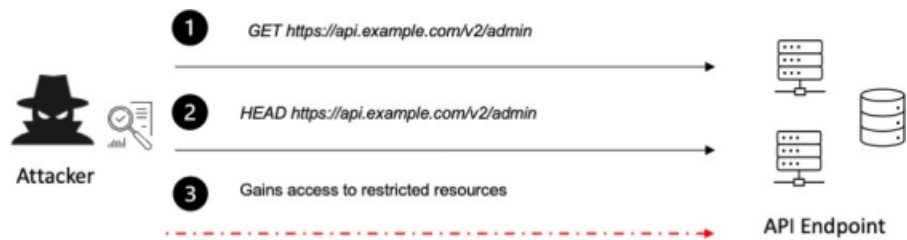
- Insecure Design

Insecure design means the security flaws within the fundamental system or application design born out of insufficient attention to security at the design time. Consequently, systems have vulnerabilities that enable unauthorized system access or breaches. Examples are poor user authentication or no network segmentation. To fix insecure design, significant changes to the architecture are needed to develop the designs securely.



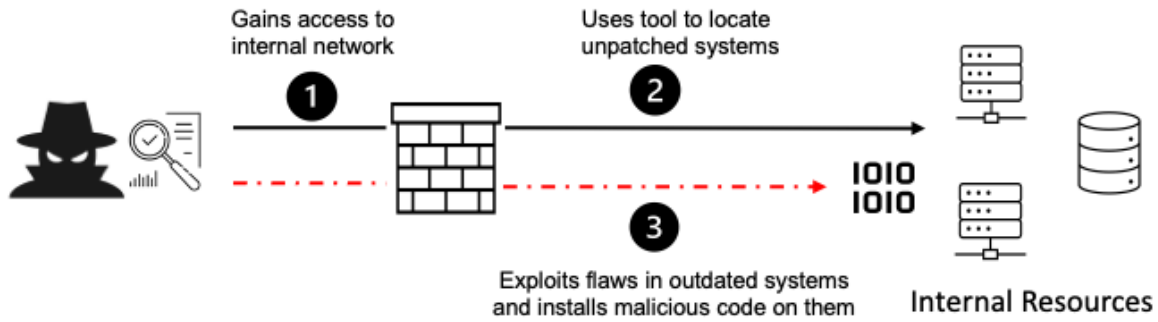
- **Security Misconfiguration**

Imagine you accidentally leave your front door closed but not locked. That's what a security misconfiguration is like. Essentially, it's not properly securing your software systems, servers, or web applications. This can include default settings, shipped insecurely, or unnecessary features. Unauthorized users might target such vulnerabilities to access your info or disrupt the operation. Therefore, one should monitor and update security measures continuously to avoid misconfiguration.



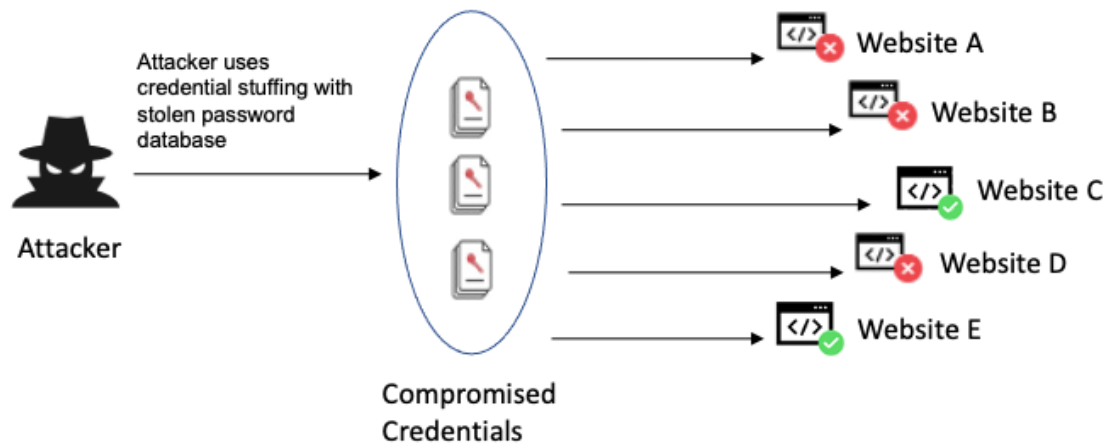
- Vulnerable and Outdated Components

Vulnerable components are software elements that are known to contain security flaws that could be exploited by hackers. However, software components that have not received an upgrade in a long time are known as outdated components, and they may not include important security updates and bug fixes. In order to maintain a secure system environment, both sorts of components present security concerns and should be routinely updated and monitored.



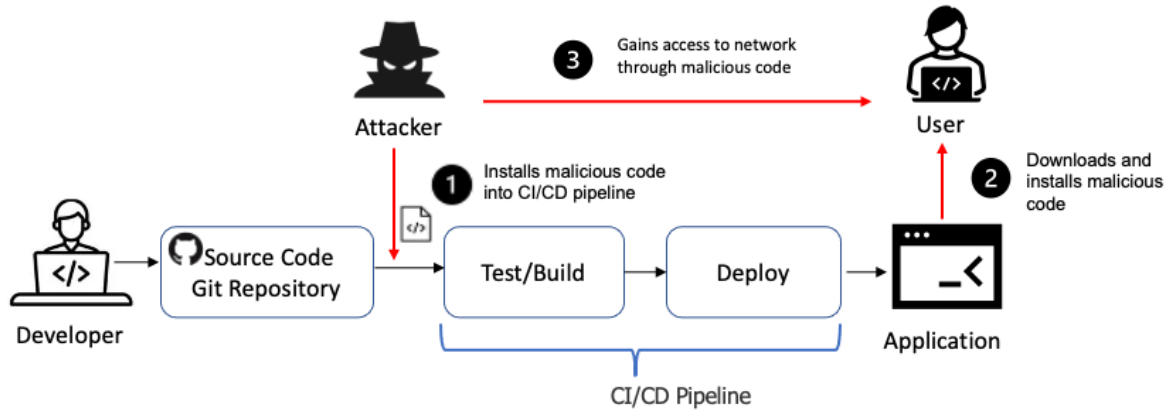
- Identification and Authentication Failures

When systems are unable to accurately confirm user identities or authenticate their access credentials, identification and authentication failures take place. Whereas authentication failures are caused by an inability to verify user identities, identification failures are the consequence of incorrect user recognition. In order to identify and fix system vulnerabilities, strong authentication procedures and frequent security assessments are essential. These failures might result in unauthorized access and security breaches.



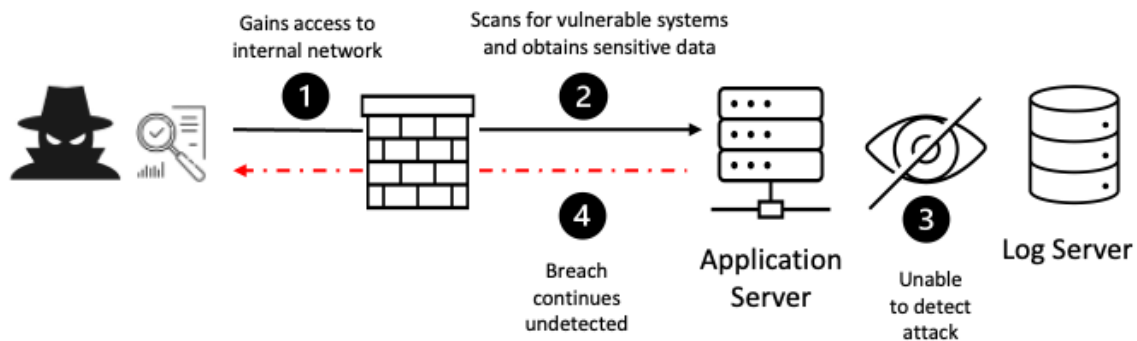
- **Software and Data Integrity Failures**

Software code or data accuracy, consistency, and reliability are jeopardized in software and data integrity issues. Data integrity problems are caused by mistakes, unauthorized access, or cyberattacks, whereas programming errors, malicious code, or unauthorized alterations are the causes of software integrity problems. To reduce risks and guarantee system security and dependability, preventive measures include backups, data encryption, access controls, and regular updates.



- Security Logging and Monitoring Failures

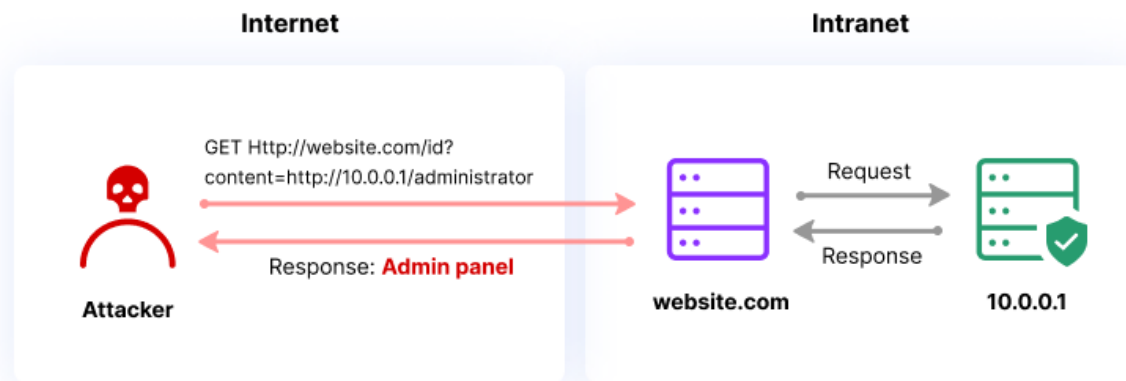
Failed security logging and monitoring systems result in delayed detection of security incidents and higher risks since they are unable to reliably capture and evaluate security-related events. Monitoring failures are caused by insufficient tools or response protocols, whereas logging failures are caused by misconfigurations or deactivated logging systems. Organizations should establish strong response protocols, use comprehensive logging practices, deploy efficient monitoring tools like SIEM tools, train security teams, and continuously improve logging and monitoring configurations in light of best practices and emerging threats in order to address these failures. By taking these steps, cybersecurity defenses are strengthened, and the effects of security events are lessened.



- Server-Side Request Forgery

A security flaw known as server-side request forgery (SSRF) allows attackers to take control of a susceptible server and send unwanted requests, usually to external or internal systems. Unauthorized access, data loss, and more exploitation may result from this. Input validation, whitelisting authorized resources, network segmentation, and access controls are all part of prevention. Frequent security testing improves overall system security by assisting in the identification and mitigation of SSRF threats.





Throughout the finding vulnerabilities of web application, I have identified many web applications that had considerable amount of OWASP Top 10 vulnerabilities. I reported to the relevant party about the existence of that vulnerability on their site.

To this journal book I have used vulnerable web sites to show case the thing I learn, vulnerabilities I found, tools I used and to explain what I learn from finding those. The following vulnerable web applications ,

- <https://www.coinhako.com>
- <http://smtp2go.com>
- <https://skinport.com>

I have employed several methodologies, theories, and different tools to identify vulnerabilities in those online apps. I have used numerous tools, as I have already mentioned. To explain it, I can divide those tools primarily into two categories.

- a. Reconnaissance tools. (Information gathering)
- b.vulnerability analysis & exploitation tools.

## Reconnaissance tools. (Information gathering)

During the information collection phase, a number of tools were employed for different tasks. There are many readily available testing tools, both automated and manual. I have used some of the most well-known tools in a range of fields for the information-gathering phase.

- 1.Target validation
- 2.Subdomain Enumeration.
- 3.DNS Enumeration.
- 4.Public Device Enumeration.

- Target validation

The vulnerability assessment process starts with this stage. We must first determine the susceptible target by collecting data on all relevant variables before conducting a bug bounty. I have used a variety of built-in and third-party applications for target validation.

### A. Nslookup

B. Censys

C. Wafw00f

D. Nmap

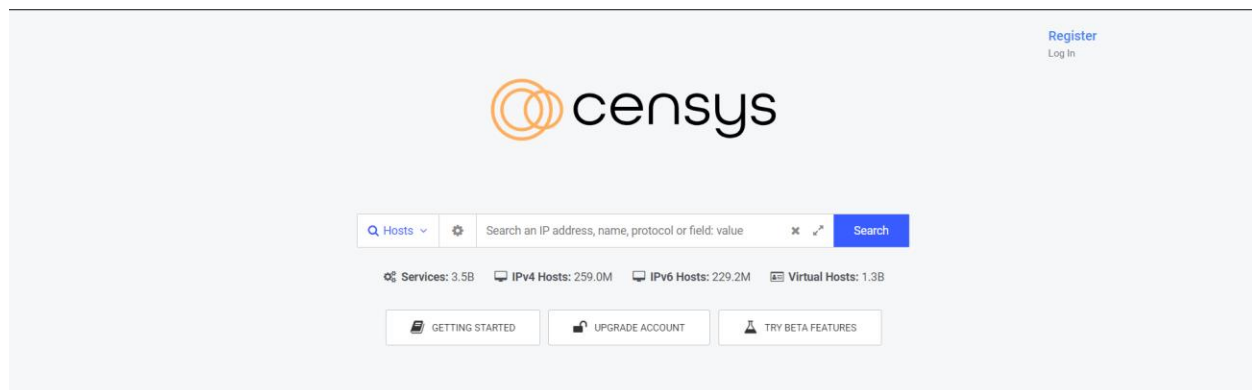
- Nslookup

A command-line utility called `nslookup` is used to query DNS (Domain Name System) servers and get DNS-related data. In addition to performing reverse DNS lookups and retrieving other DNS records like A, AAAA, MX, NS, PTR, and TXT records, it resolves domain names to IP addresses. It is flexible for diagnosing DNS problems, validating DNS configurations, and testing DNS servers because it may be used in both interactive and non-interactive modes. Network administrators and cybersecurity experts frequently utilize `nslookup`, which runs on several platforms, for DNS-related activities and diagnostics.

```
(deshan@kali)-[~]  
$ nslookup coinhako.com  
Server:          192.168.43.1  
Address:         192.168.43.1#53  
  
Non-authoritative answer:  
Name:   coinhako.com  
Address: 104.18.3.84  
Name:   coinhako.com  
Address: 104.18.2.84  
Name:   coinhako.com  
Address: 2606:4700::6812:254  
Name:   coinhako.com  
Address: 2606:4700::6812:354
```

- Censys

Censys is a potent internet scanning tool that scans and monitors devices, networks, and services online all the time. It performs thorough scans, keeps track of SSL/TLS certificates, keeps an eye on attack surfaces, finds vulnerabilities, and offers threat information. Large volumes of data may be searched and analyzed, processes can be automated with the help of the API, and Censys can be integrated into security workflows. In the connected digital world of today, Censys is useful for asset discovery, vulnerability management, compliance monitoring, and proactive risk reduction.



#### Basic Information

Forward DNS	www.hexoral.ru.cdn.cloudflare.net, public.cdr-api.fscu.com.au.cdn.cloudflare.net, www.paxlovideducacion.mx, judaspriest-namegenerator.com, uat.sales.soundunited.com, ...
Routing	104.18.36.0/24 via CLOUDFLARENET, US (AS13335)
Services (13)	80/HTTP, 443/HTTP, 2052/HTTP, 2053/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2095/HTTP, 2096/HTTP, 8080/HTTP, 8443/HTTP, 8880/HTTP

#### HTTP 80/TCP

05/07/2024 12:45 UTC

##### Software

CloudFlare Load Balancer

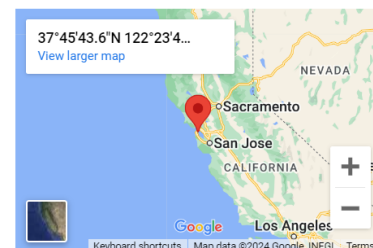
[VIEW ALL DATA](#)

[GO](#)

##### Details

http://104.18.36.214/

Status	403 Forbidden
Body Hash	sha1:b9c7109e819c12e501ea25dbcd356a7496d4e6be
HTML Title	Direct IP access not allowed   Cloudflare
Response Body	<a href="#">EXPAND</a>



##### Geographic Location

City	San Francisco
State	California
Country	United States (US)
Coordinates	37.7621, -122.3971
Timezone	America/Los_Angeles

- Wafw00f

Wafw00f is an open-source program that uses content patterns, HTTP responses, and header analysis to detect and fingerprint web application firewalls (WAFs). It gives testers and security experts information about the particular WAF technology or vendor being used as well as assists them in determining whether a web application is protected by a WAF. In addition to being user-friendly and seamlessly integrating with automated testing workflows, Wafw00f also keeps an updated database of WAF signatures and offers community support. It is a useful tool for security assessment and reconnaissance jobs, supporting the creation of efficient testing plans and workarounds.

```
└─$ wafw00f https://booking.com

( W00f! )

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

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

[*] Checking https://booking.com
[+] The site https://booking.com is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

- Nmap

Nmap, sometimes known as "Network Mapper," is a potent open-source network scanning program used for vulnerability analysis, security audits, and network discovery. It is particularly good at operating system detection, host discovery, port scanning, and service version detection. Because it supports custom scripting and automation, Nmap's scripting engine (NSE) is adaptable to a wide range of security activities and integration requirements. Because of its dependability, adaptability, and large feature set, network administrators, security experts, and penetration testers frequently use it for network reconnaissance, security audits, and network monitoring.

```

(root@kali)-[~]
# nmap -sV -A -T4 oyorooms.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-05-01 21:37 +0530
Nmap scan report for oyorooms.com (23.53.216.81)
Host is up (0.0045s latency).
rDNS record for 23.53.216.81: a23-53-216-81.deploy.static.akamaitechnologies.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  tcpwrapped
|_http-server-header: AkamaiGHost
|_http-title: Site doesn't have a title (text/html).
443/tcp   open  ssl/tcpwrapped
|_ssl-cert: Subject: commonName=www.oyorooms.com/organizationName=Oravel Stays Limited/stateOrProvinceName=Gujarat/countryName=IN
| Subject Alternative Name: DNS:www.oyorooms.com, DNS:api-pay.oyorooms.com, DNS:api.oyopay.in, DNS:api.oyopay.io, DNS:api.oyorooms.com, DNS:api.weddingz.in, DNS:assets.oyoroomscdn.com, DNS:bff.oyorooms.com, DNS:boltapi.oyorooms.com, DNS:cis.innov8.work, DNS:crs.oyorooms.com, DNS:crsms.oyorooms.com, DNS:dev-webpoc.oyorooms.com, DNS:dev.weddingz.in, DNS:emagazine.weddingz.in, DNS:feedback.oyorooms.com, DNS:hms-api.oyorooms.com, DNS:hms.oyorooms.com, DNS:hooks.oyopay.io, DNS:images.oyohotels.cn, DNS:images.oyoroomscdn.com, DNS:imagewedz.oyoroomscdn.com, DNS:info.weddingz.in, DNS:innov8.work, DNS:insights.oyorooms.com, DNS:jplife-recon-api.oyorooms.com, DNS:lifeline.oyorooms.com, DNS:lms-life.oyorooms.com, DNS:m.weddingz.in, DNS:mesh-support.oyorooms.com, DNS:meta-booking.oyopay.io, DNS:meta.oyorooms.com, DNS:mm-phatak-preprod.oyorooms.com, DNS:mm-phatak.oyorooms.com, DNS:mm-preprod.oyorooms.com, DNS:mm.oyorooms.com, DNS:mmapi.oyorooms.com, DNS:mobile.oyoliving.com, DNS:nucleus.oyorooms.com

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.22 ms a23-53-216-81.deploy.static.akamaitechnologies.com (23.53.216.81)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 71.11 seconds

```

## Subdomain Enumeration.

This is one of the most important parts of gathering information. In this phase, identify the subdomain that resides beneath the main root domain. We may therefore quickly explore each subdomain and gather data by identifying those subdomains on our own. Technologies such as subdomain enumeration have been utilized by me.

A. Sublist3r.

B. Recon-ng

- Sublist3r.

Sublist3r is an open-source subdomain enumeration tool used in cybersecurity for reconnaissance purposes. It assists security professionals, penetration testers, and researchers in identifying valid subdomains associated with a target domain. The tool employs various methods including passive search through search engine results, active search via DNS queries, and brute-force techniques using wordlists to enumerate subdomains. Sublist3r supports output in multiple formats, making it versatile for integration with other tools and workflows. It is valuable in expanding the attack surface during security assessments but should be used responsibly and with proper authorization.



```

[-]$ nslookup blackrock.com
Server:          192.168.1.1
Address:         192.168.1.1:53
Non-authoritative answer:
Name:   blackrock.com
Address: 69.52.2.199
[-] Enumerating subdomains now for blackrock.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..com
[-] Searching now in Netcraft..
[-] Searching now in DNSDumpster..org ) at 2024-05-07 23:23 +0530
[-] Searching now in Virustotal..com (69.52.13.199)
[-] Searching now in ThreatCrowd..
[-] Searching now in SSLCertificates..scanned): 69.52.2.199
[-] Searching now in PassiveDNS.. (no-response)
[!] Error: Google probably now is blocking our requests
[~] Finished now the Google Enumeration!... balancer http proxy
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 2127

```

```

www.blackrock!com
1desk.blackrock.com
1desk-amelia.blackrock?com.1
1desk-amelia-uat!blackrock.com3
www.1desk-amelia-uat.blackrock.com
1desk-automation.blackrock.com
1desk-dev!blackrock?com
1desk-uat6.blackrock?com
365monitoring.blackrock.com
AWADMIN.blackrock.com
AWCENTRAL.blackrock.com
BLKCMX.blackrock.com
BNYMIM.blackrock.com]
EDGE.blackrock?comackrock.com
EV01-PRD-US.blackrock.com
EVAU.blackrock?com ( https://nmap.
EVJP.blackrock?comor blackrock.com
EVUK.blackrock?comlatency).
EVUS.blackrock?comr blackrock.com
Edge110.blackrock!comed tcp ports
Edge111.blackrock.com          VERSIO
Edge115.blackrock?comoxy      F5 BIG
Edge116.blackrock!com BigIP
Edge310.blackrock:comoxy might be

```

- Recon-ng

Recon-ng is an open-source reconnaissance tool with Python foundation that is used for penetration testing and security evaluations. It collects data from domains, IPs, emails, and social media platforms using a modular framework with different modules. The advantages of recon-ng are its flexibility for scripting and automation, integration with many data sources, and data enrichment capabilities. It is used by security experts to gather and evaluate intelligence, spot possible weaknesses, and improve overall security posture during the first reconnaissance phase. Its vibrant community guarantees continuous upgrades and support, which makes it an invaluable addition to cybersecurity toolkits.

```
(deshan@kali)~  
$ recon-ng  
[*] Version check disabled.  
  
Sponsored by ...  
BLACK HILLS  
www.blackhillsinfosec.com  
www.practisec.com  
[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]  
  
[*] Searching Google for: site:skinport.com  
[*] Country: None  
[*] Host: status.skinport.com  
[*] Ip_Address: None  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
  
[*] Country: None  
[*] Host: docs.skinport.com  
[*] Ip_Address: None  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None  
  
[*] Country: None  
[*] Host: screenshot.skinport.com  
[*] Ip_Address: None  
[*] Latitude: None  
[*] Longitude: None  
[*] Notes: None  
[*] Region: None
```

- DNS enumeration.

In this step, all that is being done is finding all possible DNS servers and the matching records on those servers for the web application or targeted

company. We can easily determine the attack surface's size and reveal the target application's size by doing this. To complete this enumeration, I used several tools.

A. Dnsrecon

B. Dnsdumper

- Dnsrecon

For security evaluations and penetration tests, DNSRecon is a powerful open-source tool for DNS reconnaissance that finds and counts DNS information. It is particularly good at finding subdomains, enumerating DNS records (A, AAAA, MX, NS, SOA, TXT), transferring DNS zones, and it can handle wordlist-based and brute-force attacks. With its automation, customization, and integration features, it's a useful tool for figuring out possible attack points, comprehending target infrastructure, and raising security awareness in general. DNSRecon is still a dependable option for DNS reconnaissance operations because of its community support and frequent updates.

```

(deshan@kali)-[~]
$ dnsrecon -d blackrock.com

[*] std: Performing General Enumeration against: blackrock.com...
[*] DNSSEC is configured for blackrock.com
[*] DNSKEYs:
[*] NSEC3 KSK ECDSAP256SHA256 54f944852355fd5a99fd5f5a9f7bc494 ef63d2968518936dc8435342ab808885 40e060bf12e2205aa30f8a4ec93dfae1 1c5a508e7bb6a0889b17316193829f25
[*] NSEC3 KSK ECDSAP256SHA256 5552094e98a6ccf312ef5af79980d6e4 6f275f54ff368710b62f71d2bb7df01f d96977dc457b592c602567dab83e05b2 752805dc964d929bcf4e9de969ddb752
[*] NSEC3 ZSK ECDSAP256SHA256 168f74c976f5e40e22c6f051b506c2f6 7498b2724b7b5739cbab15e07ab77ee1 f27c392f0267a94ae372158712f6ae58 62f997876a38397bb0d78c36d2f3e3d9
[*] NSEC3 ZSK ECDSAP256SHA256 202303a1033cda749ee5eca5a1aca6d0 e1aff9569569aefc42ad533b7d49f73e 5fa229b64f317b8fe049f8d1d6b1d3ac 49951c36e3a6e3e9b37c4277aa5ced1b
[*] SOA ns1.blackrock.com 193.108.91.23
[*] NS ns6.blackrock.com 95.100.173.65
[*] Bind Version for 95.100.173.65 "42475.168"
[*] NS ns4.blackrock.com 184.26.160.66
[*] Bind Version for 184.26.160.66 "45416.7"
[*] NS ns1.blackrock.com 193.108.91.23
[*] Bind Version for 193.108.91.23 "35139.214"
[*] NS ns3.blackrock.com 23.61.199.64
[*] Bind Version for 23.61.199.64 "44471.190"
[*] NS ns2.blackrock.com 96.7.49.67
[*] Bind Version for 96.7.49.67 "31224.103"

```

```

[*] TXT blackrock.com MS=ms38828697
[*] TXT blackrock.com facebook-domain-verification=jgst7ahvoqwagulxzu7zstebenl0nh
[*] TXT blackrock.com amazonses:1HI9LAXiWsiJpZ4JNXwXz2gQaHC2wXzskAqDUj3RTg8=
[*] TXT blackrock.com mongodb-site-verification=ocUum2f1wfuEq7KWecCMVS3K0fwQLjaP
[*] TXT blackrock.com smartsheet-site-validation=Dh008aWdiKQgWHj44tKwLySpkgYcV7V
[*] TXT blackrock.com google-site-verification=z1Aw-cih_E2FK0WotfSW8RUFHKmTIFb1VXHbV_J6bM8
[*] TXT blackrock.com intersight-162938a7f29649663d27ccf1b81d58259224c4820fdd02fa3612e95c123f8ce7
[*] TXT blackrock.com v=spf1 include:%{ir}.*%{v}.*%{d}.spf.has.pphosted.com ~all
[*] TXT blackrock.com atlassian-domain-verification=382cypeoFrrqy4R9MkRopItq5Cbixu5CS3S0UGcjZHH56Rf6Lq/NICGahGifaMk5
[*] TXT blackrock.com 2FE6-F3BB-EDF8-C58F-D2A4-8035-EDCF-AFB0
[*] TXT blackrock.com QKhkBUJSEz0yADjEzY5RtC49rqKCWcl+c1NvPPP3l0+9gS0+nqR+Np2Zs2cpzvf7BLyScIteZHHLjt5j4EuSQ=
[*] TXT blackrock.com atlassian-domain-verification=VDrpZs9FnE3/L/dJxRC+0mkjndLafqB2r3l/ztET32a5TZyDfavvWoxVWw+0eokX
[*] TXT _dmarc.blackrock.com v=DMARC1; p=quarantine; fo=1; rua=mailto:dmarc_rua@emaildefense.proofpoint.com; ruf=mailto:dmarc_ruf@emaildefense.proofpoint.com;
[*] Enumerating SRV Records
[*] SRV _sip._tcp.blackrock.com vcs.blackrock.com 69.52.12.25 5060
[*] SRV _h323cs._tcp.blackrock.com vcs.blackrock.com 69.52.12.25 1720
[*] SRV _h323ls._udp.blackrock.com vcs.blackrock.com 69.52.12.25 1719
[*] 3 Records Found





















```

## - Dnsdumper

DNSDumpster is an online tool focused on DNS information gathering for a target domain. It assists in discovering subdomains, viewing DNS records (A, AAAA, MX, NS, SOA, TXT), mapping domain names to IP

addresses, and providing visual representations of DNS-related data. Security professionals and penetration testers use DNSDumpster during reconnaissance to understand a domain's infrastructure, identify potential vulnerabilities, and aid in security assessments. While it offers valuable insights, users should supplement its findings with other tools for a comprehensive analysis, considering that its data may not always be the most current or complete.



DNS Servers		
na1jsv.name.com.    	163.114.216.17	NSONE United States
na2ckr.name.com.    	163.114.216.49	NSONE United States
na3dgy.name.com.    	163.114.217.17	NSONE United States
na4axy.name.com.    	163.114.217.49	NSONE United States
MX Records ** This is where email for the domain goes...		
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations		
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
doncooley.skalenetwork.com     HTTP: <a href="#">https</a>	91.195.240.94	SEDO-AS Germany

## Public Device Enumeration.

Listening to every device linked to the system or web application is the aim of this stage. So far, I have only used one tool. All connected devices will receive information about the chosen domain from this tool.

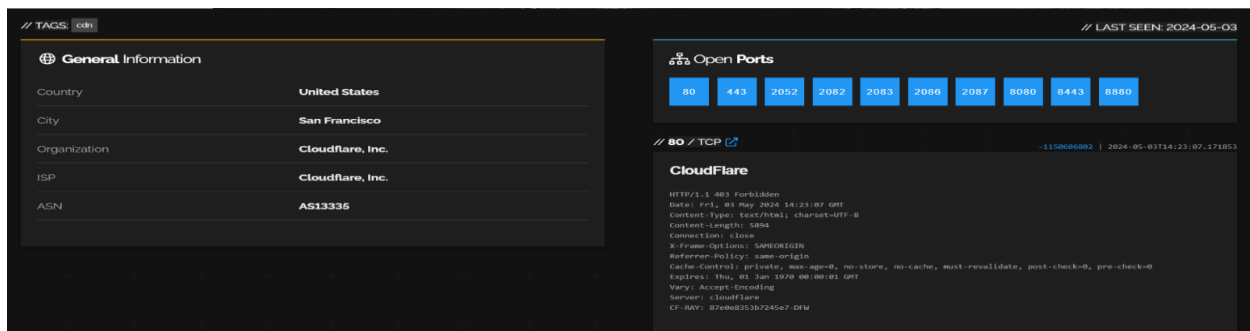
A. Shodan.io

B. whois

## C. whatweb

- Shodan.io

Shodan is a specialized search engine that indexes and provides information about internet-connected devices and systems, such as webcams, routers, servers, and IoT devices. It offers details like open ports, running services, device types, locations, and vulnerabilities. While it's a valuable tool for security professionals and researchers to analyze networks and devices, it's important to use it ethically and legally, as unauthorized access to devices is against the law.



- Whois

A key networking tool and protocol, whois is used to query databases and obtain data on IP addresses, domain names, and autonomous system numbers (ASNs). It offers information about domain registration, owner contact details, DNS information, IP address allocation, and ASN ownership. Whois is frequently used for domain research, network problems, IP geolocation, abuse investigations, and domain registration questions by network administrators, cybersecurity experts, domain registrars, and law enforcement organizations. Due to privacy concerns,

registrars have started offering privacy services that conceal personal information from view in public Whois data. While Whois provides insightful information, users should be aware of potential limits across multiple Whois servers, privacy concerns, and data accuracy.

```
(root@kali) [~]
# whois skinport.com
Domain Name: SKINPORT.COM
Registry Domain ID: 2306485802_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2020-09-23T11:10:20Z
Creation Date: 2018-09-05T18:23:35Z
Registry Expiry Date: 2026-09-05T18:23:35Z
Registrar: Namecheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: EDNA.NS.CLOUDFLARE.COM
Name Server: MARK.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation
DNSSEC DS Data: 2371 13 2 49F728E1B59EE31AEDA9ADE3A92725C8022F9D446710F1C74667C4ADC8A999CB
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-22T09:30:01Z <<<

Tech Postal Code: 101
Tech Country: IS
Tech Phone: +354.4212434
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email: 1700f877b52643d8afd44d0b3f15962e.protect@withheldforprivacy.com
Name Server: edna.ns.cloudflare.com
Name Server: mark.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-04-21T16:30:44.80Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

## • Whatweb

WhatWeb is a powerful open-source website scanner that specializes in identifying the technologies utilized by websites. It excels in detecting web servers, frameworks, content management systems (CMS), programming languages, and more through its fingerprinting and HTTP header analysis capabilities. Security professionals leverage WhatWeb during reconnaissance and vulnerability assessments to gather insights into target websites' technology stacks, assess security risks associated with detected technologies, and identify potential vulnerabilities or outdated components. Its scriptable and customizable nature, along with



integration options, makes it a valuable tool for automating scanning workflows and enhancing security assessments.

```
(root@kali)-[~]
# whatweb https://skale.network
https://skale.network [301 Moved Permanently] Country[UNITED STATES][US], IP[75.2.70.75], OpenResty, RedirectLocation[https://www.skale.network/], Title[301 Moved Permanently]
https://www.skale.network/ [301 Moved Permanently] Country[UNITED STATES][US], IP[65.0.79.182], OpenResty, RedirectLocation[https://skale.space/], Title[301 Moved Permanently], UncommonHeaders[content-security-policy,x-served-by,x-cache-hits,x-timer,x-cluster-name], X-Frame-Options[SAMEORIGIN]
https://skale.space/ [200 OK] Country[UNITED STATES][US], Frame, HTML5, IP[52.199.221.217], JQuery[3.6.3], Open-Graph-Protocol[website], PoweredBy[SKALE], Script[application/ld+json,text/javascript], Title[SKALE | Zero Gas Fee EVM Blockchain | AppChains Built for Web3 Gaming], UncommonHeaders[content-security-policy,x-lambda-id,x-served-by,x-cache-hits,x-timer,x-cluster-name], X-Frame-Options[SAMEORIGIN], YouTube
```

## Vulnerability analyzing tools.

In the vulnerability phase, numerous automated tools and frameworks are employed to identify vulnerabilities and confirm their existence. Technologies for both manual and automated testing are readily available. I have employed some of the most well-known technologies for the vulnerability collection process. In order to perform a vulnerability analysis and find any flaws, I have used both automated and manual testing techniques.

- A. Nikto scan
- B. Net sparker
- C. OWASP zap



- Nikto scan

Nikto is an open-source web server scanner made to find possible security holes in applications and web servers. With its extensive scanning capabilities, it may identify problems including out-of-date software, unsafe configurations, weak scripts, and incorrect SSL/TLS settings. In addition to producing comprehensive results after scanning, Nikto may be customized and scripted, connects with automated workflows, and receives community assistance and frequent database upgrades. For security experts performing web security assessments, it's a useful tool that helps with vulnerability discovery and mitigation to improve overall security posture.

```
(root@kali)-[~]
# nikto -h http://oyorooms.com
- Nikto v2.5.0

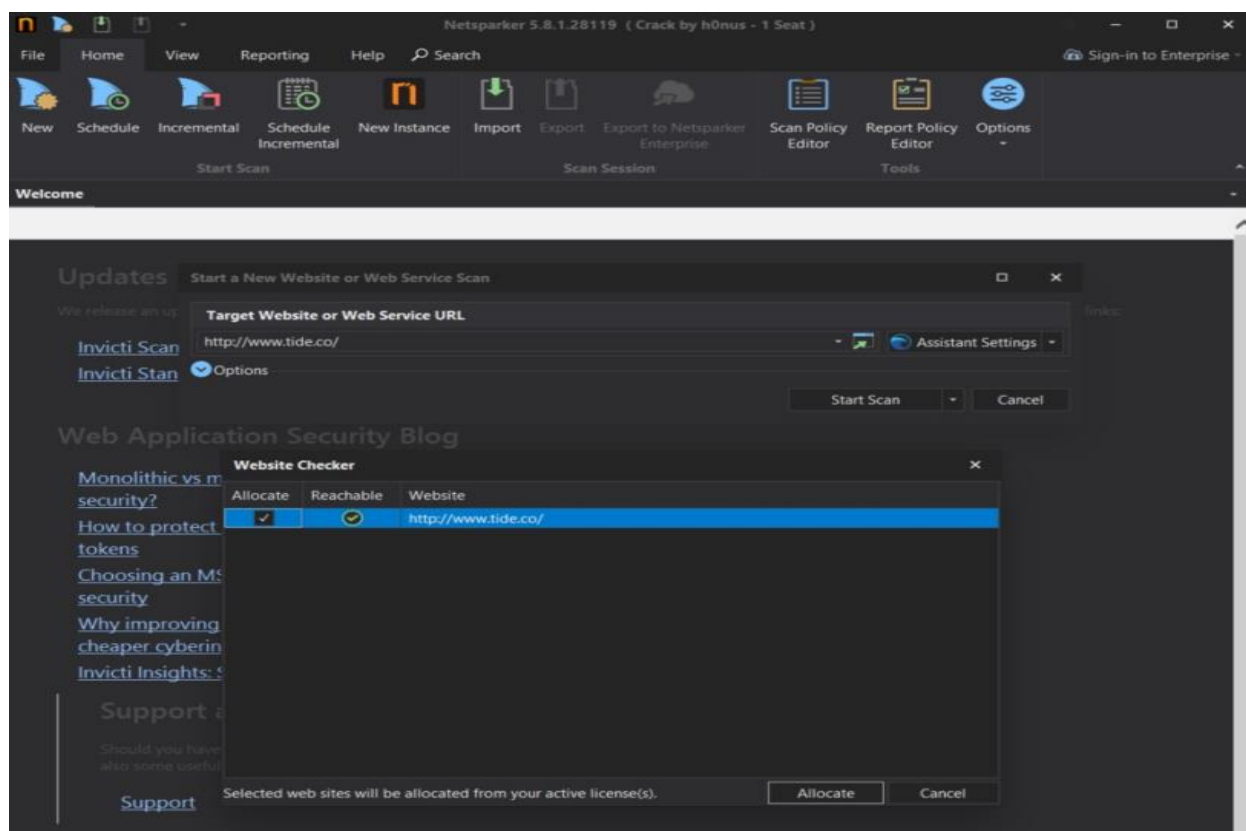
+ Target IP: 184.51.96.93
+ Target Hostname: oyorooms.com
+ Target Port: 80
+ Start Time: 2024-05-01 17:57:08 (GMT5.5)

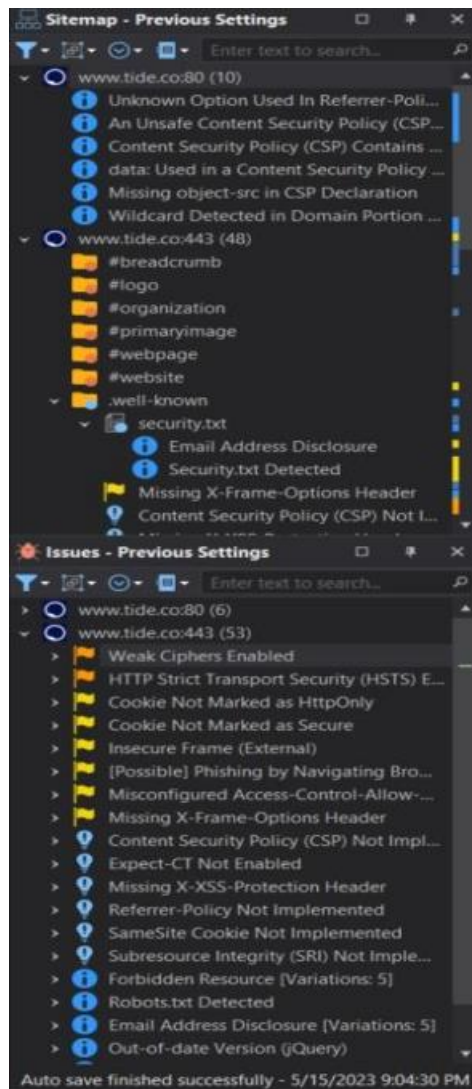
+ Server: AkamaiGHost
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: http://oyorooms.com/lk
+ /DV7uS5tL.gif: Uncommon header 'x-n' found, with contents: S.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7969 requests: 2 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-05-01 18:24:25 (GMT5.5) (1637 seconds)

+ 1 host(s) tested
```

- Net sparker

An automated web application security scanner known for its precision and extensive vulnerability finding capabilities is called Netsparker. It simplifies the procedure for examining online applications and finds many security flaws, such as SQL injection, XSS, and misconfigurations. With its ability to provide comprehensive reports for compliance audits and vulnerability monitoring, Netsparker seamlessly interacts with development workflows. Because of its intuitive interface, sophisticated features like support for continuous monitoring and authentication, and free support and upgrades, it's a great resource for security experts and companies looking to effectively strengthen their web application security posture.

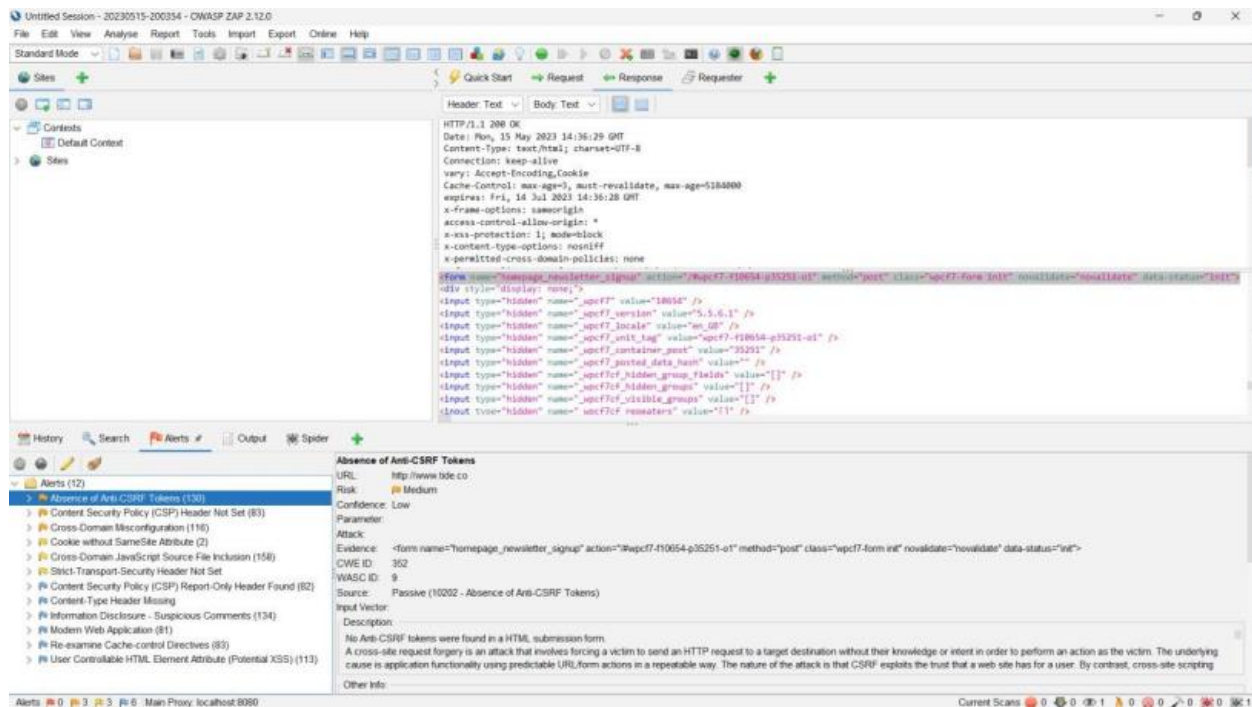




## ● OWASP ZAP

OWASP created the open-source Zed Attack Proxy (ZAP) tool for online application security testing. Users can examine and alter HTTP/HTTPS communication between web browsers and programs by using it as an intercepting proxy. ZAP provides spidering to map application structures in addition to active and passive scanning for vulnerabilities like SQL

injection and XSS. It facilitates input validation testing with fuzzing, controls sessions for authentication verification, and offers automation via scripting and APIs. ZAP helps with risk management and safe application development by providing thorough reports on vulnerabilities found.



## Identified vulnerabilities.

As part of this bug bounty program, I have tested a number of online applications against various vulnerabilities. IN order to accomplish this, I used a range of technologies at every stage of the vulnerability assessment process. To make it easier to find vulnerabilities, I have used fully automated tools like Net sparker and OWASP ZAP. I used the

frameworks and tools that come with Linux to double check the findings in case more proof of the vulnerability's existence was needed.

I have only included the most important vulnerabilities I have found in each domain in order to document the vulnerability's existence. In this journal book, I have covered every bug I found in every online application.

Target domain: <https://www.coinhako.com>

## Proof of concept:

**Coinhako**  
Coinhako is a renowned crypto exchange to buy cryptocurrencies in Singapore, and Asia. Trade crypto, manage your crypto wallet and view cryptocurrency  
<https://coinhako.com> · @coinhako

Reports resolved: 4 | Assets in scope: 4 | Average bounty: \$100

[Submit report](#)

Bug Bounty Program  
Launched in Sep 2023

Managed by HackerOne  
Includes retesting  
Collaboration enabled

[Give feedback](#) | [Bookmark](#) | [Subscribe](#)

Overview | Scope | Hacktivity | Thanks | Updates (0) | Collaborators

### Rewards

Last updated on September 6, 2023. [View changes](#)

Low	Medium	High	Critical
Avg. bounty n/a 9.52% submissions	Avg. bounty n/a 66.67% submissions	Avg. bounty \$2,300 23.81% submissions	Avg. bounty n/a 0% submissions
\$100–\$250	\$250–\$500	\$500–\$1,000	\$1,000–\$3,000

Our rewards are based on severity per CVSS (the Common Vulnerability Scoring Standard). Please note these are general guidelines, and reward decisions are up to the discretion of Coinhako.

### Response Efficiency

1 day, 15 hours  
Average time to first response

1 day, 18 hours  
Average time to triage

...  
Average time from triage to bounty

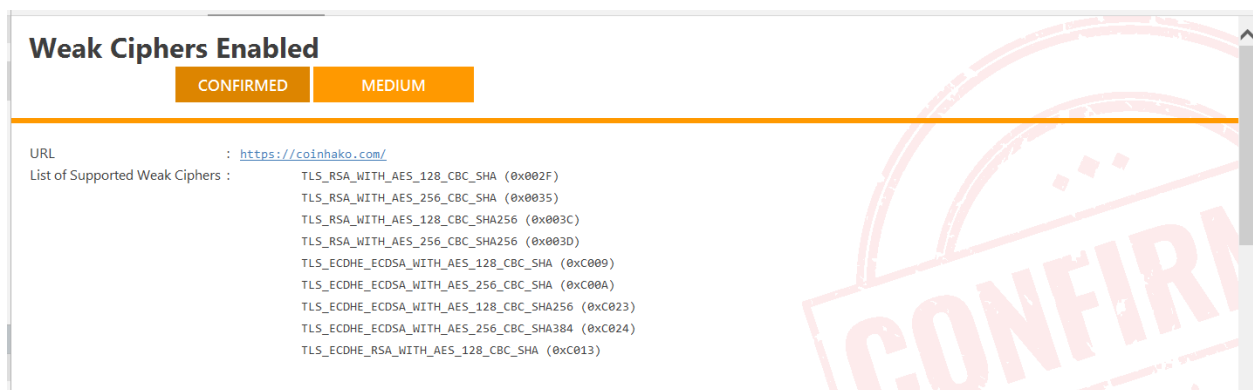
The domain <https://coinhako.com> has numerous vulnerabilities that I have discovered. Based on the OWASP Top 10 list, I found that it had

vulnerabilities. Additionally, the website has a medium overall hazard rating. Using Net Sparker, I found vulnerabilities in the following domain. A handful of the tools that were previously discussed in this part were utilized. I found the following OWASP Top Vulnerabilities,

- | a.Sensitive                   | Data | Exposure |
|-------------------------------|------|----------|
| b. Cross-Site Scripting (XSS) |      |          |
| c. Broken Access Control      |      |          |

## Sensitive Data Exposure

### 1.Weak cipher enabled (confirmed)



- **Impact assessment**

Attackers might decrypt SSL traffic between your server and your visitors.

- **Affected components**

Server's SSL/TLS configuration, cryptographic ciphers, and client-side implementations affected.

- **How to mitigate?**

Disable outdated and insecure SSL/TLS protocol versions (e.g., SSL 2.0, SSL 3.0).

Disable weak cryptographic ciphers (e.g., DES, RC4, MD5) and enable only strong ciphers recommended by security standards.

Regularly update SSL/TLS configurations, server software, and cryptographic libraries to mitigate newly discovered vulnerabilities.

## Cross-Site Scripting (XSS)

### 2.Missing X-XSS-Protection Header

#### Missing X-XSS-Protection Header

BEST PRACTICE

Certainty : 

URL : <http://coinhako.com/cdn-cgi/images/icon-exclamation.png?1376755637>

#### Vulnerability Details

Netsparker detected a missing `X-XSS-Protection` header which means that this website could be at risk of a Cross-site Scripting (XSS) attacks.

#### Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

#### Remedy

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

`X-XSS-Protection: 1; mode=block`

#### External References

#### CLASSIFICATION

CWE	<a href="#">16</a>
WASC	<a href="#">15</a>
HIPAA	<a href="#">164.308(A)</a>
ISO27001	<a href="#">A.14.2.5</a>

- **Impact assessment**

Web applications may be put at significant risk for security breaches if the "X-XSS-Protection" header is missing or incorrectly configured. The website becomes susceptible to script injection since browsers do not by default provide defense against XSS attacks in the absence of this header.

Malicious scripts can be executed by attackers using this vulnerability, which can result in undesirable results like data theft, virus dissemination, reputational harm, session hijacking, and future compliance violations. It's crucial to check user inputs, apply extra security headers like CSP and HSTS, enable XSS protection, and perform frequent security audits in order to reduce these risks. In addition to strengthening the overall security of the online application or website, these proactive actions greatly lessen the possibility of XSS assaults.

- **Affected components**

When a web application's "X-XSS-Protection" header is missing or incorrectly configured, it leaves numerous components vulnerable to serious attacks. This includes the possibility of malicious script injection into user-input forms and web pages, which could result in sensitive data compromise, data theft, and session hijacking. These flaws not only harm the website's reputation but also put industry standards compliance at danger.

- **How to mitigate?**

Using a multifaceted strategy is necessary to mitigate the risks related to the lack or incorrect setup of the "X-XSS-Protection" header. This entails deploying Strict-Transport-Security (HSTS) and other security headers, conducting frequent XSS audits, putting in place stringent input validation and a strong Content Security Policy (CSP), and enabling the header with the correct configuration. It is also essential to keep software up to date, educate stakeholders about XSS dangers and best practices, and have a plan in place for responding to security issues. When combined, these



defenses strengthen web security, lessen XSS vulnerabilities, and guard against data theft and malicious script injections.

## Broken Access Control

### 3. Forbidden Resource

**Forbidden Resource**

CONFIRMEDINFORMATION

URL : <http://coinhako.com/cdn-cgi/styles/>

**Vulnerability Details**

Netsparker identified a forbidden resource.

Access to this resource has been denied by the web server. This is generally not a security issue, and is reported here for informational purposes.

**Impact**

This issue is reported as additional information only. There is no direct impact arising from this issue.

CLASSIFICATION

OWASP PC [C8](#)

ISO27001 [A.8.1.1](#)

CONFIRMED

- **Impact assessment**

A "403 Forbidden" status code from a web server means the client does not have the required permissions to access the resource requested. There are various ramifications when a resource request results in a "403 Forbidden" message. First, it indicates the client does not have the necessary authorization or authentication, which may cause problems with functionality and user experience. It might also reveal potential

security holes or misconfigurations in access control systems, underscoring the significance of careful testing and security audits. When such mistakes happen frequently or without a clear explanation, they can undermine users' trust in the website or program.

Additionally, search engine crawlers may encounter difficulties indexing the content, affecting search visibility and potentially impacting organic traffic.

- **Affected components**

When a requested resource returns a "403 Forbidden" response code, it affects several parts of the online application. It indicates that access is being denied because of problems with authorization or authentication, indicating possible flaws in user authentication or access control systems. Users have unpleasant interactions and interrupted access, which could erode trust. In order to resolve these problems, it will be necessary to examine and modify authentication methods, enhance user error handling, improve access controls, and keep a close eye out for security threats and unauthorized access attempts. Enhancing security in these areas also maintains a smooth user experience and helps improve search engine ranking and indexing.

- **How to mitigate?**

To mitigate "403 Forbidden" errors, a methodical strategy to fortify access controls and enhance user experience is necessary:

1. Access Control Review: Make sure that user permissions and roles are appropriately reflected in access control methods like RBAC and ACLs by thoroughly reviewing them.

2. Authentication Enhancement: To stop unwanted access attempts and make sure users have the right permissions and credentials, enhance user authentication procedures.

3. Error Handling: Create personalized error pages or messages in response to "403 Forbidden" issues to give consumers clear instructions, lessen annoyance, and improve usability.

4. Monitoring and Logging: To quickly identify and look into possible security risks or misconfigurations, set up monitoring and logging for access-denied events.

5. Regular Audits: To find and fix access control flaws or misconfigurations early on, do routine security audits and vulnerability assessments.

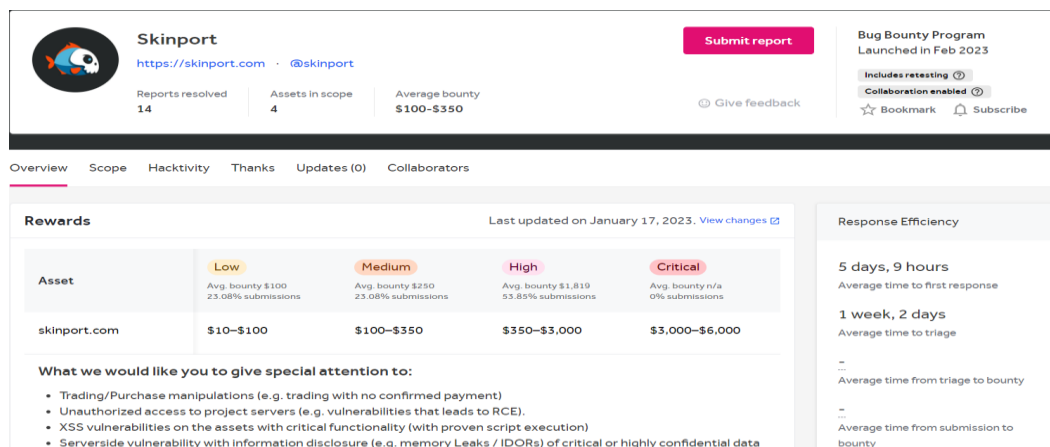
6. Education and Awareness: To lower the number of unintentional access-denied instances, educate users on access policies, permissions, and appropriate authentication procedures.

7. Automated Testing: To mimic and spot any access problems or weaknesses in access control systems, use automated testing techniques.

Organizations can improve security, increase user experience, tighten access controls, and lessen the frequency of "403 Forbidden" errors on their websites or web apps by putting these strategies into practice.

**Domain: <https://skinport.com>**

## Proof of concept:



**Skinport**  
<https://skinport.com> · @skinport

Reports resolved: 14 | Assets in scope: 4 | Average bounty: \$100-\$350

[Submit report](#) | [Give feedback](#)

Bug Bounty Program  
Launched in Feb 2023

Includes retesting | Collaboration enabled

☆ Bookmark | 🔔 Subscribe

Overview | Scope | Hacktivity | Thanks | Updates (0) | Collaborators

### Rewards

Last updated on January 17, 2023. [View changes](#)

Asset	Low Avg. bounty \$100 23.08% submissions	Medium Avg. bounty \$250 23.08% submissions	High Avg. bounty \$1,819 53.85% submissions	Critical Avg. bounty n/a 0% submissions
skinport.com	\$10-\$100	\$100-\$350	\$350-\$3,000	\$3,000-\$6,000

What we would like you to give special attention to:

- Trading/Purchase manipulations (e.g. trading with no confirmed payment)
- Unauthorized access to project servers (e.g. vulnerabilities that leads to RCE).
- XSS vulnerabilities on the assets with critical functionality (with proven script execution)
- Serverside vulnerability with information disclosure (e.g. memory Leaks / IDORs) of critical or highly confidential data

### Response Efficiency

5 days, 9 hours  
Average time to first response

1 week, 2 days  
Average time to triage

—  
Average time from triage to bounty

—  
Average time from submission to bounty

The domain <https://skinport.com> has numerous vulnerabilities that I have discovered. Based on the OWASP Top 10 list, I found that it had

vulnerabilities. Additionally, the website has a medium overall hazard rating. Using Net Sparker, I found vulnerabilities in the following domain. A handful of the tools that were previously discussed in this part were utilized. I found the following OWASP Top Vulnerabilities,

- a. XML External Entities (XXE)
- b. Broken Authentication
- c. Sensitive Data Exposure

## Security Misconfiguration

### 1.Expect-CT Not Enabled

#### **Expect-CT Not Enabled**

BEST PRACTICE

Certainty :   
URL : <https://skinport.com/cdn-cgi/>

Your website runs the danger of data theft or modification if Expect-CT is not enabled. This can result in security vulnerabilities like man-in-the-middle attacks and downgrade attacks. It may also damage trust, reputation, SEO rankings, and adherence to industry standards. It also lacks transparency in identifying unapproved certificate issuances. Security is improved when Expect-CT is enabled via HTTP headers, especially when paired with other safeguards like HSTS.

- **Impact assessment**

Your website runs the danger of data theft or modification if Expect-CT is not enabled. This can result in security vulnerabilities like man-in-the-middle attacks and downgrade attacks. It may also damage trust, reputation, SEO rankings, and adherence to industry standards. It also lacks transparency in identifying unapproved certificate issuances. Security is improved when Expect-CT is enabled via HTTP headers, especially when paired with other safeguards like HSTS.

- **Affected components**

The security and operation of your website might be significantly impacted by the lack of Expect-CT. It puts your website at danger of intrusions like data interception and unauthorized certificate issuances, which could tarnish your reputation and cause sensitive user data to be compromised. Expect-CT and other security best practices must be implemented, as evidenced by non-compliance with security requirements and possible SEO consequences. Expect-CT is an essential part of your online security infrastructure since it not only improves security but also helps you stay compliant with legislation, preserve user confidence, and rank higher in search results.

- **How to mitigate?**

The following actions should be taken to reduce the hazards related to not having Expect-CT enabled: Use HTTPS for your whole website, put HSTS in place for secure connections, enable Expect-CT to enforce certificate transparency checks, perform routine security audits, keep

software updated, keep an eye out for unauthorized certificates in CT logs, train employees on security procedures, and keep data backups with a contingency plan. Combined, these safeguards improve the security of your website, safeguard user information, and maintain the credibility of visitors.

## Broken Authentication

### 2. Email Address Disclosure

#### Email Address Disclosure

INFORMATION

Certainty : [REDACTED]

URL : <https://skinport.com/static/main.ceb72ef4003400ce.1s>

Email Address(es) : [affiliate@skinport.com](mailto:affiliate@skinport.com)  
[hello@skinport.com](mailto:hello@skinport.com)  
[jobs@skinport.com](mailto:jobs@skinport.com)  
[98577efcbca24e6daef4a099b6611076@o298045.ingest.sentry.io](mailto:98577efcbca24e6daef4a099b6611076@o298045.ingest.sentry.io)

#### Vulnerability Details

Netsparker identified an Email Address Disclosure.

#### Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

#### Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

- **Impact assessment**

Email address exposure can have many harmful effects, such as a rise in phishing and spam emails, privacy infringement, dangers of identity theft, harm to one's reputation, legal repercussions, communication problems, and data security threats. Strong data protection rules, user information security, user consent, regulatory compliance, employee education, and

incident response strategies are all necessary to mitigate these effects. By taking these precautions, you can preserve user privacy, uphold confidence, and lessen the chance of data breaches and their repercussions.

- **Affected components**

Email address disclosure affects many elements, including communication routes, data protection procedures, legal compliance, user privacy, security infrastructure, and customer relationships. Strong data protection measures, regulatory compliance, improved security protocols, stakeholder education, and openness in data handling procedures are all necessary to mitigate these effects. By taking these steps, companies may preserve user privacy, uphold confidence, and avoid negative legal and reputational effects.

- **How to mitigate?**

Organizations should concentrate on putting in place a mix of organizational, administrative, and technical safeguards to reduce the risks related to email address disclosure. They consist of employing secure communication channels, enforcing access controls, masking data, conducting frequent security audits, getting user consent, offering security training, creating an incident response plan, making sure regulations are followed, and putting data retention policies into place. Together, these initiatives support user privacy protection, uphold confidence, and lessen



the possibility and consequences of email address-related data breaches or leaks.

## Sensitive Data Exposure

### 3.Content Security Policy (CSP) Not Implemented

#### **Content Security Policy (CSP) Not Implemented**

BEST PRACTICE

URL : <https://skinport.com/cdn-cgi/styles/>

- **Impact assessment**

Websites are vulnerable to serious security concerns such as client-side code execution, XSS attacks, and data breaches if Content Security Policy (CSP) is not implemented. User trust may be eroded, reputations may be tarnished, compliance problems may arise, and financial losses may result. It is essential to implement CSP with clear policies, frequent security audits, and developer training to reduce these risks, safeguard user data, uphold confidence, and guarantee regulatory compliance.

- **Affected components**


Web application integrity, user experience, reputation, compliance, development efforts, and website security against cross-site scripting (XSS) attacks are just a few of the elements that are impacted when there is no Content Security Policy (CSP). Ensuring legal compliance, protecting user data, preserving trust, and preserving operational stability all depend on the implementation of CSP with clear regulations, frequent assessments, and staff training.

- **How to mitigate?**

Content Security Policy (CSP) can be deployed and defined for your website; inline scripts can be used with nonces and hashes; policy violations can be reported; CSP can be gradually implemented; third-party content from CDNs can be taken into account; additional XSS prevention measures can be implemented; regular security audits can be carried out; developer training can be given; compliance can be monitored; and content security policies can be kept up to date. All together, these steps improve web security, lower the danger of XSS attacks, safeguard user information, guarantee compliance, and increase user confidence.

Target domain: <http://smtp2go.com>

**Proof of concept:**



**SMTP2GO BBP**  
<http://smtp2go.com>

Submit report

Bug Bounty Program  
 Launched in Mar 2022

Managed by HackerOne  
 Includes retesting ⓘ

☆ Bookmark    🔔 Subscribe

Reports resolved  
179

Assets in scope  
3

Average bounty  
\$300

☺ Give feedback

[Overview](#)
[Scope](#)
[Hacktivity](#)
[Thanks](#)
[Updates \(0\)](#)

**Rewards**

Last updated on May 11, 2021. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$100 42.22% submissions	Avg. bounty \$298 48.89% submissions	Avg. bounty \$653 8.89% submissions	Avg. bounty n/a 0% submissions
\$100	\$300	\$750	\$2,000

Our rewards are based on severity per CVSS (the Common Vulnerability Scoring Standard). Please note these are general guidelines, and reward decisions are up to the discretion of SMTP2GO.

**Response Efficiency**

1 week, 8 hours  
 Average time to first response

1 week, 6 days  
 Average time to triage

2 months, 1 week  
 Average time from triage to bounty

The domain <http://www.booking.com> has numerous vulnerabilities that I have discovered. Based on the OWASP Top 10 list, I found that it had vulnerabilities. Additionally, the website has a medium overall hazard rating. Using Net Sparker, I found vulnerabilities in the following domain. A handful of the tools that were previously discussed in this part were utilized. I found the following OWASP Top Vulnerabilities,

- a. Security Misconfiguration
- b. Cross-Site Request Forgery (CSRF)
- c. Sensitive Data Exposure

## Security Misconfiguration

### 1. Hidden File Found

<b>Alert tags</b>	<ul style="list-style-type: none"> <li>▪ <a href="#">OWASP_2021_A05</a></li> <li>▪ <a href="#">WSTG-v42-CONF-05</a></li> <li>▪ <a href="#">OWASP_2017_A06</a></li> </ul>
<b>Alert description</b>	<p>A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.</p>
<b>Request</b>	<p>▼ Request line and header section (226 bytes)</p> <pre>GET http://smtp2go.com/.hg HTTP/1.1 host: smtp2go.com user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.0.0 Safari/537.36 pragma: no-cache cache-control: no-cache</pre> <p>▼ Request body (0 bytes)</p>

## • Impact assessment

A hidden file's impact assessment process includes actions including alert creation, impact analysis, reaction, and post-event review. Understanding the file's intended use, place of origin, and possible risks is the aim, along with implementing the necessary countermeasures and strengthening security protocols to avert future occurrences of the same kind.

- **Affected components**

The affected components, including system components, data, dependencies, user roles, services, and compliance needs, must be identified to evaluate the impact of a hidden file or any security incident. By providing focused mitigation solutions, restoring affected components, and preventing future occurrences of the same type of incident, this thorough investigation aids in understanding the magnitude of the impact.

- **How to mitigate?**

A methodical strategy is necessary to minimize the consequences of a hidden file or security event. As you analyze the hidden file to determine its sources and potential hazards, start by isolating and quarantining the impacted computers. Updating software and applying security patches can help avert similar problems in the future. Detection skills are improved by using security tools like intrusion detection systems and antivirus software. Risks are reduced by putting in place stringent access control procedures and regularly training users on security. Rapid containment and recovery are ensured by having a clearly established incident response plan. A strong mitigation strategy is complemented by regular data backups and anomaly monitoring tools, which increase overall cybersecurity resilience.

## Cross-Site Request Forgery (CSRF)

- **Absence of Anti-CSRF Tokens**

▼ GET http://smtp2go.com

**Alert tags**

- [OWASP\\_2021\\_A05](#)
- [OWASP\\_2017\\_A06](#)

**Alert description**

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

**Request**

▼ Request line and header section (222 bytes)

```
GET http://smtp2go.com HTTP/1.1
host: smtp2go.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Request body (0 bytes)

## • Impact assessment

Understanding the susceptibility of online applications to cross-site request fraud (CSRF) assaults is a necessary step in performing an impact assessment when Anti-CSRF tokens are not present. Possible consequences encompass illicit activities, falsification of data, or breach of account. Enhancing access controls, verifying requests, and deploying Anti-CSRF tokens are examples of mitigation techniques. An all-encompassing mitigation approach to lower CSRF threats and enhance overall web application security must include extensive testing, monitoring, user education, and response protocols.

## • Affected components

When assessing the effects of not having Anti-CSRF tokens, one must consider potential risks to user data and transactions, vulnerabilities in web interfaces, effects on authentication systems and back-end services, risks associated with third-party integrations, implications for compliance, and effects on user trust and application reputation. To effectively reduce CSRF risks and improve overall security, mitigating efforts and implementing Anti-CSRF solutions are guided by an understanding of these components.

- **How to mitigate?**

Using several techniques to defend web applications against CSRF attacks is necessary to mitigate the lack of Anti-CSRF tokens. Implementing HTTP headers like Same-Site and Referer, deploying Anti-CSRF tokens in forms and API requests, making sure secure authentication procedures are followed, verifying request origins, using Content Security Policy (CSP), putting security headers in place, carrying out routine security audits, training users, and thinking about using a Web Application Firewall (WAF) are important steps to take. When combined, these steps improve web applications' security posture by lowering the possibility of CSRF vulnerabilities and boosting defenses against harmful activity.

## Sensitive Data Exposure

### 3.Cloud Metadata Potentially Exposed

Cloud Metadata Potentially Exposed							
URL:	<a href="http://smtp2go.com/latest/meta-data/">http://smtp2go.com/latest/meta-data/</a>						
Risk:	High						
Confidence:	Low						
Parameter:							
Attack:	169.254.169.254						
Evidence:							
CWE ID:	0						
WASC ID:	0						
<b>Description:</b> The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.							
<b>Other Info:</b> Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.							
<b>Solution:</b> Do not trust any user data in NGINX configs. In this case it is probably the use of the \$host variable which is set from the 'Host' header and can be controlled by an attacker.							
<b>Reference:</b> <a href="https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/">https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/</a>							
<b>Alert Tags:</b> <div> <div>+</div> <div>—</div> <div>✎</div> </div> <table border="1"> <thead> <tr> <th>Key</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>OWASP_2021_A05</td> <td><a href="https://owasp.org/Top10/A05_2021-Security_Misconfiguration/">https://owasp.org/Top10/A05_2021-Security_Misconfiguration/</a></td> </tr> <tr> <td>OWASP_2017_A06</td> <td><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></td> </tr> </tbody> </table>		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>
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>						

## • Impact assessment

The vulnerabilities in data security, data integrity, confidentiality, account compromise, resource exploitation, and operational disruptions can all be greatly affected by the exposure of cloud metadata. Quick vulnerability discovery, strong access controls, encryption of sensitive data, ongoing monitoring, compliance with security best practices, frequent audits, employee training, and incident response planning are some examples of mitigation techniques. By working together, these steps improve cloud security and resilience against hacking and data leaks.

## • Affected components

The impact of exposed cloud metadata must be assessed by examining all impacted components, including monitoring systems, security



configurations, cloud resources, metadata stores, access keys, network infrastructure, and third-party integrations. Organizations can create focused mitigation plans by having a thorough understanding of the risks and vulnerabilities related to each component. Encrypting sensitive data, enforcing regulatory compliance, monitoring for unwanted access, safeguarding metadata repositories, and putting strong access controls in place are a few examples of these tactics. Organisations can enhance their cloud security posture and prevent potential dangers resulting from exposed metadata by implementing a holistic approach towards resolving these concerns.

- **How to mitigate?**

Implementing stringent access controls, encrypting data in transit and at rest, keeping secure configurations, enabling audit logging and monitoring, taking metadata redaction into consideration, carrying out routine security assessments, educating staff members, creating an incident response plan, and making sure applicable laws are followed are all necessary to reduce the risks associated with exposed cloud metadata. By doing these steps together, the cloud environment's security posture is improved, risks of unauthorized access are decreased, and data protection is strengthened.

- **The challenges I faced and how I handled them**

First Challenge: Determining Goals and Extent

- Performed an extensive analysis of scoping papers and program guidelines.

- Used methods such as subdomain enumeration, Google dorking, and recon-ng to identify targets.

## Task 2: Giving Vulnerabilities Priority

- Used a risk-based approach to assess exploitability and effect.
- Vulnerabilities with high effect and ease of exploitation were given priority.

## Challenge 3: Getting Around Security Measures

- Used strategies to get around security measures including IP blocking, rate limitation, and WAFs.
- Relentlessly observed and modified strategies to evade detection.

## Conclusion.

My bug bounty journey has been a profound exploration into the ever-evolving realm of cybersecurity. In this report, I've shared my discoveries, triumphs over challenges, and the invaluable insights gained, showcasing significant strides and expertise gained through bug bounty engagements.

Participating in bug bounty programs has not only honed my technical prowess but has also fostered critical thinking, problem-solving skills, and effective communication. From tackling common misconfigurations to unraveling complex logic flaws, I've uncovered various vulnerabilities, contributing to overall system security enhancements.

Reflecting on this transformative journey, I am filled with pride and satisfaction, relishing the substantial expansion of my knowledge and network within the cybersecurity community. Bug bounty initiatives have proven to be indispensable platforms for continuous learning and self-improvement. I am deeply grateful for the opportunities they've provided and the unwavering support from fellow enthusiasts along this path.

As I wrap up this bug bounty report, I eagerly anticipate the ongoing evolution of my cybersecurity journey. I am committed to further refining my skills, staying vigilant against emerging threats, and continuing to make a positive impact in safeguarding digital ecosystems.

These bug bounty experiences have not only propelled personal growth but have also reignited my unyielding passion for defending organizations and individuals from the grasp of malicious actors.