



Sri Lanka Institute of Information Technology

IE2062-Web Security

IT Number	Name
IT22581402	C.D.Aluthge

Information gathering and reconnaissance phase

- a. Subdomain enumeration
 - i. Recon-*ng*
- b. Getting alive subdomains
 - i. Nslookup
- c. DNS enumeration
 - i. Dnsrecon
 - ii. nikto
 - iii. Dnsdumper
- d. Public devices enumeration
 - i. Censys
 - ii. Whatweb
 - iii. Whois
- e. Find WAF (web application firewall) protection.
 - i. Wafwoof
- f. Find open ports.
 - i. Nmap
- g. Exploitation
 - i. sqlmap

vulnerability analysis phase

1. Target domain: <http://oyorooms.com>
 - a. Missing X-Frame-Options Header
 - b. HTTP Strict Transport Security (HSTS) Policy Not Enabled
 - c. Weak Ciphers Enabled
 - d. Missing X-XSS-Protection Header

Conclusion

Scope:

OYO Rooms is an Indian hospitality company founded in 2013 by Ritesh Agarwal. It specializes in providing standardized, budget-friendly

accommodations through partnerships with hotels and guesthouses. OYO gained popularity for its easy booking process and clean, comfortable rooms with basic amenities. The company expanded internationally and diversified into vacation rentals, mid-market hotels, and premium economy hotels under different brands. OYO's innovative approach and rapid growth have made it a significant player in the budget and mid-market hospitality sectors.

The screenshot shows the OYO website homepage. At the top, there are navigation links for 'Become a Member' (Additional 10% off on stays), 'OYO for Business' (Trusted by 5000 Corporates), 'List your property' (Start earning in 30 mins), 'Call us to Book now' (0124-6201611), 'English' (dropdown), 'Login / Signup', and a 'Login now to get upto 15% lower prices' button. Below the header, there are dropdown menus for cities: Bangalore, Chennai, Delhi, Gurgaon, Hyderabad, Kolkata, Mumbai, and Noida. A large banner in the background features a person in a scuba diving suit. Overlaid on the banner is the text 'Over 174,000+ hotels and homes across 35+ countries'. Below the banner is a search bar with fields for 'Search by city, hotel, or neighborhood', 'Near me', 'Wed, 1 May – Thu, 2 May', '1 Room, 1 Guest', and a green 'Search' button. To the right of the search bar is a promotional section for 'Quality stays, Always.' featuring a large '70% OFF' graphic and a woman looking out a window. On the far right, there is a QR code with the text 'Scan to download the App'.

In Scope:

Asset name ↑	Type ↑	Coverage ↑	Max. severity ↓	Bounty ↑	Last update ↑
com.oyo.consumer	Android: Play Store	In scope	Critical	\$ Ineligible	Oct 4, 2022
com.oyo.ryo-ios	iOS: App Store	In scope	Critical	\$ Ineligible	Oct 4, 2022
http://*.oyohotels.cn	Wildcard	In scope	Critical	\$ Ineligible	Oct 12, 2022
http://*.oyohotels.top	Wildcard	In scope	Critical	\$ Ineligible	Oct 12, 2022
http://*.yoosoos.com	Wildcard	In scope	Critical	\$ Ineligible	Oct 12, 2022
http://*.oyorooms.com	Wildcard	In scope	Critical	\$ Ineligible	Oct 12, 2022
http://*.dancenter.se	Wildcard	In scope	Critical	\$ Ineligible	Oct 12, 2022
http://*.belvilla.com	Wildcard	In scope	Critical	\$ Ineligible	Oct 12, 2022
http://*.traum-ferienwohnungen.de	Wildcard	In scope	Critical	\$ Ineligible	Oct 12, 2022
com.oyo.partnerapp	Android: Play Store	In scope	High	\$ Ineligible	Oct 12, 2022
com.oyo.property	Android: Play Store	In scope	High	\$ Ineligible	Oct 12, 2022
com.belvilla.rental	iOS: App Store	In scope	High	\$ Ineligible	Oct 12, 2022
com.oyo.partnerapp	iOS: App Store	In scope	High	\$ Ineligible	Oct 12, 2022
com.oyo.campus	iOS: App Store	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.admiralstrand.dk	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.villaxl.com	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.tui-ferienhaus.de	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.leisure-partners.net	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.oyocircle.com	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.topictravel.nl	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
traum-ferienwohnungen.de	Domain	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.danland.dk	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.stugsommar.se	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022
http://*.belvilla.fr	Wildcard	In scope	High	\$ Ineligible	Oct 12, 2022

preprod.oyorooms.ms	Domain	In scope	Medium	Ineligible	Oct 12, 2022
http://patron.ryo.com/blog/in	URL	In scope	Medium	Ineligible	Oct 12, 2022
http://*.oyolasvegas.com	Wildcard	In scope	Medium	Ineligible	Oct 12, 2022
http://*.weddingz.in	Wildcard	In scope	Medium	Ineligible	Oct 12, 2022
http://*.oyorooms.io	Wildcard	In scope	Medium	Ineligible	Jul 21, 2023
com.jedi.jediaudit	Android: Play Store	In scope	Low	Ineligible	Oct 12, 2022
com.oyorooms.coworkfoodvendor	Android: Play Store	In scope	Low	Ineligible	Oct 12, 2022
com.ryo.consumerlite	Android: Play Store	In scope	Low	Ineligible	Oct 12, 2022
com.guerrilla.innov8coworking	Android: Play Store	In scope	Low	Ineligible	Oct 12, 2022
com.oyorooms.weddingz.content	Android: Play Store	In scope	Low	Ineligible	Oct 12, 2022
work.innov8.mobilecowork	iOS: App Store	In scope	Low	Ineligible	Oct 12, 2022
com.oyorooms.weddingz.content	iOS: App Store	In scope	Low	Ineligible	Oct 12, 2022
work.innov8.mobilecowork	iOS: App Store	In scope	Low	Ineligible	Oct 12, 2022
com.oyorooms.weddingz.content	iOS: App Store	In scope	Low	Ineligible	Oct 12, 2022
http://*.innov8.work	Wildcard	In scope	Low	Ineligible	Oct 12, 2022
http://*.oyotownhouse.com	Wildcard	In scope	Low	Ineligible	Oct 12, 2022
http://*.workflobyoyo.com	Wildcard	In scope	Low	Ineligible	Oct 12, 2022
http://*.oyoworkspaces.com	Wildcard	In scope	Low	Ineligible	Oct 12, 2022

OWASP top 10 vulnerabilities

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures

- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

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 a 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.

Information gathering and reconnaissance phase.

The objective is to gather as much pertinent data as you can about the intended system or organization. Understanding the target's infrastructure, seeing potential vulnerabilities, and organizing additional security testing operations are all made easier with the aid of this information.

Domain: <http://oyorooms.com>

Subdomain enumeration

- 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.

Proof of concept:

A screenshot of the recon-NG command-line interface. The top left shows the command '\$ recon-NG' followed by '[*] Version check disabled.' Below this is a large decorative banner consisting of many stylized 'J' and 'L' characters. To the left of the banner, the text 'Sponsored by ...' is visible. In the center, there is a logo for 'BLACK HILLS' with the URL 'www.blackhillsinfosec.com'. Below the logo is the quote 'the quieter you become, the more you are able to hear'. At the bottom, there is a logo for 'PRACTISEC' with the URL 'www.practisesec.com'. The bottom right corner shows the text '[recon-NG v5.1.2, Tim Tomes (@lanmaster53)]'.

To get google website give this command.

```
[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ...

+-----+
|          Path           | Version | Status | Updated | D | K |
+-----+
| recon/domains-hosts/google_site_web | 1.0     | installed | 2019-06-24 |   |   |
+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
[recon-ng][default] > show info
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ...
```

- You can see it's not installed yet. We must download installation path.
- After installing path using show info to see its download or not.

```
+-----+
|          Path           | Version | Status | Updated | D | K |
+-----+
| recon/domains-hosts/google_site_web | 1.0     | installed | 2019-06-24 |   |   |
+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > info

    Name: Google Hostname Enumerator
    Author: Tim Tomes (@lanmaster53)
    Version: 1.0
Description:
    Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with
    the results.
```

Load the installed module path and use info see options.

Go to options and set source to our targeted domain indrive.com and run it.

```

Options:
  Name    Current Value  Required  Description
  ____  _____ / _____ / _____
  SOURCE  booking.com   yes        source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

[recon-ng][default][google_site_web] > options set source oyorooms.com
SOURCE => oyorooms.com
[recon-ng][default][google_site_web] > run

```

OYOROOMS.COM

```

[*] Searching Google for: site:oyorooms.com
[*] Country: None
[*] Host: business.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: www.oyorooms.com      "the quieter you become, the more you are able to hear"
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

```

```

[*] Searching Google for: site:oyorooms.com -site:business.oyorooms.com -site:www.oyorooms.com
[*] Country: None
[*] Host: link.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: deals.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: share.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]

```

```
[*] _____
[*] Country: None
[*] Host: share.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: globaldesk.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: details.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Searching Google for: site:oyorooms.com -site:business.oyorooms.com -site:www.oyorooms.com -site:link.oyorooms.com -site:deals.oyorooms.com -site:share.oyorooms.com -site:globaldesk.oyorooms.com -site:details.oyorooms.com -site:holead-dancercenter-dk-prod.oyorooms.com -site:web.oyorooms.com -site:travelagent.oyorooms.com -site:tech.oyorooms.com -site:patron.oyorooms.com -site:identity-gateway.oyorooms.com -site:partners.oyorooms.com -site:games.oyorooms.com -site:holead-dancercenter-se-prod.oyorooms.com -site:hub.oyorooms.com
[*] Country: None
[*] Host: holead-admiralstrand-dk-prod.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: internalcst.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: ovh-images.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: mpower.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] _____
[*] Country: None
[*] Host: hr.oyorooms.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
```

SUMMARY

```
[*] 32 total (32 new) hosts found.  
[recon-ng][default][google_site_web] > █
```

Getting alive subdomains

- 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.

Proof of concept:

```
File System
└──(deshan㉿kali)-[ ~ ]
└─$ nslookup oyorooms.com
Server:          192.168.43.1
Address:         192.168.43.1#53

Non-authoritative answer:
Name:    oyorooms.com
Address: 23.52.113.122
```

DNS enumeration

- Dnsdumpster

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.

- **Proof of concept:**

DNS Servers		
a1-173.akam.net. dns.icann.org.	193.108.91.173 	AKAMAI-ASN2 The Netherlands
a16-65.akam.net. dns.icann.org.	23.211.132.65 	AKAMAI-ASN2 United States
a3-67.akam.net. dns.icann.org.	96.7.49.67 	AKAMAI-ASN2 United States
a11-64.akam.net. dns.icann.org.	84.53.139.64 	AKAMAI-ASN2 The Netherlands
a8-64.akam.net. dns.icann.org.	2.16.40.64 	AKAMAI-ASN2 The Netherlands
a24-66.akam.net. dns.icann.org.	2.16.130.66 	AKAMAI-ASN2 The Netherlands

- Proof of concept:

MX Records ** This is where email for the domain goes...		
10 alt3.aspmx.l.google.com. 	142.250.27.26 	GOOGLE United States
10 alt4.aspmx.l.google.com. 	142.250.153.26 	GOOGLE United States
30 aspmx3.googlemail.com. 	64.233.184.27 	GOOGLE United States
5 alt1.aspmx.l.google.com. 	209.85.202.26 	GOOGLE United States
10 aspmx.l.google.com. 	172.253.122.27 	GOOGLE United States
0 oyorooms-com.mail.protection.outlook.com. 	52.101.144.3 	MICROSOFT-CORP-MSN-AS-BLOCK India
5 alt2.aspmx.l.google.com. 	64.233.184.26 	GOOGLE United States
30 aspmx2.googlemail.com. 	209.85.202.27 	GOOGLE United States

TXT Records :: Find more hosts in Sender Policy Framework (SPF) configurations

```
"v=spf1 ip4:3.7.196.96 ip4:3.7.127.96 ip4:40.92.0.0/15 ip4:50.31.55.210 ip4:52.203.5.138 ip4:35.158.71.15 ip4:52.66.154.99 ip4:3.7.25.40/2 ip4:170.52.3.228 ip4:170.52.4.253 ip4:40.107.0" "-.0/16 ip4:52.100.0.0/14 ip4:104.47.0.0/17 ip4:66.102.0.0/20 ip4:74.125.0.0/16 ip4:35.191."
"amazonaws.com:dn:0qiyiu04u61qd0iqy0aREry4M0as2odt/PA=-"
"google-site-verification=mW0acVbKPkkrmBEExamWcg9PGfBU051xx-11EWUZE8M"
"google-site-verification=Otarwnj5LYV78lia5tIAtpSEebH0c2YfjCzqTys8kg1"
"b5b6hqsh491zj7jylzbx35fa3wh17dm"
"GOOM_verify_AskftfOnBNmin3RFpKD2Vq"
"google-site-verification=gJbs9v9tUlplkLkTGozokBXgHUpdY59j5jkGFFGanZk" "google-site-verification=lCKLu-780Eb5LogDgmoWxSWshopNEsEKO1ZEe31ds"
"google-site-verification=D4sainicMagEm2H1195CshPsKUcV6nu8Vg2OWLvsJdc"
"atlaxian-domain-verification=v7LaRHcowen9A9uraxpRP7kMKhKJU9dt43nWD1qh8j33n/12x2eyN6cRRyV0NVHF"
"google-site-verification=p86ty4X3p2YV2baXo_NZwAGxggCALxkPEC6sg2KyAlo"
"google-site-verification=VA_R_gwpdk6UJgpmmS8ldxzq5AewyPZtDcPm-3ochiT0"
"google-site-verification=8KdxzXx-7K09FeBxGqHQxb5FqnisudrTNiy01G_O"
"ea4cqke2aig6u2e6b110mf=ea3l"
"apple-domain-verification=NOREWUSDgtitkTe6"
"google-site-verification=1IBXm51AjxFv6aC1Ro0KC9mb5JYe0gpdafOHfaew1K8"
"google-site-verification=czdQg43yxkN4laopB-1Ky83amthYN0y-PyoElayYzns"
"google-site-verification=BM_f8C2ctiYnMeECNMvoa9N2U_spvFlp68hkvw17urk"
```

- Proof of concept:

"google-site-verification=Orjdksh12pteyI9fGYbU9iiwm91b4088XsB5P-REOhw"
"google-site-verification=RQFZHwBImWAk31dCRpzvBAHfCF4tldGofjEogr5BYnw"
"google-site-verification=m7l7TV-q9AUqxUe3ckfcLnbulT6JI64x7SB3s5YR8kI"
"apple-domain-verification=KIKhLGoyNlPVlyZ3mTpY6uK7vzinHRNo02mj1ODJWRo"
"eo8r7i80vcmc81m05o5chnf5k"
"google-site-verification=rxxJ7engyEkoLbBwR002d7EPGnBDxajVxHiThAaj5sDI"
"v=DKIM1; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCCTuJN72YGOpwDzAbPWVBAIlMvwOCCNDuZgWeleCGgrPeYYUbcD1EZMPYqgFohkGTDSpfb8Hj2HnrwYiwqYsu9pNTDVVVoCjpq
"google-site-verification=tHZK-vk0mx_6K7pHxDLACjNUhgH316r7Gr_1MGjlP4s"
"k1dpqgqhq8m62km9r9pjcl0kzyseyclvpy"
"cp64dz3bbs0kyhchdpvnrzarqt68hpwn"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
oyorooms.com ■ ■ ○ ✎ ☀ ♡	23.222.204.98 a23-222-204- 98.deploy.static.akamaitechnologies.com	AKAMAI-ASN United States
email11.oyorooms.com ■ ■ ○ ✎ ☀ ♡	153.92.246.231 email11.oyorooms.com	BENDINBLUE-ASN France
o223.env.asia.oyorooms.com ■ ■ ○ ✎ ☀ ♡	149.72.136.185 o362.e.info.oyoroomsmailer.com	SENDGRID United States
o42.e.triggered.oyorooms.com ■ ■ ○ ✎ ☀ ♡	149.72.57.110 o653.env.nanovest.io	SENDGRID United States
o36.mail.triggered.oyorooms.com ■ ■ ○ ✎ ☀ ♡	167.89.17.148 o36.mail.triggered.oyorooms.com	SENDGRID United States
o37.mail.triggered.oyorooms.com ■ ■ ○ ✎ ☀ ♡	167.89.37.150 o37.mail.triggered.oyorooms.com	SENDGRID United States
holead-dancenter-se-prod.oyorooms.com ■ ■ ○ ✎ ☀ ♡	51.137.9.15	MICROSOFT-CORP-MSN-AS-BLOCK Netherlands
holead-admiralstrand-dk-prod.oyorooms.com ■ ■ ○ ✎ ☀ ♡	51.137.9.15	MICROSOFT-CORP-MSN-AS-BLOCK Netherlands
holead-dancenter-dk-prod.oyorooms.com ■ ■ ○ ✎ ☀ ♡	51.137.9.15	MICROSOFT-CORP-MSN-AS-BLOCK Netherlands
dcous-dancenter-dk-prod.oyorooms.com ■ ■ ○ ✎ ☀ ♡	51.137.9.15	MICROSOFT-CORP-MSN-AS-BLOCK Netherlands
obscn-prod.oyorooms.com ■ ■ ○ ✎ ☀ ♡	152.70.173.205	ORACLE-BMC-31898 Germany
holead-dancenter-no-prod.oyorooms.com ■ ■ ○ ✎ ☀ ♡	51.137.9.15	MICROSOFT-CORP-MSN-AS-BLOCK Netherlands

- Proof of concept:

<code>corporate.oyorooms.com</code>	23.44.237.217 a23-44-237- 217.deploy.static.akamaitechnologies.com	AKAMAI-ASN1 United States	   
<code>ownerstaging.oyorooms.com</code>	52.74.234.187 ec2-52-74-234-187.ap-southeast- 1.compute.amazonaws.com	AMAZON-02 Singapore	
<code>tech.oyorooms.com</code>	162.159.153.4	CLOUDFLARENET unknown	
<code>o1408.e.mail.oyorooms.com</code>	149.72.219.186 o1408.e.mail.oyorooms.com	SENDGRID United States	
<code>o609.e.mail.oyorooms.com</code>	149.72.112.99 o609.e.mail.oyorooms.com	SENDGRID United States	
<code>o38.mail.em.oyorooms.com</code>	167.89.37.190 o38.mail.em.oyorooms.com	SENDGRID United States	
<code>pepimail145.info.oyorooms.com</code>	175.158.64.145 pepimail145.info.oyorooms.com	WEBWERKSAS1 India	
<code>pepimail146.info.oyorooms.com</code>	175.158.64.146 pepimail146.info.oyorooms.com	WEBWERKSAS1 India	
<code>pepimail147.info.oyorooms.com</code>	175.158.64.147 pepimail147.info.oyorooms.com	WEBWERKSAS1 India	
<code>ebs.oyorooms.com</code>	10.200.4.186	Reserved (Local Network) unknown	
<code>ebs-dev.oyorooms.com</code>	10.200.1.110	Reserved (Local Network) unknown	
<code>o225.env.notify.oyorooms.com</code>	149.72.136.179 wrqvvvbp.outbound-mail.sendgrid.net	SENDGRID United States	

- Nikto

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.

- **Proof of concept:**

```
(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
```

- 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.

Proof of concept:

```
(deshan㉿kali)-[~] ~ com.google-site-verifications-RQF7HwB1mWAK31dCRpzvBAHFCF4tLd0ofjEogr5BYnw
$ dnsrecon -d oyorooms.com -D /user/share/wordlists/dnsmap.txt -t std --xml oyorooms.xml
[*] std: Performing General Enumeration against: oyorooms.com ...PFeBxGaqHQXh5Fqn1zudrTN1yQ1G0_Q
[-] DNSSEC is not configured for oyorooms.com
[*] SOA a1-173.akam.net 193.108.91.173
[*] SOA a1-173.akam.net 2600:1401:2::ad
[*] NS a16-65.akam.net 23.211.132.65
[*] Bind Version for 23.211.132.65 "28109.140"
[*] ip4:: NS a16-65.akam.net 2600:1406:1b::41
[*] ip4:: NS a8-64.akam.net 2.16.40.64
[*] ip4:: NS a1-173.akam.net 193.108.91.173
[*] ip4:: NS a3-67.akam.net 96.7.49.67
[*] Bind Version for 96.7.49.67 "31224.101"
[*] NS a3-67.akam.net 2600:1408:1c::43
[*] com: NS a11-64.akam.net 84.53.139.64
[*] Bind Version for 84.53.139.64 "36241.227"
[*] No SRV NS a11-64.akam.net 2600:1480:1::40
[*] Savin: NS a24-66.akam.net 2.16.130.66
[*] Bind Version for 2.16.130.66 "18706.36"
[*] NS a24-66.akam.net 2600:1480:9800::42
[*] MX oyorooms-com.mail.protection.outlook.com 52.101.145.2
```

Proof of concept:

```
[*] MX oyorooms-com.mail.protection.outlook.com 52.101.144.3
[*] MX oyorooms-com.mail.protection.outlook.com 52.101.144.0 ·BxGAqHQXb5FqnizudrTN1yQ1G0_Q
[*] MX aspmx.l.google.com 74.125.200.27 action=moacVbKPkjkrmEBEzamWcg9PGfBU051xx-l1EWUZE8M
[*] MX alt2.aspmx.l.google.com 142.250.141.27 T18Xm51AjTfV6aClRo0KCmb5JYe0gpdaf0Hfaewlk8
[*] MX alt3.aspmx.l.google.com 142.250.115.26 gJbz9vTIULpkLKTGoZorKBXgHHPdY59j5jkGFFGanZkgoogle
[*] MX alt4.aspmx.l.google.com 64.233.171.26 ·o
[*] MX alt1.aspmx.l.google.com 173.194.202.27 ·3.7.127.96 ip4:40.92.0.0/15 ip4:50.31.55.210 ip4:
[*] ip4: MX aspmx2.googlemail.com 173.194.202.27.40/29 ip4:65.2.2.76/30 ip4:3.25.47.0/29 ip4:52.62.15
[*] 237.4 MX aspmx3.googlemail.com 142.250.141.27 ·4:40.107.0.0/16 ip4:52.100.0.0/14 ip4:104.47.0.0/17
[*] 0/20 MX aspmx.l.google.com 2404:6800:4003:c11::1b 9.0.0/17 ip4:50.31.32.0/19 include:_spf0000000
[*] ~all MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*] MX alt3.aspmx.l.google.com 2607:f8b0:4023:1004 ::1b ·2YV2bsXo_NZwAGxggCAlkrPEC6sgZKyAhS
[*] MX alt4.aspmx.l.google.com 2607:f8b0:4003:c15::1b ·YNlFVlyZ3mTp6uK7vz1nHRN02mj10DJWRo
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00 ::1b ·3DQEBAQUA4GNADCBiQKBgQCBTUJN7YG0pwDzAbPw
[*] DuZgW MX aspmx2.googlemail.com 2607:f8b0:400e:c00 ::1a ·9pNTDVVVYoCjpq8ygvaOsci3yDnFolLoiFHE2uFFSDep
[*] 5cILP MX aspmx3.googlemail.com 2607:f8b0:4023:c0b ::1b
[*] A oyorooms.com 23.43.33.118 ·ARC1) p=quarantine; pct=100; sp=quarantine; rua=mailto:dmarc-ale
[*] com TXT oyorooms.com google-site-verification=rXJ7engyEkoLbBwR00Zd7EPGnBDxajVxHiThAaj5sDI
[*] Enum TXT oyorooms.com eo8r7i80vcmc81m05o5chfm5k
[*] No S TXT oyorooms.com cp64dz3bbs0kyhchdpvnrzsrqt68hpwn
[*] Savi TXT oyorooms.com google-site-verification=0tarWnj5lYV781ia5tHATpSEebHD02YfjCzgTysSkgI
[*] TXT oyorooms.com ea40qke2aig6u2e6bll0mfes3l
[*] Root TXT oyorooms.com google-site-verification=p86tY4X3p2YV2bsXo_NZwAGxggCAlkrPEC6sgZKyAhS
[*] TXT oyorooms.com google-site-verification=Qrjdks1h2pteyI9fGybU9iiwm91b4088xsB5P-REOhw
```

```
[*]     TXT oyorooms.com google-site-verification=RM_f8C2ctiYnMeECNmVQa9N2U_spvFip68hkvw17urk
[*]     TXT oyorooms.com google-site-verification=tHZK-vk0mx_6K7pHxDLACjNUhgH316r7Gr_1MGjlp4s
[*]     TXT oyorooms.com vxv62d665k5bs2593xyxn0995ky45y9
[*]     TXT oyorooms.com google-site-verification=m7l7TV-q9AUqxUe3ckfcLNbult6JI64x7SB3s5YRSKI
[*]     TXT oyorooms.com google-site-verification=SKDZ7Xh-7K09FeBxGaqHQXb5FqnizudrTN1yQ160_Q
[*]     TXT oyorooms.com v=spf1 ip4:3.7.196.96 ip4:3.7.127.96 ip4:40.92.0.0/15 ip4:50.31.55.210 ip4:52.203.5.
138 ip4:35.158.71.15 ip4:52.66.154.99 ip4:3.7.25.40/29 ip4:65.2.2.76/30 ip4:3.25.47.0/29 ip4:52.62.151.40 ip4:
13.237.4.248 ip4:170.52.3.228 ip4:170.52.4.253 ip4:40.107.0.0/16 ip4:52.100.0.0/14 ip4:104.47.0.0/17 ip4:66.10
2.0.0/20 ip4:74.125.0.0/16 ip4:35.191.0.0/16 ip4:167.89.0.0/17 ip4:50.31.32.0/19 include:_spf0000000.oyorooms.
com ~all
[*]     TXT oyorooms.com google-site-verification=gJbz9vTIUlPklkTg0z0rkBXgHHpdY59j5jkGFFGanZkgoogle-site-veri
fication=lCkLu-7S0Eb5L0gDgmoWxSWzbopNfzKw01ZE3lds0c
[*]     TXT oyorooms.com atlassian-domain-verification=v7LaRHcowom9A9urapxRP7kmkNkJU9dt43nWDlqh8j33n/12x2cYB6
cRhY0NVHF
[*]     TXT oyorooms.com google-site-verification=mW0acVbKPkqkrmEBEzamWcg9PGFBU05lx-l1EWUZE8M
[*]     TXT oyorooms.com apple-domain-verification=KIKhLGoYnLFVlyZ3mTp6uK7vz1nHRN0o2mjioDjWro SQd4PS96b251t
[*]     TXT oyorooms.com b5b6hqsh491zj7kjy1zbx35fs3wh17dm
[*]     TXT _dmarc.oyorooms.com v=DMARC1; p=quarantine; pct=100; sp=quarantine; rua=mailto:dmarc-alerts@oyoro
oms.com ,mailto:dmarc_agg@vali.email;
[*]     Enumerating SRV Records
[-] No SRV Records Found for oyorooms.com
[*]     Saving records to XML file: oyorooms.xml
```

Public devices enumeration

- 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.

Proof of concept:

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 CLOUDFLARENENET, 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

05/01/2024 12:34 UTC

Software CloudFlare Load Balancer

Details http://104.18.36.214/
Status 403 Forbidden
Body Hash sha1:7f6c347c83b72276a9aa533e1790a5364d18fd3c
HTML Title Direct IP access not allowed | Cloudflare

Response Body EXPAND

Geographic Location

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



Proof of concept:

HTTP 443/TCP

05/01/2024 03:32 UTC

Software

CloudFlare Load Balancer [🔗](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:443/>

Status 400 Bad Request

Body Hash sha1:108b6115dc6ebfde76aef4336126f605252d957f

HTML Title 400 The plain HTTP request was sent to HTTPS port

Response Body

[EXPAND](#)

HTTP 2052/TCP

05/01/2024 14:13 UTC

Software

CloudFlare Load Balancer [🔗](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:2052/>

Status 403 Forbidden

Body Hash sha1:d27392f1d1c28d0773a12a41bfcea465c1022845

HTML Title Direct IP access not allowed | Cloudflare

Response Body

[EXPAND](#)

HTTP 2052/TCP

05/01/2024 14:13 UTC

Software

CloudFlare Load Balancer [🔗](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:2052/>

Status 403 Forbidden

Body Hash sha1:d27392f1d1c28d0773a12a41bfcea465c1022845

HTML Title Direct IP access not allowed | Cloudflare

Response Body

[EXPAND](#)

HTTP 2053/TCP

05/01/2024 01:29 UTC

Software

CloudFlare Load Balancer [🔗](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:2053/>

Status 400 Bad Request

Body Hash sha1:108b6115dc6ebfde76aef4336126f605252d957f

HTML Title 400 The plain HTTP request was sent to HTTPS port

Response Body

[EXPAND](#)

Proof of concept:

HTTP 2082/TCP

05/01/2024 12:29 UTC

Software

 CloudFlare Load Balancer [↗ GO](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:2082/>

Status 403 Forbidden

Body Hash sha1:23dad10030a0fce4289082120318ea13df07fd18

HTML Title Direct IP access not allowed | Cloudflare

Response Body

[EXPAND](#)

HTTP 2083/TCP

05/01/2024 12:42 UTC

Software

 CloudFlare Load Balancer [↗ GO](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:2083/>

Status 400 Bad Request

Body Hash sha1:108b6115dc6ebfde76aef4336126f605252d957f

HTML Title 400 The plain HTTP request was sent to HTTPS port

Response Body

[EXPAND](#)

HTTP 2086/TCP

04/30/2024 14:21 UTC

Software

 CloudFlare Load Balancer [↗ GO](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:2086/>

Status 403 Forbidden

Body Hash sha1:20673b620f82d0095e6851e6581f06179288472d

HTML Title Direct IP access not allowed | Cloudflare

Response Body

[EXPAND](#)

HTTP 2087/TCP

04/29/2024 15:35 UTC

Software

 CloudFlare Load Balancer [↗ GO](#)

[VIEW ALL DATA](#)

[↗ GO](#)

Details

<http://104.18.36.214:2087/>

Status 400 Bad Request

Body Hash sha1:108b6115dc6ebfde76aef4336126f605252d957f

HTML Title 400 The plain HTTP request was sent to HTTPS port

Response Body

[EXPAND](#)

Proof of concept:

HTTP 2095/TCP

05/01/2024 09:44 UTC

Software

CloudFlare Load Balancer ↗

[VIEW ALL DATA](#)

↗ GO

Details

http://104.18.36.214:2095/

Status 403 Forbidden

Body Hash sha1:17903f222f7d99f4c4f6aa6c28af7540be780644

HTML Title Direct IP access not allowed | Cloudflare

Response Body

[EXPAND](#)

HTTP 2096/TCP

05/01/2024 06:04 UTC

Software

CloudFlare Load Balancer ↗

[VIEW ALL DATA](#)

↗ GO

Details

http://104.18.36.214:2096/

Status 400 Bad Request

Body Hash sha1:108b6115dc6ebfde76aef4336126f605252d957f

HTML Title 400 The plain HTTP request was sent to HTTPS port

Response Body

[EXPAND](#)

HTTP 8080/TCP

04/30/2024 10:33 UTC

Software

CloudFlare Load Balancer ↗

[VIEW ALL DATA](#)

↗ GO

Details

http://104.18.36.214:8080/

Status 403 Forbidden

Body Hash sha1:61cc701bfeecb03b93fd778cdc8c73e43be40ae7

HTML Title Direct IP access not allowed | Cloudflare

Response Body

[EXPAND](#)

HTTP 8443/TCP

04/30/2024 19:13 UTC

Software

CloudFlare Load Balancer ↗

[VIEW ALL DATA](#)

↗ GO

Details

http://104.18.36.214:8443/

Status 400 Bad Request

Body Hash sha1:108b6115dc6ebfde76aef4336126f605252d957f

HTML Title 400 The plain HTTP request was sent to HTTPS port

Response Body

[EXPAND](#)

Proof of concept:

HTTP 8880/TCP

05/01/2024 01:11 UTC

Software

CloudFlare Load Balancer 

[VIEW ALL DATA](#)

 GO

Details

<http://104.18.36.214:8880/>

Status 403 Forbidden

Body Hash sha1:0aa70eeb3d8a73b0fd4043178b8d7994475856ed

HTML Title Direct IP access not allowed | Cloudflare

Response Body 

• 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.

• Proof of concept:

```
[root@kali)-[~]# whatweb http://oyorooms.com
http://oyorooms.com [200 OK] Akamai-Global-Host, Country[UNITED STATES][US], HTML5, HTTPServer[AkamaiGHost], IP[23.54.58.31] - Uncommon header 'x-nl' found, with contents: 5
```

- 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.

- Proof of concept:

```
[root@kali:~]# whois oyorooms.com
Domain Name: OYOROOMS.COM
Registry Domain ID: 1818414297_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Updated Date: 2022-09-14T16:18:40Z
Creation Date: 2013-07-29T18:17:31Z +38 (GMT5.5)
Registry Expiry Date: 2024-07-29T18:17:31Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: 480-624-2505
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: A1-173.AKAM.NET
Name Server: A11-64.AKAM.NET
Name Server: A16-65.AKAM.NET
Name Server: A24-66.AKAM.NET
Name Server: A3-67.AKAM.NET
Name Server: A8-64.AKAM.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```

```
>>> Last update of whois database: 2024-05-01T15:10:07Z <<<
+-- nmap -A oyorooms.com
For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and/or
automated except as reasonably necessary to register domain names or to
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
```

- Proof of concept:

```
repackaging, dissemination or other use of this Data is expressly prohibited without the prior written consent of VeriSign. You agree not to use electronic processes that are automated and high-volume to access or query the Whois database except as reasonably necessary to register domain names or modify existing registrations. VeriSign reserves the right to restrict your access to the Whois database in its sole discretion to ensure operational stability. VeriSign may restrict or terminate your access to the Whois database for failure to abide by these terms of use. VeriSign reserves the right to modify these terms at any time.
```

```
+ Server: AkamaiGHost
```

```
The Registry database contains ONLY .COM, .NET, .EDU domains and . See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
```

```
Domain Name: OYOROOMS.COM options header is not set. This could allow the user agent to render the content of the Registry Domain ID: 1818414297_DOMAIN_COM-VRSN. See: https://www.netsparker.com/web-vulnerability-scanner/vuln
```

```
Registrar WHOIS Server: whois.godaddy.com
```

```
Registrar URL: https://www.godaddy.com/rooms/lk
```

```
Updated Date: 2014-10-30T15:10:45Z (n't found, with contents: S.)
```

```
Creation Date: 2013-07-29T13:17:31Z (all' to force check all possible dirs)
```

```
Registrar Registration Expiration Date: 2024-07-29T13:17:31Z host
```

```
Registrar: GoDaddy.com, LLC 15-01 18:24:51 (GMT5.5) (1693 seconds)
```

```
Registrar IANA ID: 146
```

```
Registrar Abuse Contact Email: abuse@godaddy.com
```

```
Registrar Abuse Contact Phone: +1.4806242505
```

```
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
```

```
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
```

```
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
```

```
Registry Registrant ID: Not Available From Registry
```

```
Registrant Name: Registration Private
```

```
Registrant Organization: Domains By Proxy, LLC
```

```
Registrant Street: DomainsByProxy.com
```

```
Registrant Street: 2155 E Warner Rd
```

```
Registrant City: Tempe
```

```
Registrant State/Province: Arizona 15-01 18:24:51 (GMT5.5)
```

```
Registrant Postal Code: 85284
```

```
Registrant Country: US
```

```
Registrant Phone: +1.4806242599
```

```
Registrant Phone Ext: 1800-222-0505 X-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
```

```
Registrant Phone Ext: 1800-222-0505
```

```
Registrant Fax: X-Options header is not set. This could allow the user agent to render the content of the
```

```
Registrant Fax Ext: fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vuln
```

```
Registrant Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=OYORO
```

```
OMS.COM
```

```
Registry Admin ID: Not Available From Registry with contents: S.)
```

```
Admin Name: Registration Private (all' to force check all possible dirs)
```

```
Admin Organization: Domains By Proxy, LLC reported on remote host
```

```
Admin Street: DomainsByProxy.com 15-01 18:24:51 (GMT5.5) (1693 seconds)
```

```
Admin Street: 2155 E Warner Rd
```

```
Admin City: Tempe
```

```
Admin State/Province: Arizona
```

```
Admin Postal Code: 85284
```

```
Admin Country: US
```

- Proof of concept:

```
Admin Phone: +1.4806242599
Admin Phone Ext: rooms.Com
Admin Fax: 0
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=OYOROOMS.COM
Org Target Hostname: oyorooms.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private 17:56:38 (GMT+5.5)
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Frame-Options
Tech City: Tempe
Tech State/Province: Arizona Content-Type header is not set. This could allow the user agent to render the content of the response as plain text. See: https://www.netsparker.com/web-vulnerability-scanner/vuln/no-content-type-header/
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext: http://oyorooms.com/lk
Tech Fax: Uncommon header 'X-n' found, with contents: 5.
Tech Fax Ext: Directories found (use '-c all' to force check all possible dirs)
Tech Fax Ext: 2 error(s) and 3 item(s) reported on remote host
Tech Email: Select Contact Domain Holder link at https://www.godaddy.com/whois/results.aspx?domain=OYOROOMS.COM
Name Server: A1-173.AKAM.NET
Name Server: A11-64.AKAM.NET
Name Server: A16-65.AKAM.NET
Name Server: A24-66.AKAM.NET
```

```
Name Server: A3-67.AKAM.NET
Name Server: A8-64.AKAM.NET
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-05-01T15:10:28Z <<
For more information on Whois status codes, please visit https://icann.org/epp
Last Update Time: 2024-05-01 17:15:38 (GMT+5.5)
TERMS OF USE: The data contained in this registrar's Whois database, while believed by the registrar to be reliable, is provided "as is" with no guarantee or warranties regarding its accuracy. This information is provided for the sole purpose of assisting you in obtaining information about domain name registration records. Any use of this data for any other purpose is expressly forbidden without the prior written permission of this registrar. By submitting an inquiry, you agree to these terms and limitations of warranty. In particular, you agree not to use this data to allow, enable, or otherwise support the dissemination or collection of this data, in part or in its entirety, for any purpose, such as transmission by e-mail, telephone, postal mail, facsimile or other means of mass unsolicited, commercial advertising or solicitations of any kind, including spam. You further agree not to use this data to enable high volume, automated or robotic electronic processes designed to collect or compile this data for any purpose, including mining this data for your own personal or commercial purposes. Failure to comply with these terms may result in termination of access to the Whois database. These terms may be subject to modification at any time without notice.
```

Find WAF (web application firewall) protection.

Wafwoof

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.

Proof of concept:

```
[root@kali) ~]# wafw00f oyorooms.com
+ Target IP: 23.54.58.31
+ Target Hostname: oyorooms.com
+ Target Port: 80
+ Start Time: 2024-05-01 17:56:38 (GMT5.5)
+ Server: AkamaiGHost
+ /: 404 Hack Not Found
+ /: 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 user agent to request content in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerabilities/misconfig-content-type-header/ 405 Not Allowed
+ Root page redirects to: http://oyorooms.com/ 403 Forbidden
+ /wvlyRe3: Uncommon header found. 502 Bad Gateway, 500 Internal Error
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ 7968 requests: 2 error(s) and 3 item(s) reported on remote host
+ End Time: 2024-05-01 17:56:38 (~ WAFW00F: v2.2.0 (~MT5.5) (1693 seconds))

The Web Application Firewall Fingerprinting Toolkit
+ 1 host(s) tested
[*] Checking https://oyorooms.com
[+] The site https://oyorooms.com is behind Kona SiteDefender (Akamai) WAF.
[~] Number of requests: 2
```

Find open ports.

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.

Proof of concept:

```
[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: AkamaiGHosts
|_http-title: Site doesn't have a title (text/html). This could allow the user agent to render the content of the page to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vuln/
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:boltpapi.oyorooms.com, DNS:cis.innov8.work, DNS:crs.oyorooms.com, DNS:crsms.oyorooms.com, DNS:dev-webpoc.oyorooms.com, DNS:e.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
```

Proof of concept:

```
om, DNS:oyovacationhomes.com, DNS:oyoworkspaces.com, DNS:partner-app.oyorooms.com, DNS:partner.oyocircle.com, D  
NS:partner.oyorooms.com, DNS:partners-admin.oyorooms.com, DNS:pay.oyorooms.com, DNS:plugin.oyorooms.com, DNS:pr  
eprod.oyolife.in, DNS:proctor.oyopay.io, DNS:property-insights.oyorooms.com, DNS:refunds.oyorooms.com, DNS:scan  
.oyorooms.com, DNS:scm-api.oyorooms.com, DNS:secure.oyopay.io, DNS:staging.oyoos.com, DNS:staging.weddingz.in,  
DNS:stayyourway.oyorooms.com, DNS:stg-api.weddingz.in, DNS:testbff.oyorooms.com, DNS:vikreta.oyorooms.com, DNS:  
virtualoffice.oyoworkspaces.com, DNS:wakai.oyorooms.com, DNS:weddingz.in, DNS:workflobyoyo.com, DNS:www.innov8.  
work, DNS:www.mobile.oyoliving.com, DNS:www.oyocampus.in, DNS:www.oyocircle.com, DNS:www.oyohotels.cn, DNS:www.  
.oyohotels.com, DNS:www.oyolife.co.id, DNS:www.oyolife.co.in, DNS:www.oyolife.in, DNS:www.oyoliving.com, DNS:www.  
.oyoos.com, DNS:www.oyopay.in, DNS:www.oyopay.io, DNS:www.oyotownhouse.com, DNS:www.oyoworkspaces.com, DNS:www.  
powerstationbyoyo.com, DNS:www.weddingz.in, DNS:www.workflobyoyo.com, DNS:zp-api-pay.oyorooms.com, DNS:zp-hooks  
.oyopay.io, DNS:zp-proctor.oyopay.io, DNS:zp-proxy.oyopay.io, DNS:zp-secure.oyopay.io  
| Not valid before: 2023-10-19T00:00:00  
| Not valid after: 2024-06-25T23:59:59  
| _http-trane-info: Problem with XML parsing of /evox/about  
| _http-server-header: AkamaiGHostheader  
| _ssl-date: TLS randomness does not represent time  
| _http-title: Site doesn't have a title (text/html).contents: S.  
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port  
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete  
No OS matches for host 024-05-01 18:24:51 (GMT5.5) (1693 seconds)  
Network Distance: 1 hop
```

```
TRACEROUTE (using port 80/tcp)er 'x-n' found, with contents: S.  
HOP RTT 1 ADDRESS found (use '-c all' to force check all possible dirs)  
1 ✓ 0.22 ms a23-53-216-81.deploy.static.akamaitechnologies.com (23.53.216.81)  
End Time: 2024-05-01 18:24:51 (GMT5.5) (1693 seconds)  
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
```

Exploitation

- Sqlmap

Web applications with SQL injection vulnerabilities can be automatically found and exploited with SQLMap, an open-source penetration testing tool. It employs a number of detecting methods, supports a number of database management systems, and provides customization choices. Security experts and penetration testers find SQLMap useful as it automates testing, enumeration, data extraction, and reporting procedures during security assessments. It should, therefore, be utilized sensibly, morally, and with the appropriate authorization to test programs and systems.

Proof of concept:

Proof of concept:

```
[00:36:34] [INFO] searching for dynamic contenter is not present. See: https://developer.mozilla.org/en-US/doc
[00:36:34] [INFO] dynamic content marked for removal (1 region)
[00:36:34] [CRITICAL] target URL content appears to be heavily dynamic. sqlmap is going to retry the request(s)
[00:36:34] [INFO] dynamic content marked for removal (2 regions) netsparker.com/web-vulnerability-scanner/vuln
[00:36:34] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.s
ite.com/index.php?id=1') - http://oyorooms.com/lk
[00:36:34] [WARNING] HTTP error codes detected during run: 500, 403 (Forbidden) - 7 times (use '-C all' to force check all possible dirs)
[00:36:34] [WARNING] your sqlmap version is outdated remote host
End Time: 2024-05-01 18:24:51 (GMT5.5) (1693 seconds)
[*] ending @ 00:36:34 /2024-05-02/
1 host(s) tested
```

Vulnerability analysis phase

I used tool like netsparker to process and catch bugs and vulnerabilities are based on OWASP top 10.

Targeted Domain: - <http://oyorooms.com>

- Netsparker

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.

Vulnerability title

Missing X-Frame-Options Header

Netsparker detected a missing X-Frame-Options header on the website, leaving it vulnerable to clickjacking attacks. This header, sent in HTTP responses, controls whether the site's content can be embedded in frames or iframes on other domains. Clickjacking involves tricking users into unintended actions by overlaying deceptive elements on legitimate pages. By correctly implementing the X-Frame-Options header with directives like "DENY" or "SAMEORIGIN," websites can prevent malicious framing and enhance overall security against clickjacking threats.

Impact assessment

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on a framed page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account but are instead typing into an invisible frame controlled by the attacker.

Affected components

The missing X-Frame-Options header affects the security of the entire website, as it leaves all pages vulnerable to potential clickjacking attacks. Clickjacking attacks can target any part of a website that can be displayed within a frame or iframe on another domain. This includes login forms, sensitive data, action buttons, or any interactive elements that users might interact with. Therefore, all components and functionalities of the website that can be manipulated or misused through clickjacking would be affected by the absence of the X-Frame-Options header.

How to mitigate?

To mitigate the risk of clickjacking attacks caused by the missing X-Frame-Options header:

1. **Set X-Frame-Options Header:** Configure your web server to include the X-Frame-Options header in HTTP responses.
2. **Choose Correct Directive:** Decide on the appropriate directive (DENY, SAMEORIGIN, or ALLOW-FROM) based on your security needs.
3. **Implement Header:** Add the X-Frame-Options header to your server's HTTP responses in the server configuration or .htaccess file.
4. **Test Implementation:** Verify the header implementation using security tools or browser developer tools.
5. **Regular Audits:** Conduct periodic security audits to detect and address any new vulnerabilities, including clickjacking risks.

These steps will help prevent unauthorized framing of your website's content and enhance overall security against clickjacking threats.

Proof of concept:

Missing X-Frame-
Options Header

GET http://oyorooms.com/

Vulnerabilities

3.1. http://oyorooms.com/

Certainty

Request

```
GET / HTTP/1.1
Host: oyorooms.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
```



Other vulnerabilities were identified during the scan

- HTTP Strict Transport Security (HSTS) Policy Not Enabled

Proof of concept:

👤 🏟 [HTTP Strict Transport Security \(HSTS\) Policy Not Enabled](#)

GET https://oyorooms.com/

Vulnerabilities

1.1. https://oyorooms.com/

Certainty

Request

```
GET / HTTP/1.1
Host: oyorooms.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
Connection: Keep-Alive
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
```

Proof of concept:

Response

Response Time (ms) : 351.6657 Total Bytes Received : 606 Body Length : 362 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: AkamaiGHost
Content-Length: 362
Expires: Wed, 01 May 2024 16:12:27 GMT
Connection: close
Mime-Version: 1.0
Content-Type: text/html
Date: Wed, 01 May 2024 16:12:27 GMT
Cache-Control: no-store, max-age=0

<HTML><HEAD>
<TITLE>Access Denied</TITLE>
</HEAD><BODY>
<H1>Access Denied</H1>

You don't have permission to access "http://oyorooms.com/" on this server.<P>
Reference#35;18#deac3017#1714579947#95fc229d
<P>https://errors.edgesuite.net/18#deac3017#1714579947#95fc229d</P>
</BODY>
</HTML>
```

Remedy

Configure your webserver to redirect HTTP requests to HTTPS.

i.e. for Apache, you should have modification in the httpd.conf. For more configurations, please refer to External References section.

```
# load module
LoadModule headers_module modules/mod_headers.so

# redirect all HTTP to HTTPS (optional)
<VirtualHost *:80>
    ServerAlias *
    RewriteEngine On
    RewriteRule ^(.*)$ https:// %{HTTP_HOST}$1 [redirect=301]
</VirtualHost>

# HTTPS-Host-Configuration
<VirtualHost *:443>
    # Use HTTP Strict Transport Security to force client to use secure connections only
    Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains"

    # Further Configuration goes here
    [...]
```

4 / 28

```
</VirtualHost>
```

- Weak Ciphers Enabled

Proof of concept:

  [Weak Ciphers Enabled](#) GET <https://oyorooms.com/>

MEDIUM  | 1 CONFIRMED  | 1

Netsparker detected that weak ciphers are enabled during secure communication (SSL).

You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact

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

Vulnerabilities

2.1. <https://oyorooms.com/>

CONFIRMED

List of Supported Weak Ciphers

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)

Request

[NETSPARKER] SSL Connection

Proof of concept:

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:

6 / 28

```
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 `regedit`, and then click OK.
- b.In Registry Editor, locate the following registry key: `HKEY_LOCAL_MACHINE\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
```

Remedy

Configure your web server to disallow using weak ciphers.

- Missing X-XSS-Protection Header

Proof of concept:

		Missing X-XSS-Protection Header	GET	http://oyorooms.com/
--	--	---	-----	----------------------

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.

Vulnerabilities

5.1. http://oyorooms.com/

Certainty



Request

```
GET / HTTP/1.1
Host: oyorooms.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
```

Proof of concept:

Response

Response Time (ms) : 160.227 Total Bytes Received : 606 Body Length : 362 Is Compressed : No

```
HTTP/1.1 403 Forbidden
Server: AkamaiGHost
Content-Length: 362
Expires: Wed, 01 May 2024 16:12:18 GMT
Connection: close
Mime-Version: 1.0
Content-Type: text/html
Date: Wed, 01 May 2024 16:12:18 GMT
Cache-Control: no-store, max-age=0

<HTML><HEAD>
<TITLE>Access Denied</TITLE>
</HEAD><BODY>
<H1>Access Denied</H1>

You don't have permission to access "http&#58;&#47;&#47;oyorooms&#46;com&#47;" on this server.<P>
Reference&#32;&#35;18&#46;deac3017&#46;1714579938&#46;95fafd68
<P>https&#58;&#47;errors&#46;edgesuite&#46;net&#47;18&#46;deac3017&#46;1714579938&#46;95fafd68</P>
</BODY>
</HTML>
```

Remedy

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

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

Conclusion

The security assessment of <http://oyorooms.com> using various tools like Recon-*ng*, nslookup, Dnsrecon, Nikto, and others revealed critical vulnerabilities including Weak Ciphers, Missing X-Frame-Options Header, Missing X-XSS-Protection Header, and absence of HTTP Strict Transport Security (HSTS) Policy. Of these, the missing X-Frame-Options Header poses a significant risk of clickjacking attacks, impacting the entire website's security. Mitigation strategies recommended include configuring appropriate HTTP headers, conducting regular security audits, and promptly addressing identified vulnerabilities. Implementing these measures is crucial to fortify the website's overall security posture and protect against common web application threats.