

**CENTRE FOR DEVELOPMENT OF ADVANCED
COMPUTING (C-DAC),
THIRUVANANTHAPURAM, KERALA**

A PROJECT REPORT ON

“Security and Vulnerability Assessment on Unstop.com”

SUBMITTED TOWARDS THE



PG-DCSF September 2023

BY

Group Number - 05

Atharva Anil Ghodmare

PRN: 230960940007

Danish Mahmood

PRN: 230960940011

Devilal Singh Parihar

PRN: 230960940013

Manish Singh Chowhan

PRN: 230960940025

Sanatan Sameer Bramhane

PRN: 230960940046

Under The Guidance Of

Mr. Jayaram P.

Centre Co- Ordinator

Mr. Jayaram P.

Project Guide

TABLE OF CONTENTS

Contents	Page No.
1. Abstract	1
2. Introduction	2
3. Literature survey.....	3
4. Scope and objective.....	4
5. Methodology	5
6. Passive Reconnaissance	7
7. Active Reconnaissance	22
8. Web Application Pentesting	27
9. Conclusion	47
10. Conclusion	48

Abstract

The objective of our project is to conduct a vulnerability assessment and penetration testing on unstop.com, a web application. This process involves a systematic and comprehensive examination of the organization's information systems, technology infrastructure, processes, and policies to assess the effectiveness of security measures, identify vulnerabilities, and ensure compliance with security best practices and standards.

Our primary goal is to evaluate unstop.com ability to protect its digital assets, sensitive information, and technology resources from cyber threats and attacks. To achieve this, we will perform DNS reconnaissance and mapping of the target application, as well as identify potential vulnerabilities through manual testing following the OWASP Top 10 guidelines.

Additionally, we will utilize more than 8 well-known automated tools, including Nessus, to ensure comprehensive coverage and minimize the risk of overlooking critical vulnerabilities. Throughout the project, we will assess the security posture of unstop.com, identify potential attack vectors, analyze the scope of vulnerabilities, and determine their impact. Based on our findings, we will develop a remediation plan to address the identified security issues effectively.

Moreover, our project will culminate in providing unstop.com with an actionable set of security recommendations to ensure the secure operation of the web application and mitigate potential risks effectively.

INTRODUCTION

In an ever-evolving landscape of technological advancements and digital transformation, ensuring the security and integrity of systems, networks, and data has become paramount. As organizations increasingly rely on digital infrastructure to operate, communicate, and store sensitive information, the potential risks and vulnerabilities also escalate. A proactive approach to identifying, mitigating, and managing these risks is essential to safeguarding an organization's assets, reputation, and stakeholder trust.

This Security Audit Project Report delves into the comprehensive assessment conducted to evaluate the security posture of **Unstop**'s digital ecosystem. The primary objective of this security audit is to systematically examine the effectiveness of existing security measures, policies, and practices, and to recommend improvements that align with industry best practices and regulatory requirements. By performing a thorough analysis of the organization's information technology infrastructure, data handling procedures, and access controls, this audit aims to provide actionable insights for enhancing the organization's overall security framework.

The report is structured to provide a clear understanding of the audit scope, methodology employed, findings uncovered, and subsequent recommendations. Additionally, it underscores the importance of a security-centric mind-set within the organization's culture and emphasizes the significance of continuous monitoring and adaptation to counter the ever-changing threat landscape.

In the subsequent sections, we will explore the key aspects of the security audit, highlighting its significance in the context of modern-day cyber threats and underscoring the collaborative efforts undertaken by the audit team to ensure the confidentiality, integrity, and availability of **Unstop**'s critical assets.

LITERATURE SURVEY

The OWASP Top 10 is a well-known list of the top 10 most critical security risks commonly found in web applications. Including these in your Security Audit Project Report helps to highlight key vulnerabilities that should be addressed. As of my last update in September 2021, here's the OWASP Top 10 list:

OWASP Top 10 Security Risks - 2021

1. Broken Access Control
2. Cryptographic Failures
3. Injection
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failure
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery

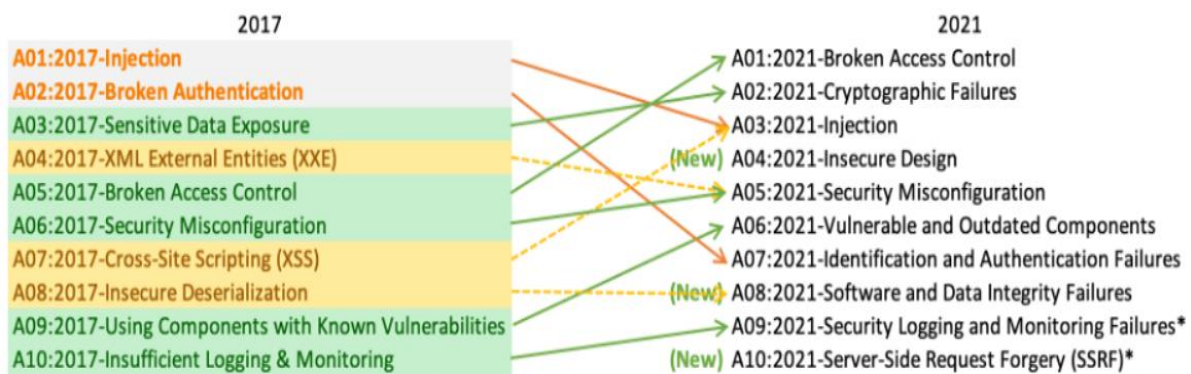


Fig1.1: OWASP Top 10 (2017 Vs 2021)

Reference Link: <https://owasp.org/www-project-top-ten/>

SCOPE AND OBJECTIVES

The scope of the project involves a comprehensive evaluation of its digital infrastructure, applications, and data protection mechanisms. The primary focus will be on identifying vulnerabilities, weaknesses, and potential threats that could compromise the confidentiality, integrity, and availability of resources of the website. The security audit will cover both technical and operational aspects, including the assessment of software, network architecture, user access controls, and adherence to relevant security standards and best practices. The security audit will be done both manually and automatically using latest and legitimate tools available.

The project will also extend to evaluating user authentication mechanisms, encryption practices, and incident response procedures. The audit will primarily concentrate on online security, as the project is done completely online.

The main objective of the project is to identify the vulnerabilities by Conducting a thorough assessment of the website's infrastructure to identify potential security vulnerabilities, such as SQL injection, cross-site scripting (XSS), file upload vulnerabilities, password policy etc. Further we aim to provide actionable recommendations and best practices to address identified vulnerabilities and enhance the overall security posture and reputation of the website, thereby enhancing user trust and safeguarding user data.

METHODOLOGY

The current security systems need to be tested for both substantive and compliance aspects. Compliance testing is done to assess whether controls are being applied according to the documentation offered by the client. It also checks if IT controls follow the compliance levels in accordance with management procedures and policies. In substantive testing, the adequacy of the controls is substantiated by whether they are able to protect the organization from cyber threats. These tests need an in-depth understanding of the different kinds of threats such as unauthorized access to assets including data, unusual interactions with the system, data corruption, inaccuracy in information, etc. Application controls are application-specific controls and have a high impact on individual transactions. These controls ensure and verify that all transactions are authorized, safe, and recorded. To proceed with this phase of the audit, there is a need for a deep understanding of the working of the system. For this analysis, a brief description of the application is required, along with details of transactions including volume, involved data, and flow. Most organizations either use local area networks for their operations. This leads to the risk of access by unauthorized users if not monitored and protected properly. The fundamental requirement of a network is to be accessible by only authorized users. Controls should be implemented to eliminate issues like data corruption, data loss, or interception while being transmitted.

IT Audit standards

The IT audit should comply with internationally accepted security standards. Some of these are mentioned below:

- **ISO Compliance:** The ISO publishes a slew of guidelines that ensure reliability, quality, and safety. ISO 27001 is suitable for information security requirements.
- **PCI DSS Compliance:** These standards apply to any company that is involved with customer payments. This is necessary to ensure that all transactions are secure and protected.

Phases of Security Audit

There are 4 significant phases in a security audit:

1. Planning phase

Preliminary information gathering and assessment

Planning is an integral part of any audit. In the beginning, planning is done to create a process flow based on an initial reconnaissance of the entire system. The plan is updated according to the test results of the initial assessment.

2. Audit scope and objective

From the above steps, the auditor gains relevant information and details to define the objective and scope of the audit in a clear and detailed format. The initial risk assessment forms an important part of the process and answers questions pertaining to three primary security goals, confidentiality, integrity, and reliability.

Risk assessment consists of ranking the potential threats from low to high, or other scientific or complex metrics. The ranking depends on the severity of the issue with respect to the extent of damage it can cause or the ease of exploitation. Vulnerabilities that are easy to exploit and those causing a high degree of damage must be ranked comparatively higher.

3. Evaluating collected evidence

Through rigorous testing and prodding of the security infrastructure, various types of evidence are gathered that must be interpreted to compile the results of the audit. There are various techniques to test a system and obtain results. Evidence can be majorly 3 types:

- Documentary evidence
- System analysis
- Observation of processes

4. Documenting audit results

Proper documentation of the results forms an integral part of security audit methodology. The final report should be in a very consumable format for stakeholders at all levels to understand and interpret. It must contain details such as the audit plan, audit scope, tests carried out, findings and detailed solutions, and next steps to remedy the security issues.

Reconnaissance

Reconnaissance is the information-gathering stage of ethical hacking, where you collect data about the target system. This data can include anything from network infrastructure to employee contact details. The goal of reconnaissance is to identify as many potential attack vectors as possible.

How Reconnaissance Works

Reconnaissance generally follows seven steps:

1. Collect initial information
2. Determine the network range
3. Identify active machines
4. Find access points and open ports
5. Fingerprint the operating system
6. Discover services on ports
7. Map the network

PASSIVE RECONNAISSANCE:

Passive reconnaissance involves collecting information about a target without directly interacting with it, typically through publicly available sources. This information can include domain names, IP addresses, email addresses, employee names, and other details that can be useful for conducting further attacks or assessments.

Passive reconnaissance techniques can include:

- Open Source Intelligence (OSINT): Gathering information from publicly available sources such as websites, social media, news articles, and government records.
- DNS Enumeration: Collecting information about a target's domain names and associated IP addresses through DNS queries.
- Network Mapping: Identifying hosts, services, and network infrastructure using tools like Nmap or Shodan.
- Social Engineering: Extracting information through interactions with individuals associated with the target organization, such as employees or vendors, without directly revealing malicious intent.
- Traffic Analysis: Observing network traffic to gather information about communication patterns, network architecture, and potentially sensitive information transmitted in plaintext.
- Dumpster Diving: Physically searching through an organization's trash or recycling bins to find documents or electronic devices containing sensitive information.

➤ Following are the tools which we used to perform reconnaissance on website “Unstop.com”

1) Netcraft

Netcraft can be a useful tool in the context of penetration testing (pentesting) for several reasons:

- **Discovering Technology Stack:** Netcraft's Web Server Survey can help pentesters identify the technology stack used by a target organization. Understanding the web server, operating system, and other components in use can provide valuable insight into potential vulnerabilities and attack vectors.
- **Identifying Phishing Sites:** Pentesters can use Netcraft's anti-phishing services to identify phishing sites that mimic the target organization's web presence. This can help assess the potential impact of phishing attacks and evaluate the effectiveness of the organization's anti-phishing measures.
- **Checking SSL Certificates:** Netcraft offers tools to check SSL certificates, which can be valuable for identifying misconfigurations or weaknesses in SSL/TLS implementations. Pentesters can use this information to assess the security of encrypted connections to the target organization's web servers.
- **Monitoring for Malicious Activity:** Netcraft monitors the internet for malware, phishing, and other malicious activity. Pentesters can leverage this data to identify potential threats targeting the target organization or its customers, helping to prioritize security assessments and response efforts.
- **Analyzing Hosting Providers:** Pentesters can use Netcraft's analysis of hosting providers to assess the security posture of third-party services used by the target organization. This can include evaluating the reliability, performance, and security practices of hosting providers to identify potential risks or vulnerabilities.
- **Research and Reports:** Netcraft publishes research reports and analysis on internet security trends, vulnerabilities, and emerging threats. Pentesters can leverage this information to stay informed about the latest security issues and adapt their testing strategies accordingly.

[LEARN MORE](#)[REPORT FRAUD](#)

Site report for https://unstop.com






► 🔍 Look up another site?

Share:

Background

Site title	Unstop - Competitions, Quizzes, Hackathons, Scholarships and Internships for Students and Corporates	Date first seen	June 2022
Site rank	9267	Primary language	English
Description	Explore student/corporate competitions & engagements for B-schools, Engineering & Graduate colleges. We are an employer branding consultant & help conceptualize & organize these engagements Unstop - India		

Network

Site	https://unstop.com 
Netblock Owner	Amazon.com, Inc.
Hosting company	Amazon
Hosting country	 US 
IPv4 address	3.162.140.119 (VirusTotal )
IPv4 autonomous systems	AS16509 
IPv6 address	Not Present
IPv6 autonomous systems	Not Present
Reverse DNS	server-3-162-140-119.dub56.r.cloudfront.net

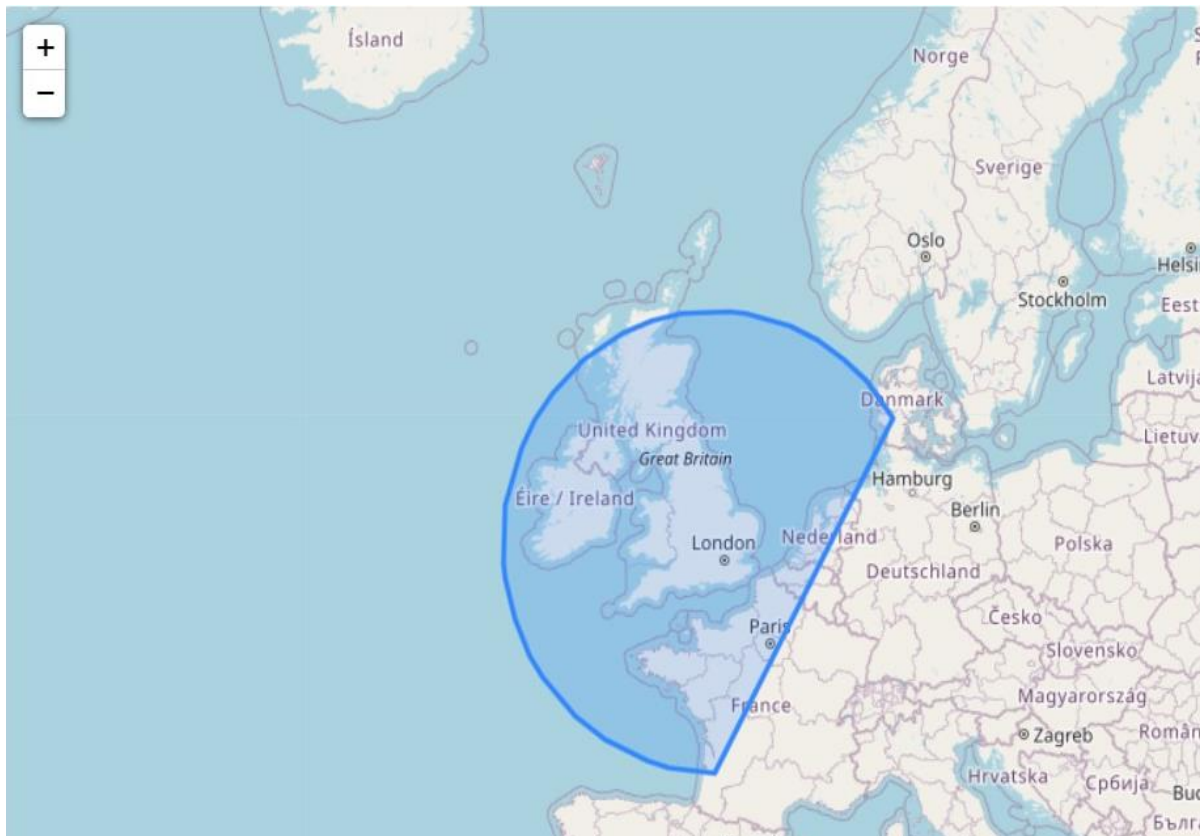
Domain	unstop.com
Nameserver	ns-1881.awsdns-43.co.uk
Domain registrar	amazon.com
Nameserver organisation	whois.nic.uk
Organisation	Identity Protection Service, PO Box 786, Hayes, UB3 9TR, United Kingdom
DNS admin	awsdns-hostmaster@amazon.com
Top Level Domain	Commercial entities (.com)
DNS Security Extensions	Unknown

IP delegation

IPv4 address (3.162.140.119)

IP range	Country	Name
::ffff:0.0.0.0/96	 United States	IANA-IPV4-MAPPED-ADDRESS
 3.0.0.0-3.255.255.255	 United States	NET3
 3.128.0.0-3.255.255.255	 United States	AT-88-Z
 3.160.0.0-3.163.255.255	 United States	AMAZON-CF
 3.162.140.119	 United States	AMAZON-CF


IP Geolocation :



SSL/TLS :

SSL (Secure Sockets Layer) and its successor TLS (Transport Layer Security) are cryptographic protocols crucial for establishing secure and encrypted connections between clients and servers over the internet. These protocols ensure that data exchanged remains confidential, safeguarding sensitive information like passwords and credit card numbers from interception. SSL/TLS encrypts data, verifies server identity to prevent man-in-the-middle attacks, and ensures data integrity, protecting against tampering during transmission. Widely used in various online applications, SSL/TLS plays a fundamental role in securing transactions, preserving user privacy, and maintaining the integrity and authenticity of data transmitted over the internet.

SSL/TLS

Assurance	Domain validation
Common name	unstop.com
Organisation	Not Present
State	Not Present
Country	Not Present
Organisational unit	Not Present
Subject Alternative Name	unstop.com , *.unstop.com
Validity period	From Mar 24 2023 to Apr 22 2024 (12 months, 4 weeks, 1 day)
Matches hostname	Yes
Server	nginx
Public key algorithm	rsaEncryption
Protocol version	TLSv1.3
Perfect Forward Secrecy	Yes
Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC7301 application-layer protocol negotiation
Application-Layer Protocol Negotiation	h2
Next Protocol Negotiation	Not Present
Issuing organisation	Amazon
Issuer common name	Amazon RSA 2048 M02
Issuer unit	Not Present
Issuer location	Not Present
Issuer country	 US
Issuer state	Not Present
Certificate Revocation Lists	http://crl.r2m02.amazontrust.com/r2m02.crl
Certificate Hash	W+TOY9H6oEj9PcYWYPhFpFBXnyM
Public Key Hash	413bd4eb3d50f1ef819e7a1bdc4d90ac4252ee75db6816e9faa74118561bc7d5

2) Shodan :

Shodan is a powerful search engine that allows users to find internet-connected devices and systems, providing insights into the global network landscape. It enables users to search for specific types of devices, such as webcams, routers, servers, and industrial control systems, by querying metadata and banners. Shodan's capabilities extend beyond simple search, offering tools for analyzing network vulnerabilities, identifying misconfigured devices, and assessing the security posture of internet-connected assets. It is widely used by security professionals, researchers, and hackers to gather intelligence, identify potential targets, and assess the security risks associated with exposed devices and systems on the internet.

The screenshot displays the Shodan search interface for the IP address 3.162.140.58. At the top, a map shows the location of the IP in Dublin, Ireland. Below the map, the IP address is prominently displayed. The interface is divided into two main sections: 'General Information' on the left and 'Open Ports' on the right. The 'General Information' section lists various details about the IP, including its hostnames, domains, cloud provider, region, service, country, city, organization, and ISP. The 'Open Ports' section shows the open ports (80 and 443) and the corresponding TCP connections. The 'CloudFront http' section provides a detailed view of the HTTP response, including the status code (403 Forbidden), server information, date, content type, and various headers.

General Information	
Hostnames	server-3-162-140-58.dub56.r.cloudfront.net
Domains	CLOUDFRONT.NET
Cloud Provider	Amazon
Cloud Region	GLOBAL
Cloud Service	CLOUDFRONT
Country	Ireland
City	Dublin
Organization	Amazon.com, Inc.
ISP	Amazon.com, Inc.

Open Ports	
80	443

// 80 / TCP 1748579541 | 2024-02-15T11:37:43.168392

CloudFront httpd

HTTP/1.1 403 Forbidden
Server: CloudFront
Date: Thu, 15 Feb 2024 11:37:42 GMT
Content-Type: text/html
Content-Length: 915
Connection: keep-alive
X-Cache: Error from cloudfront
Via: 1.1 eu9b4db61765a75b18918cece9b2.cloudfront.net (CloudFront)
X-Amz-CF-Pop: DUB56-P2
X-Amz-CF-Id: Aqzu-csPtpc4UjJlsc91lmsIwS81skttabgu6Kk8Z0VgDW5Q==

// 443 / TCP 1285968913 | 2024-02-15T11:43:15.791170

3) Censys

Censys is a comprehensive internet scanning platform that provides users with detailed insights into the composition and security of the global internet infrastructure. It continuously scans the internet, collecting data on various devices, services, and protocols, including websites, servers, IoT devices, and more. Users can search Censys' vast database to discover specific devices or networks, analyze their configurations, and assess their security posture. Censys is widely utilized by security professionals, researchers, and organizations for identifying vulnerabilities, monitoring their digital footprint, and proactively addressing potential security risks across their internet-connected assets.

[Register](#)
[Log In](#)

HTTP 80/TCP

02/15/2024 07:24 UTC

Software
 Amazon CloudFront Load Balancer

Details
<http://3.162.140.58/>

Status	403 Forbidden
Body Hash	sha1:fbfcb45e3454be3d6bc53048deab622fe0650a24
HTML Title	ERROR: The request could not be satisfied
Response Body	<input type="button" value="EXPAND"/>

Geographic Location

City	Dublin
Province	Leinster
Country	Ireland (IE)
Coordinates	53.33306, -6.24889
Timezone	Europe/Dublin

HTTP 443/TCP

02/15/2024 15:37 UTC

Software
 Amazon CloudFront Load Balancer

Details
<http://3.162.140.58:443/>

Status	400 Bad Request
Body Hash	sha1:4a85640d3cf228764a58e7c91562185f9bbc8588
HTML Title	ERROR: The request could not be satisfied
Response Body	<input type="button" value="EXPAND"/>

4) DNSdumpster

DNSDumpster is a web-based tool used for gathering information about a domain's DNS infrastructure. It provides insights into a domain's DNS records, including hostnames, IP addresses, mail servers (MX records), name servers (NS records), TXT records (for SPF, DKIM, and other purposes), and more. Users can input a domain name into DNSDumpster's interface, and it generates a detailed report, which can help with reconnaissance, identifying potential vulnerabilities, and understanding an organization's online presence. DNSDumpster is commonly used by security professionals, penetration testers, and researchers to gather intelligence about domains and perform footprinting during security assessments.



DNS Servers

ns-1469.awsdns-55.org. 🌐 🚫 🛡️ 🌱	205.251.197.189	AMAZON-02 United States
ns-1881.awsdns-43.co.uk. 🌐 🚫 🛡️ 🌱	205.251.199.89	AMAZON-02 United States
ns-249.awsdns-31.com. 🌐 🚫 🛡️ 🌱	205.251.192.249	AMAZON-02 United States
ns-716.awsdns-25.net. 🌐 🚫 🛡️ 🌱	205.251.194.204	AMAZON-02 United States

MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com. 🌐 🚫 🛡️ 🌱	172.253.115.27	GOOGLE United States
10 alt3.aspmx.l.google.com. 🌐 🚫 🛡️ 🌱	142.250.27.27	GOOGLE United States
10 alt4.aspmx.l.google.com. 🌐 🚫 🛡️ 🌱	142.250.153.27	GOOGLE United States
5 alt1.aspmx.l.google.com. 🌐 🚫 🛡️ 🌱	209.85.202.27	GOOGLE United States
5 alt2.aspmx.l.google.com. 🌐 🚫 🛡️ 🌱	64.233.184.27	GOOGLE United States

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

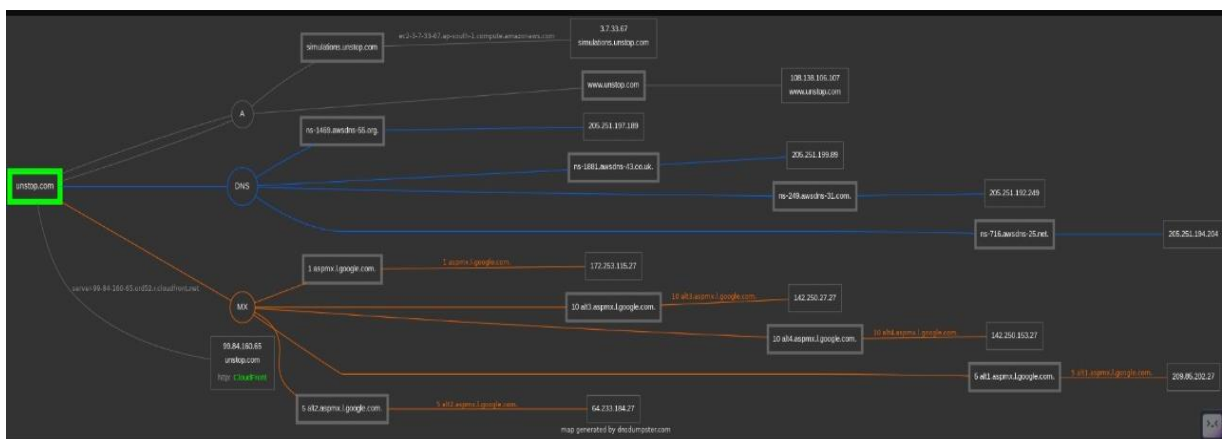
"MS=ms63587331"

"google-site-verification=hhPHoACOXAEkyle3Xn7K975C0sT7RPjAULclmfHLE28"

"v=spf1 include:_spf.google.com include:amazonses.com"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

unstop.com 🌐 🚫 🛡️ 🌱 HTTP: CloudFront	99.84.160.65 server-99-84-160-65.ord52.r.cloudfront.net	AMAZON-02 United States
simulations.unstop.com 🌐 🚫 🛡️ 🌱	3.7.33.67 ec2-3-7-33-67.ap-south-1.compute.amazonaws.com	AMAZON-02 India
www.unstop.com 🌐 🚫 🛡️ 🌱	108.138.106.107 server-108-138-106-107.jfk50.r.cloudfront.net	AMAZON-02 United States



5) Security Trails :

SecurityTrails is a cybersecurity platform that provides comprehensive intelligence about domain and IP address history, DNS data, and other digital footprints. It offers detailed information on domain ownership, historical DNS records, SSL certificates, WHOIS data, subdomains, and associated IP addresses. SecurityTrails enables users to track changes to a domain's infrastructure over time, identify potential security issues, investigate cyber threats, and monitor their digital assets for unauthorized changes or vulnerabilities. It is widely utilized by security professionals, threat hunters, incident responders, and organizations to enhance their cybersecurity posture and protect against online threats.

unstop.com DNS records as of Feb 15, 2024		
A records		
Amazon.com, Inc.		
99.84.191.10		0
99.84.191.100		0
99.84.191.52		0
99.84.191.56		0

MX records		
Google LLC		
1	aspmx.l.google.com	0
10	alt4.aspmx.l.google.com	0
10	alt3.aspmx.l.google.com	0
5	alt2.aspmx.l.google.com	0
5	alt1.aspmx.l.google.com	0

NS records

Amazon.com, Inc.

ns-716.awsdns-25.net

0

ns-249.awsdns-31.com

0

ns-1881.awsdns-43.co.uk

0

ns-1469.awsdns-55.org

0

SOA records

ttl: 7200

email: awsdns-hostmaster.amazon.com

0

TXT

v=spf1 include:_spf.google.com include:amazonses.com

google-site-verification=hhPHoACOXAEkylE3Xn7K975C0sT7RPjAUlclmfHLE28

Show more ▼

CNAME records pointed here

www.unstop.in

6) CiscoTalos










Cisco Talos is a threat intelligence organization and research group within Cisco Systems that focuses on identifying and analyzing cybersecurity threats worldwide. They provide security solutions and research to help protect organizations against a wide range of cyber threats, including malware, phishing attacks, and vulnerabilities. Cisco Talos offers threat intelligence feeds, real-time updates on emerging threats, and comprehensive research reports to help security professionals stay ahead of evolving threats and effectively mitigate risks. Their expertise and resources are utilized by security teams, incident responders, and organizations across various industries to enhance their cybersecurity defenses and resilience against cyber attacks.

```
Domain Name: unstop.com
Registry Domain ID: 1554421739_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon.com
Registrar URL: https://registrar.amazon.com
Updated Date: 2022-12-04T21:13:12Z
Creation Date: 2009-05-04T18:07:25Z
Registrar Registration Expiration Date: 2032-05-04T18:07:25Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: abuse@amazonaws.com
Registrar Abuse Contact Phone: +1.2067406200
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: On behalf of unstop.com owner
Registrant Organization: Identity Protection Service
Registrant Street: PO Box 786
Registrant City: Hayes
Registrant State/Province: Middlesex
Registrant Postal Code: UB3 9TR
Registrant Country: GB
Registrant Phone: +44.1483307527
Registrant Phone Ext:
Registrant Fax: +44.1483304031
Registrant Fax Ext:
Registrant Email: 2d67f52c-0ccf-44d4-908a-5cd46f20f940@identity-protect.org
Registry Admin ID: Not Available From Registry
Admin Name: On behalf of unstop.com owner
Admin Organization: Identity Protection Service
Admin Street: PO Box 786
Admin City: Hayes
Admin State/Province: Middlesex
Admin Postal Code: UB3 9TR
```










7) IPlocation.net

IPlocation.net is a web-based tool that provides geolocation information for a given IP address. Users can input an IP address into the tool's interface, and it generates a report detailing the approximate geographic location of the IP address, including country, region, city, latitude, longitude, and timezone. IPlocation.net also offers additional information such as the ISP (Internet Service Provider), organization, and ASN (Autonomous System Number) associated with the IP address. This tool is commonly used for geofencing, tracking website visitors, analyzing network traffic, and investigating potential security threats based on IP addresses.










Geolocation data from IP2Location (Product: DB6, 2024-2-1)

 IP ADDRESS: 3.162.140.58	 ISP: Amazon.com Inc.
 COUNTRY: Ireland 	 ORGANIZATION: Not available
 REGION: Dublin	 LATITUDE: 53.3442
 CITY: Dublin	 LONGITUDE: -6.2672

Geolocation data from ipinfo.io (Product: API, real-time)



 IP ADDRESS: 3.162.140.58	 ISP: Not available
 COUNTRY: Ireland 	 ORGANIZATION: AS16509 Amazon.com, Inc.
 REGION: Leinster	 LATITUDE: 53.3331
 CITY: Dublin	 LONGITUDE: -6.2489

Geolocation data from DB-IP (Product: API, real-time)

 IP ADDRESS: 3.162.140.58	 ISP: Amazon.com, Inc.
 COUNTRY: Ireland 	 ORGANIZATION: Amazon Technologies Inc.
 REGION: Leinster	 LATITUDE: 53.3498
 CITY: Dublin	 LONGITUDE: -6.26031

8) OSINT (Hunter) :

Hunter is a web-based tool and API designed for discovering email addresses associated with a given domain or individual. It allows users to input a domain name or the name of a person along with their company's domain, and it provides a list of email addresses associated with that domain or individual. Hunter leverages various sources to gather this information, including publicly available data, domain name system (DNS) records, and other online sources. It is commonly used by sales professionals, marketers, recruiters, and security experts to find contact information for leads, potential candidates, or security contacts within organizations.


<input type="checkbox"/>	Himanshu Sadhwani	 himanshu@dare2compe...  himanshu@unstop.com	Senior Program Manager	<input type="button" value="unstop"/>
<input type="checkbox"/>	Yashvi Das	 yashvi@unstop.com	D2C Chief Igniter	<input type="button" value="unstop"/>
<input type="checkbox"/>	Srishti Kataria	 srishti.kataria@dare2co...  srishti@unstop.com	Operations Manager	<input type="button" value="unstop"/>


<input type="checkbox"/>	Shivam Bandeja	<div>● shivamb@dare2compet...</div> <div>● shivam@unstop.com</div>	Head - Sales and Strategy	unstop
<input type="checkbox"/>	Naman Jain	<div>● namanj@dare2compete....</div> <div>● naman@unstop.com</div>	Product Manager	unstop
<input type="checkbox"/>	Mayank Gupta	<div>● mayank@dare2compete...</div>	D2C Lead Igniter	unstop
<input type="checkbox"/>	Mayur Nanda	<div>● mayur@unstop.com</div>	Lead igniter	unstop
<input type="checkbox"/>	Harshit Mittal	<div>● harshit@unstop.com</div>	Business Strategy Intern	unstop
<input type="checkbox"/>	Ankit Aggarwal	<div>● ankit@unstop.com</div>	Founder & CEO	unstop

9) WHOis :

WHOIS is a protocol and web-based tool used to query databases that store registration information about internet resources such as domain names, IP addresses, and autonomous system numbers (ASNs). By inputting a domain name, IP address, or other identifier, WHOIS provides detailed information about the registrant, registrar, registration and expiration dates, name servers, and contact information associated with the internet resource. WHOIS data is commonly used by domain administrators, registrars, law enforcement agencies, cybersecurity professionals, and researchers to investigate domain ownership, identify network issues, and enforce internet policies and regulations.

Registrar Info	
Name	Amazon Registrar, Inc.
Whois Server	whois.registrar.amazon.com
Referral URL	https://registrar.amazon.com
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited clientTransferProhibited https://icann.org/epp#clientTransferProhibited clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Important Dates	
Expires On	2032-05-04
Registered On	2009-05-04
Updated On	2022-12-04
Name Servers	
NS-1469.AWSDNS-55.ORG	205.251.197.189
NS-1881.AWSDNS-43.CO.UK	205.251.199.89
NS-249.AWSDNS-31.COM	205.251.192.249
NS-716.AWSDNS-25.NET	205.251.194.204




[Premium Domains](#)
[Transfer](#)
[Features](#)

Registrar Data

We will display stored WHOIS data for up to 30 days.

[Make Private Now](#)

Registrant Contact Information:	
Name	On behalf of unstop.com owner
Organization	Identity Protection Service
Address	PO Box 786
City	Hayes
State / Province	Middlesex
Postal Code	UB3 9TR
Country	GB
Phone	+44.1483307527
Fax	+44.1483304031
Email	2d67f52c-0ccf-44d4-908a-5cd46f20f940@identity-protect.org
Administrative Contact Information:	
Name	On behalf of unstop.com owner
Organization	Identity Protection Service
Address	PO Box 786
City	Hayes
State / Province	Middlesex
Postal Code	UB3 9TR
Country	GB
Phone	+44.1483307527
Fax	+44.1483304031
Email	2d67f52c-0ccf-44d4-908a-5cd46f20f940@identity-protect.org
Technical Contact Information:	
Name	On behalf of unstop.com owner
Organization	Identity Protection Service
Address	PO Box 786
City	Hayes
State / Province	Middlesex
Postal Code	UB3 9TR

10) ASNlookup :

ASNlookup is a web-based tool used to query and gather information about Autonomous System Numbers (ASNs). ASNs are unique identifiers assigned to networks and organizations that control blocks of IP addresses. With ASNlookup, users can input an IP address or domain name, and the tool provides details about the ASN associated with that IP address or domain. This includes information such as the ASN owner, registration details, and the prefixes of IP addresses allocated to that ASN. ASNlookup is commonly used by network administrators, cybersecurity professionals, and researchers to understand internet routing, identify network owners, and analyze IP address allocations.

AMAZON-02				
AS Handle	AS16509			
ASN Name	AMAZON-02			
Organization Name	AMAZON-02			
Organization ID	AMAZON-4-ARIN			
Country	🇺🇸 United States of America			
Regional Registry	ARIN			
IPv4 CIDRs	<ul style="list-style-type: none"> 1.44.96.0/24 3.0.0.0/15 3.2.48.0/22 3.5.32.0/22 3.5.72.0/23 3.5.160.0/21 3.5.212.0/23 3.5.224.0/23 3.5.240.0/20 3.24.0.0/14 3.33.43.0/24 3.36.0.0/14 3.104.0.0/13 3.144.0.0/13 2.57.12.0/24 3.2.0.0/24 3.3.6.0/23 3.5.40.0/21 3.5.76.0/22 3.5.168.0/23 3.5.216.0/22 3.5.226.0/24 3.6.0.0/15 3.28.0.0/15 3.33.44.0/22 3.64.0.0/12 3.112.0.0/14 3.160.0.0/19 2.59.57.0/24 3.2.2.0/23 3.3.8.0/21 3.5.48.0/21 3.5.80.0/21 3.5.172.0/22 3.5.220.0/23 3.5.228.0/22 3.8.0.0/13 3.33.35.0/24 3.33.128.0/17 3.96.0.0/14 3.120.0.0/13 3.160.47.0/24 2.255.190.0/23 3.2.8.0/21 3.3.16.0/20 3.5.64.0/21 3.5.128.0/19 3.5.208.0/22 3.5.222.0/24 3.5.232.0/21 3.16.0.0/13 3.33.40.0/23 3.34.0.0/15 3.101.0.0/16 3.128.0.0/12 3.160.63.0/24 			

ACTIVE RECONNAISSANCE:

Active reconnaissance refers to the proactive and deliberate probing of a target network or system by an attacker to gather information and identify potential vulnerabilities. Unlike passive reconnaissance, which involves gathering publicly available data without directly interacting with the target, active reconnaissance involves direct engagement, such as port scanning, network probing, and enumeration techniques, to map out the network architecture, identify active hosts, services, and potential entry points for exploitation. This phase is crucial for attackers to gain insights into the target environment, assess its security posture, and plan subsequent stages of an attack, ultimately aiming to breach the system's defenses and achieve their malicious objectives.

Nmap:

Nmap, short for Network Mapper, is a powerful open-source tool used for network discovery and security auditing. It operates by sending packets to target hosts and analyzing their responses to provide detailed information about the network, including host availability, open ports, running services, operating system details, and network topology. With its flexible and extensible architecture, Nmap supports various scanning techniques such as TCP SYN scan, UDP scan, and comprehensive OS detection. It is widely utilized by security professionals, system administrators, and ethical hackers for vulnerability assessment, penetration testing, and network monitoring tasks, providing valuable insights into the security posture of a network and aiding in the mitigation of potential threats.

```
(root@kali)~[/home/kali/Desktop]
# nmap -p- -sV -O --reason 3.162.140.58
Starting Nmap 7.94 ( https://nmap.org ) at 2024-02-16 00:57 EST
Nmap scan report for server-3-162-140-58.dub56.r.cloudfront.net (3.162.140.58)
Host is up, received reset ttl 128 (0.0074s latency).
Not shown: 65530 filtered tcp ports (no-response)
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  tcpwrapped  syn-ack ttl 128
80/tcp    open  tcpwrapped  syn-ack ttl 128
443/tcp   open  tcpwrapped  syn-ack ttl 128
554/tcp   open  tcpwrapped  syn-ack ttl 128
1723/tcp  open  tcpwrapped  syn-ack ttl 128
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (97%), DD-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP
evice (97%), Linux 3.2 (94%), Linux 4.4 (94%), Microsoft Windows XP SP3 (94%), BlueArc Titan 2100 NAS device (91%)
No exact OS matches for host (test conditions non-ideal).

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 359.83 seconds
```

Result:

The Nmap tool has been used to conduct a network scan on the domain "unstop.com" while enabling OS detection (-O flag). Nmap is a versatile network scanning tool that aids in discovering open ports, services, and potentially the operating system of target hosts.

During the scan, Nmap sends various network packets to the target host and analyzes the responses to infer information about the underlying operating system. This is achieved by examining unique characteristics of the network stack implementation and behavior of the target system.

The output of the scan will include a list of open ports and services detected on the target host. Additionally, Nmap's OS detection mechanism will attempt to provide an educated guess about the operating system running on the host. This information is based on patterns in the responses received from the target system.


Please note that OS detection is not always 100% accurate, as it relies on heuristics and patterns that might be masked or altered by various factors. However, Nmap's OS detection feature can still provide valuable insights into the likely operating system running on the scanned host.

In summary, the Nmap scan with OS detection on the domain "unstop" aims to identify open ports, services, and potentially the underlying operating system of the target host. The results will aid in understanding the network infrastructure and the technology stack in use, contributing to security assessments and network management activities.

Nessus:

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools. In fact, Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. Nessus is a tool that checks computers to find vulnerabilities that hackers could exploit.

Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack.



Report generated by Nessus™

unstop

Sun, 11 Feb 2024 14:49:43 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- unstop.com

Vulnerabilities by Host

Collapse All

Expand All

unstop.com

0	0	1	0	5
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Sun Feb 11 14:28:48 2024
End time: Sun Feb 11 14:46:56 2024

Host Information

DNS Name: unstop.com
IP: 54.182.0.61
OS: Ubuntu 16.04 Linux Kernel 4.4

Vulnerabilities

142960 - HSTS Missing From HTTPS Server (RFC 6797)

Synopsis

The remote web server is not enforcing HSTS, as defined by RFC 6797.

Description

The remote web server is not enforcing HSTS, as defined by RFC 6797. HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

Solution

Configure the remote web server to use HSTS.

Risk Factor

Medium

CVSS v3.0 Base Score

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

CVSS v2.0 Base Score

5.8 (CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N)

Plugin Information

Published: 2020/11/17, Modified: 2024/01/15

Plugin Output

tcp/443/http_proxy

The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/http_proxy

```
The remote web server type is :  
CloudFront
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2019/11/22

Plugin Output

tcp/80/http_proxy

Response Code : HTTP/1.1 301 Moved Permanently

Protocol version : HTTP/1.1

SSL : no

Keep-Alive : no

Options allowed : (Not implemented)

Headers :

Server: CloudFront

Date: Sun, 11 Feb 2024 09:02:10 GMT

Content-Type: text/html

Content-Length: 167

Connection: keep-alive

Location: https://unstop.com/

X-Cache: Redirect from cloudfront

Via: 1.1 c7983ba65d8ecd40bb8af63a608b71f2.cloudfront.net (CloudFront)

X-Amz-Cf-Pop: BOM52-C1

X-Amz-Cf-Id: yt79HlzWdrVXXXvYgkYORR-GRHC5nbt5w4eUiQV8DDSAhDmbimBHUA==

Response Body :

```
<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>CloudFront</center>
</body>
</html>
```

Web Application Pentesting

OWASP ZAP:

OWASP ZAP (short for Zed Attack Proxy) is an open-source web application security scanner. It is intended to be used by both those new to application security as well as professional penetration testers.

It has been one of the most active Open Web Application Security Project (OWASP) projects and has been given Flagship status.

When used as a proxy server it allows the user to manipulate all of the traffic that passes through it, including traffic using HTTPS.

It can also run in a daemon mode which is then controlled via a REST API.

Features :

- An intercepting proxy server,
- Traditional and AJAX Web crawlers
- An automated scanner
- A passive scanner
- Forced browsing
- A fuzzer
- WebSocket support
- Scripting languages

Report:

1. Content Security Policy (CSP) Header Not Set

Source raised by a passive scanner ([Content Security Policy \(CSP\) Header Not Set](#))

CWE ID [693](#)

WASC ID 15

- Reference**
1. https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
 2. https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
 3. <https://www.w3.org/TR/CSP/>
 4. <https://w3c.github.io/webappsec-csp/>
 5. <https://web.dev/articles/csp>
 6. <https://caniuse.com/#feat=contentsecuritypolicy>
 7. <https://content-security-policy.com/>

2. Hidden File Found

Source raised by an active scanner ([Hidden File Finder](#))

CWE ID [538](#)

WASC ID 13

- Reference**
1. <https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html>

3. Missing Anti-clickjacking Header

Source raised by a passive scanner ([Anti-clickjacking Header](#))

CWE ID [1021](#)

WASC ID 15

- Reference**
1. <https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options>

Tool: pentest-tools

Findings:

Insecure cookie setting: missing Secure flag

CONFIRMED

URL	Cookie Name	Evidence
https://unstop.com	country	Set-Cookie: country=GB; path=/

▼ Details

Risk description:

Since the **Secure** flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

Recommendation:

Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.

References:

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html

Classification:

CWE : [CWE-614](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Insecure cookie setting: missing HttpOnly flag

CONFIRMED

URL	Cookie Name	Evidence
https://unstop.com	country	The server responded with Set-Cookie header(s) that does not specify the HttpOnly flag: Set-Cookie: country=GB

▼ Details

Risk description:

A cookie has been set without the **HttpOnly** flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site. In case of a session cookie, this could lead to session hijacking.

Recommendation:

Ensure that the HttpOnly flag is set for all cookies.

References:

<https://owasp.org/www-community/HttpOnly>

Classification:

CWE : [CWE-1004](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Robots.txt file found

CONFIRMED

URL
https://unstop.com/robots.txt

▼ Details

Risk description:

There is no particular security risk in having a robots.txt file. However, this file is often misused by website administrators to try to hide some web pages from the users. This should not be considered a security measure because these URLs can be easily read directly from the robots.txt file.

Recommendation:

We recommend you to manually review the entries from robots.txt and remove the ones which lead to sensitive locations in the website (ex. administration panels, configuration files, etc).

References:

<https://www.theregister.co.uk/2015/05/19/robotstxt/>

Classification:

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Missing security header: X-Content-Type-Options

CONFIRMED

URL	Evidence
https://unstop.com	Response headers do not include the X-Content-Type-Options HTTP security header

▼ Details

Risk description:

The HTTP header `X-Content-Type-Options` is addressed to the Internet Explorer browser and prevents it from reinterpreting the content of a web page (MIME-sniffing) and thus overriding the value of the Content-Type header). Lack of this header could lead to attacks such as Cross-Site Scripting or phishing.

Recommendation:

We recommend setting the X-Content-Type-Options header such as `X-Content-Type-Options: nosniff`.

References:

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options>

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Missing security header: X-Frame-Options

CONFIRMED

URL	Evidence
https://unstop.com	Response headers do not include the HTTP X-Frame-Options security header

▼ Details

Risk description:

Because the **X-Frame-Options** header is not sent by the server, an attacker could embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user consent (ex: delete user, subscribe to newsletter, etc). This is called a Clickjacking attack and it is described in detail here:

<https://owasp.org/www-community/attacks/Clickjacking>

Recommendation:

We recommend you to add the **X-Frame-Options** HTTP header with the values **DENY** or **SAMEORIGIN** to every page that you want to be protected against Clickjacking attacks.

References:

https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html

Classification:

CWE : [CWE-693](#)

OWASP Top 10 - 2013 : [A5 - Security Misconfiguration](#)

OWASP Top 10 - 2017 : [A6 - Security Misconfiguration](#)

Result:

- Website is accessible.
- Nothing was found for vulnerabilities of server-side software.
- Nothing was found for client access policies.
- Nothing was found for absence of the security.txt file.
- Nothing was found for use of untrusted certificates.
- Nothing was found for enabled HTTP debug methods.
- Nothing was found for secure communication.
- Nothing was found for directory listing.
- Nothing was found for domain too loose set for cookies.
- Nothing was found for unsafe HTTP header Content Security Policy.

Nikto:

Nikto is an open-source web server scanner designed to perform comprehensive security audits of web servers. Developed by Chris Sullo and David Lodge, Nikto is widely used by security professionals and penetration testers to identify potential vulnerabilities and security loopholes in web applications. It conducts a variety of tests, including server misconfigurations, outdated software versions, and common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure server settings. Nikto's extensive plugin architecture allows for customization and flexibility in scanning, making it a valuable tool for assessing the security posture of web servers and applications.

```
(root@kali)-[/home/kali/Desktop]
# nikto -h unstop.com
- Nikto v2.5.0

+ Multiple IPs found: 18.67.233.9, 18.67.233.88, 18.67.233.122, 18.67.233.76
+ Target IP: 18.67.233.9
+ Target Hostname: unstop.com
+ Target Port: 80
+ Start Time: 2024-02-16 05:26:16 (GMT-5)

+ Server: CloudFront
+ /: Retrieved via header: 1.1 2292be0f38a3235417f498559c101624.cloudfront.net (CloudFront).
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Heade
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a diff
web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://unstop.com/
+ : Server banner changed from 'CloudFront' to 'nginx'.
+ /IQf0RYwJ.asp+: Uncommon header 'x-country' found, with contents: IN.
+ /IQf0RYwJ.jse: Uncommon header 'server-timing' found, with contents: cdn-upstream-layer;desc="REC",cdn-upstream-dns;dur=0,cd
dn-pop;desc="CCU50-P3",cdn-rid;desc="6QrpUYWzu2XFI9c8qa_cMzMw2PYOx--kJlfP7H6ulfWeKhRr0Al4SA=",cdn-downstream-fbl;dur=132.
+ /robots.txt: contains 138 entries which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Ro
+ /unstop.com.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /18.67.233.9.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop.com.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /18.67.233.9.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstopcom.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop.com.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop.com.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /18.67.233.9.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstopcom.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop.com.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop_com.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.tar.lzma: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.cer: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop_com.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /site.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /18.67.233.9.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop_com.war: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstopcom.alz: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /unstop.com.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /database.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /18.67.233.9.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /backup.egg: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /18.67.233.9.pem: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /archive.tar.bz2: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
+ /18.67.233.9.jks: Potentially interesting backup/cert file found. . See: https://cwe.mitre.org/data/definitions/530.html
```

The `nikto` tool has been used to perform a security scan on the domain "unstop.com". `nikto` is a web server scanner that identifies potential vulnerabilities and security issues on web servers by sending a series of requests and analyzing the responses.

The scan results provide insights into the security posture of the web server associated with the provided domain name. `nikto` conducts a comprehensive scan that includes checks for known vulnerabilities, outdated software, misconfigurations, and potential security risks.

The output of the scan may include information about open ports, discovered directories, files, and server-specific issues. It can also highlight potential security vulnerabilities such as outdated software versions, insecure configurations, or exposed sensitive information.

It's important to note that `nikto` is a tool that helps identify potential security issues; it doesn't guarantee the presence of vulnerabilities. The results should be carefully reviewed and verified, and any identified issues should be further investigated and addressed.

In summary, the `nikto` scan on the domain "unstop.com" aims to uncover potential security vulnerabilities and misconfigurations on the web server. The results will aid administrators and security professionals in understanding the current security state of the web server and taking appropriate measures to mitigate any identified risks.

Burpsuite:

Burp Suite is a powerful set of web application security testing tools developed by PortSwigger Security. It is widely used by security professionals and penetration testers to identify vulnerabilities and perform security assessments of web applications. Burp Suite offers a range of features including a web proxy, scanner, crawler, repeater, sequencer, and intruder, allowing users to intercept and modify web traffic, identify security flaws such as SQL injection and cross-site scripting (XSS), analyze application responses, and automate attacks for further exploitation. Its intuitive user interface and extensive functionality make it a staple tool for both beginners and experienced security analysts in testing the security of web applications.

1. Spider

It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

2. Proxy

BurpSuite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in BurpSuite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.

3. Intruder

It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. BurpSuite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.

4. Repeater

Repeater lets a user send requests repeatedly with manual modifications. It is used for:

- Verifying whether the user-supplied values are being verified.
- If user-supplied values are being verified, how well is it being done?
- What values is the server expecting in an input parameter/request header?
- How does the server handle unexpected values?
- Is input sanitation being applied by the server?
- How well the server sanitizes the user-supplied inputs?
- What is the sanitation style being used by the server?
- Among all the cookies present, which one is the actual session cookie.

5. Sequencer

The sequencer is an entropy checker that checks for the randomness of tokens generated by the webserver. These tokens are generally used for authentication insensitive operations: cookies and anti-CSRF tokens are examples of such tokens. Ideally, these tokens must be generated in a fully random manner so that the probability of appearance of each possible character at a position is distributed uniformly. This should be achieved both bit-wise and character-wise.

6. Decoder

Decoder lists the common encoding methods like URL, HTML, Base64, Hex, etc. This tool comes handy when looking for chunks of data in values of parameters or headers. It is also used for payload construction for various vulnerability classes. It is used to uncover primary cases of IDOR and session hijacking.

7. Extender

BurpSuite supports external components to be integrated into the tools suite to enhance its capabilities. These external components are called BApps. These work just like browser extensions. These can be viewed, modified, installed, uninstalled in the Extender window.

When the user credentials were entered by a user we used Burp Suite and trapped the Username and Password of the data as transferred in plain text format which is a major risk and can lead

to MITM (Man In The Middle) Attack

Result:

Also, the Protocol used for data communication on the World Wide Web is HTTP 1.1 (Hypertext Transfer Protocol 1.1) version of HTTP protocol. HTTP 1.1 was not designed with modern security and performance considerations in mind. While HTTP1.1 supports compression through the Accepting Encoding header, it does not mandate its use. This means that a response can be sent uncompressed leading to slower data transfer

It is worth noting that many of the limitations of HTTP 1.1 have been addressed in a subsequent version, mostly notably in HTTP/2 and HTTP/3. These newer protocols address the drawbacks of HTTP 1.1 while introducing new features and optimization to improve speed effectiveness and the security of web communication

SQL Injection

SQL injection (SQLi) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior. In some situations, an attacker can escalate a SQL injection attack to compromise the underlying server or other back-end infrastructure, or perform a denial-of-service attack.

A successful SQL injection attack can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information. Many high-profile data breaches in recent years have been the result of SQL injection attacks, leading to reputational damage and regulatory fines. In some cases, an attacker can obtain a persistent backdoor into an organization's systems, leading to a long-term compromise that can go unnoticed for an extended period.

How to detect SQL injection:

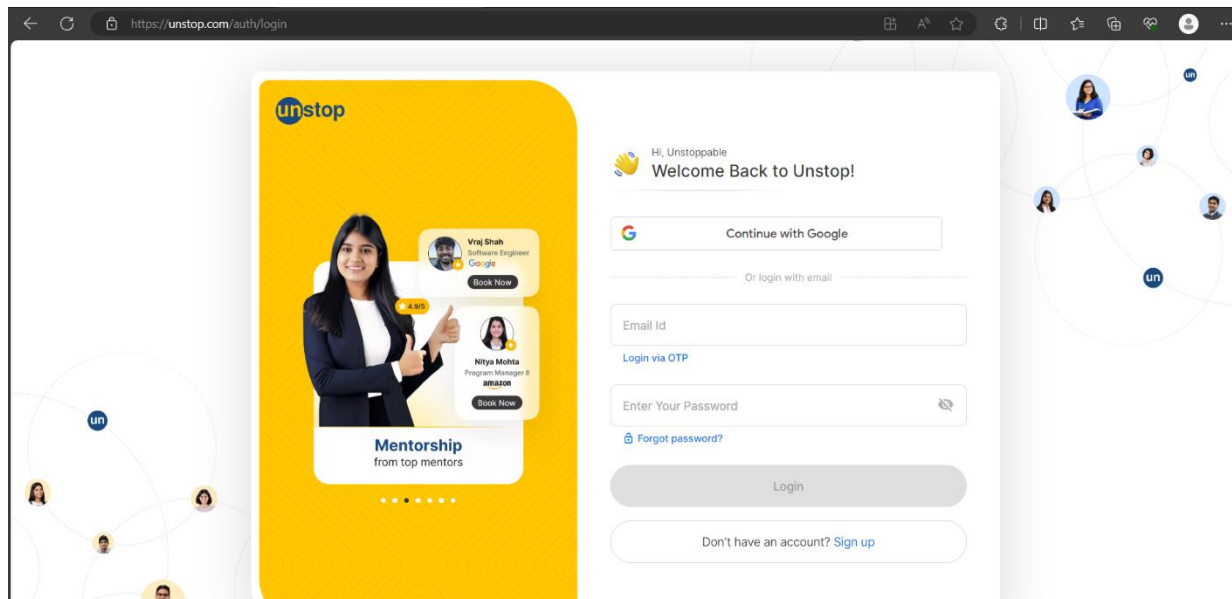
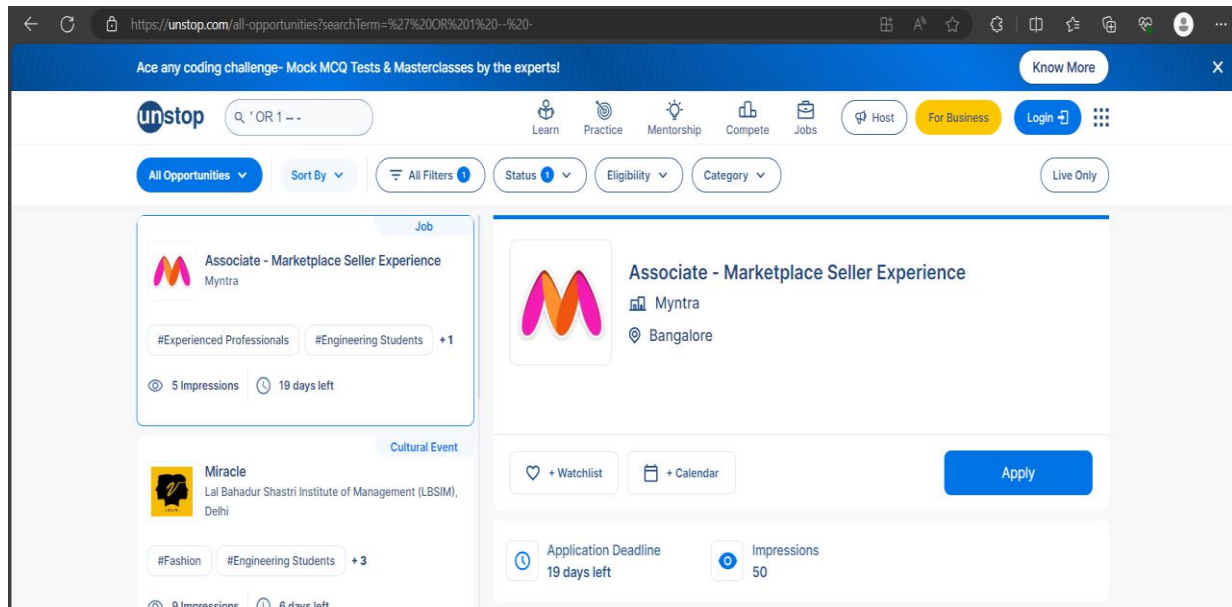
The majority of SQL injection vulnerabilities can be found quickly and reliably using Burp Suite's web vulnerability scanner.

SQL injection can be detected manually by using a systematic set of tests against every entry point in the application. This typically involves:

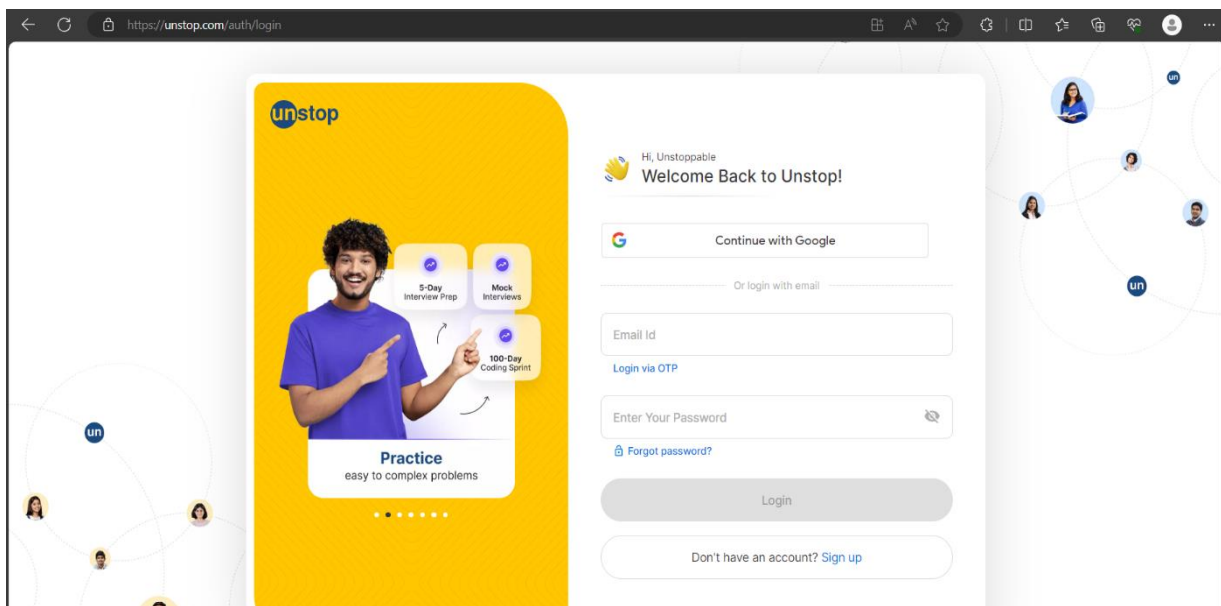
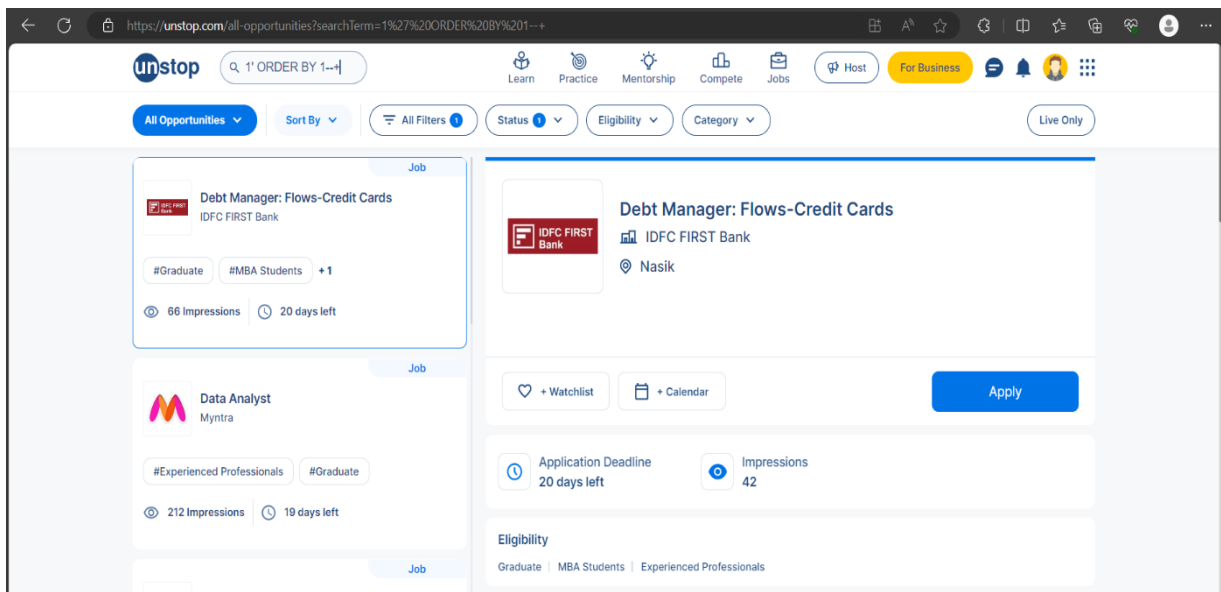
- Submitting the single quote character ' and looking for errors or other anomalies.
- Submitting some SQL-specific syntax that evaluates to the base (original) value of the entry point, and to a different value, and looking for systematic differences in the resulting application responses.
- Submitting Boolean conditions such as OR 1=1 and OR 1=2, and looking for differences in the application's responses.
- Submitting payloads designed to trigger time delays when executed within a SQL query, and looking for differences in the time taken to respond.
- Submitting OAST payloads designed to trigger an out-of-band network interaction when executed within a SQL query, and monitoring for any resulting interactions.

Code Execution :

(Without LOGIN)



(With LOGIN)



The website unstop.com employs security measures to detect and prevent SQL injection attacks. When an attempt is made to inject SQL commands into the search box, the website recognizes the malicious behavior and redirects the user to the login page as a precautionary measure. This redirection serves to mitigate the potential risks associated with SQL injection, safeguarding the website's database and user data from exploitation. By requiring authentication before further interaction, the website ensures that only authorized users can access sensitive functionality, thereby enhancing overall security posture.

Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it. An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

What are the types of XSS Attacks?

There are three main types of XSS attacks. These are:

- Reflected XSS, where the malicious script comes from the current HTTP request.
- Stored XSS, where the malicious script comes from the website's database.
- DOM-based XSS, where the vulnerability exists in client-side code rather than server-side code.

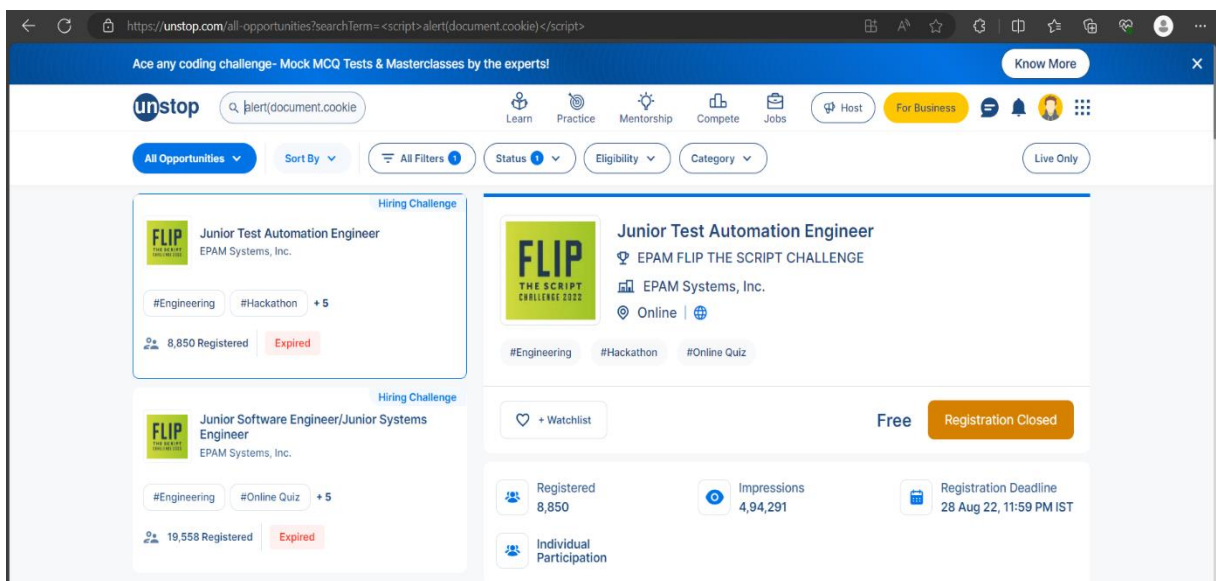
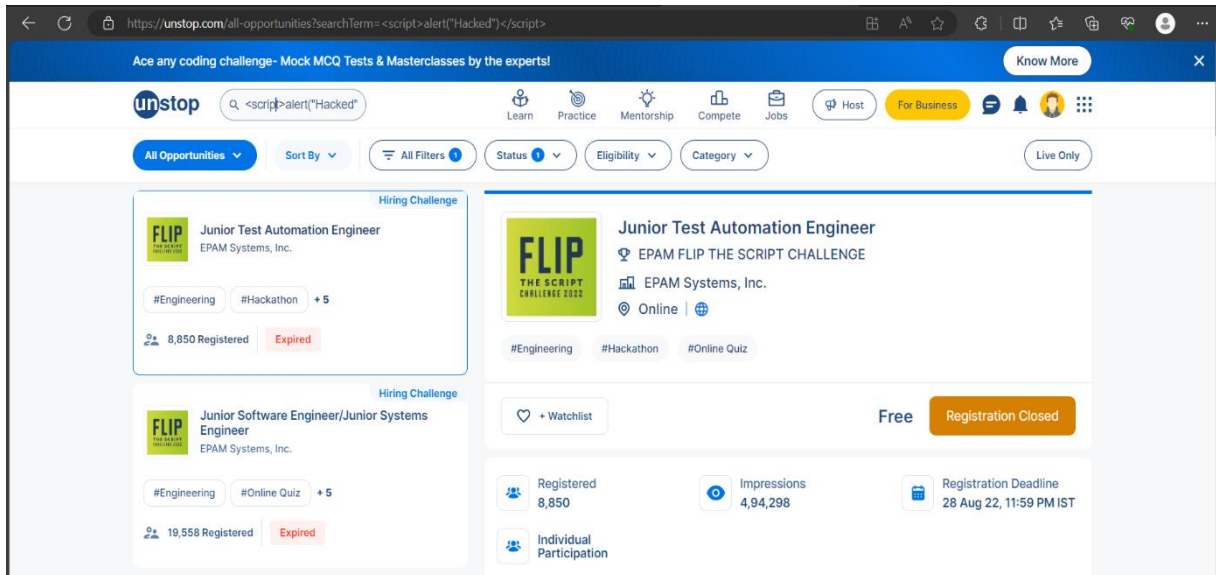
1.1 What can XSS be used for?

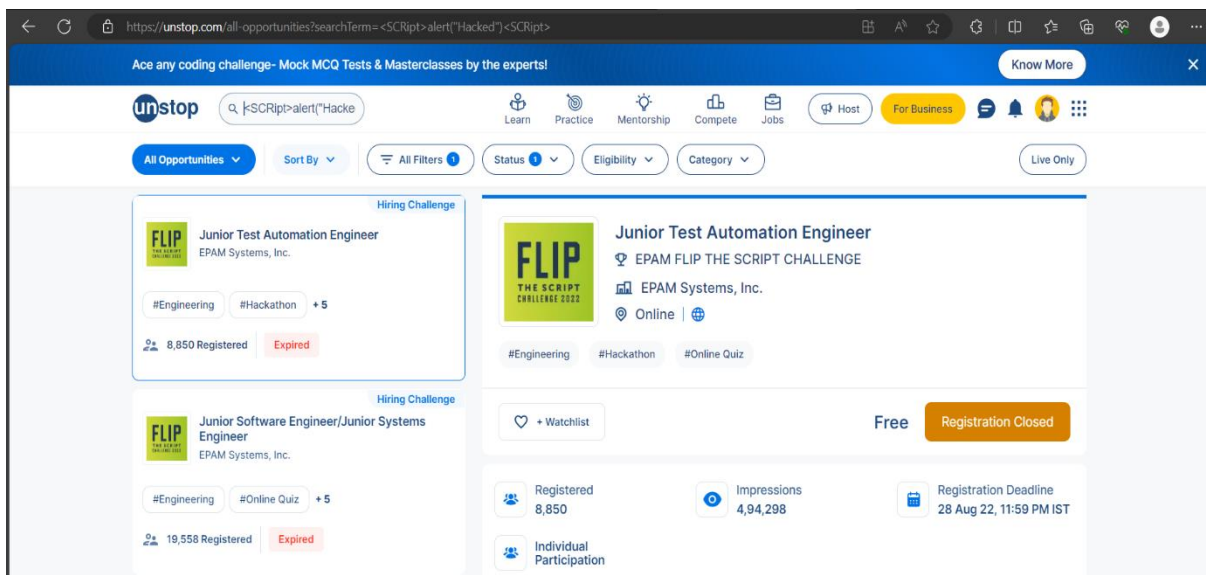
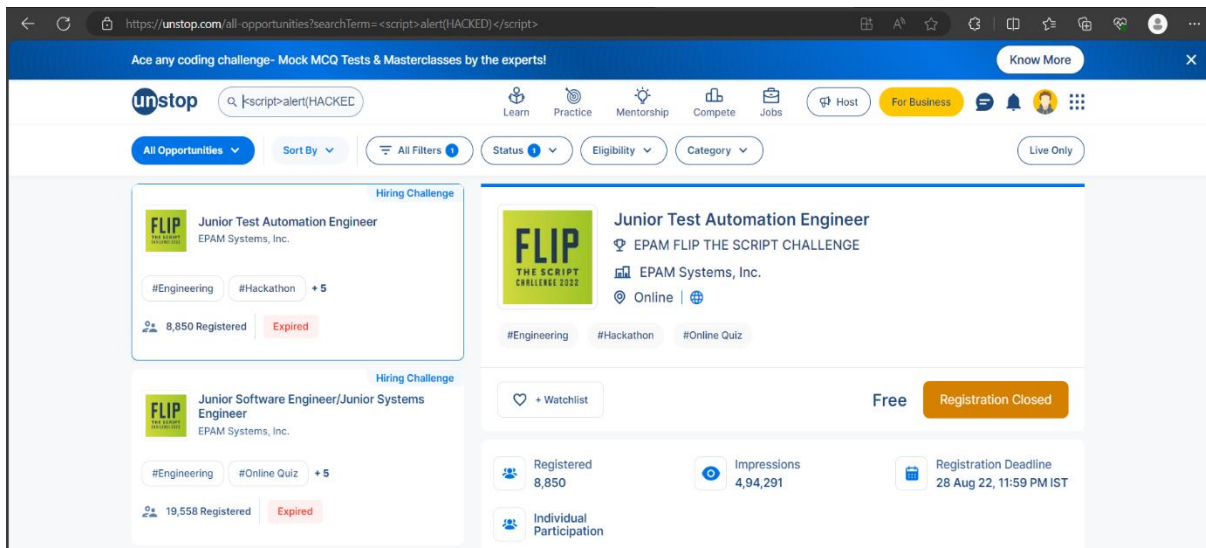
An attacker who exploits a cross-site scripting vulnerability is typically able to:

- Impersonate or masquerade as the victim user.
- Carry out any action that the user is able to perform.
- Read any data that the user is able to access.
- Capture the user's login credentials.
- Perform virtual defacement of the web site.
- Inject trojan functionality into the web site.

Code Execution:

Reflected XSS

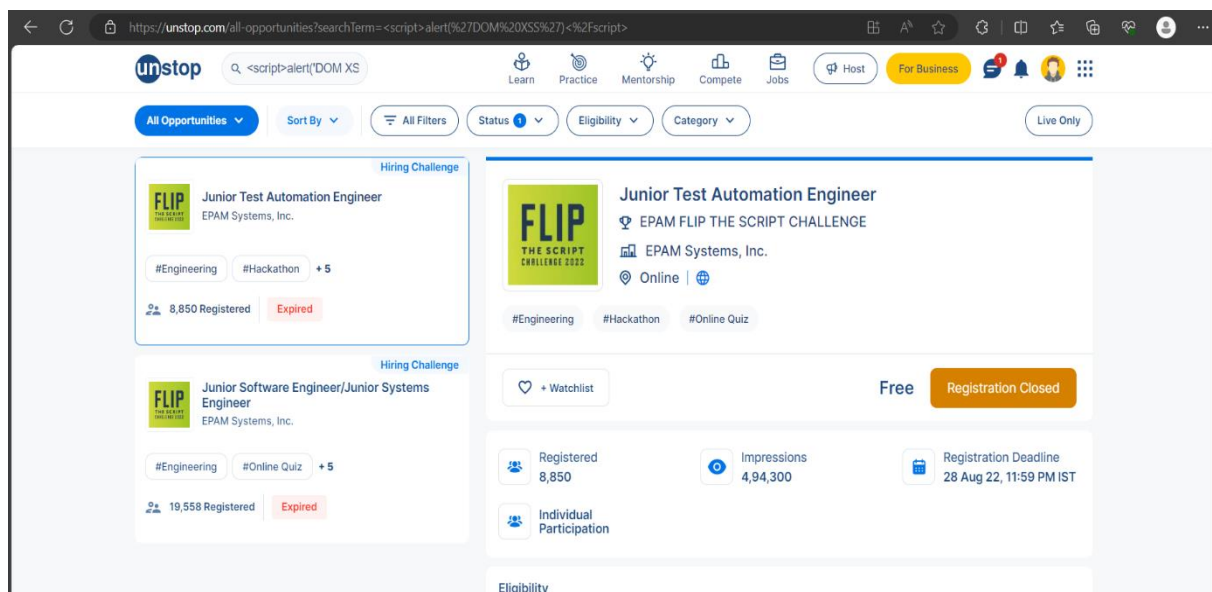
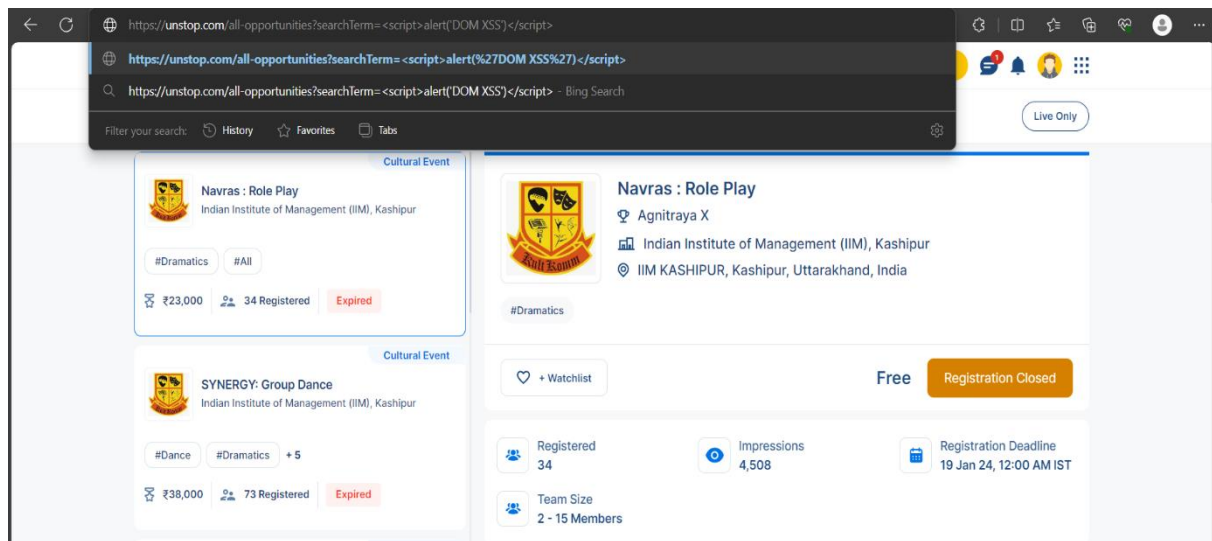




In attempting reflected XSS attacks on unstop.com with various script payloads such as `<Script> alert(Hacked) </Script>`, `<Script> alert(document.cookie) </Script>`, `<Script> alert("Hacked") </Script>`, and `<SCRIPT> alert("Hacked") </SCRIPT>`, it appears that the website's security measures are specifically targeting the keyword "script" rather than the contents of the script itself. This suggests that the website has implemented a filtering mechanism to block any input containing the term "script" in an attempt to mitigate XSS vulnerabilities. Such filtering techniques are commonly employed to sanitize user input and prevent malicious scripts from being executed within the web application. However, it's important to note that effective XSS protection requires more sophisticated filtering mechanisms that consider the entire context of user input, rather than solely focusing on specific keywords. Additionally, thorough input validation and output encoding are essential to fully mitigate the risk of XSS attacks.

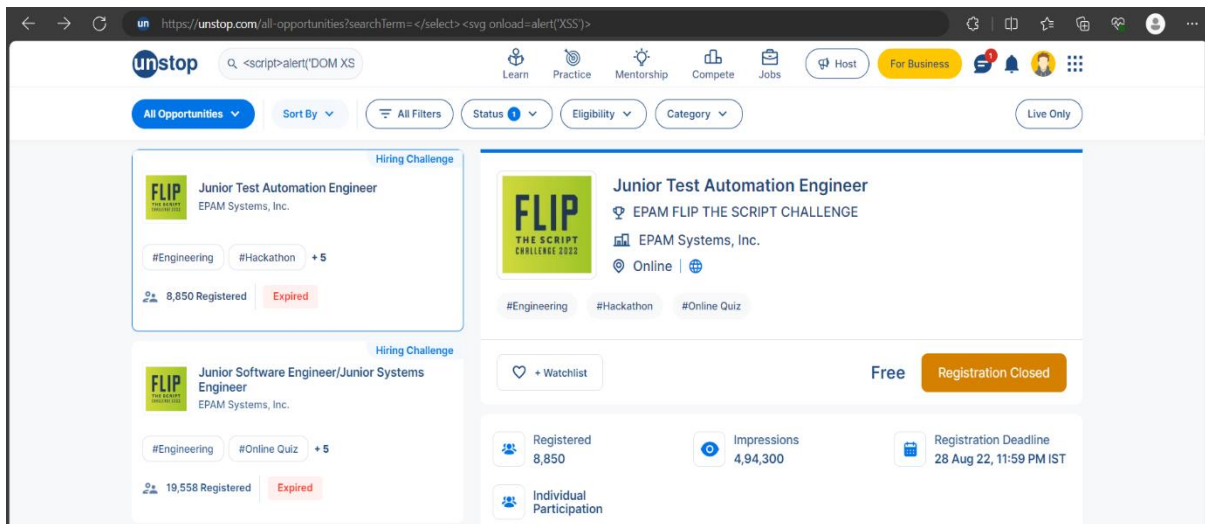
Code Execution:

DOM XSS

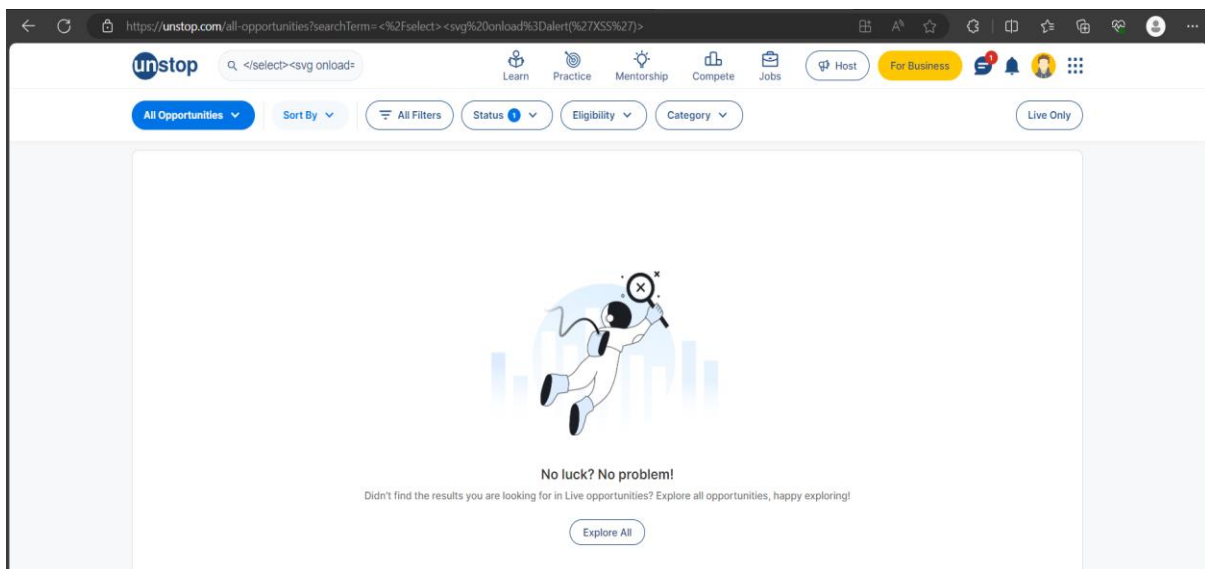


Trying the following script in the URL

- </select><svg onload=alert('XSS')>
- </select>
- </select><body onload=alert('XSS')>

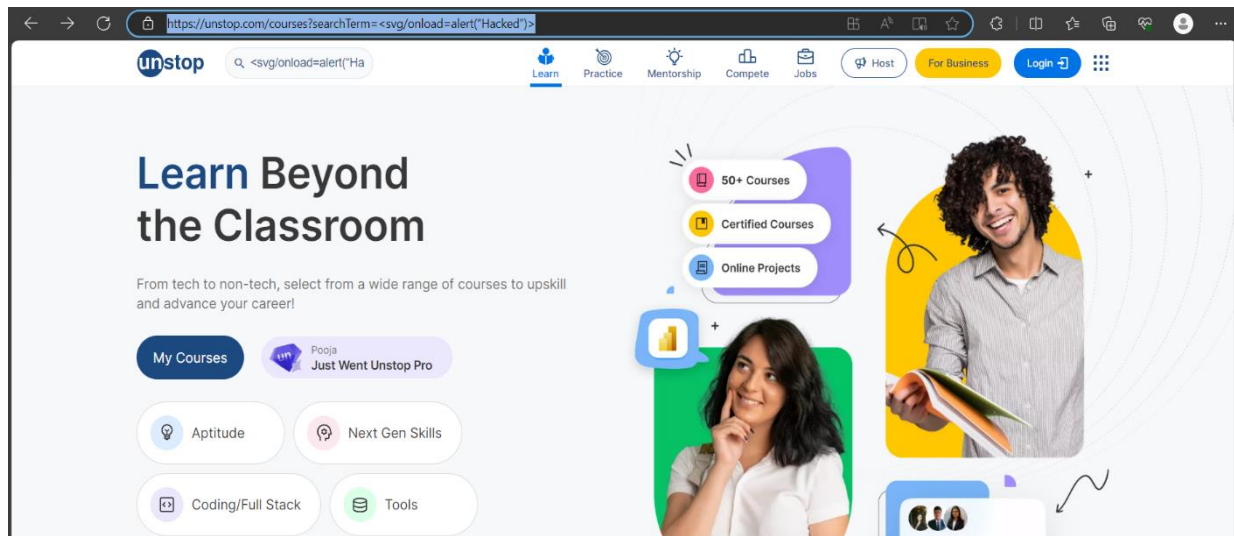


All the three scripts are redirecting to the following page:



In attempting DOM-based XSS attacks on unstop.com by injecting scripts like `</select><svg onload=alert('XSS')>`, `</select>`, and `</select><body onload=alert('XSS')>` directly into the URL, the observed outcome of a generic page indicating "no luck, no problem" suggests that the website may have implemented security measures to mitigate against such attacks. This response indicates that the injected scripts were likely not executed as intended, possibly due to client-side sanitization or filtering mechanisms in place that intercept and neutralize potentially malicious content. It's also possible that the website's security infrastructure is capable of detecting and preventing DOM-based XSS attempts, thereby safeguarding against unauthorized script execution within the browser environment. Nonetheless, comprehensive security measures, including input validation, output encoding, and consistent security updates, are crucial for effectively mitigating the risks posed by DOM-based XSS vulnerabilities.

Stored XSS



In attempting stored XSS attacks on `unstop.com`, which involves injecting malicious scripts into the website's storage system (such as databases) to be later served to users, the lack of success in obtaining any vulnerable results indicates that the website may have robust security measures in place to prevent such exploits. It's possible that `unstop.com` employs stringent input validation and output encoding techniques to sanitize user-generated content before storing it in its database or rendering it to users. Additionally, the website might utilize other security mechanisms like Content Security Policy (CSP) or web application firewalls (WAFs) to detect and block suspicious script injections. Another possibility is that the website actively monitors for unusual activity or patterns that could indicate an attempted attack and takes proactive measures to mitigate such risks. While the absence of vulnerable results is a positive sign for the website's security posture, continuous monitoring, regular security audits, and staying up-to-date with the latest security best practices are essential to maintain resilience against evolving threats like stored XSS attacks.

Hping for DOS Attack:

hping is a command-line oriented TCP/IP packet assembler/analyzer. It can be used to generate and manipulate network packets, probe hosts, firewalls, and more. The primary purpose of hping is to test networks and hosts for vulnerabilities or to perform network diagnostics.

Here are some common use cases for hping:

- **Firewall testing:** hping can be used to test the effectiveness of firewalls by sending various types of packets and observing the responses.
- **Network testing:** It allows you to perform various types of network tests, such as ping sweeps, traceroutes, and port scans.
- **Packet crafting:** hping enables the creation of custom packets with specific characteristics, which can be useful for testing network security or for crafting specific network traffic.
- **Security auditing:** It can be used by security professionals to test network devices and servers for potential vulnerabilities.
- **Network troubleshooting:** hping can help diagnose network connectivity issues by sending packets and analyzing responses.

hping has various options and modes of operation, allowing users to customize its behavior for different purposes. However, it's important to note that hping can be misused and may be seen as a security threat if used for malicious purposes. Therefore, it should only be used responsibly and ethically, preferably in controlled environments or with proper authorization.

What is DOS Attack?

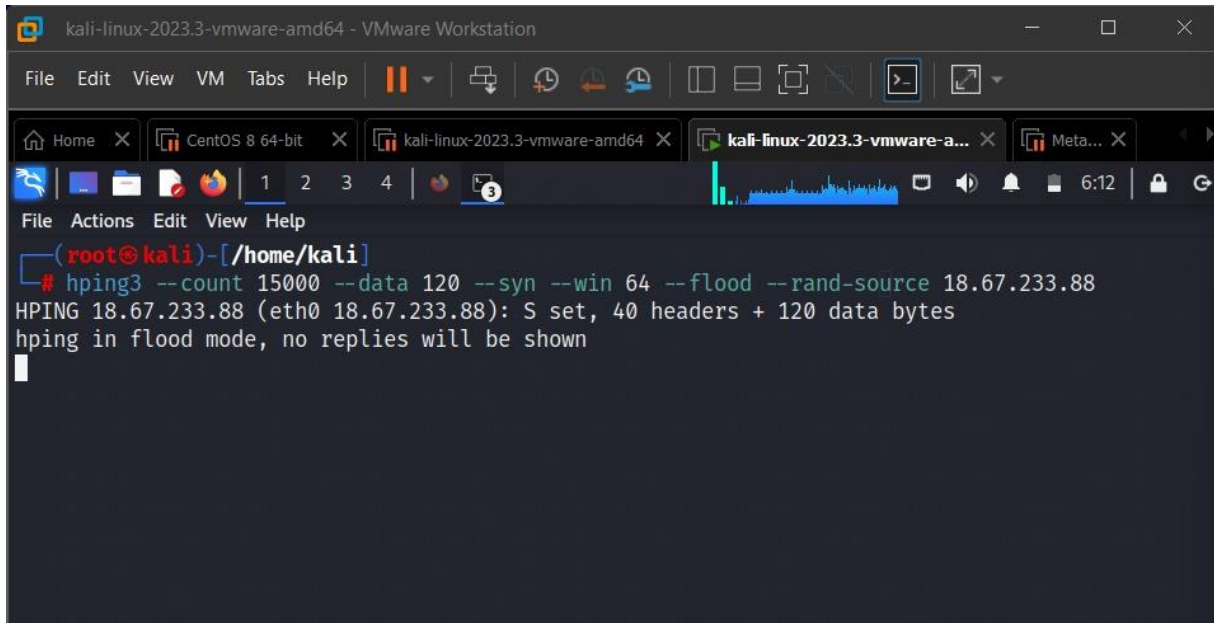
A Denial-of-Service (DoS) attack is a malicious attempt to disrupt the normal functioning of a targeted server, service, or network by overwhelming it with a flood of illegitimate traffic. The goal of a DoS attack is to make a resource unavailable to its intended users, causing disruption or downtime.

There are several types of DoS attacks, including:

- **Traffic Flooding:** In this type of attack, the attacker sends a massive volume of traffic to the target, consuming its available bandwidth and resources, thereby making it inaccessible to legitimate users. This can be achieved using techniques such as UDP flooding, SYN flooding, ICMP flooding, and HTTP flooding.
- **Resource Exhaustion:** Some DoS attacks focus on exploiting vulnerabilities in the target's resources, such as CPU, memory, or disk space. For example, a Ping of Death attack sends oversized packets to a target, causing it to crash or become unresponsive.
- **Application Layer Attacks:** These attacks target specific applications or services running on the target server, overwhelming them with requests or exploiting their vulnerabilities. Examples include HTTP GET/POST floods, Slowloris attacks, and DNS amplification attacks.
- **Distributed Denial-of-Service (DDoS) Attacks:** In a DDoS attack, multiple compromised systems, often referred to as "bots" or "zombies," are used to launch coordinated attacks

against a single target. This amplifies the attack's impact and makes it more challenging to mitigate.

DoS attacks can have serious consequences, including loss of revenue, damage to reputation, and disruption of critical services. Organizations often employ various defense mechanisms, such as firewalls, intrusion detection systems (IDS), and DoS mitigation services, to protect against these attacks. Additionally, implementing best practices for network and server security can help mitigate the risk of DoS attacks.



```
kali-linux-2023.3-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home CentOS 8 64-bit kali-linux-2023.3-vmware-amd64 kali-linux-2023.3-vmware-a... Meta...
File Actions Edit View Help
(root@kali)-[/home/kali]
# hping3 --count 15000 --data 120 --syn --win 64 --flood --rand-source 18.67.233.88
HPING 18.67.233.88 (eth0 18.67.233.88): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Result:

In learning about network testing or tools like `hping`, it's essential to do so in a responsible and ethical manner. Always ensure that you have explicit permission from the target network owner before performing any kind of network testing or scanning.

CONCLUSION

We conclude that the project we undertook i.e. Security audit of website [Unstop.com](https://unstop.com), using OWASP Methodology for identifying vulnerabilities and potential security threats in the website has followed a thorough and systematic process for identifying vulnerabilities and carrying out required analysis.

OWASP Top 10, is a framework for list of prioritized top 10 website vulnerabilities, that helps for assessing security risks and is used to baseline required website vulnerability testing. The approach helps to improve security of the application and furthermore reduces risk by providing mitigation to reduce risk due to potential cyber attacks and data theft.

It is an underline fact that website application testing is a repetitive methodology since it's not possible to have full proof secure website due to cyber criminals being smart and coming up with new and complex ways to exploit and thereby impact smooth functioning of the application, which reside within the website. Therefore, yearly or half yearly website security audit should ideally ensure security of website from emerging new cyber threats and associated cyber attacks.

REFERENCES

1. <https://owasp.org/www-project-top-ten/>
2. <https://cheatsheetseries.owasp.org/IndexTopTen.html>
3. <https://portswigger.net/web-security/cross-site-scripting>
4. <https://github.com/payloadbox/sql-injection-payload-list>
5. <https://www.kali.org/tools/nmap/>
6. <https://www.kali.org/tools/nikto/>
7. <https://unstop.com/>
8. <https://sitereport.netcraft.com/>
9. <https://dnsdumpster.com/>
10. <https://www.shodan.io/>
11. <https://github.com/payloadbox/sql-injection-payload-list>
12. <https://search.censys.io/>
13. <https://securitytrails.com/>
14. <https://www.kali.org/tools/sqlmap/>

