

task 7

(01/09/23): Select a website do footprinting and reconnaissance like collect information about website use like Nslookup Osint framework

so for footprinting and reconnaissance work we will use different websites and will collect the information of vit.ac.in its an website of VIT so we will collect info on this website

—Footprinting & Reconnaissance-----

Google dorks

Who.is

OSINT

mxtoolbox

netcraft

Census

theHarvester

sherlock

DNSDumpster

Shodan

archive.org

these are the websites we can go through for collecting information on any website

but we will go with the some of the mentioned websites like nslookup and osint framework and more

1.....so firstly we will use nslookup.io (<https://www.nslookup.io/domains/vit.ac.in/dns-records/>) to get the ipv4 address and get some more details about AAAA records and other records although they dont have in this case

DNS for developers module 3 just dropped — 10 lessons on operational DNS 🚀

Nslookup.io [Learning](#) [Browser extension](#) [API](#)

DNS records for **vit.ac.in**

[Cloudflare](#) [Google DNS](#) [OpenDNS](#) [Authoritative](#) [Local DNS](#) ⌵

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

A records

IPv4 address	Revalidate in
> 136.233.9.13	1m

AAAA records

No AAAA records found.

CNAME record

No CNAME record found.

By Nslookup.io

DNS for Developers

Never be confused
about DNS again.

2..... now we will use [shodan.io](https://www.shodan.io/host/136.233.9.13) (<https://www.shodan.io/host/136.233.9.13>) to gain more information like total ports and open ports of the website along with their location and the isp and other information regarding the ports in this case we can see the open ports are 80 and 443

Port 80 allows HTTP protocol means the information remains in plain text between the browser and the server, while Port 443 allows HTTPS protocol means all the information travels between the server and the browser remains encrypted. and hence more details of these ports are being shown in the page

136.233.9.13 Regular View Raw Data

General Information

Hostnames	vit.ac.in
Domains	VIT.AC.IN
Country	India
City	Vellore
Organization	Reliance Jio Infocomm Limited
ISP	Reliance Jio Infocomm Limited
ASN	AS55836

Open Ports

80 / TCP

HTTP/1.1 307 Moved Temporarily
Location: https://136.233.9.13/
Content-Length: 0

443 / TCP

Apache httpd

HTTP/1.1 200 OK
Date: Thu, 05 Oct 2023 12:31:05 GMT
Server: Apache
X-Content-Type-Options: nosniff
X-Generator: off
X-Drupal-Cache: off
X-Forwarded-By: off
Expires: Sat, 13 Nov 2026 05:00:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
X-Content-Type-Options: nosniff
Content-Security-Policy: no-trust /script

Web Technologies

Analytics JavaScript Libraries

further if we move into the page we can see the web technologies used in the server and also the possible vulnerabilities of the website based on their software

their vulnerabilities are

<u>CVE-2023-31250</u>	The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.
<u>CVE-2022-25271</u>	4.3 Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.
<u>CVE-2021-41184</u>	4.3 jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `of` option of the `.position()` util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `of` option is now treated as a CSS selector. A workaround is to not accept the value of the `of` option from untrusted sources.
<u>CVE-2021-41183</u>	4.3 jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of various `*Text` options of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI

	1.13.0. The values passed to various `*Text` options are now always treated as pure text, not HTML. A workaround is to not accept the value of the `*Text` options from untrusted sources.
<u>CVE-2021-41182</u>	4.3 jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the `altField` option of the Datepicker widget from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value passed to the `altField` option is now treated as a CSS selector. A workaround is to not accept the value of the `altField` option from untrusted sources.
<u>CVE-2020-36193</u>	5.0 Tar.php in Archive_Tar through 1.4.11 allows write operations with Directory Traversal due to inadequate checking of symbolic links, a related issue to CVE-2020-28948.
<u>CVE-2020-28949</u>	6.8 Archive_Tar through 1.4.10 has `://` filename sanitization only to address phar attacks, and thus any other stream-wrapper attack (such as file:// to overwrite files) can still succeed.
<u>CVE-2020-28948</u>	6.8 Archive_Tar through 1.4.10 allows an unserialization attack because phar: is blocked but PHAR: is not blocked.
<u>CVE-2020-13672</u>	2.6 Cross-site Scripting (XSS) vulnerability in Drupal core's sanitization API fails to properly filter cross-site scripting under certain circumstances. This issue affects: Drupal Core 9.1.x versions prior to 9.1.7; 9.0.x versions prior to 9.0.12; 8.9.x versions prior to 8.9.14; 7.x versions prior to 7.80.
<u>CVE-2020-13671</u>	6.5 Drupal core does not properly sanitize certain filenames on uploaded files, which can lead to files being interpreted as the incorrect extension and served as the wrong MIME type or executed as PHP for certain hosting configurations. This issue affects: Drupal Core 9.0 versions prior to 9.0.8, 8.9 versions prior to 8.9.9, 8.8 versions prior to 8.8.11, and 7 versions prior to 7.74.
<u>CVE-2020-13666</u>	4.3 Cross-site scripting vulnerability in Drupal Core. Drupal AJAX API does not disable JSONP by default, allowing for an XSS attack. This issue affects: Drupal Core 7.x versions prior to 7.73; 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.
<u>CVE-2020-13663</u>	6.8 Cross Site Request Forgery vulnerability in Drupal Core Form API does not properly handle certain form input from cross-site requests, which can lead to other vulnerabilities.
<u>CVE-2020-13662</u>	5.8 Open Redirect vulnerability in Drupal Core allows a user to be tricked into visiting a specially crafted link which would redirect them to an arbitrary

	external URL. This issue affects: Drupal Drupal Core 7 version 7.70 and prior versions.
<u>CVE-2020-11023</u>	4.3 In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
<u>CVE-2020-11022</u>	4.3 In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
<u>CVE-2010-5312</u>	4.3 Cross-site scripting (XSS) vulnerability in jquery.ui.dialog.js in the Dialog widget in jQuery UI before 1.10.0 allows remote attackers to inject arbitrary web script or HTML via the title option.

Web Technologies

Analytics

Google Analytics

CMS

Drupal 7

JavaScript Libraries

OWL Carousel

jQuery

Programming Languages

PHP

Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version

CVE-2023-31250

The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.

CVE-2022-25271

Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.

CVE-2021-41184

jQuery-UI is the official jQuery user interface library. Prior to version 1.13.0, accepting the value of the 'of' option of the 'position()' util from untrusted sources may execute untrusted code. The issue is fixed in jQuery UI 1.13.0. Any string value

X-Drupal-cache: off

X-Powered-By: off

Expires: Sun, 19 Nov 1978 05:00:00 GMT

Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0

X-Content-Type-Options: nosniff

Content-Security-Policy: policy-uri 'self'

X-Content-Security-Policy: policy-uri 'self'

X-WebKit-CSP: policy-uri 'self'

X-XSS-Protection: 1

X-Frame-Options: SAMEORIGIN

Strict-Transport-Security: max-age=31536000

Content-Language: en

X-Generator: Drupal

Link: <https://vit.ac.in/>; rel="canonical"

Vary: Accept-Encoding

Content-Type: text/html; charset=utf-8

Transfer-Encoding: chunked

SSL Certificate

Certificate:

Data:

Version: 3 (Rev2)

Serial Number:

46:53:67:b6:23:c5:be:ee:b9:6e:e2:c8:5f:46:c9:f7

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Setigo Limited, CN=Setigo RSA Domain Validation Secure Serve

r CA

Validity

Not Before: Sep 4 00:00:00 2023 GMT

Not After : Aug 3 23:59:59 2024 GMT

Subject: CN=*.vit.ac.in

Subject Public key info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:c6:7d:eb:33:38:3e:4e:57:73:99:54:94:1b:98:

c7:df:1a:6a:9b:2e:3c:31:18:33:ed:4e:fd:7c:a9:

93:11:4f:b5:b3:c6:85:e7:29:fe:79:e2:4e:77:a7:

04:05:10:73:06:20:8c:00:0d:03:f0:7b:3c:3d:94:

00:f2:0b:cd:11:db:09:cf:7e:5d:fe:39:13:6b:24:

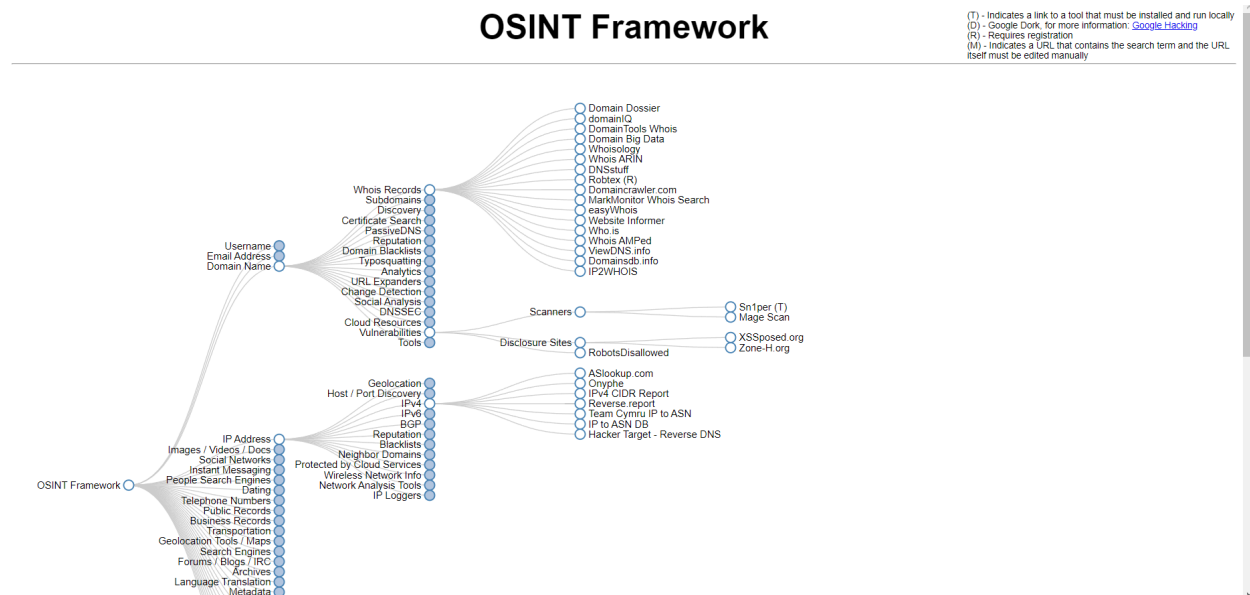
bc:fe:98:6a:40:a0:0f:08:a7:77:cd:cb:1b:01:79:

39:78:09:2f:03:7d:1d:40:f0:11:24:93:00:a5:09:

0a:0a:00:00:00:00:00:00:00:00:00:00:00:00:00:

with the help of this website we can gather enough information to exploit a website

3..... with the help of osint framework we can understand which tool should be used to exploit which kind of vulnerabilities



see in this for domain name vulnerabilities and for scanning we can use a tool which needs to be locally installed called sn1per as mentioned or we can use mentioned sites similarly for ip address ipv4 we can use the mentioned tools for finding our ipv4 so this website helps informing us to use the desired tools to gather the information of different types depending on our needs

4....okay back to website so we got different vulnerabilities in website of VIT now we can use different websites to get more information like what type of vulnerability it is like as of now we only have CWE number right what does it stand for????

okay so for this we will use cwe.mitre.org website to get the details of the common weaknesses

Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home | About | CWE List | Mapping | Top-N Lists | Community | News | Search

CWE™ is a community-developed list of software and hardware weakness types. It serves as a common language, a measuring stick for security tools, and as a baseline for weakness identification, mitigation, and prevention efforts.

2023 CWE Top 25 Most Dangerous Software Weaknesses New!

This list demonstrates the currently most common and impactful software weaknesses. Often easy to find and exploit, these can lead to exploitable vulnerabilities that allow adversaries to completely take over a system, steal data, or prevent applications from working.

[Top 25 List](#) | [Key Insights](#) | [Methodology](#)

CWE List Quick Access

Search CWE

ENHANCED BY Google

View CWE

by Software Development

by Hardware Design

by Research Concepts

Community Engagement

Hardware CWE Special Interest Group [Join HW CWE SIG](#)

ICS/OT Special Interest Group [Join ICS/OT SIG](#)

REST API Working Group [Join REST API WG](#)

User Experience Working Group [Join UE WG](#)

CWE/CAPEC Board [Read meeting minutes](#)

CWE News

News [Stubborn Weaknesses in the CWE Top 25 \(Updated\)](#)

News [CWE Top 25 Weaknesses Trends from 2019 Through 2023 Now Available](#)

News [2023 CWE Top 25 Weaknesses "On the Cusp" List Now Available](#)

News [2023 "CWE Top 25" Now Available!](#)

News [CWE Version 4.12 Now Available](#)

like we took CVE-2023-31250 from shodan report

Search CVE List | Downloads | Data feeds | Update a CVE record | Request CVE ID

TOTAL CVE Records: 213519

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG and CVE Record Format JSON are underway.





NOTICE: Legacy CVE List download formats will be phased out beginning January 1, 2024. New CVE List download format is available now.


HOME > CVE > CVE-2023-31250



[Printer-Friendly View](#)

CVE-ID	
CVE-2023-31250	Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information	
Description	
The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none"> CONFIRM: https://www.drupal.org/sa-core-2023-005 URL: https://www.drupal.org/sa-core-2023-005 	
Assigning CNA	
Drupal.org	
Date Record Created	
20230426	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20230426)	
Votes (Legacy)	

it gave more information on the website vulnerability

Affected Vendor/Software:  Drupal - Core version < 10.0.8			
Affected Vendor/Software:  Drupal - Core version < 9.5.8			
Affected Vendor/Software:  Drupal - Core version < 9.4.14			
Affected Vendor/Software:  Drupal - Core version 7.96			

CVSS3 Score: 6.5 - MEDIUM			
Attack Vector 	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVE References		
Description	Tags 	Link
Drupal core - Moderately critical - Access bypass - SA-CORE-2023-005 Drupal.org	web.archive.org text/html Inactive Link Not Archived	 CONFIRM www.drupal.org/sa-core-2023-005

5.... now we can use more websites like exploit-db.com to get more about the different attack methods on different exploits so The Exploit Database is a CVE compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

here for drupal see how many different public exploits are coming

The screenshot shows the Exploit-DB website interface. At the top, there's a navigation bar with the Exploit-DB logo and a search bar. Below the navigation bar, there are filters for 'Verified' and 'Has App'. A 'Show' dropdown is set to '120'. The search bar contains the text 'Drupal'. The results are displayed in a table with columns: Date, D (Download), A (Add), V (Verify), Title, Type, Platform, and Author.

Date	D	A	V	Title	Type	Platform	Author
2023-09-08				Drupal 10.1.2 - web-cache-poisoning-External-service-interaction	WebApps	PHP	nu11secu1ty
2022-03-30				Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)	WebApps	PHP	Milad karimi
2021-10-01				Drupal Module MiniorangeSAML 8.x-2.22 - Privilege escalation	WebApps	PHP	Cristian \void\ Giustini
2019-03-07				Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)	Remote	PHP	Metasploit
2019-02-25				Drupal < 8.6.9 - REST Module Remote Code Execution	WebApps	PHP	leorjza
2019-02-23				Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	WebApps	PHP	Charles Fol
2018-04-30				Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)	WebApps	PHP	SixP4ck3r
2018-04-25				Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)	WebApps	PHP	Blaklis
2018-04-23				Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure	WebApps	PHP	Larry W. Cashdollar
2018-04-17				Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)	Remote	PHP	José Ignacio Rojo
2018-04-13				Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	WebApps	PHP	Hans Topo & q0tm1k

so these are the several websites that we can use to gather information on some website and by conducting thorough reconnaissance footprinting, security professionals can assess risks, strengthen defences, and prevent potential cyber threat