

Task 7

Select a website do footprinting and reconnaissance like collect information about website use like Nslookup Osint framework

For foot printing and reconnaissance work we will use different websites and will collect the information of vit.ac.in it's a website of VIT so we will collect info on this website

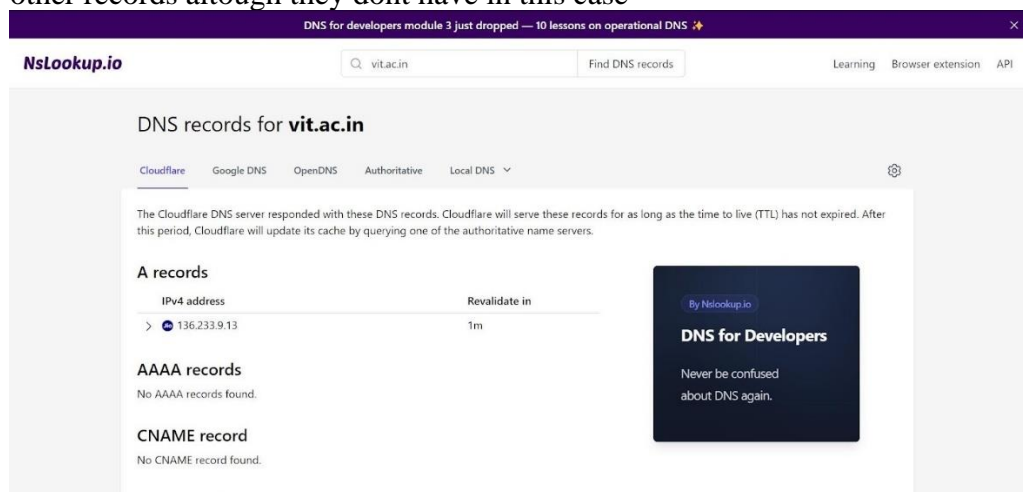
Footprinting & Reconnaissance

Google
dorks
Who.is
OSINT
mxtoo
lbox
netcra
ft
Census
theHarv
ester
sherlock
DNSDum
pster
Shodan
archive.or
g

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

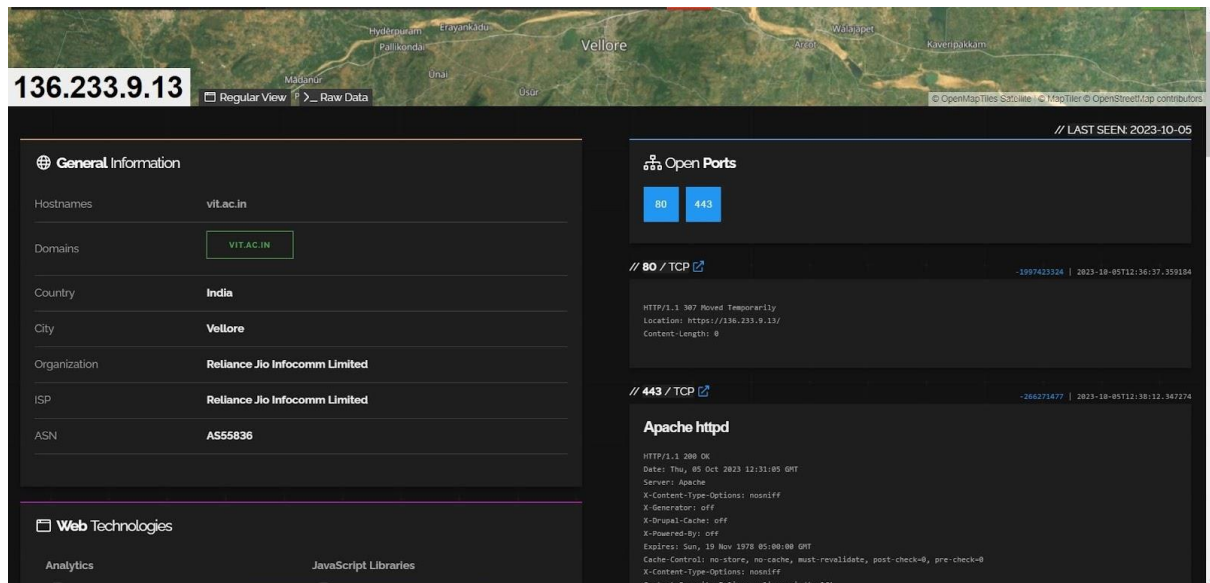
but we will go with the some of the mentioned websites like nslookup and osint framework and more

1. Firstly we will use [nslookup.io](https://www.nslookup.io/domains/vit.ac.in/dns-records/) (<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



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



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 :

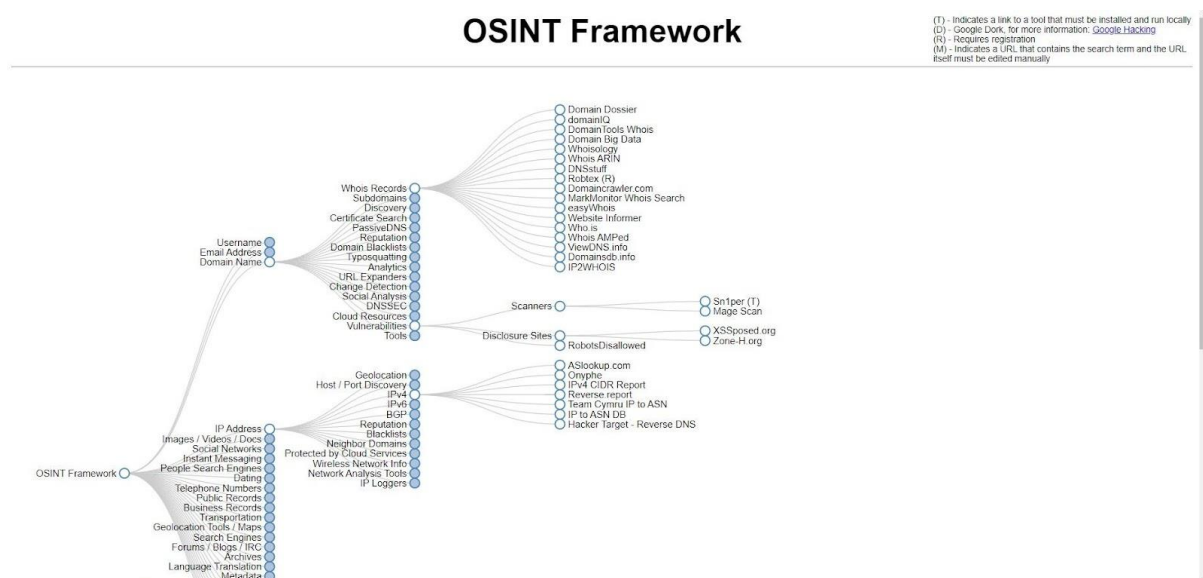
CVE-2023- 31250	The file download facility doesn't sufficiently sanitize file paths in certain situations. This may result in users gaining access to private files that they should not have access to. Some sites may require configuration changes following this security release. Review the release notes for your Drupal version if you have issues accessing private files after updating.
CVE-2022- 25271	4.3Drupal 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	4.3jQuery-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.
CVE-2021-41183	4.3jQuery-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. This 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.
CVE-2021- 41182	4.3jQuery-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.
CVE-2020- 36193	5.0Tar.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.
CVE-2020- 28949	6.8Archive_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.
CVE-2020- 28948	6.8Archive_Tar through 1.4.10 allows an unserialization attack because phar: is blocked but PHAR: is not blocked.
CVE-2020- 13672	2.6Cross-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.
CVE-2020- 13671	6.5Drupal 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.

CVE-2020- 13666	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 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.
CVE-2020- 13663	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.
CVE-2020- 13662	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.
CVE-2020- 11023	4.3In 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.
CVE-2020- 11022	4.3In 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.
CVE 2010-5312	4.3Cross-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	JavaScript Libraries	<pre> X-Dropul-Scale: 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 K-Generator: Drupal Link: <https://vlt.ac.in/>; rel="canonical" Vary: Accept-Encoding Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked </pre>			
Google Analytics	OWL Carousel				
CMS	jQuery				
Drupal	PHP				
Programming Languages					
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	<p>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.</p>				
CVE-2022-25271	<p>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.</p>				
CVE-2021-41184	<p>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</p>				
SSL Certificate					
<pre> Certificate: Data Version: 3 (B2) Serial Number: 461537106231c5beceeb956e1c2c8f546c7f7 Signature Algorithm: sha256WithRSAEncryption Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Section Limited, CN=Section RSA Domain Validation Secure Ser r CA Validity Not Before: Sep 4 00:00:00 2023 GMT Not After : Aug 3 23:59:59 2024 GMT Subject: CN=vlt.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:90: 72:0f:1a:8a:90:2a:3c:33:1b:33:ed:4e:fd:7c:a9: 93:11:4f:b5:b3:c6:85:c7:29:fe:79:c2:4e:77:a7: a4:45:1d:72:95:2d:ac:e0:2d:63:f8:7b:3c:3d:54: 00:f2:0b:c0:13:00:99:c7:9e:54:fe:39:13:00:24: bc:4e:98:da:49:0b:10:00:77:cd:c6:0b:1b:70: 39:78:09:2f:03:7d:1d:40:f8:b1:34:91:00:a5:89: </pre>					

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

3. 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 we will use cwe.mitre.org website to get the details of the common weaknesses

The screenshot shows the homepage of the CWE (Common Weakness Enumeration) website. The header includes the CWE logo and the text "Common Weakness Enumeration - A Community-Developed List of Software & Hardware Weakness Types". The navigation bar includes links to Home, About, CWE List, Mapping, Top-N Lists, Community, News, and Search. The main content area features a "2023 CWE Top 25 Most Dangerous Software Weaknesses" section, which includes a "Top 25" badge and a "New!" badge. Below this, there is a "CWE List Quick Access" section with a search bar and a "View CWE" button. The "Community Engagement" section lists various groups and boards, including the Hardware CWE Special Interest Group, ICS/OT Special Interest Group, REST API Working Group, User Experience Working Group, and CWE/CAPEC Board. The "CWE News" section lists recent updates, including "Stubborn Weaknesses in the CWE Top 25 (Updated)", "CWE Top 25 Weaknesses Trends from 2019 Through 2023 Now Available", "2023 CWE Top 25 Weaknesses 'On the Cusp' List Now Available", "2023 'CWE Top 25' Now Available!", and "CWE Version 4.12 Now Available".

like we took CVE-2023-31250 from shodan report

Personal HomeTraining | ASPENVitaSource Booksh...P-FolioMITRE ATT&CK®104.107.105.27Nessus Essentials /...Student DashboardLive Cyber Threat...MAP | Kaspersky Cy...312-50v11 Exam Q...

SEARCH CVE LISTCONTINUOUSDATA FEEDSUPDATE A CVE RECORDREQUEST CVE IDS

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.

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

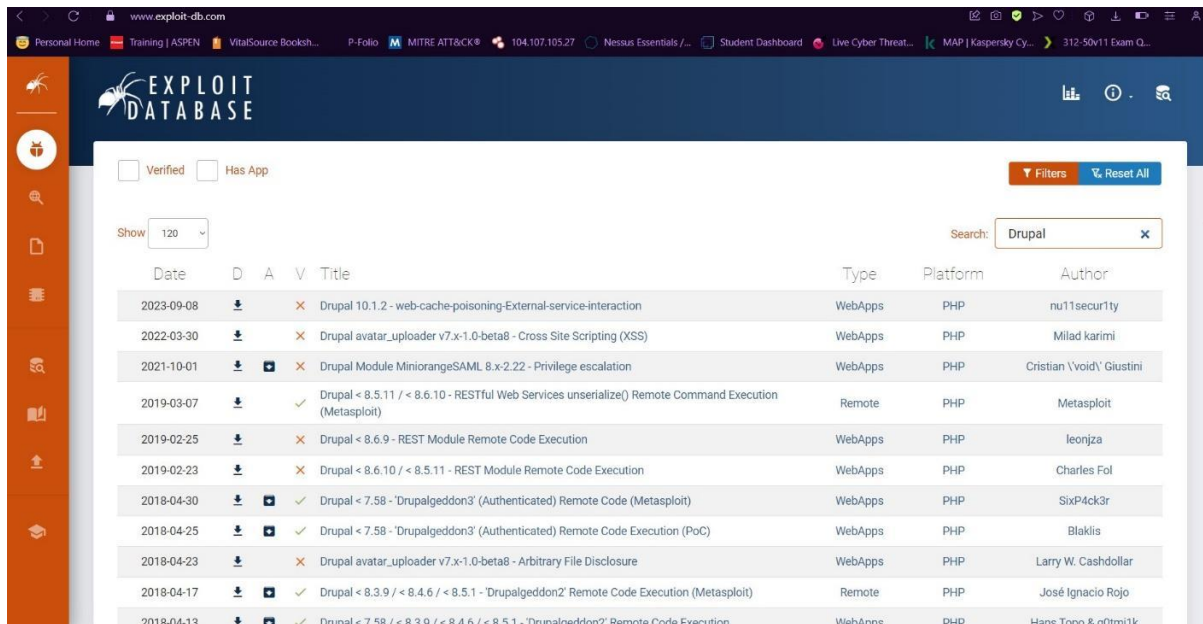
CVSS3 Score: 6.8 - MEDIUM

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

4. 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.



www.exploit-db.com

Personal Home Training | ASPEN VitalSource Booksh... P-Folio MITRE ATT&CK® 104.107.105.27 Nessus Essentials /... Student Dashboard Live Cyber Threat... MAP | Kaspersky Cy... 312-50v11 Exam Q...

EXPLOIT DATABASE

Verified Has App

Show 120

Search: Drupal

Date	D	A	V	Title	Type	Platform	Author
2023-09-08	📄	✗		Drupal 10.1.2 - web-cache-poisoning-External-service-interaction	WebApps	PHP	nu11secr1ty
2022-03-30	📄	✗		Drupal avatar_uploader v7.x-1.0-beta8 - Cross Site Scripting (XSS)	WebApps	PHP	Milad karimi
2021-10-01	📄	📄	✗	Drupal Module MinorangeSAML 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	leonzja
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 & q0tmi1k

here for drupal see how many different public exploits are coming. 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