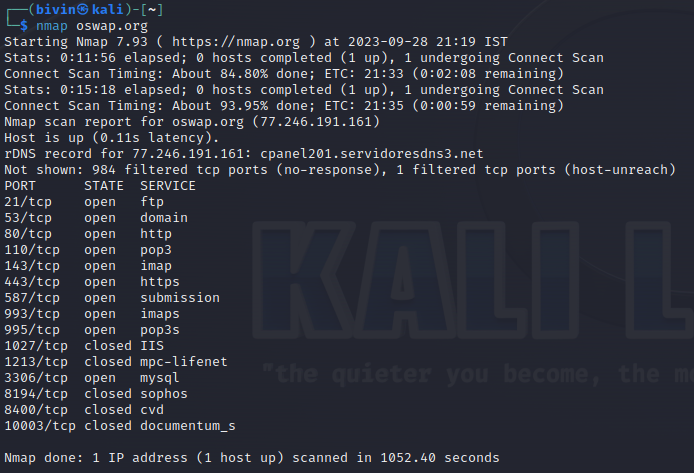
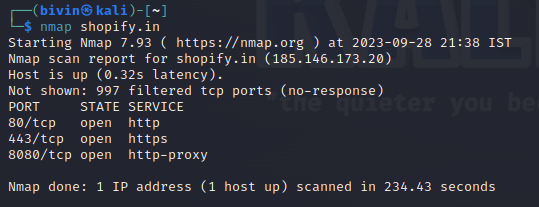
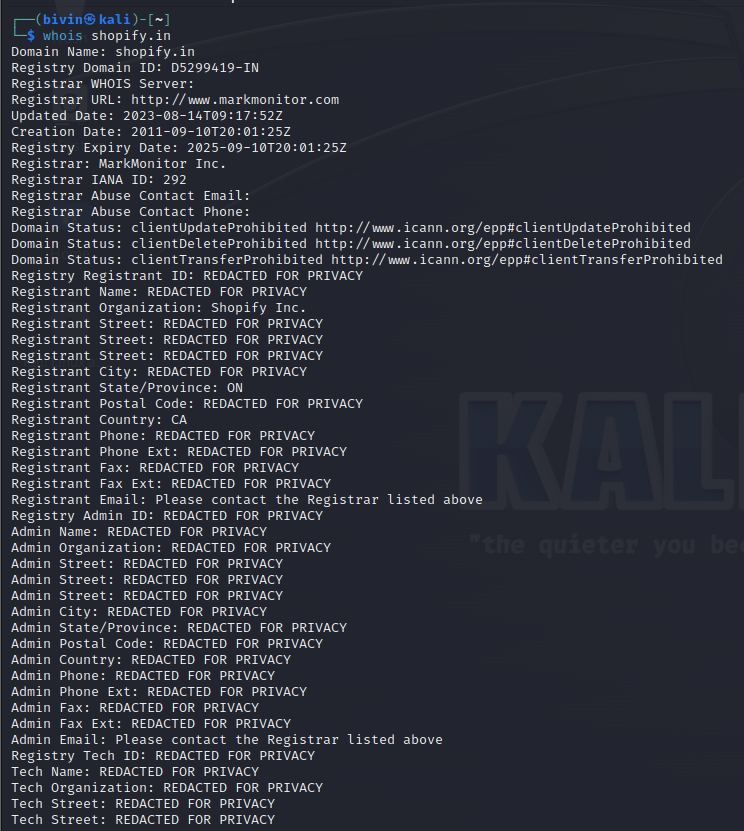
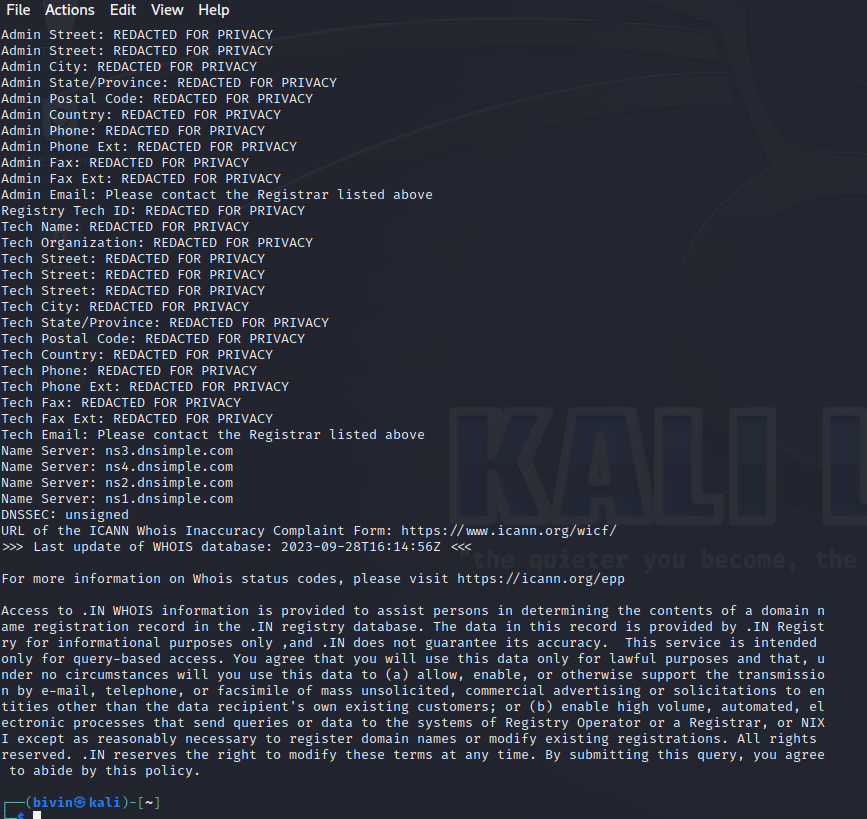
**WEB PENTESTING USING NMAP AND METASPLOIT**





WHOIS





**OUTPUT :**

Name: shopify.in

Domain Name: shopify.in

Registry Domain ID: D5299419-IN

Registrar WHOIS Server:

Registrar URL: <http://www.markmonitor.com>

**Important dates :**

Updated Date: 2023-08-14T09:17:52Z

Creation Date: 2011-09-10T20:01:25Z

Registry Expiry Date: 2025-09-10T20:01:25Z

**Registrar details:**

Registrar: MarkMonitor Inc.

Registrar IANA ID: 292

Registrar Abuse Contact Email:

Registrar Abuse Contact Phone:

**Domain status :**

Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited

Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited

Domain Status: clientTransferProhibited <http://www.icann.org/epp#clientTransferProhibited>

Registrant details :

Registry Registrant ID: REDACTED FOR PRIVACY

Registrant Name: REDACTED FOR PRIVACY

Registrant Organization: Shopify Inc.

Registrant Street: REDACTED FOR PRIVACY

Registrant Street: REDACTED FOR PRIVACY

Registrant Street: REDACTED FOR PRIVACY

Registrant City: REDACTED FOR PRIVACY

Registrant State/Province: ON

Registrant Postal Code: REDACTED FOR PRIVACY

Registrant Country: CA

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

Admin details :

Admin Name: REDACTED FOR PRIVACY

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

Tech details:

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 details :

Name Server: ns3.dnsimple.com

Name Server: ns4.dnsimple.com

Name Server: ns2.dnsimple.com

Name Server: ns1.dnsimple.com

DNSSEC: unsigned

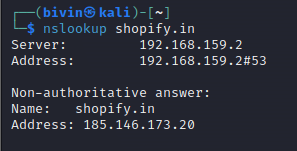
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/

>>> Last update of WHOIS database: 2023-09-28T16:14:56Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

SUMMARY:Domain: shopify.in  
- Creation Date: September 10, 2011  
- Registrar: MarkMonitor Inc.  
- Registrant: Shopify Inc. (based in Canada)  
- Updated Date: August 15, 2021  
- Domain Status: clientDeleteProhibited, clientTransferProhibited, clientUpdateProhibited  
- Name Servers: ns1.dnsimple.com, ns2.dnsimple.com, ns3.dnsimple.com, ns4.dnsimple.com  
-specific contact details have been redacted for privacy reasons. The domain is associated with  
Shopify Inc., a company that offers e-commerce solutions.

**NSLOOKUP**



OUTPUT :

Server: 192.168.159.2

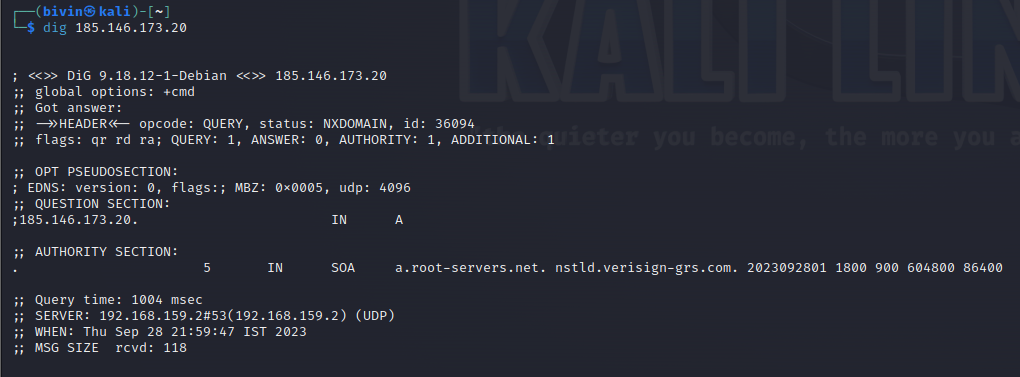
Address: 192.168.159.2#53

Non-authoritative answer:

Name: shopify.in

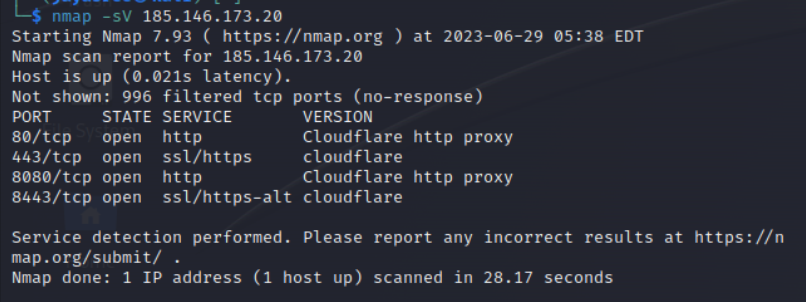
Address: 185.146.173.20

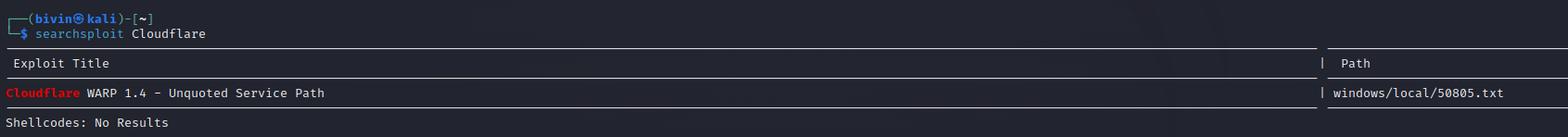
the command queried the DNS server at IP address 192.168.159.2for the domain "shopify.in". The  
non-authoritative answer states that the corresponding IP address for "shopify.in" is 185.146.173.20

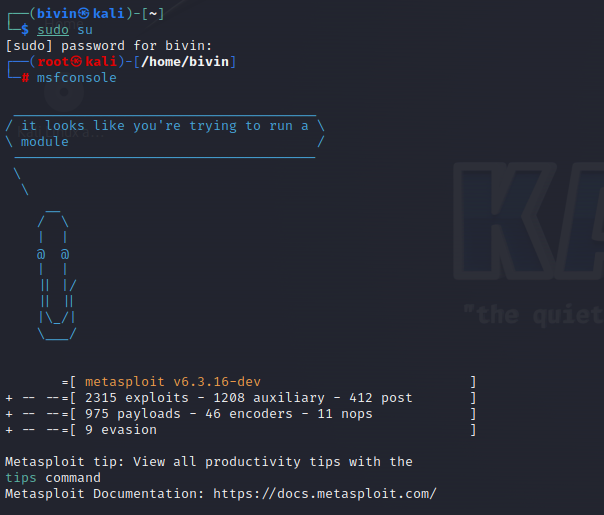
**DIG COMMAND :**

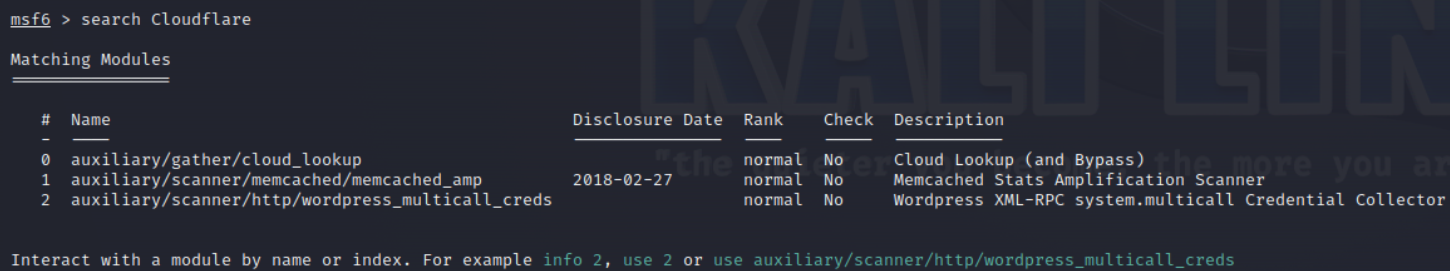
SUMMARY:The DIG command was used to query the IP address 185.146.173.20. The summary of the  
output is as follows:  
- The query was successful (status: NOERROR) and received an authoritative answer.  
- The answer section states that the IP address 185.146.173.20 has an A record associated  
with it.  
- The query was made to the DNS server at IP address 192.168.159.2.  
- The query time was 1004 milliseconds.  
- The response was received on Thursday, September 28,2023 at 21:59:47 IST.  
- The size of the received message was 118 bytes.  
Overall, the output confirms that the IP address 185.146.173.20 has a corresponding A record  
indicating the same IP address

**EXPLOITING:  
MAIN WEBSITE : SHOPIFY**

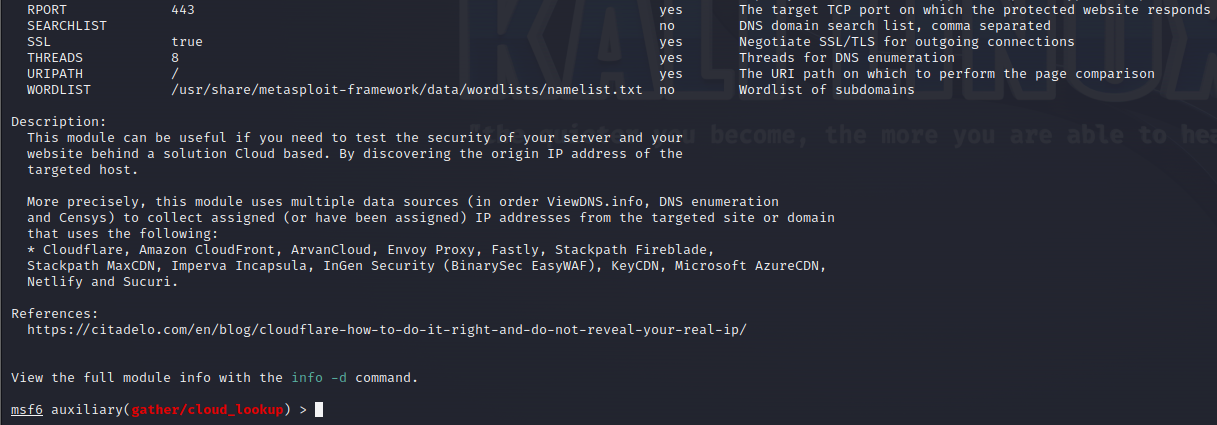


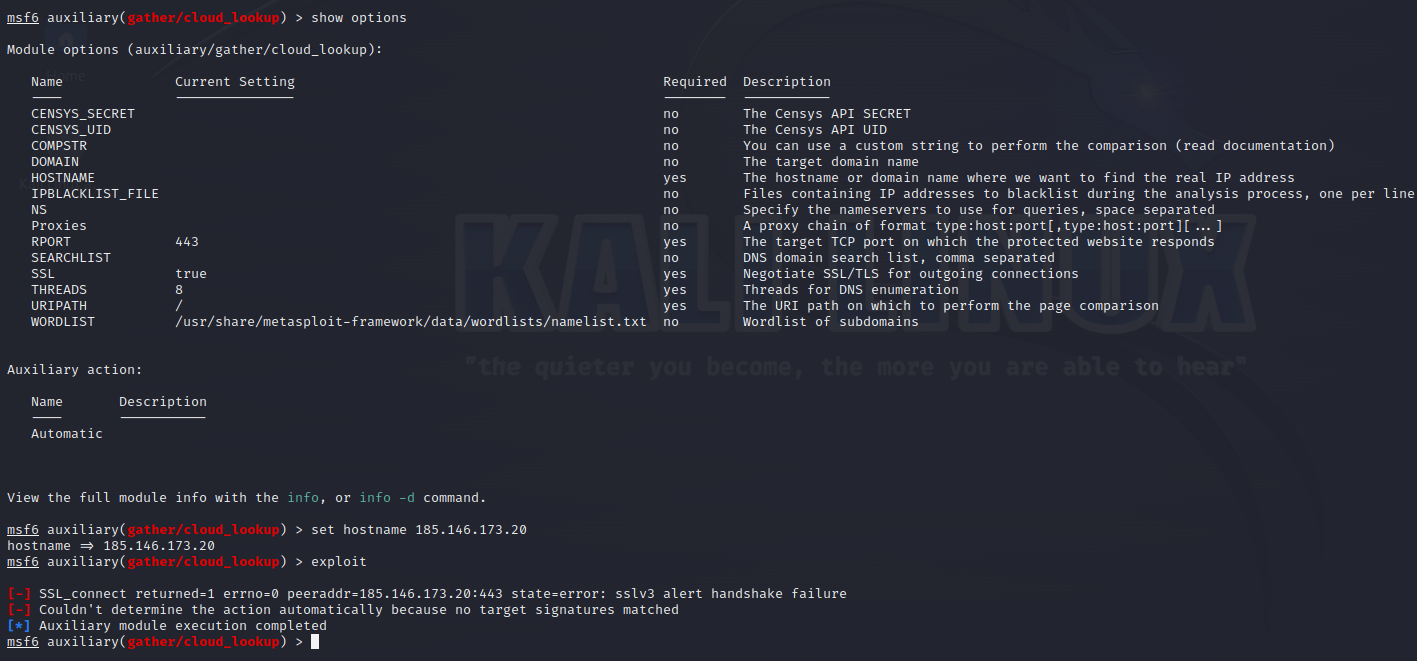




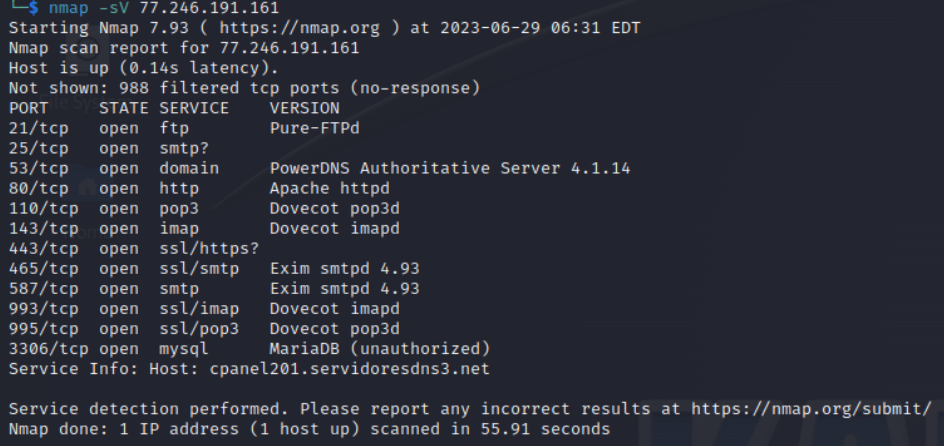


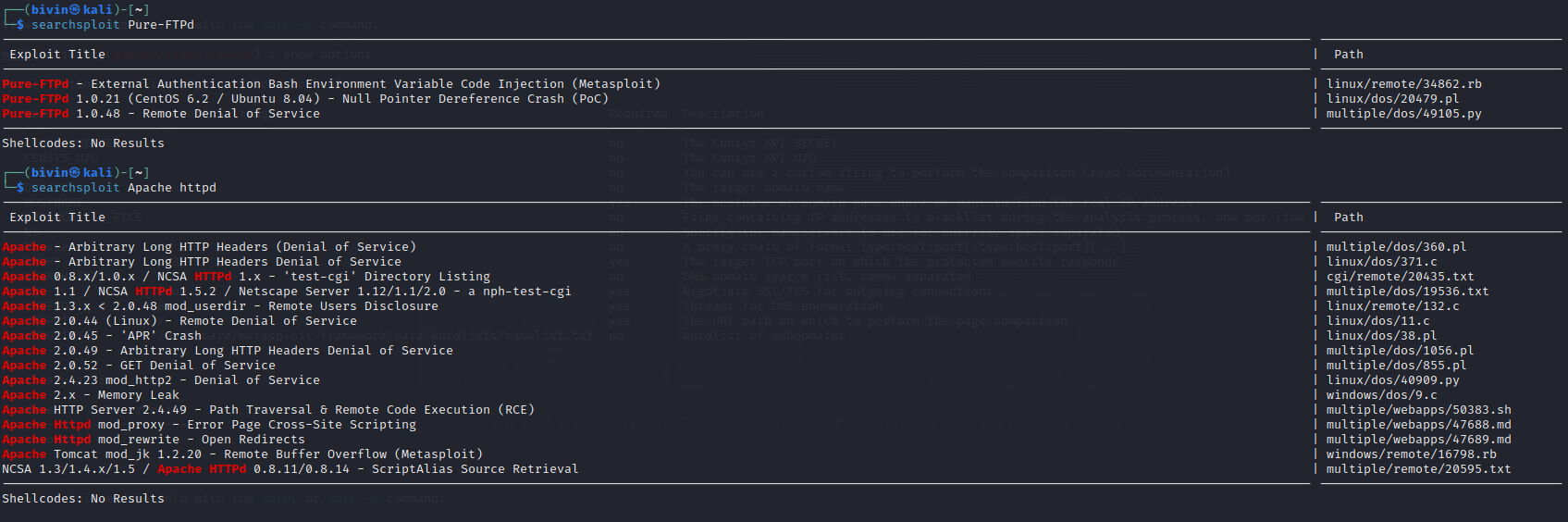




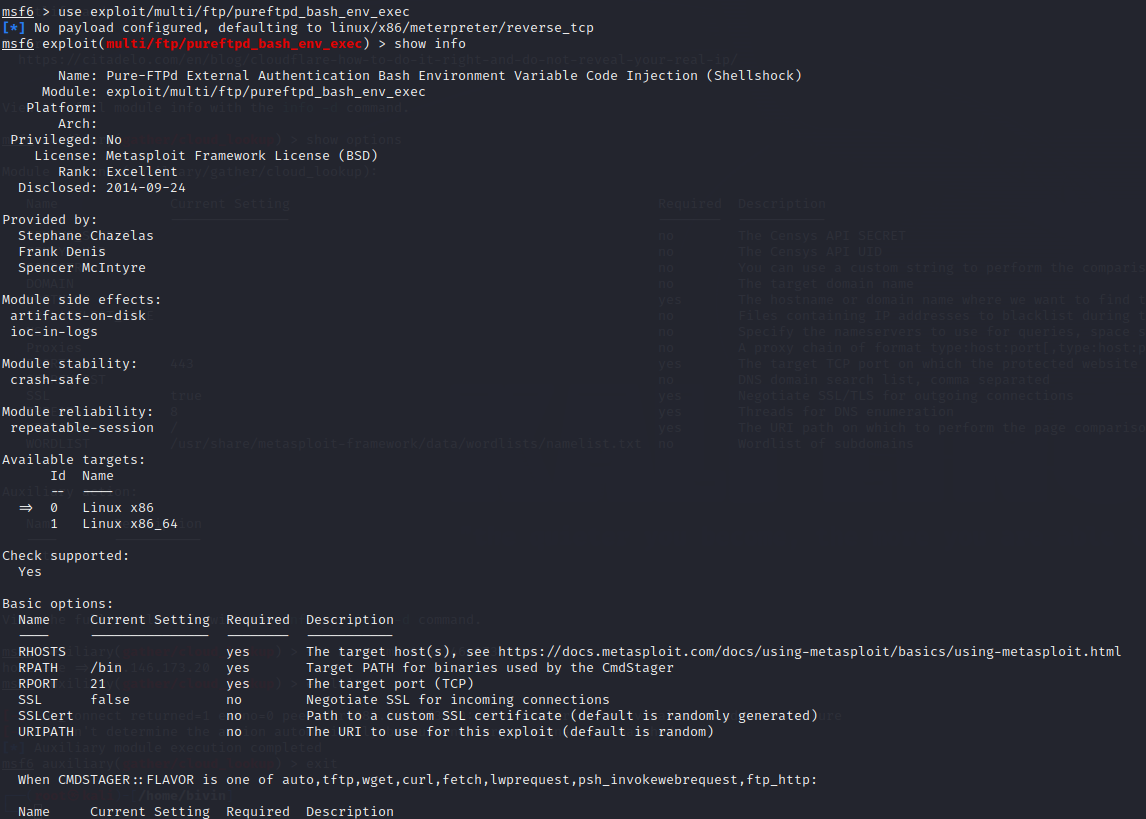


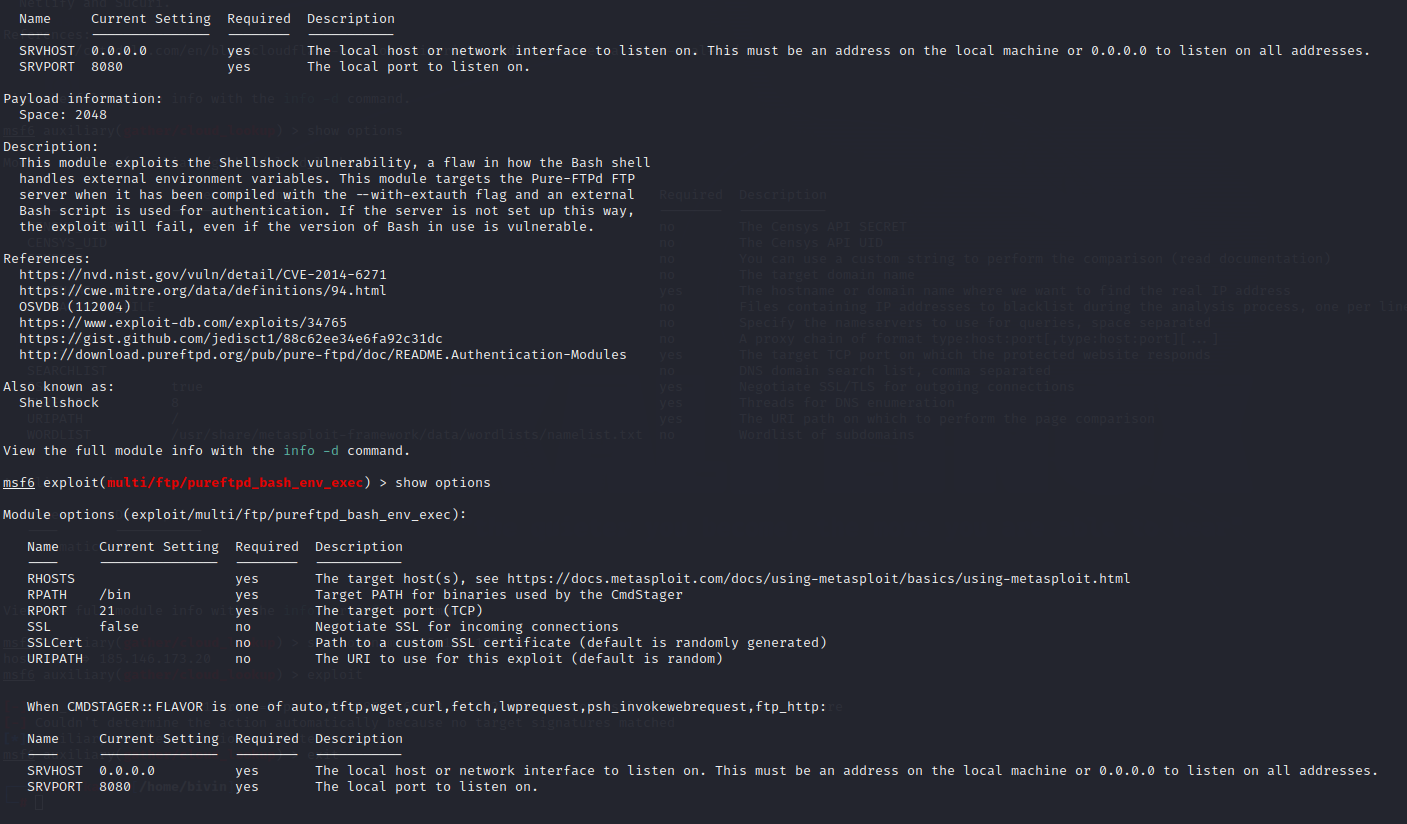
TARGET WEBSITE : OWASP.ORG

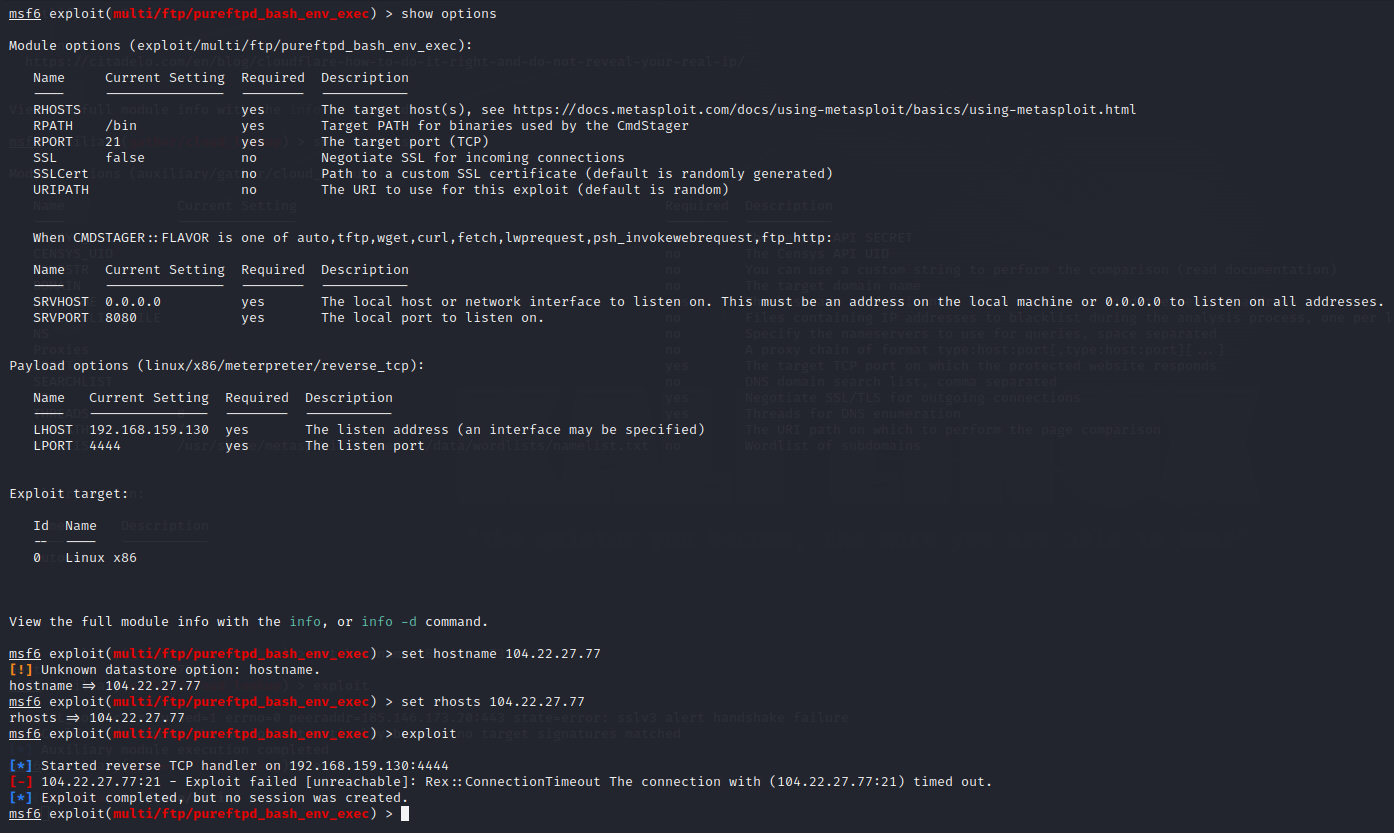




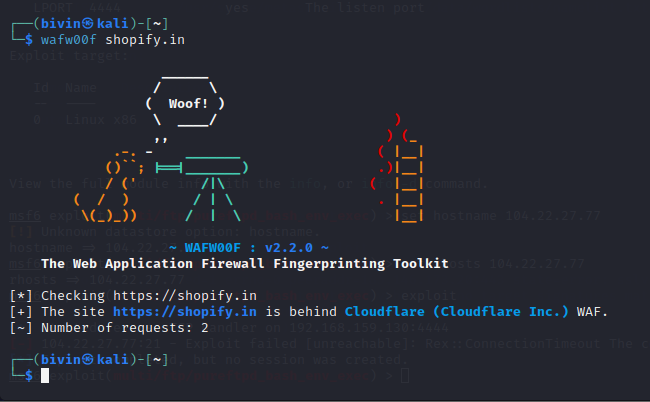






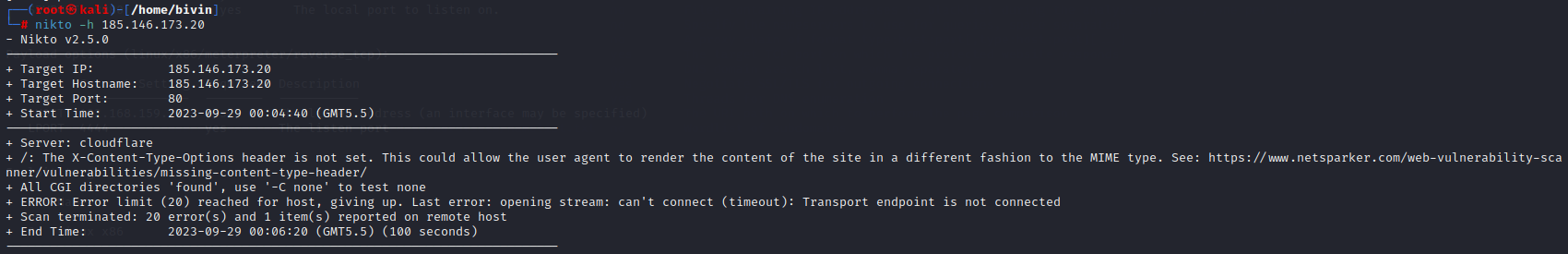


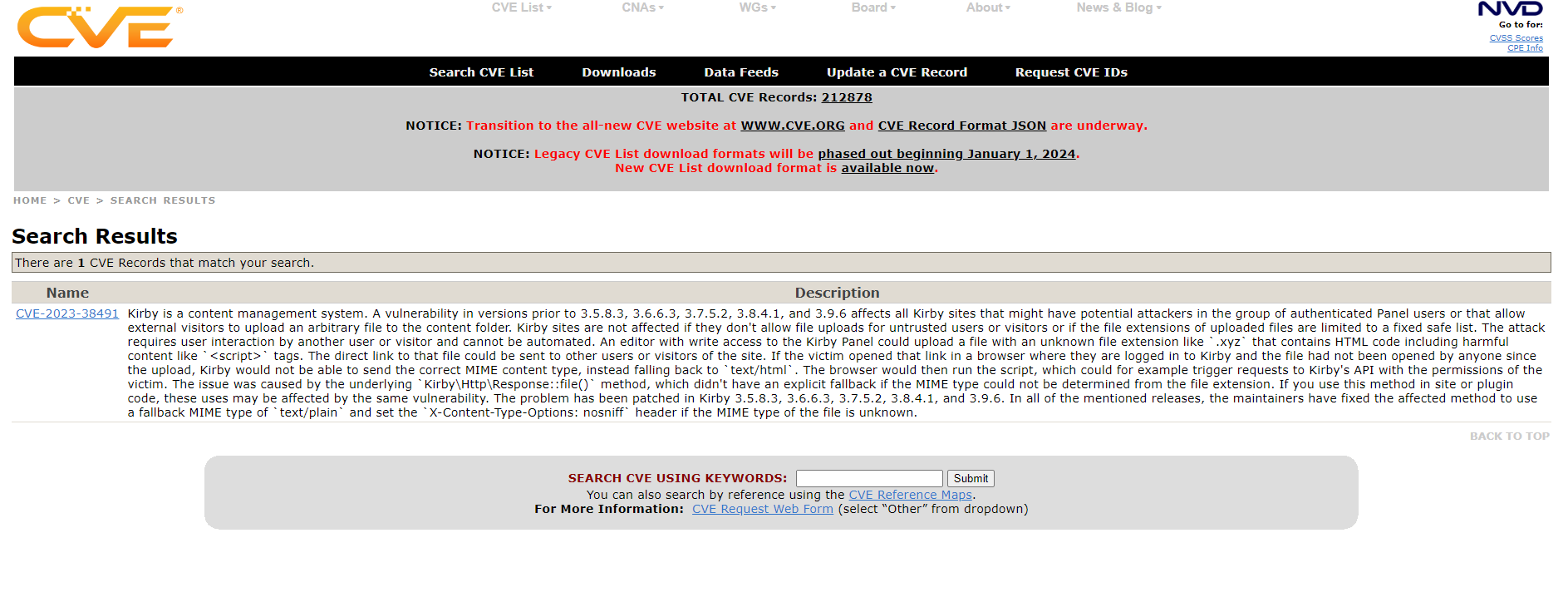
FIREWALL :

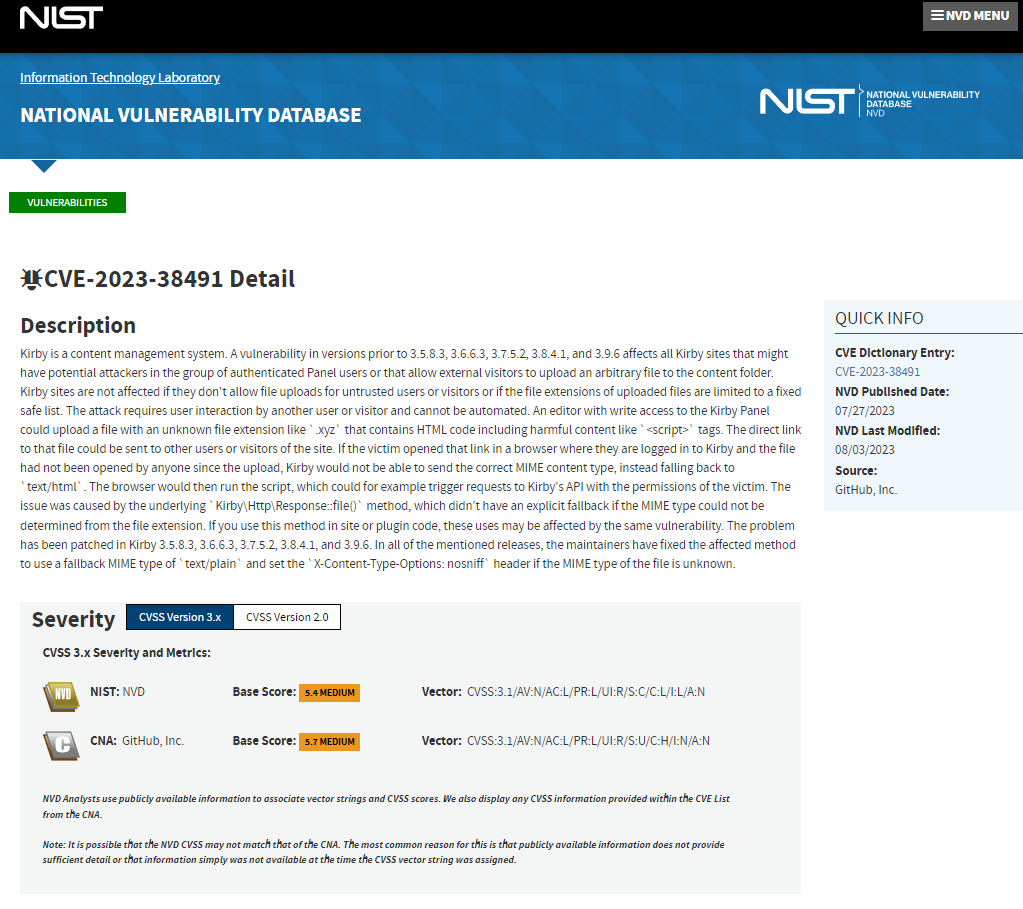


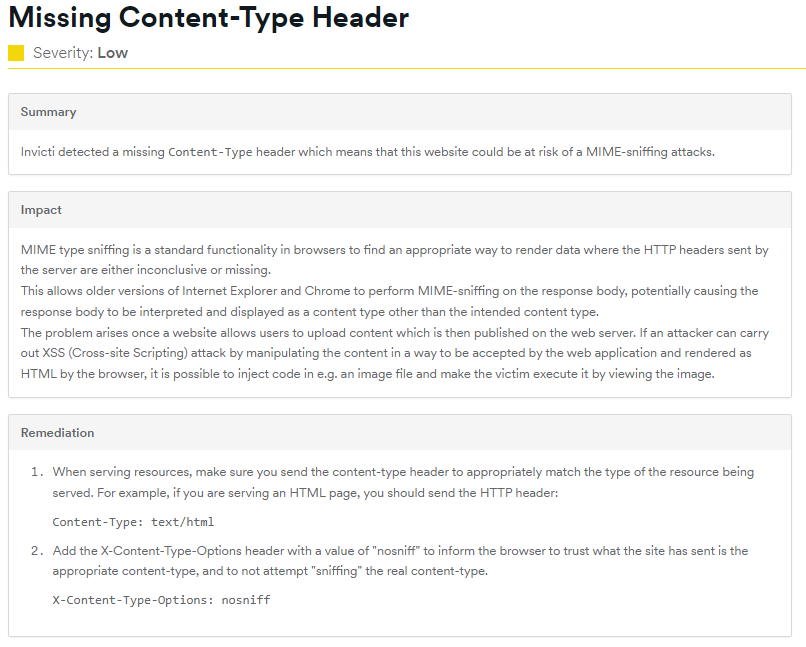
**Vulnerability Assessment  
Tool: nikto**By default, the nikto command performs a comprehensive scan against the target,  
checking for a wide range of potential vulnerabilities and misconfigurations. It examines  
the server's HTTP response headers, performs directory and file enumeration, and tests  
for known vulnerabilities in web applications and server software.  
nikto provides an extensive set of options and configurations that allow you to  
customize the scan according to your needs. Here are a few commonly used options:  
-p <port>: Specifies a specific port to scan (default is port 80).  
-ssl: Enables SSL/TLS scanning on the specified port (default is HTTP).  
-Cgidirs <directories>: Specifies additional directories to treat as CGI directories.  
-evasion <technique>: Uses evasion techniques to avoid detection and IDS/IPS  
systems.  
-id <username:password>: Provides HTTP Basic authentication credentials for  
protected areas.  
It's important to note that nikto should be used responsibly and only on systems you  
have permission to scan

VULNERABILITIES: (FOR SHOPIFY)

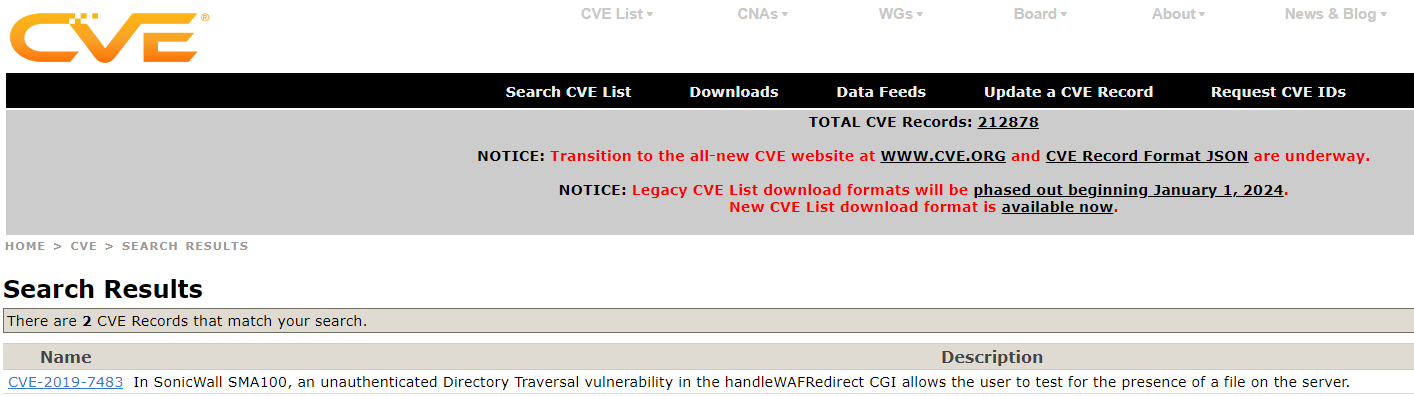
  
1. The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type





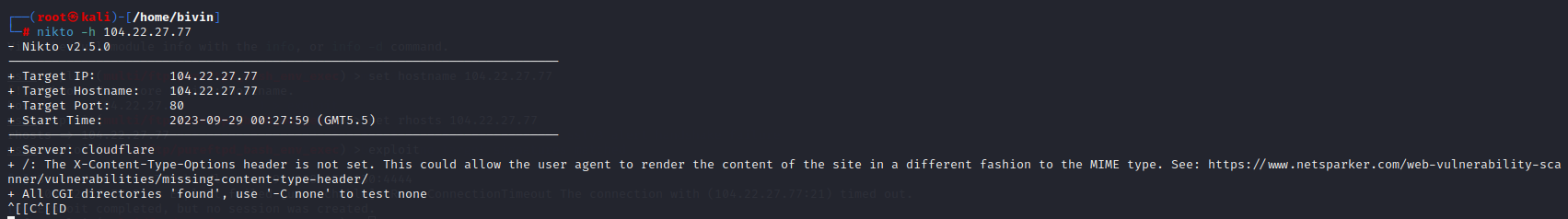


2. All CGI directories 'found', use '-C none' to test none

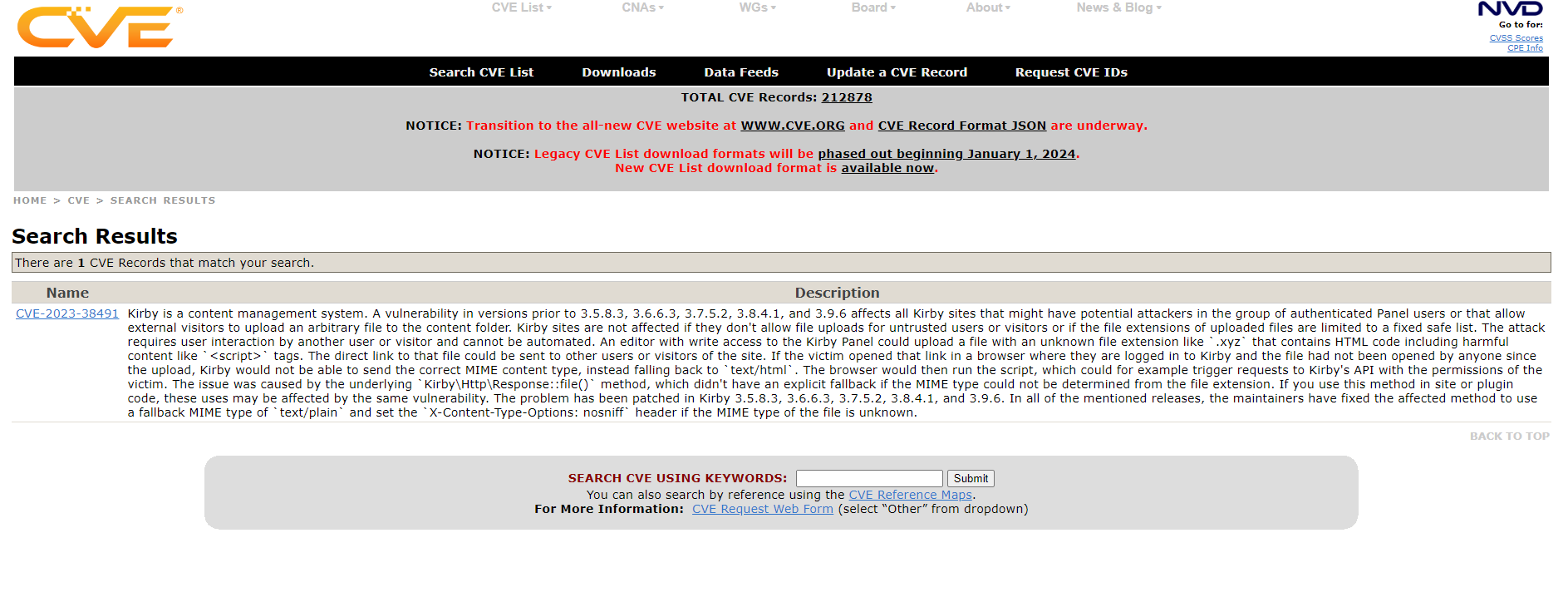


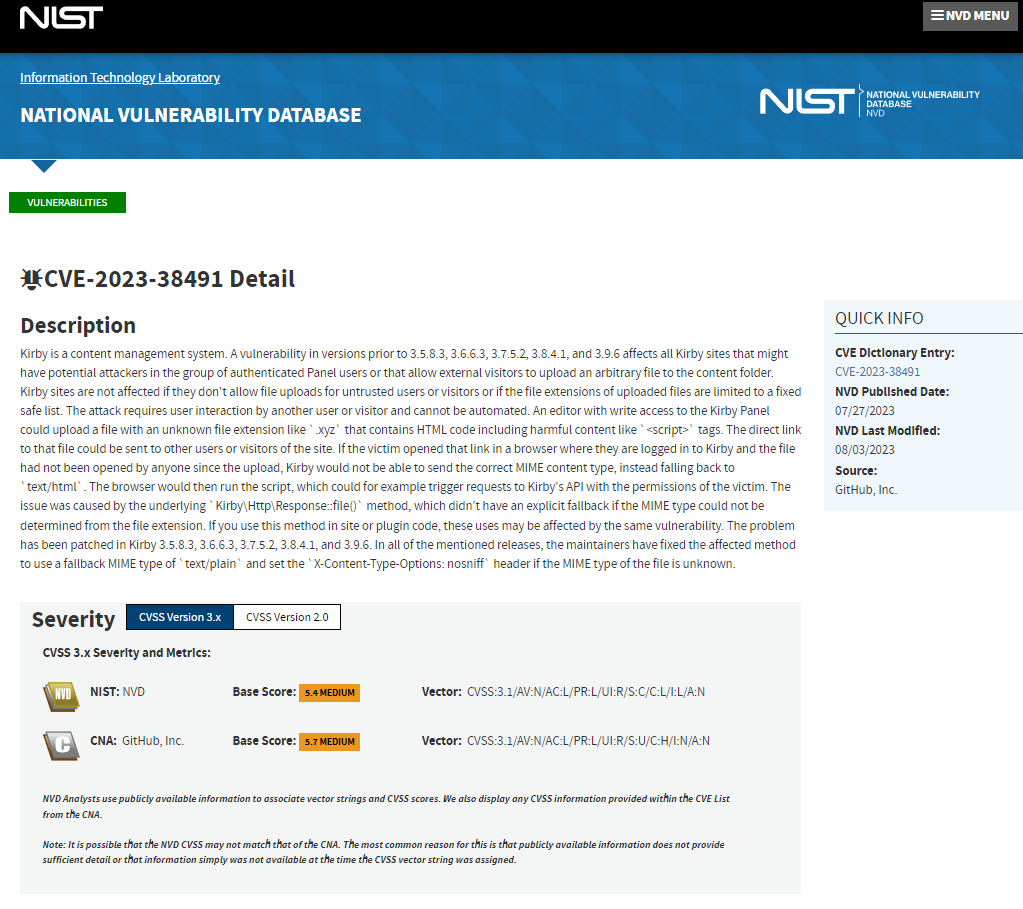


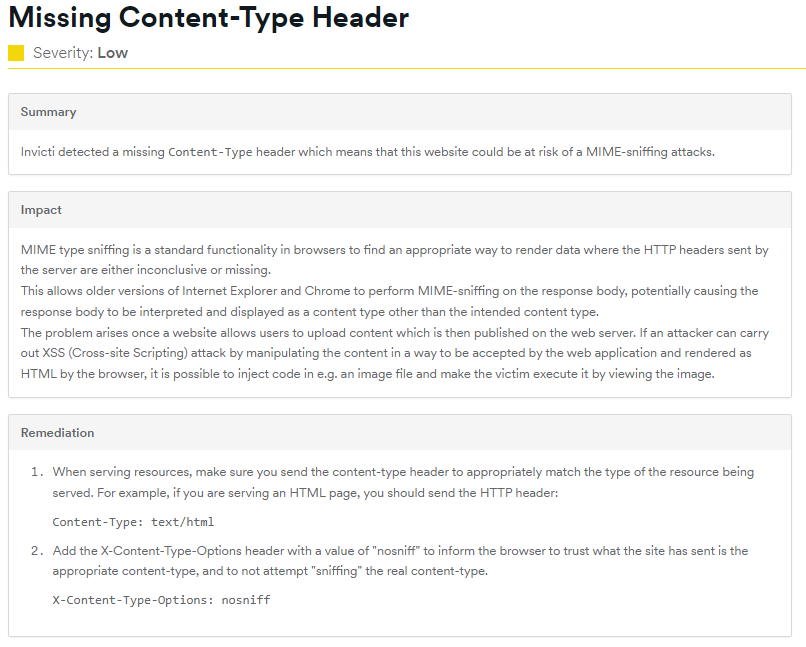
VULNERABILITY SCANING : (FOR OSWAP.ORG)



1. The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type







2. All CGI directories 'found', use '-C none' to test none

