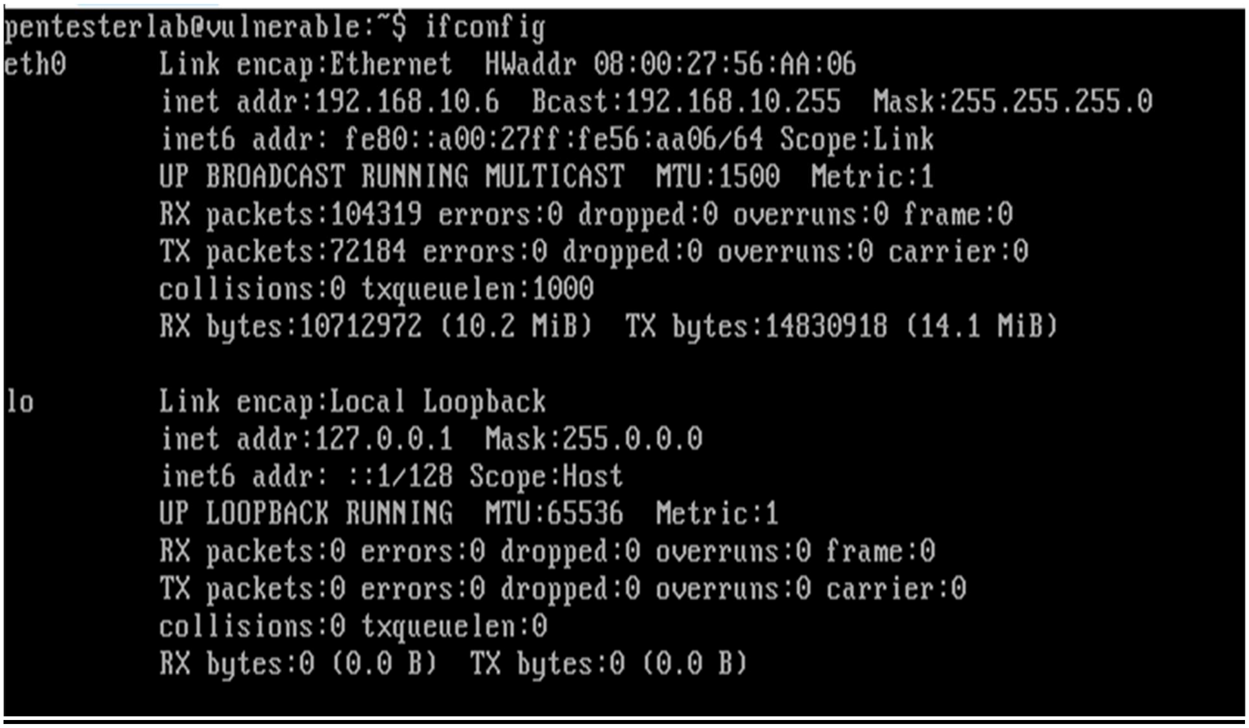
Session_6_Task

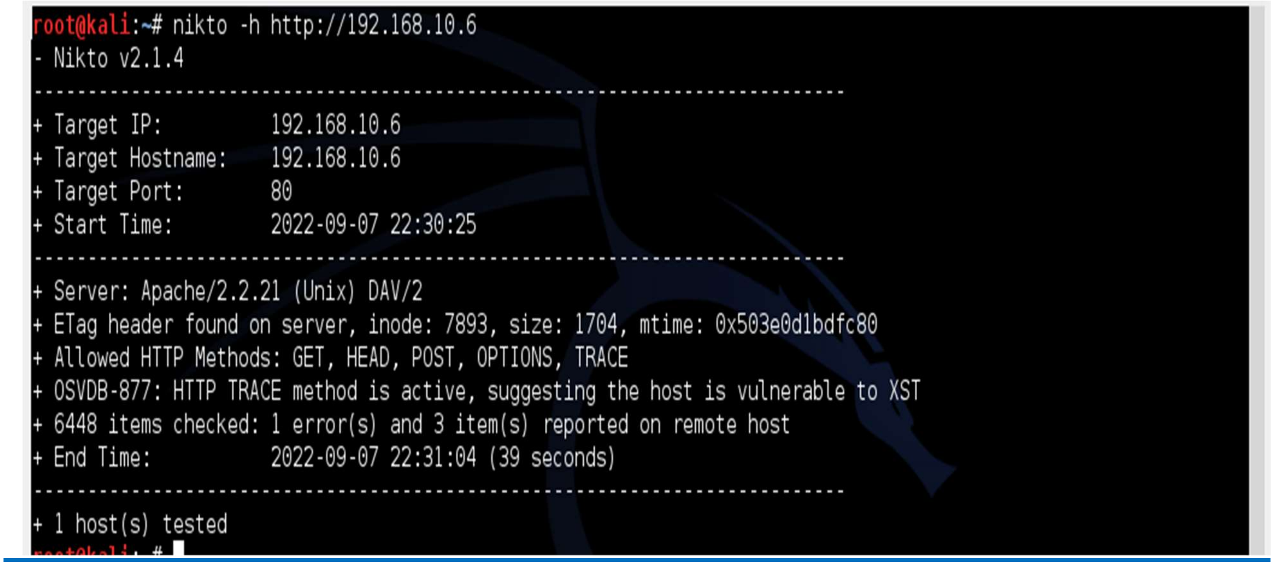
1. CVE Machine ip address(192.168.10.6):



```
pentesterlab@vulnerable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:56:AA:06
          inet addr:192.168.10.6  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe56:aa06/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:104319 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72184 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:10712972 (10.2 MiB)  TX bytes:14830918 (14.1 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2. Scanning Vulnerability using Nikto:

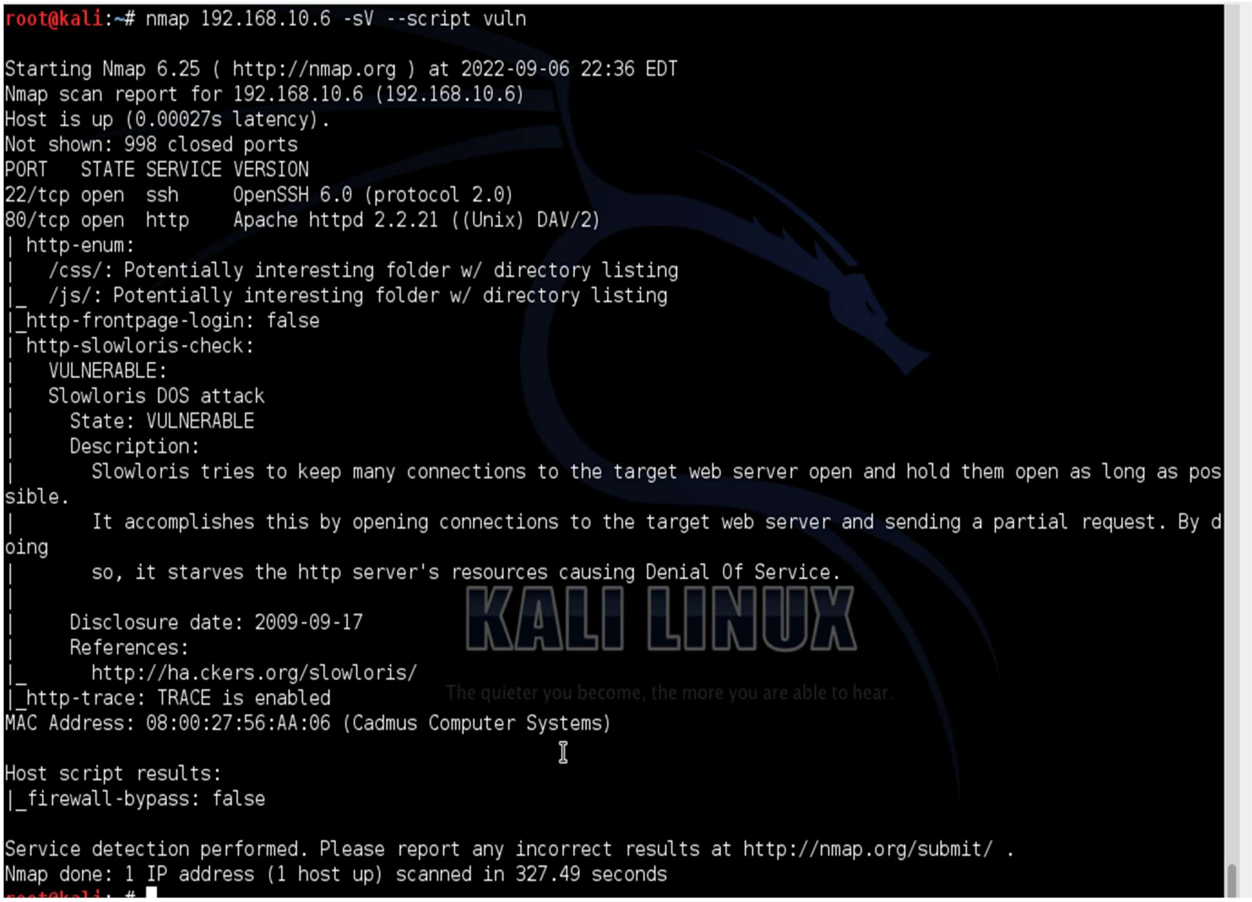
→Exist suggestion the host is vulnerable to XST



```
root@kali:~# nikto -h http://192.168.10.6
- Nikto v2.1.4
---------------------------------------------------------------------------
+ Target IP:          192.168.10.6
+ Target Hostname:    192.168.10.6
+ Target Port:        80
+ Start Time:         2022-09-07 22:30:25
---------------------------------------------------------------------------
+ Server: Apache/2.2.21 (Unix) DAV/2
+ ETag header found on server, inode: 7893, size: 1704, mtime: 0x503e0d1bdfc80
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ 6448 items checked: 1 error(s) and 3 item(s) reported on remote host
+ End Time:           2022-09-07 22:31:04 (39 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@kali:~# 
```

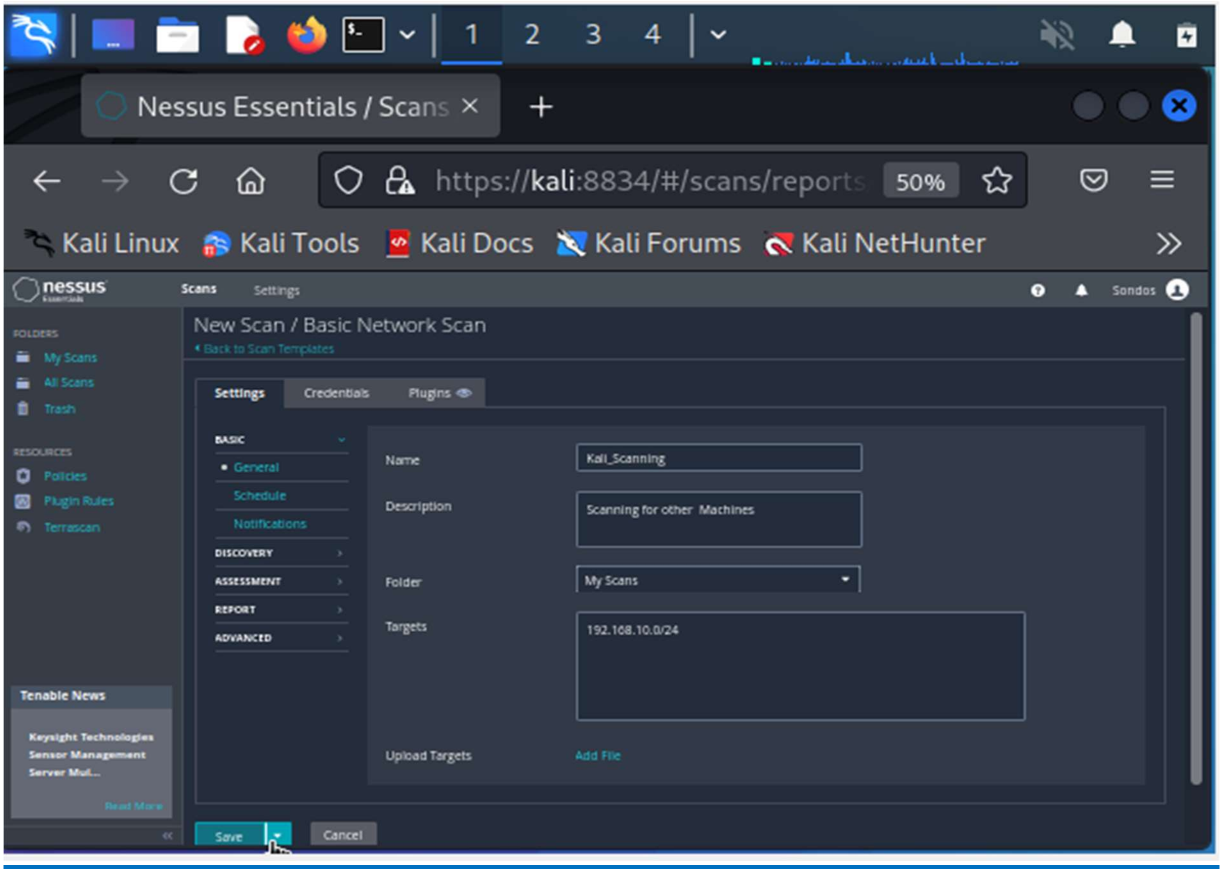
3. Scanning Vulnerability using Nmap:

→Exist Slowloris Dos attack.



```
root@kali:~# nmap 192.168.10.6 -sV --script vuln

Starting Nmap 6.25 ( http://nmap.org ) at 2022-09-06 22:36 EDT
Nmap scan report for 192.168.10.6 (192.168.10.6)
Host is up (0.00027s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.21 ((Unix) DAV/2)
| http-enum:
|   /css/: Potentially interesting folder w/ directory listing
|_  /js/: Potentially interesting folder w/ directory listing
|_http-frontpage-login: false
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: VULNERABLE
|     Description:
|       Slowloris tries to keep many connections to the target web server open and hold them open as long as pos
sible.
|       It accomplishes this by opening connections to the target web server and sending a partial request. By d
oing
|       so, it starves the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|_      http://ha.ckers.org/slowloris/
|_http-trace: TRACE is enabled
MAC Address: 08:00:27:56:AA:06 (Cadmus Computer Systems)

Host script results:
|_firewall-bypass: false

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 327.49 seconds
root@kali:~# 
```

4. Use Nessus to make scan:



https://kali:8834/#/scans/reports 50%

New Scan / Basic Network Scan

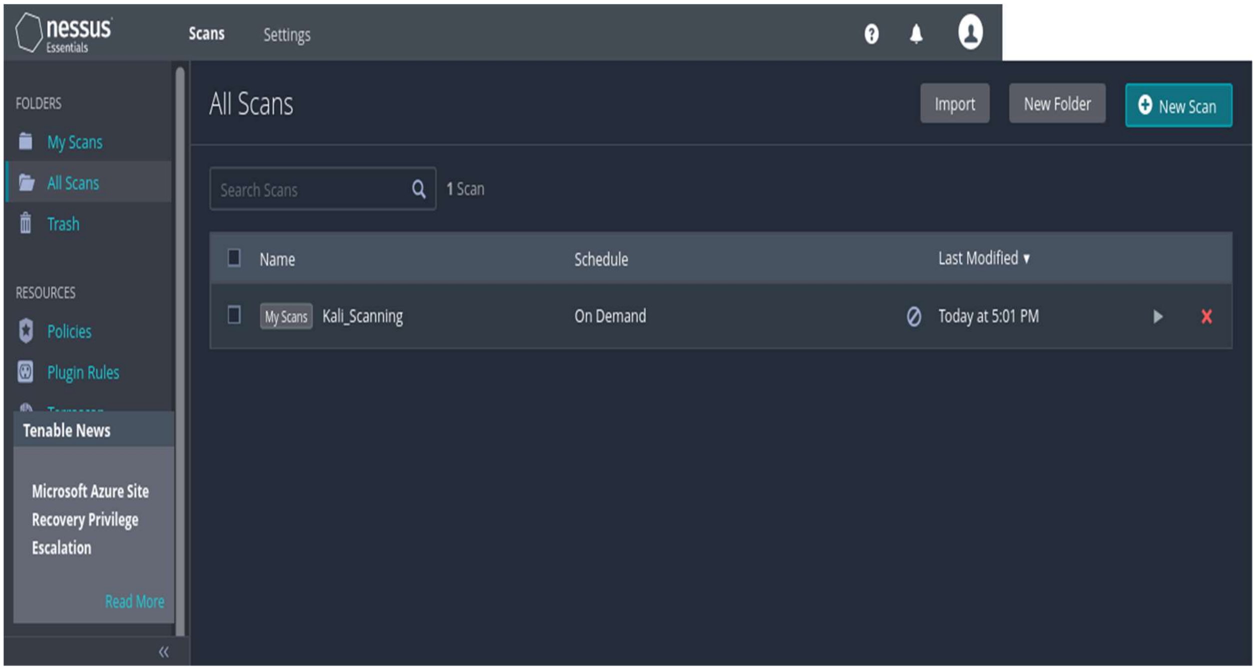
‹ Back to Scan Templates

Name: Kali_Scanning

Description: Scanning for other Machines

Folder: My Scans

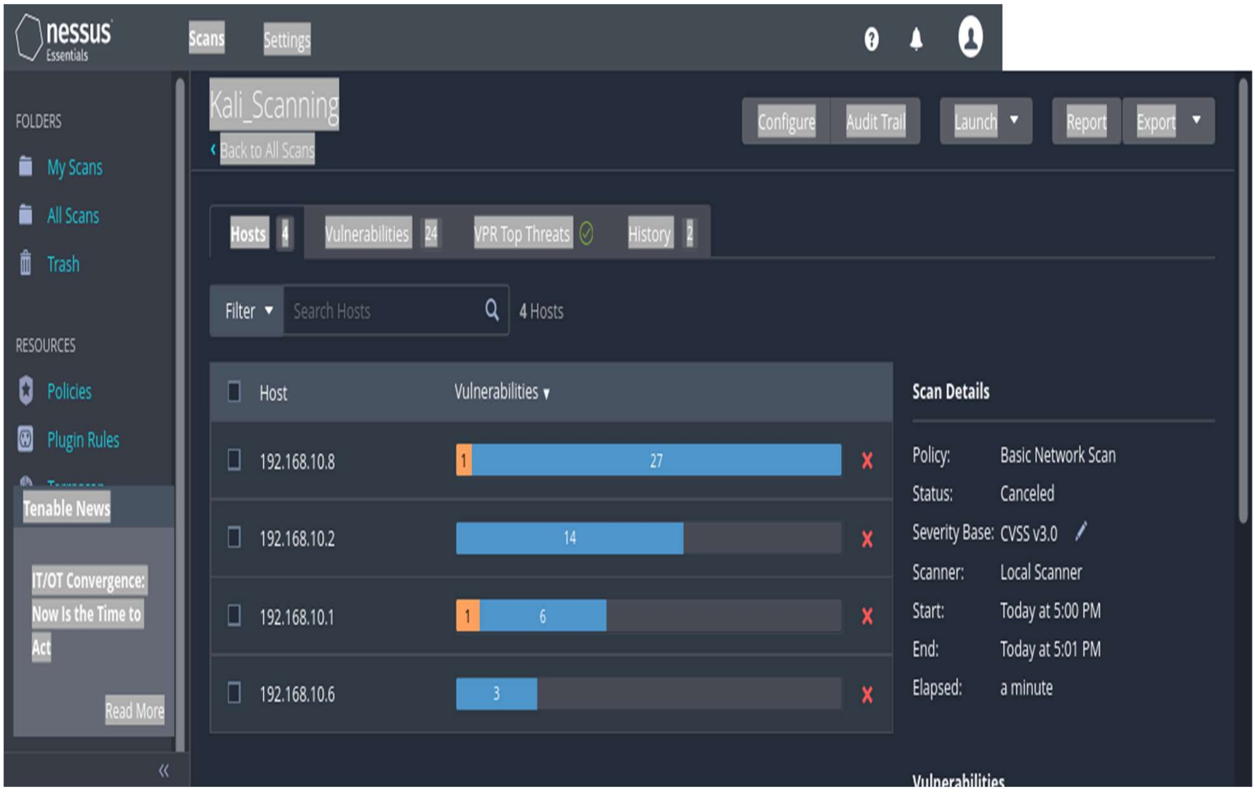
Targets: 192.168.10.0/24



All Scans

1 Scan

Name	Schedule	Last Modified ▾
My Scans Kali_Scanning	On Demand	Today at 5:01 PM



Kali_Scanning

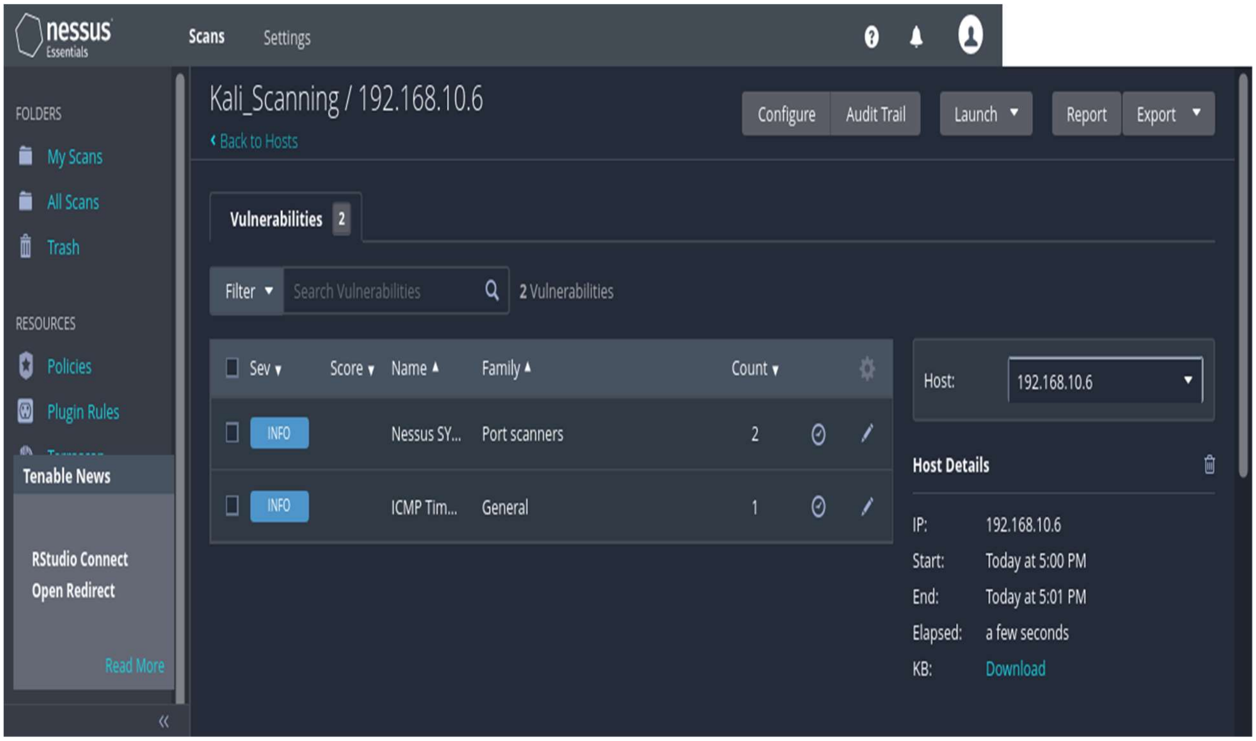
‹ Back to All Scans

4 Hosts

Host	Vulnerabilities
192.168.10.8	1 27
192.168.10.2	14
192.168.10.1	1 6
192.168.10.6	3

Scan Details

Policy: Basic Network Scan
Status: Canceled
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 5:00 PM
End: Today at 5:01 PM
Elapsed: a minute



Kali_Scanning / 192.168.10.6

‹ Back to Hosts

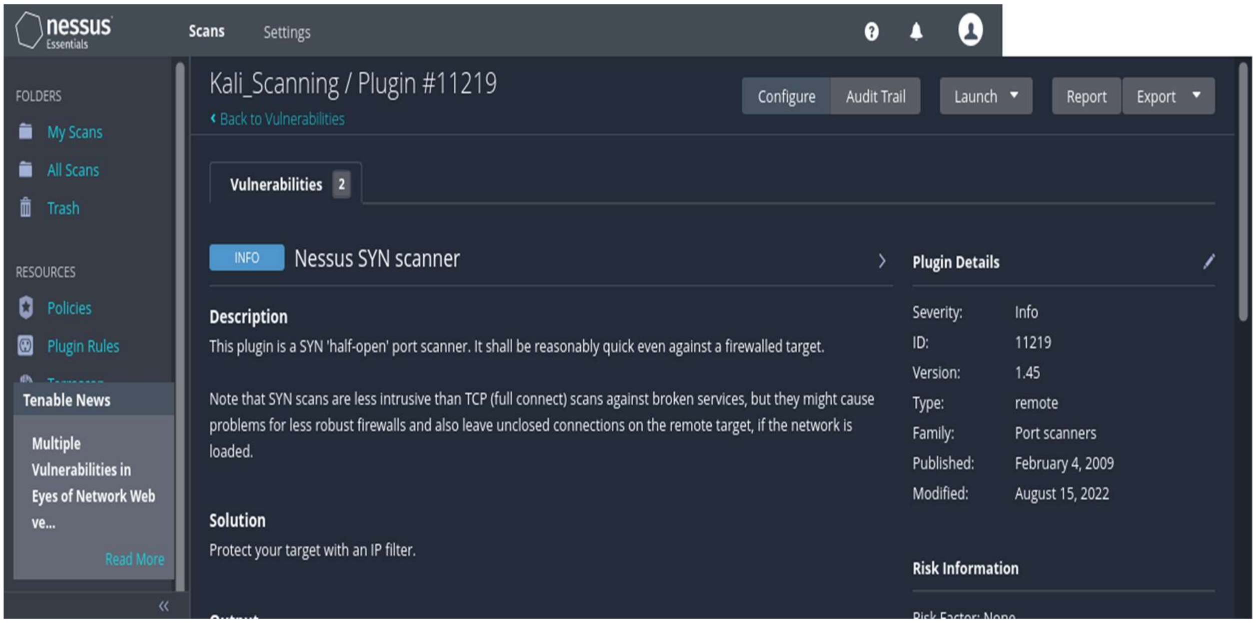
2 Vulnerabilities

Sev	Score	Name	Family	Count
INFO		Nessus SY...	Port scanners	2
INFO		ICMP Tim...	General	1

Host: 192.168.10.6

Host Details

IP: 192.168.10.6
Start: Today at 5:00 PM
End: Today at 5:01 PM
Elapsed: a few seconds
KB: Download



Kali_Scanning / Plugin #11219

‹ Back to Vulnerabilities

Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Plugin Details

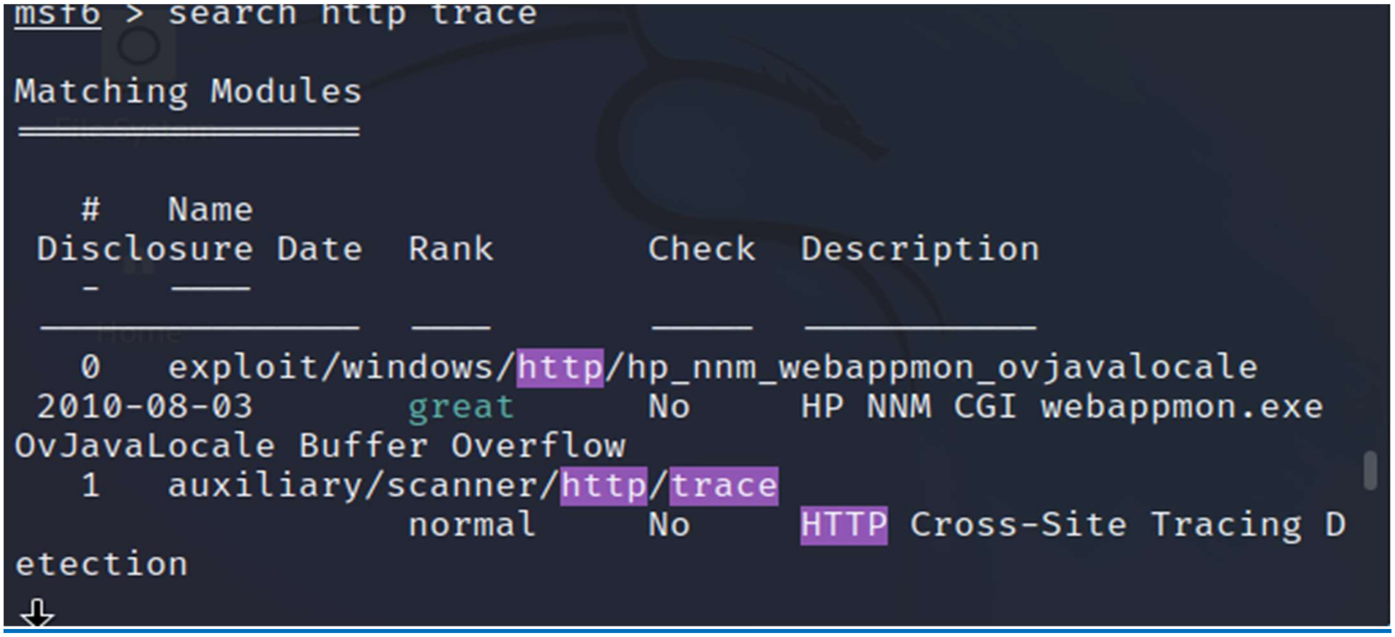
Severity:	Info
ID:	11219
Version:	1.45
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	August 15, 2022

Risk Information

Risk Factor: None

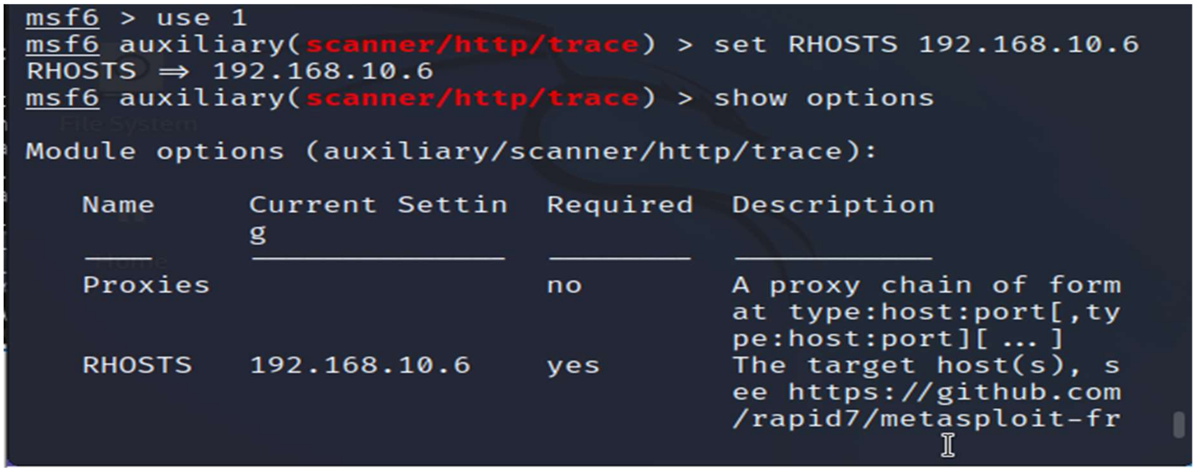
5. Use Kali Linuix msfConsole to make http trace that appear in Scanning Vulnerability using Nikto:

- search for trace in msfconsole.

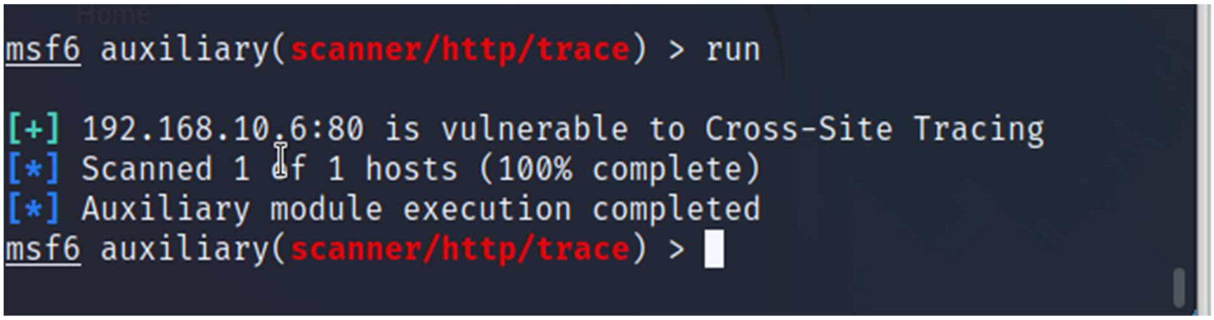


```
msf6 > search http trace

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


   #   Name
 Disclosure Date  Rank       Check  Description
   -   ----
 ---------------  ----       -----  -----------
   0   exploit/windows/http/hp_nnm_webappmon_ovjavalocale
 2010-08-03       great      No     HP NNM CGI webappmon.exe
OvJavaLocale Buffer Overflow
   1   auxiliary/scanner/http/trace
                  normal     No     HTTP Cross-Site Tracing D
etection
```

- use first (auxiliary/scanner/http/trace) and change RHOST to (192.168.10.6) then run.



```
msf6 > use 1
msf6 auxiliary(scanner/http/trace) > set RHOSTS 192.168.10.6
RHOSTS ⇒ 192.168.10.6
msf6 auxiliary(scanner/http/trace) > show options

Module options (auxiliary/scanner/http/trace):

   Name      Current Settin  Required  Description
             g
   ----      --------------  --------  -----------
   Proxies                   no        A proxy chain of form
                                       at type:host:port[,ty
                                       pe:host:port][ ... ]
   RHOSTS    192.168.10.6    yes       The target host(s), s
                                       ee https://github.com
                                       /rapid7/metasploit-fr
```



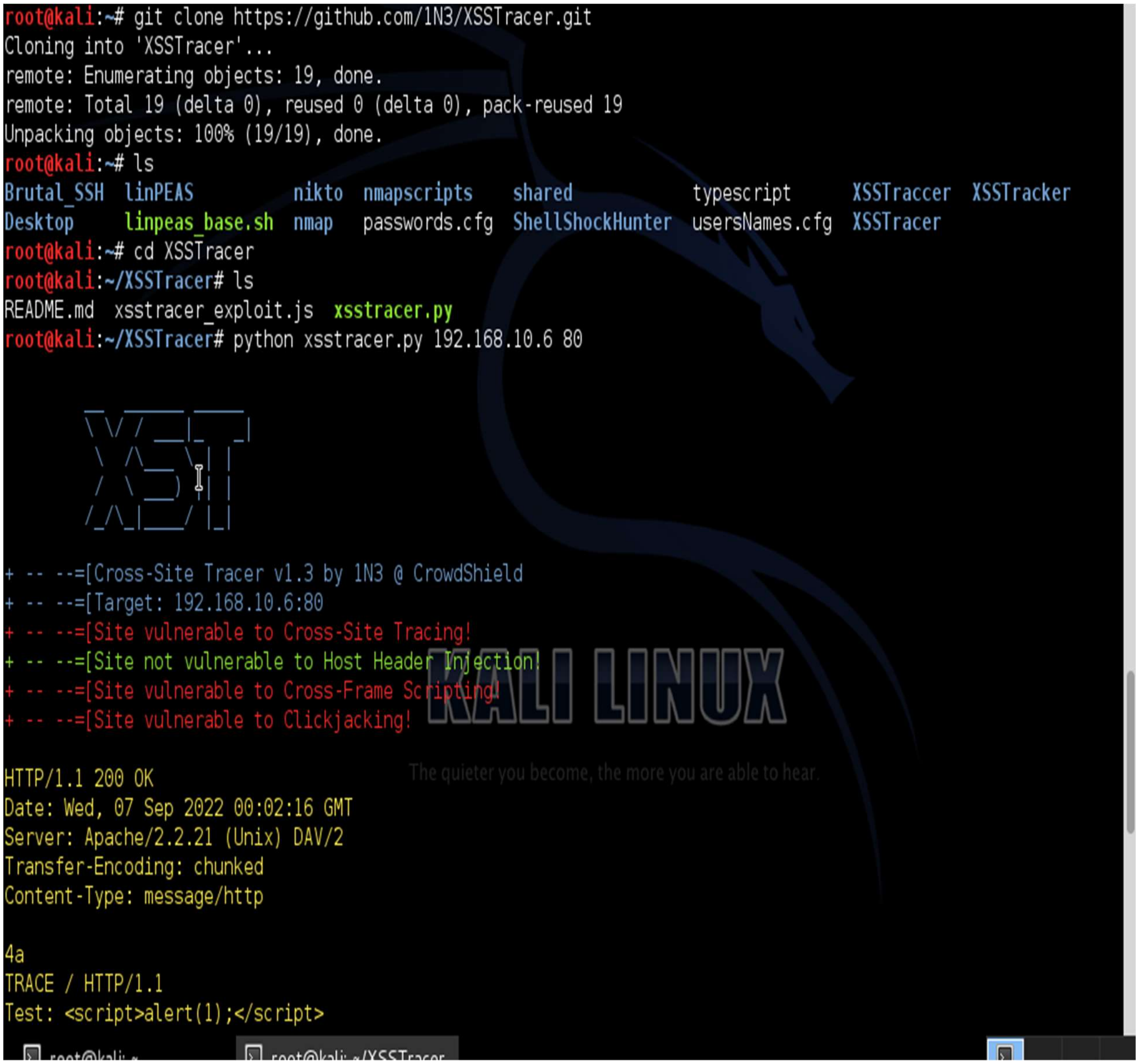
```
msf6 auxiliary(scanner/http/trace) > run

[+] 192.168.10.6:80 is vulnerable to Cross-Site Tracing
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/trace) > 
```

6. Download XSS Tracer to make trace of the Machine (192.168.10.6) (HTTP Trace)

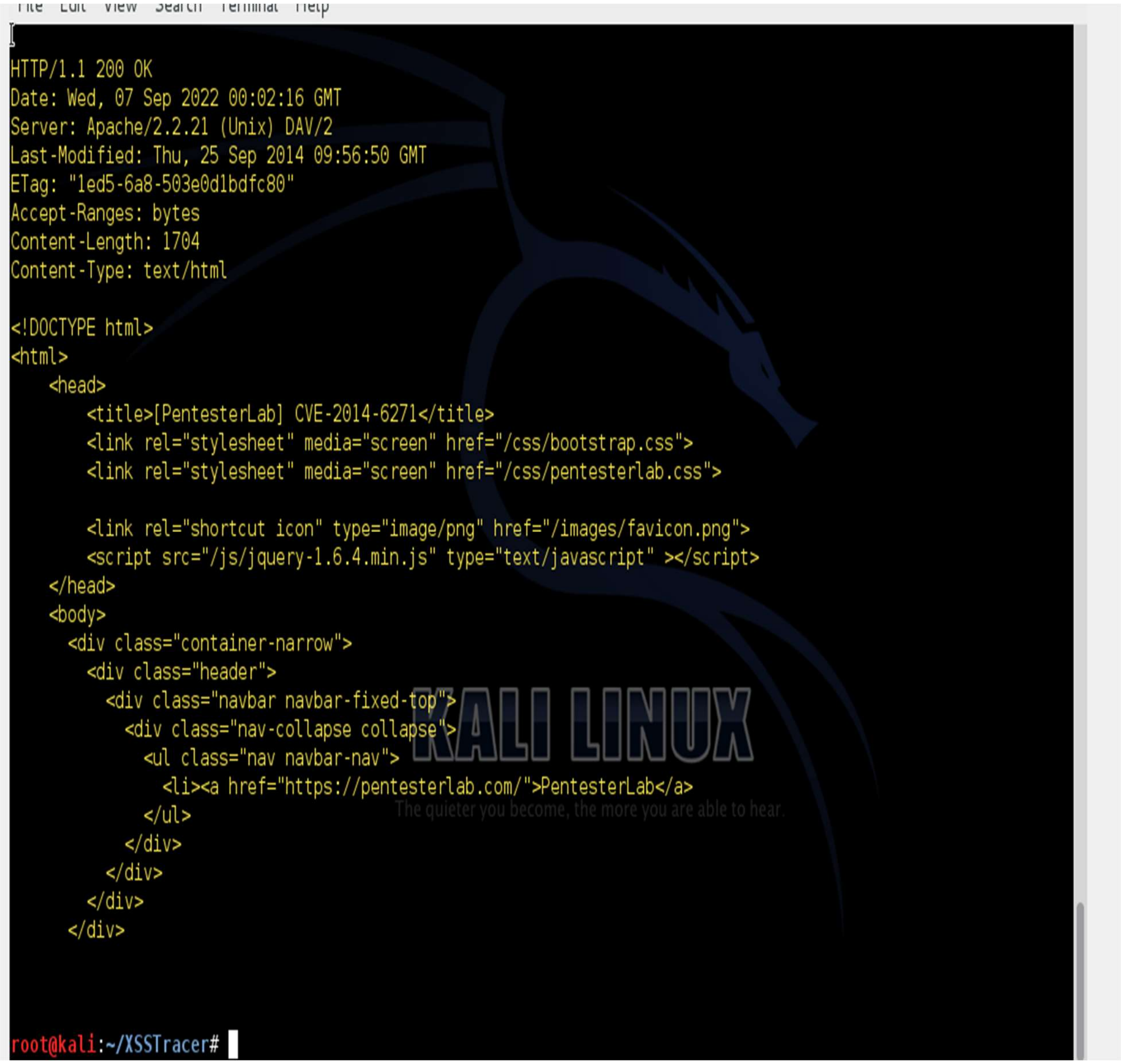
Cross-Site Scripting (XSS) attacks→Search for 192.168.10.6 port 80 .

- Web application vulnerability.
- Code-injunction attack.
- Attacker can use cookies.

So the Attacker will make http trace of the IP Machine with port 80.



```
root@kali:~# git clone https://github.com/1N3/XSSTracer.git
Cloning into 'XSSTracer'...
remote: Enumerating objects: 19, done.
remote: Total 19 (delta 0), reused 0 (delta 0), pack-reused 19
Unpacking objects: 100% (19/19), done.
root@kali:~# ls
Brutal_SSH  linPEAS        nikto  nmapscripts   shared         typescript      XSSTraccer  XSSTracker
Desktop     linpeas_base.sh nmap  passwords.cfg ShellShockHunter usersNames.cfg XSSTracer
root@kali:~# cd XSSTracer
root@kali:~/XSSTracer# ls
README.md  xsstracer_exploit.js  xsstracer.py
root@kali:~/XSSTracer# python xsstracer.py 192.168.10.6 80


    __  ______ _____
    \ \/ / ___|_   _|
     \  /\___ \ | |
     /  \ ___) || |
    /_/\_\____/ |_|

+ -- --=[Cross-Site Tracer v1.3 by 1N3 @ CrowdShield
+ -- --=[Target: 192.168.10.6:80
+ -- --=[Site vulnerable to Cross-Site Tracing!
+ -- --=[Site not vulnerable to Host Header Injection!
+ -- --=[Site vulnerable to Cross-Frame Scripting!
+ -- --=[Site vulnerable to Clickjacking!

HTTP/1.1 200 OK
Date: Wed, 07 Sep 2022 00:02:16 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Transfer-Encoding: chunked
Content-Type: message/http

4a
TRACE / HTTP/1.1
Test: <script>alert(1);</script>
```


File Edit View Search Terminal Help
KALI LINUX
The quieter you become, the more you are able to hear.

```
HTTP/1.1 200 OK
Date: Wed, 07 Sep 2022 00:02:16 GMT
Server: Apache/2.2.21 (Unix) DAV/2
Last-Modified: Thu, 25 Sep 2014 09:56:50 GMT
ETag: "1ed5-6a8-503e0d1bdfc80"
Accept-Ranges: bytes
Content-Length: 1704
Content-Type: text/html

<!DOCTYPE html>
<html>
    <head>
        <title>[PentesterLab] CVE-2014-6271</title>
        <link rel="stylesheet" media="screen" href="/css/bootstrap.css">
        <link rel="stylesheet" media="screen" href="/css/pentesterlab.css">

        <link rel="shortcut icon" type="image/png" href="/images/favicon.png">
        <script src="/js/jquery-1.6.4.min.js" type="text/javascript" ></script>
    </head>
    <body>
      <div class="container-narrow">
        <div class="header">
          <div class="navbar navbar-fixed-top">
            <div class="nav-collapse collapse">
              <ul class="nav navbar-nav">
                <li><a href="https://pentesterlab.com/">PentesterLab</a>
              </ul>
            </div>
          </div>
        </div>
      </div>



root@kali:~/XSSTracer# 
```