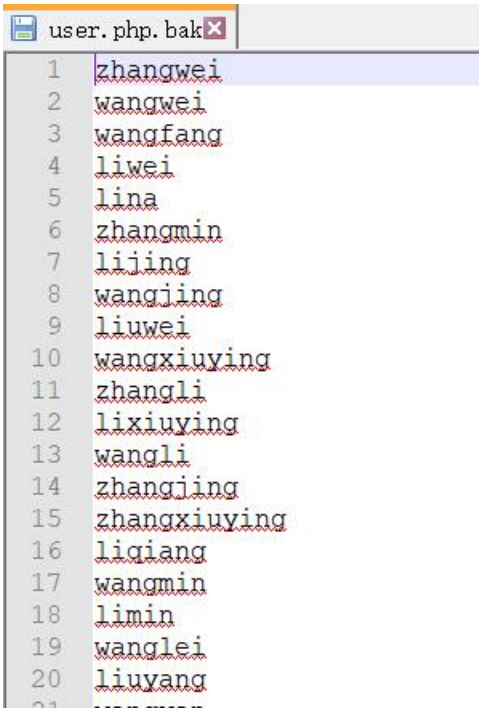
CTFhtml解析php,i春秋——“百度杯”CTF比賽 九月場——123（Apache解析pht,phtml,php3,phps等 php別名）...

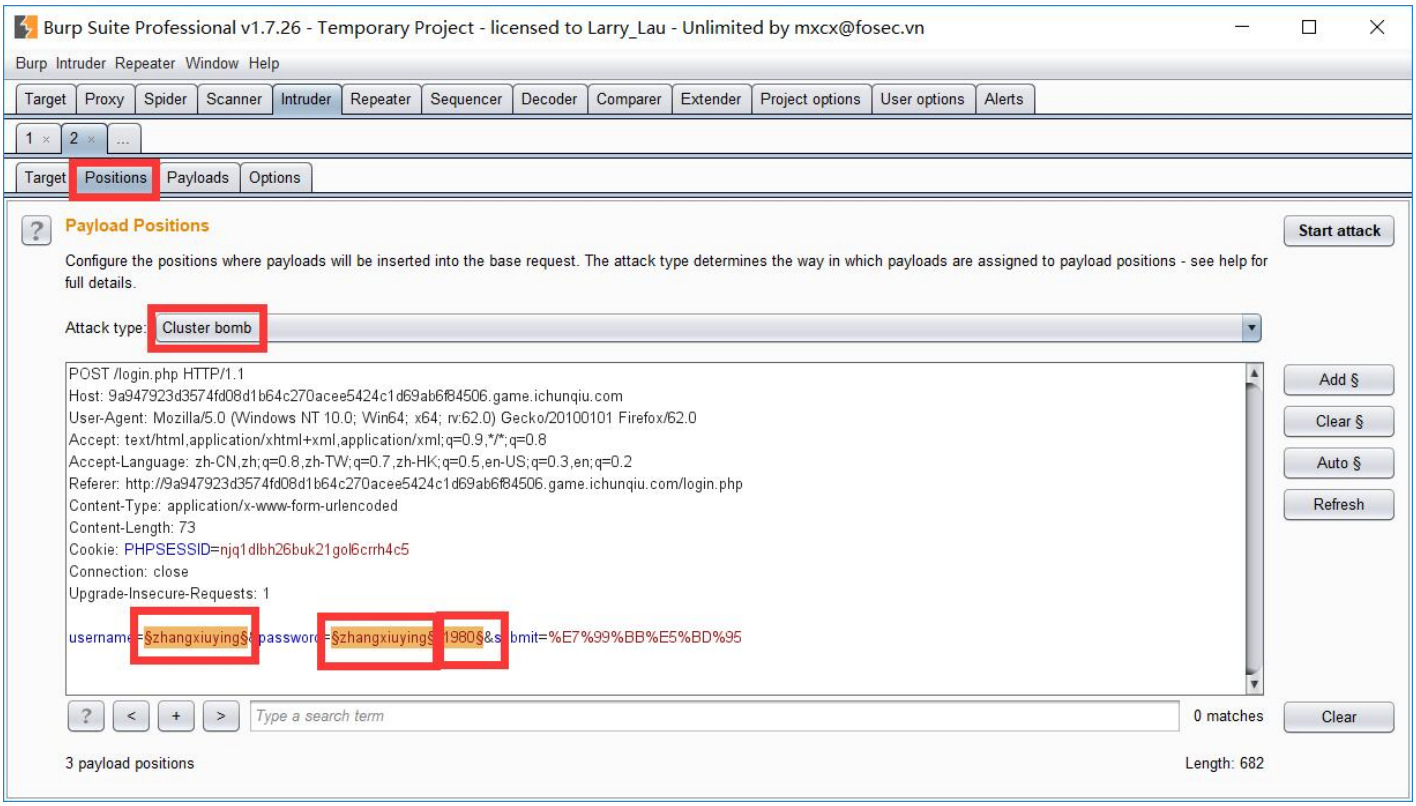
转载

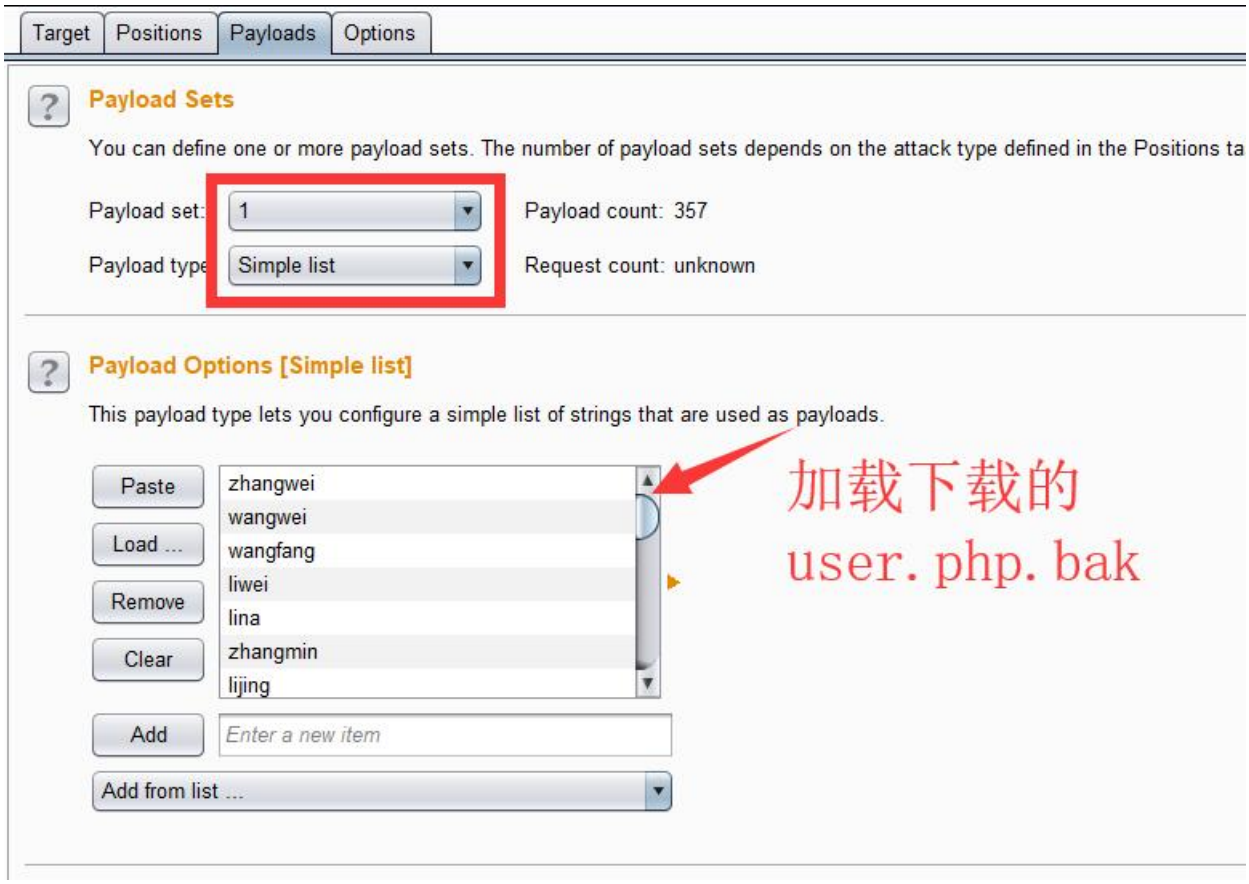
weixin_39532699 于 2021-04-01 06:47:55 发布 134 收藏
文章标签： CTFhtml解析php

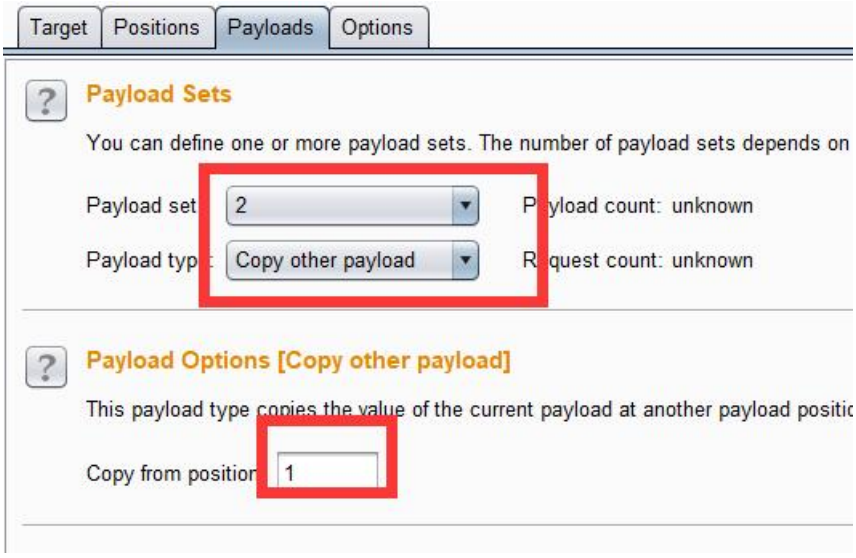
網頁源碼提示用戶信息在user.php中，直接訪問是不會有顯示的，於是查找相應的備份文件，vim交換文件等，最后發現/user.php.bak

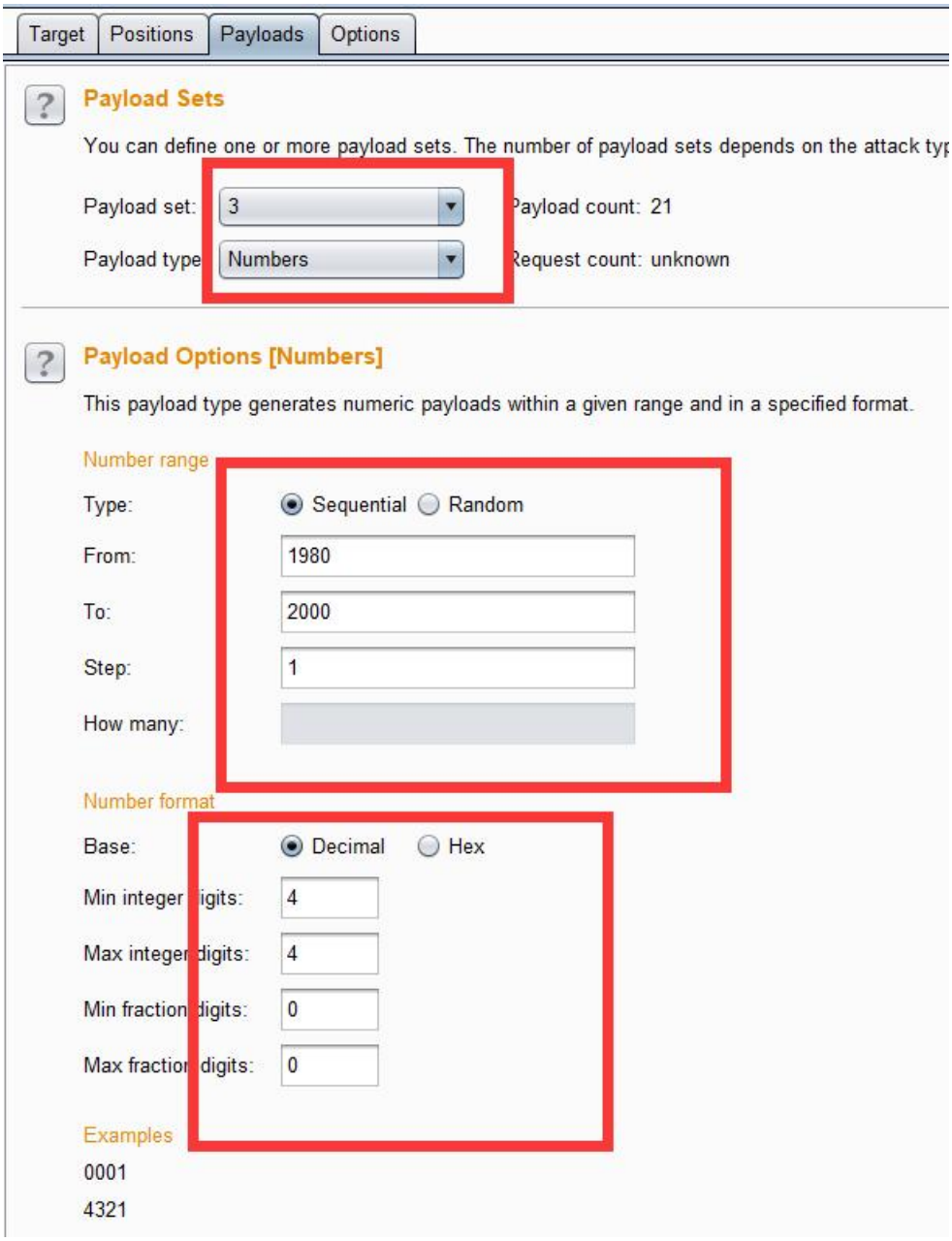


用burp采用如下配置開始爆破

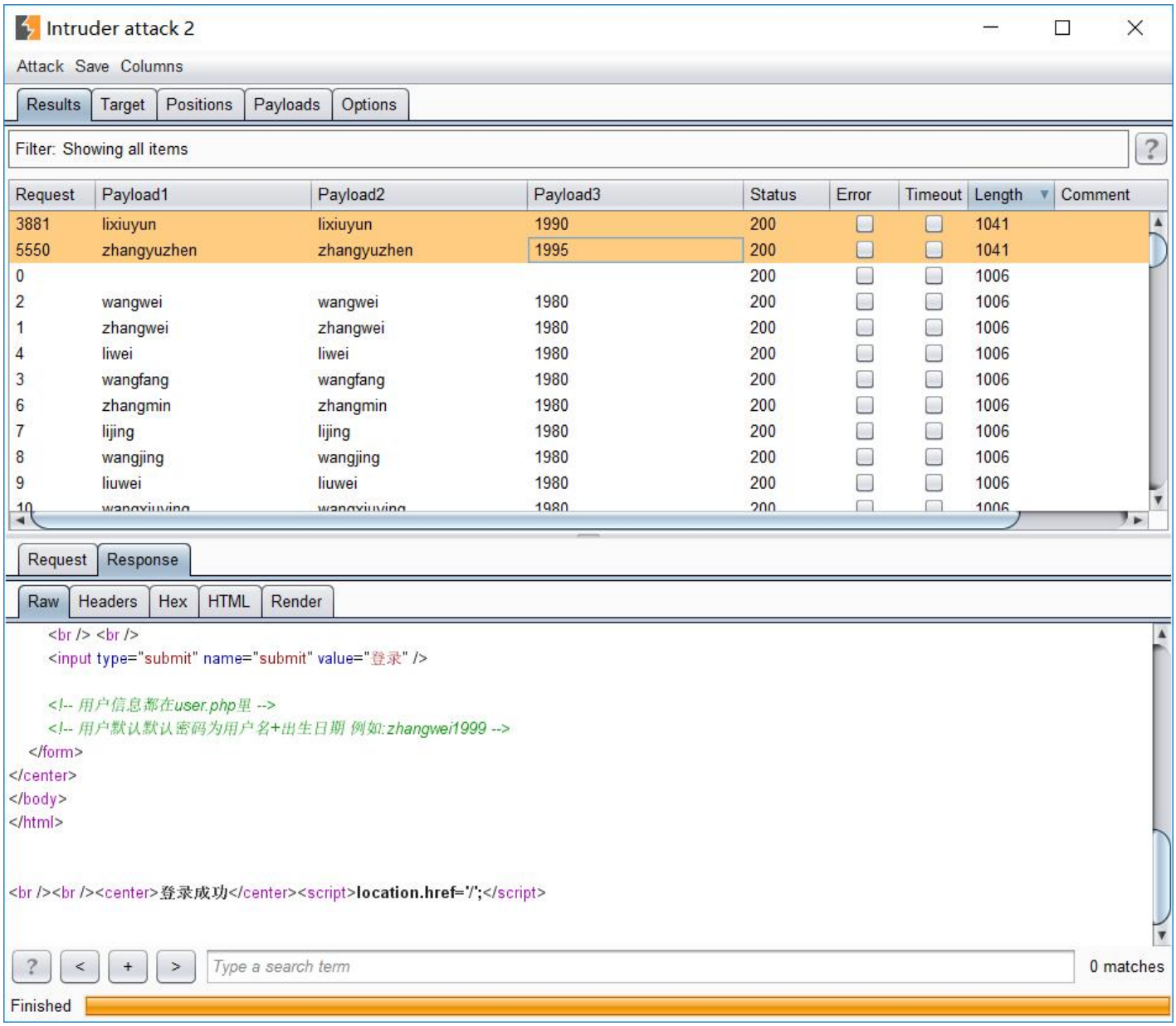



Target
Positions
Payloads
Options
Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions ta
Payload set:
1
Payload count: 357
Payload type
Simple list
Request count: unknown
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
zhangwei
wangwei
wangfang
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 typ
Copy other payload
Request count: unknown
Payload Options [Copy other payload]
This payload type copies the value of the current payload at another payload positic
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 typ
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



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

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，猜想這里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

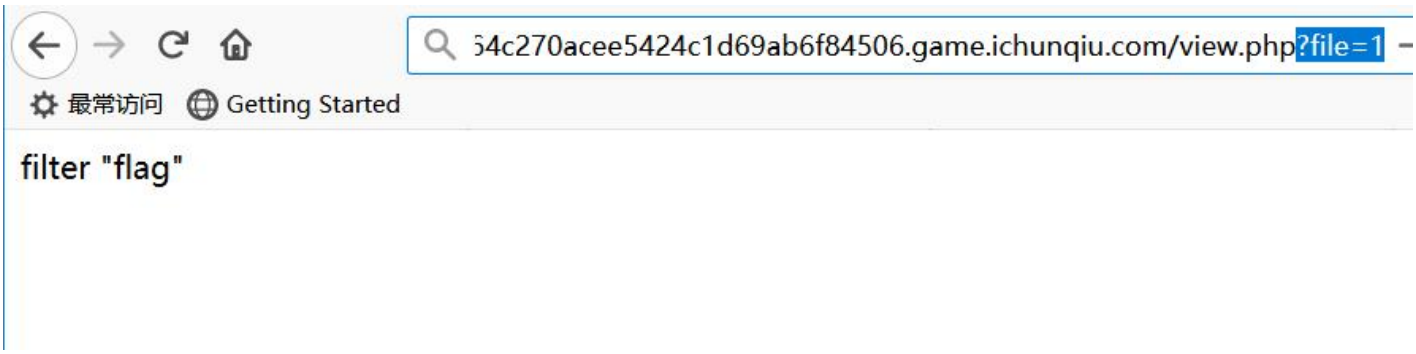
.+.ph(p[345]?|t|tml)

.+\.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都是可以被解析的。

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