攻防世界--WEB题之weak_auth

原创

LT.XQ 于 2021-02-21 09:21:00 发布 97 收藏

分类专栏： CTF学习--刷题

本文链接：https://blog.csdn.net/qq_45786729/article/details/113859003

问题描述：

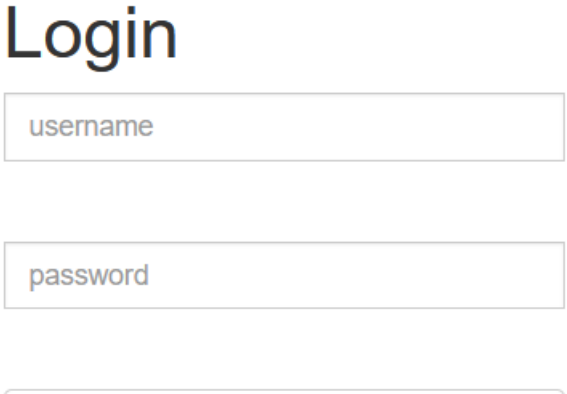
> 难度系数：一颗星
> 题目来源： Cyberpeace-n3k0
> 题目描述：小宁写了一个登陆验证页面，随手就设了一个密码。
> 题目场景：
> 点击获取在线场景
> 题目附件： 暂无

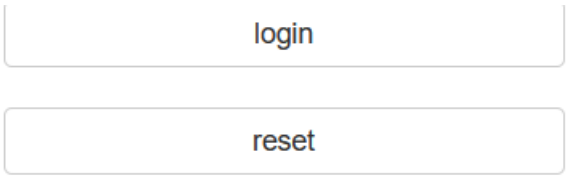
解题工具：

> burp suite

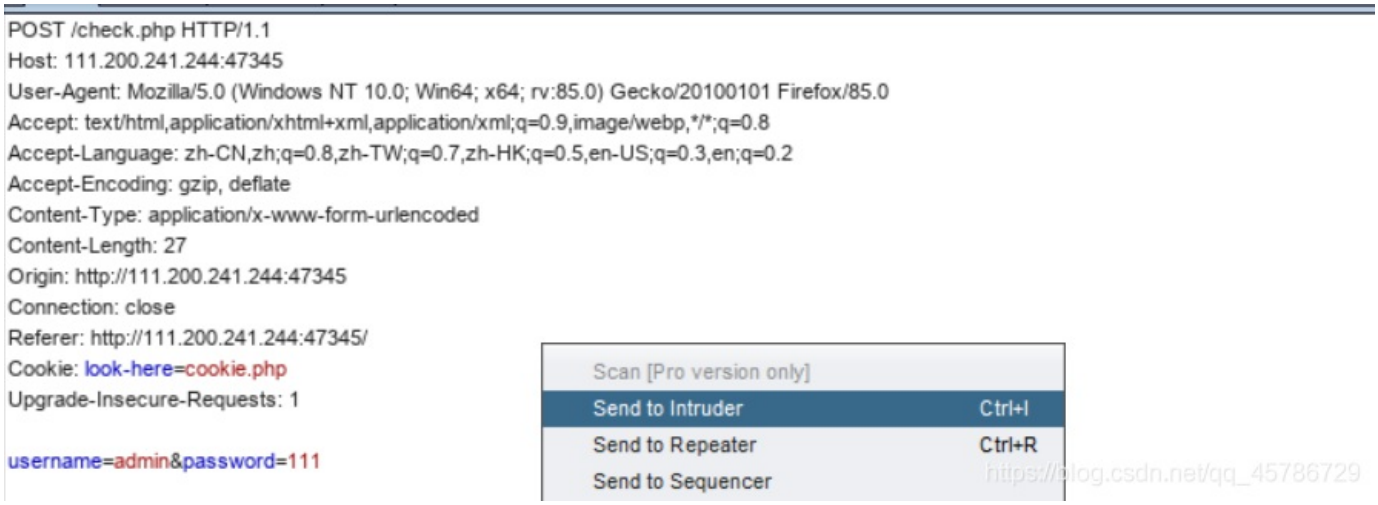
解题步骤：

1. 打开题目网站，可以看到一个登录界面。源代码等，都没有任何有用信息。猜测是是弱口令，需要暴力破解。

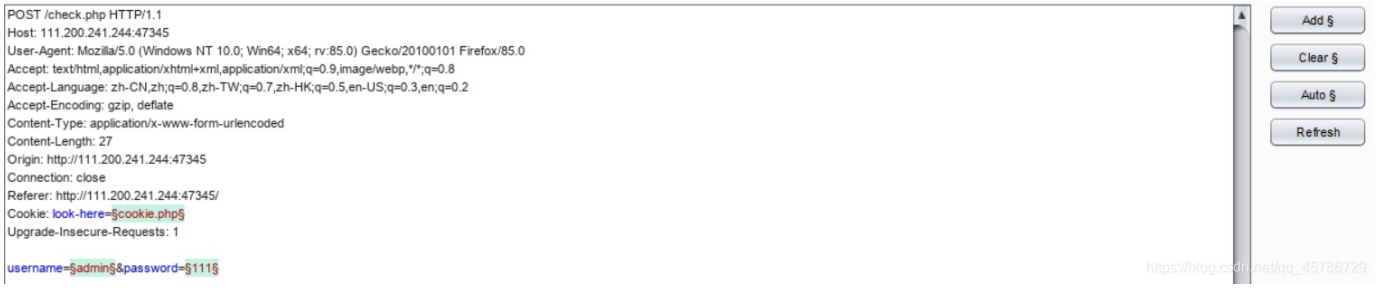




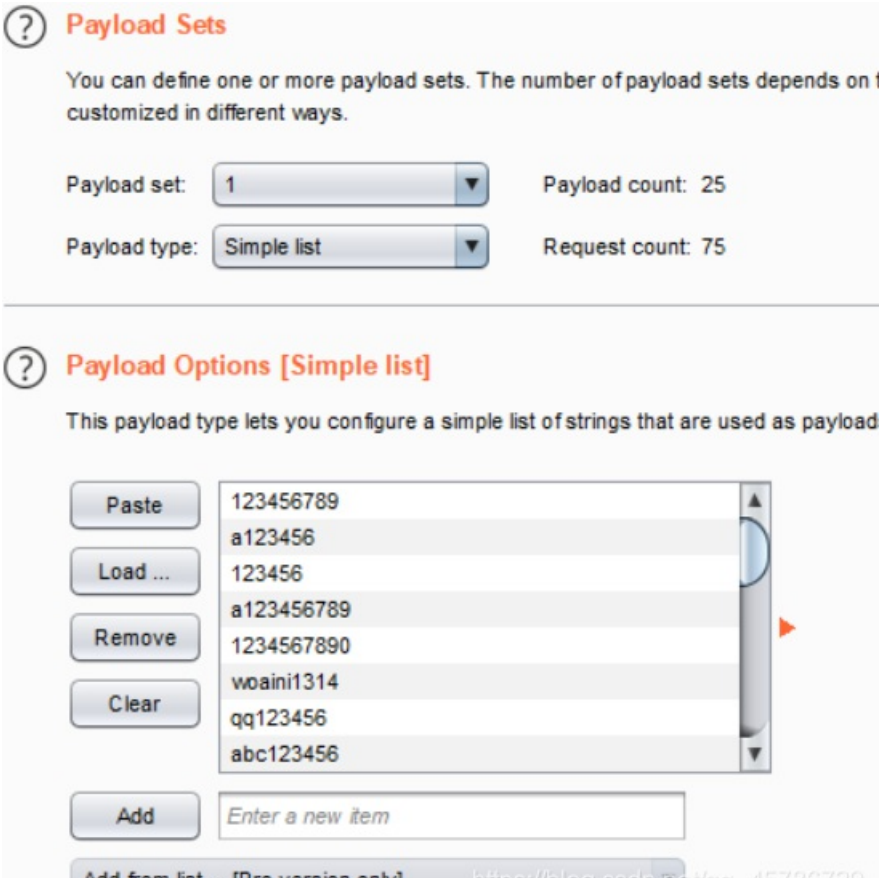
2. 随便填写，点击登录。并用burp suite进行抓包。我们填写的信息都在里面。点击鼠标右键，点击send to intruder。



3. 点击工具栏上的intruder，在点击positions，再点击‘clear§’,清除所有变量，选中password的值，并点击‘add§’，设为变量。



4. 点击payloads，点击load添加密码本。(密码本可以自己写，常见的密码合集，也可以再网上找）



Add from list ... [Pro version only]

5. 点击opdions，再点击start attack开始爆破。，会得到不同密码的‘length’。不同的‘length’则为目标密码。

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	434	
1	abcabc	200	☐	☐	434	
2	123456789	200	☐	☐	434	
3	123456789	200	☐	☐	434	
4	a123456	200	☐	☐	434	
5	123456	200	☐	☐	437	
6	a123456789	200	☐	☐	434	
7	1234567890	200	☐	☐	434	
8	woaini1314	200	☐	☐	434	
9	qq123456	200	☐	☐	434	
10	abc123456	200	☐	☐	434	
11	123456a	200	☐	☐	434	

6. 点击该目标记录，再点击Response，查看相应信息。发现了目标flag。

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>weak auth</title>
</head>
<body>

cyberpeace{492b9d999c0e12ae80ad87ba22932aad}<!--maybe you need a dictionary-->


</body>
</html>
```


7. 提交，正确。