Writeup2

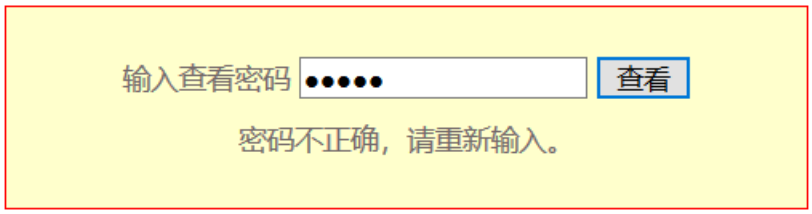
原创

想学python的元气汪 于 2019-12-02 19:21:48 发布 53 收藏
版权声明：本文为博主原创文章，遵循 CC 4.0 BY-SA 版权协议，转载请附上原文出处链接和本声明。
本文链接：https://blog.csdn.net/qq_43641982/article/details/103160542
版权

十一月份下旬总结

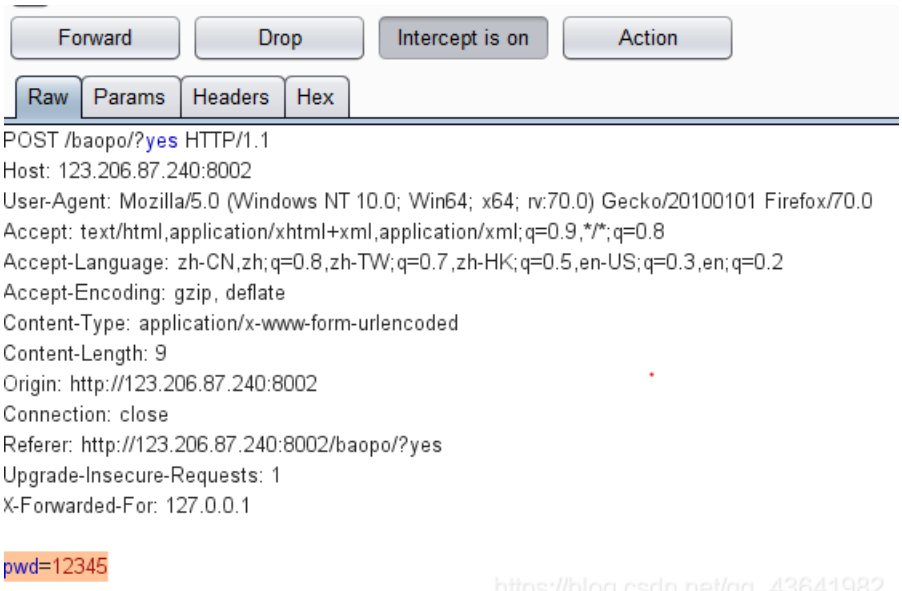
Burpsuite

通过抓包来展示用法
从wctf选了一道题
题目要求输入五位数字



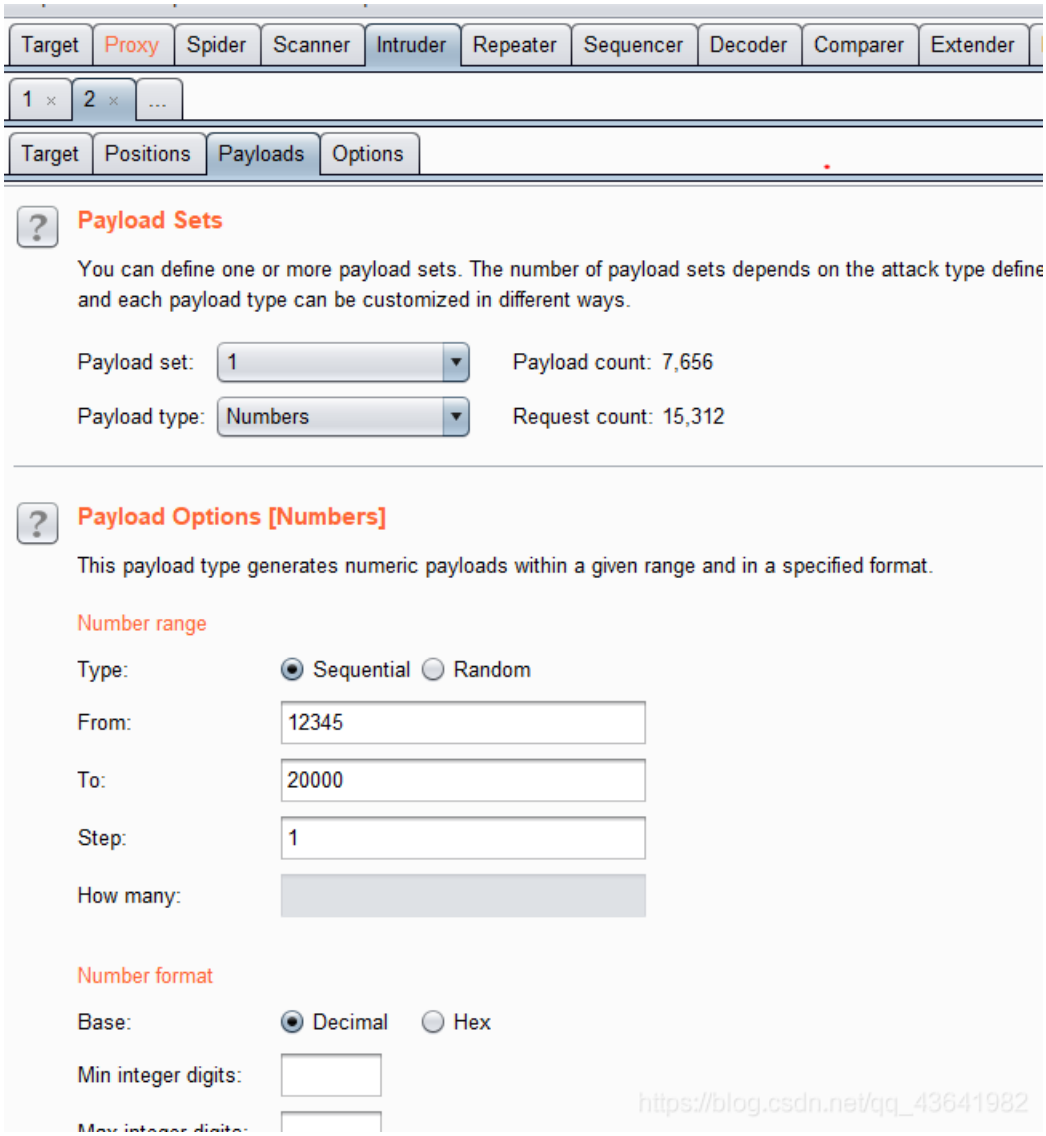
https://blog.csdn.net/qq_43641982

随便输入五位数字然后软件就捕获到了



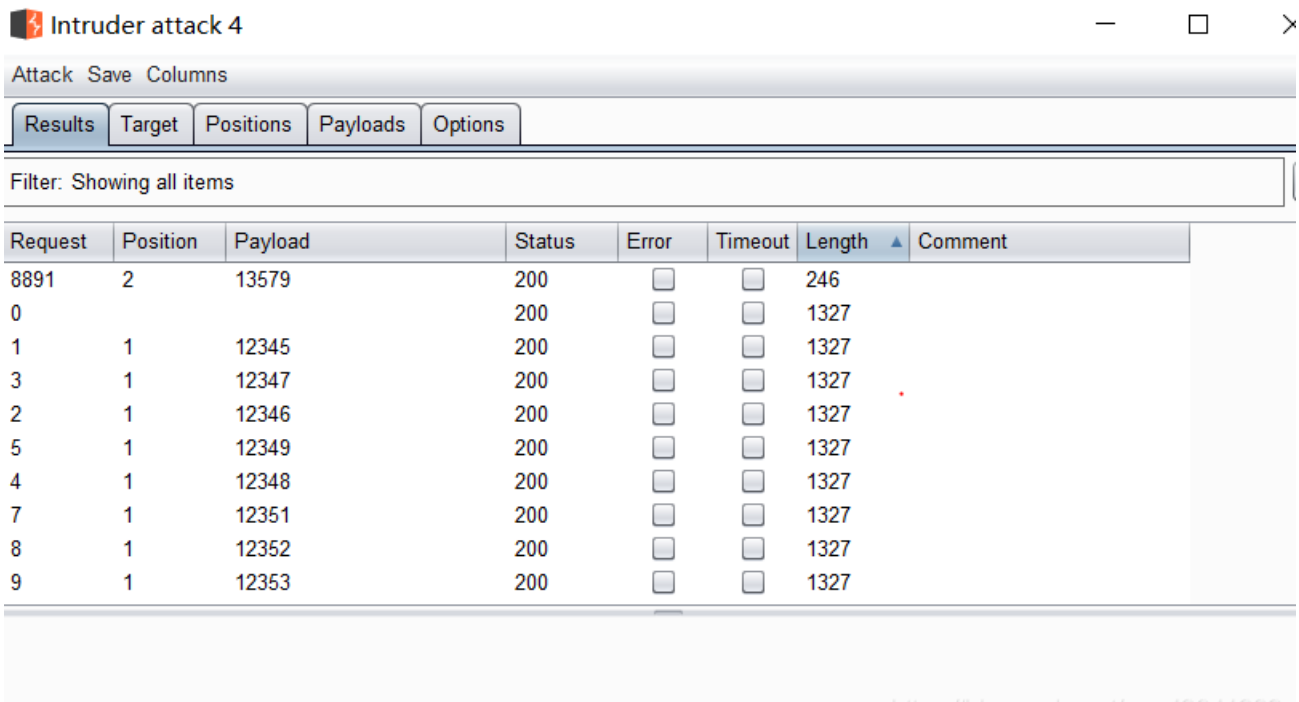
https://blog.csdn.net/qq_43641982

复制pwd一段然后Atcion send to Intruder



然后在payload里面把类型调成数字

下面就是把起始位置和终止位置还有间隔调好就可以start attack，在右上角位置



Request	Position	Payload	Status	Error	Timeout	Length	Comment
8891	2	13579	200			246	
0			200			1327	
1	1	12345	200			1327	
3	1	12347	200			1327	
2	1	12346	200			1327	
5	1	12349	200			1327	
4	1	12348	200			1327	
7	1	12351	200			1327	
8	1	12352	200			1327	
9	1	12353	200			1327	

https://blog.csdn.net/qq_43641982

爆破，观察length的变化，点击一下length显示不同长度的那一段就是我们需要的密码了

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
8891	2	13579	200			246	
0			200			1327	
1	1	12345	200			1327	
3	1	12347	200			1327	
2	1	12346	200			1327	
5	1	12349	200			1327	
4	1	12348	200			1327	
7	1	12351	200			1327	
8	1	12352	200			1327	
9	1	12353	200			1327	

Request | Response

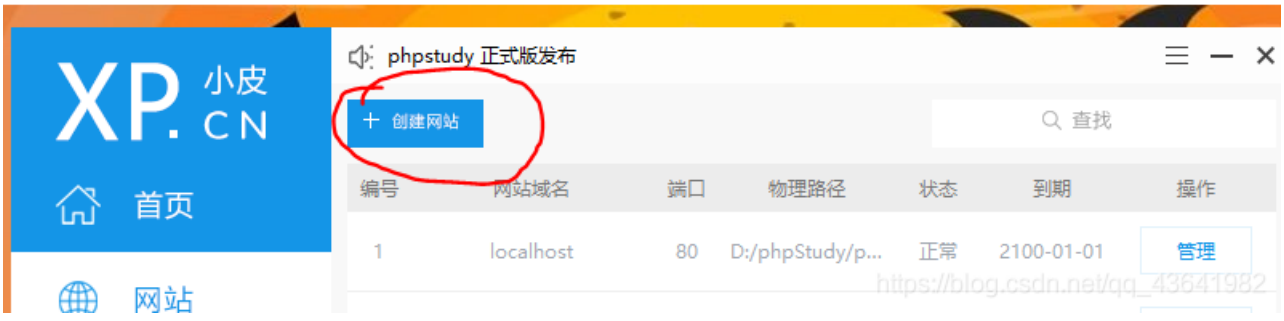
Raw | Headers | Hex

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 20 Nov 2019 05:13:27 GMT
Content-Type: text/html
Connection: close
Set-Cookie: isview=13579; expires=Wed, 20-Nov-2019 08:13:27 GMT
Content-Length: 46

flag{bugku-baopo-hah}

</body>
</html>
```

https://blog.csdn.net/qq_43641982

点击response得到了flag

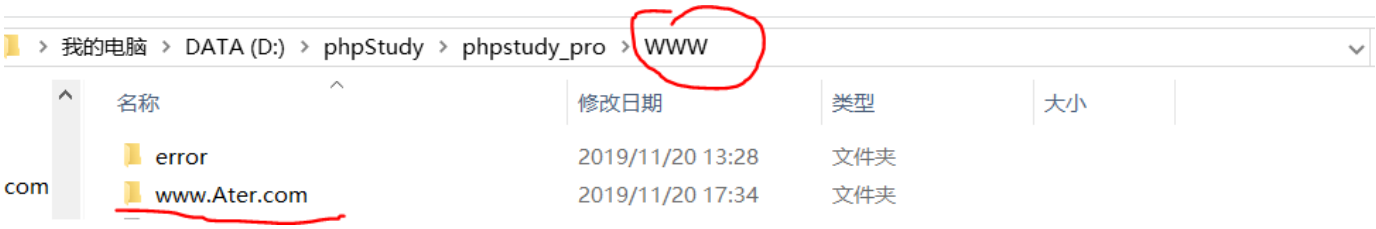
用phpstudy做一个简易的主页



https://blog.csdn.net/qq_43641982

1.创建网站（启动web服务）

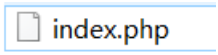
1. 我将域名取为www.Ater.com
2. 根目录放在一个www文件夹里
3. 创建数据库（先去新建数据库）
4. 创建完成后然后去找该文件了



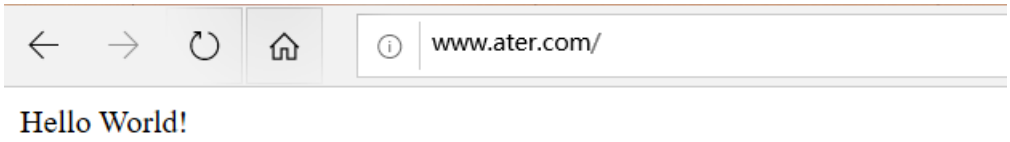
5. 进入该网站文件夹
6. 新建一个文本文件，并输入一段简单的php代码

```
<?
echo "Hello World!"
?>
```

然后保存文件，重命名改后缀名，index.php



然后在浏览器中输入网址



网站创建完成

网站是如何被访问到信息----之我见

网站利用Cookie来记录用户信息
客户端保存数据，访问http的时候顺带发送

HTTP基础

状态码:
1**—信息
2**—成功
3**—重定向
4**—服务器错误
5**—服务器错误
常见头部:
allow：服务器接收的请求方式
content-length：内容长度
content-encoding：文档的编码方式
content-type：文档类型
sever：服务器名字

Get和Post区别

get是在url进行的操作，有长度限制，也不安全，因为网址上就暴露了信息
post传参是把数据放在body里面，比较安全，没有长度限制

put和delete

put：传递数据来替代内容
delete：删除指定页面

.