

Form-实验吧

原创

Gunther17 于 2017-08-09 20:37:46 发布 928 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/dongyanwen6036/article/details/77016502>

版权



[web 专栏收录该内容](#)

5 篇文章 0 订阅

订阅专栏

<http://www.shiyanbar.com/ctf/1819>

Forms:

似乎有人觉得PIN码是不可破解的，让我们证明他是错的。

格式：ctf{ }

解题链接：<http://ctf5.shiyanbar.com/10/main.php>

解：在浏览器中直接按f12,修改代码把value改为1，然后直接提交，

```
<html>
  <#shadow-root (open)
  <head>...</head>
  <body>
    "
    Congratulations! The flag is ctf{forms_are_easy}
    "
  <form action method="post">
    "
    PIN:"
    <br> http://blog.csdn.net/dongyanwen6036
    <input type="password" name="PIN" value>
    * <input type="hidden" name="showsource" value="0" == $0
    <button type="submit">Enter</button>
  </form>
  <div id="js-atavi-extension-install"></div>
</body>
</html>
```

```
$a = $_POST["PIN"];
if ($a == -19827747736161128312837161661727773716166727272616149001823847) {
  echo "Congratulations! The flag is $flag";
} else {
  echo "User with provided PIN not found.";
}
```

<http://blog.csdn.net/dongyanwen6036>

User with provided PIN not found.

PIN:

a的值就是密码提交得到下图;

Congratulations! The flag is ctf{XXXXXXXXXX}

PIN:

<http://blog.csdn.net/dongyanwen6036>