Form-实验吧

原创

Gunther17 于 2017-08-09 20:37:46 发布 928 收藏

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>
      <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.";
}
```


User with provided PIN not found.
PIN:
Enter

a的值就是密码提交得到下图;

Congratulations! The flag is ctf{f[redacted]}
PIN:
Enter