



GrimTheRipper

Follow

Jul 11 · 2 min read · Listen



Open in app

Get started

ChurchCRM Version 4.4.5 — Stored XSS Vulnerability at sHeader

Vulnerability Explanation:

ChurchCRM Version 4.4.5 has XSS vulnerabilities that allow attackers to store XSS via location input sHeader.

Affected Component:

http://ip_address:port/churchcrm/SystemSettings.php

Payload :

```

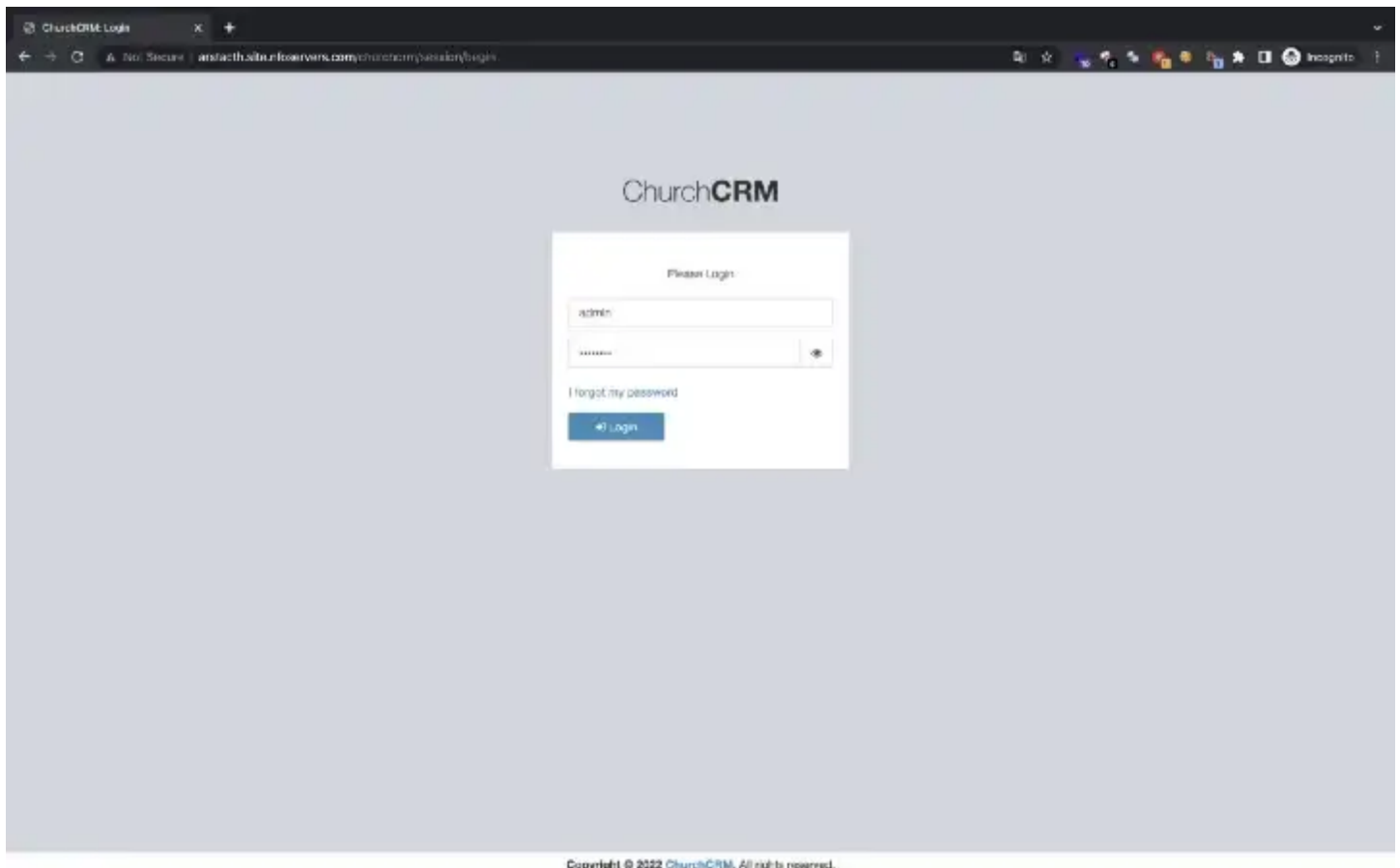
```

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 "Admin" as show in the picture and Click on the "Edit General Settings"



[Open in app](#)[Get started](#)

Welcome to

1 Families
[View all Families](#)

50 People
[View All People](#)

0 Sunday School Classes
[View all](#)

0 Groups
[View all](#)

0 Attendance Check-in
[View all](#)

Today's Birthdays

Today's Wedding Anniversaries

Deposit Tracking

People

[Add New Person](#) [Add New Family](#)

3. Next, Go to the "System Settings". click on the "sHeader" input then enter the XSS payload and press the Save Settings button.

Not secure | arstach.site:8080/churchcrm/SystemSettings.php?saved=true

Church Information User Setup Email Setup People Setup Enabled Features Map Settings Report Settings Financial Settings

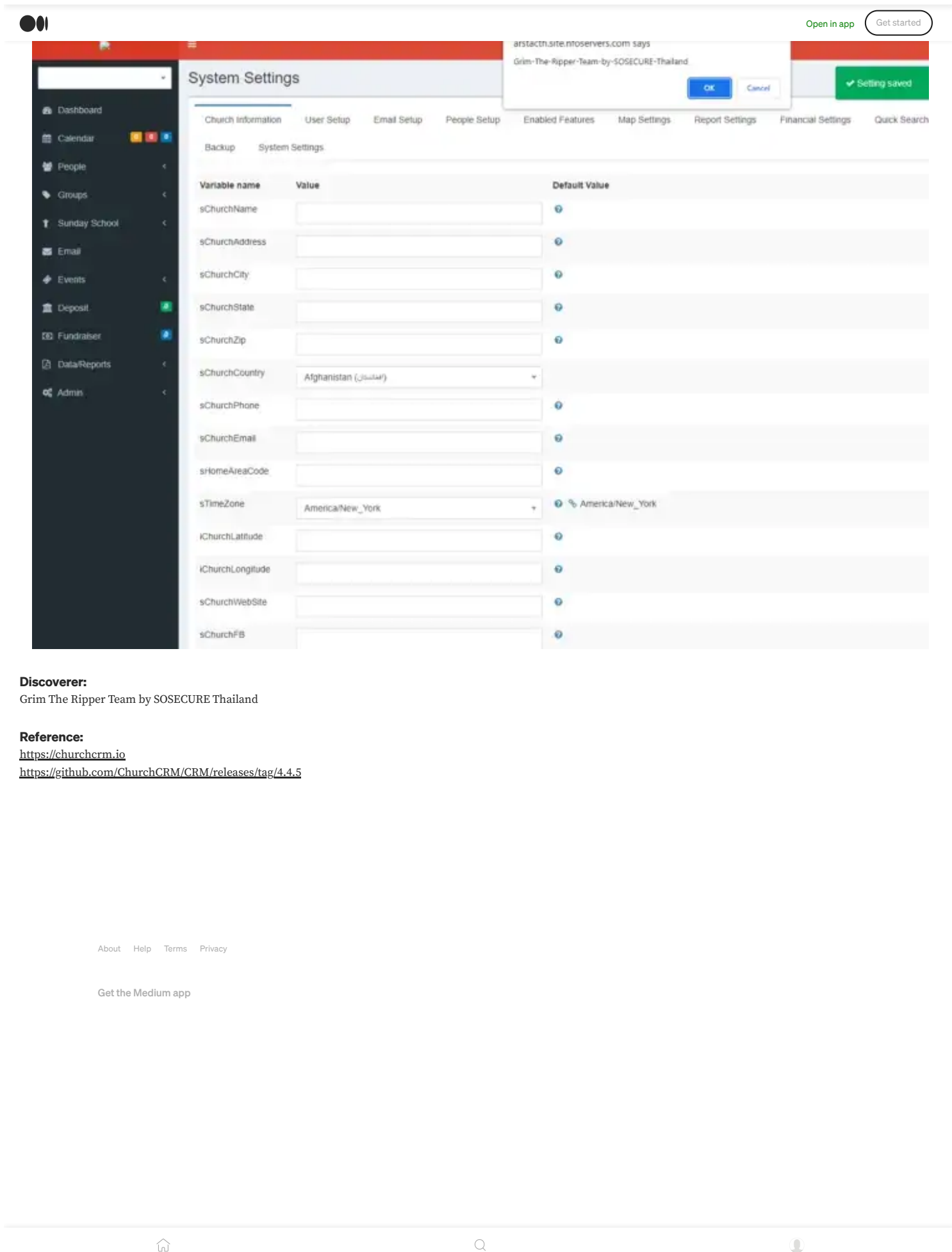
Backup **System Settings**

Variable name	Value	Default Value
sLogLevel	INFO [200]	200
bRegistered	True	False
bCSVAdminOnly	True	True
sHeader		
bEnableIntegrityCheck	True	True
iIntegrityCheckInterval	168	168
sLastIntegrityCheckTimeStamp	20220706-233312	
iPhotoClientCacheDuration	3600	3600
bHSTSEnable	False	False
iDashboardServiceIntervalTime	60	60
iSoftwareUpdateCheckInterval	24	24
sLastSoftwareUpdateCheckTimeStamp	20220706-233312	
bAllowPrereleaseUpgrade	False	False

Save Settings

4. After refresh this page The XSS payload will run immediately.





Discoverer:

Grim The Ripper Team by SOSECURE Thailand

Reference:

<https://churchcrm.io>

<https://github.com/ChurchCRM/CRM/releases/tag/4.4.5>