GrimTheRipper Follow
Jul 11 · 2 min read · Listen

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.

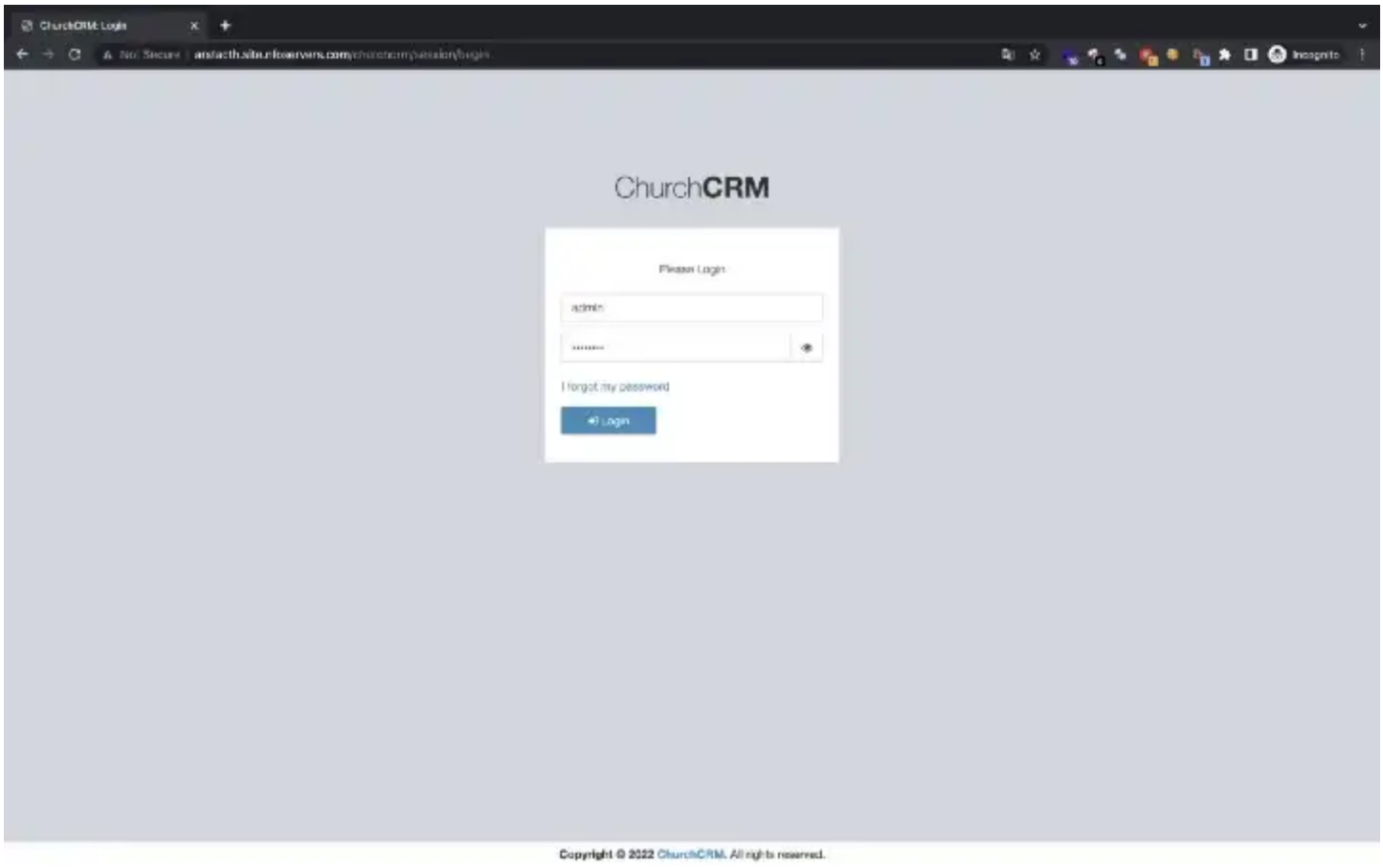
Affected Component:
http://ip_address:port/churchcrm/SystemSettings.php

Payload :

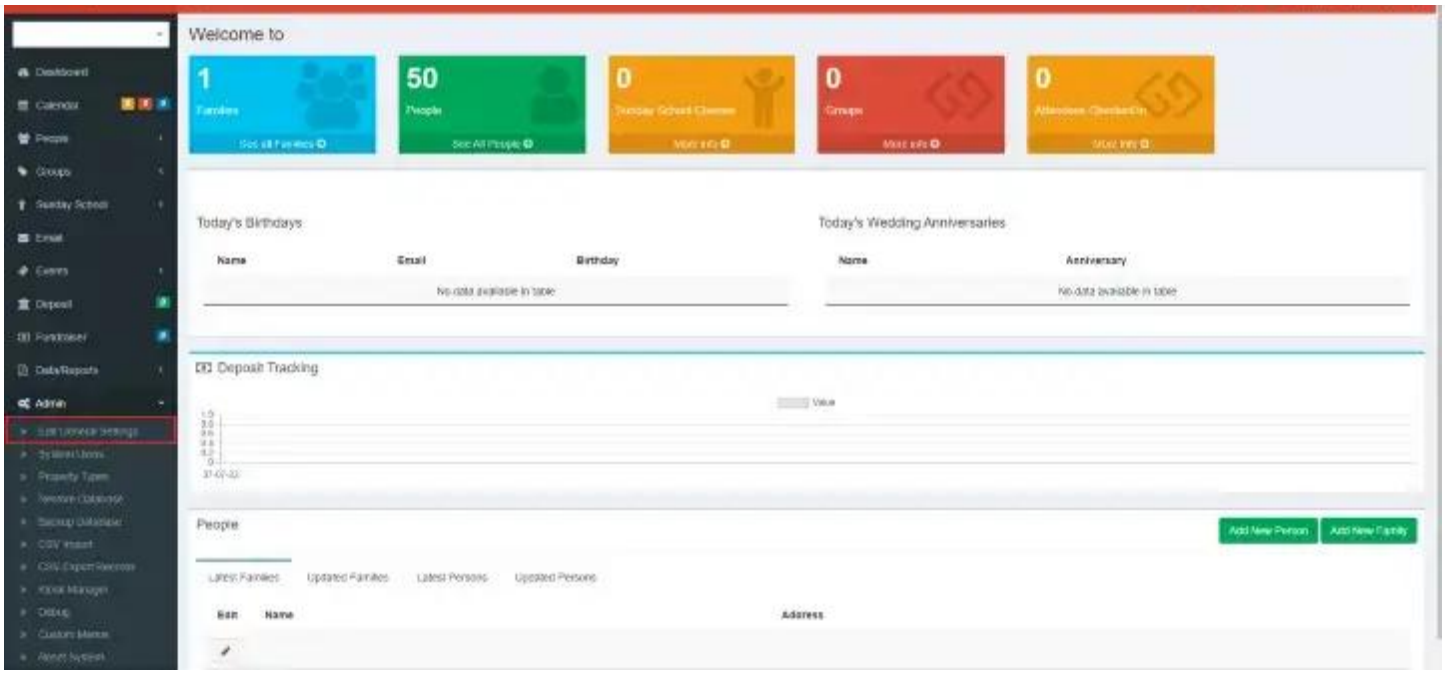
```
<img src="test" onerror=confirm("Grim-The-Ripper-Team-by-SOSECURE-Thailand")>
```

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)

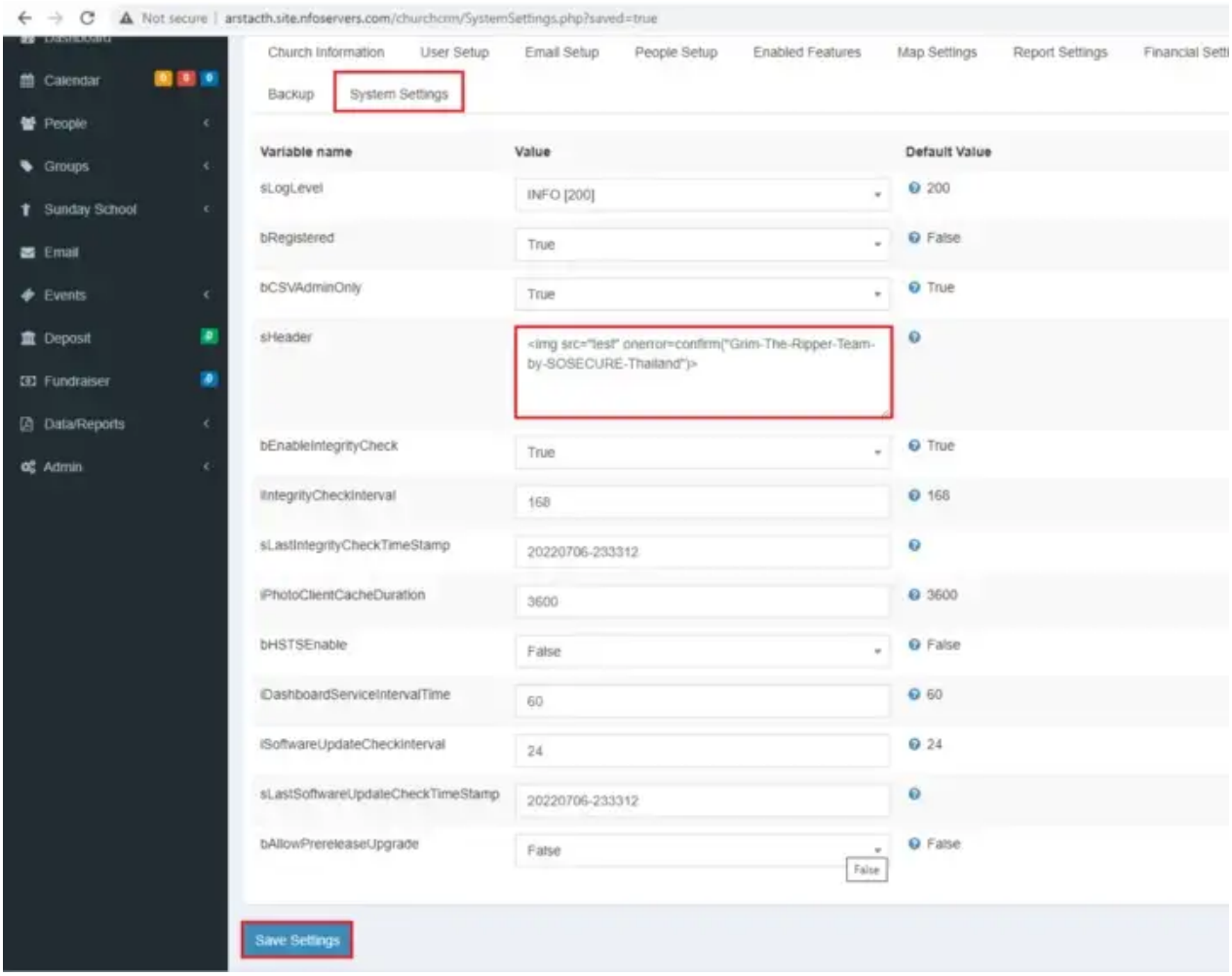
Steps to attack:
1. Login with admin credential.



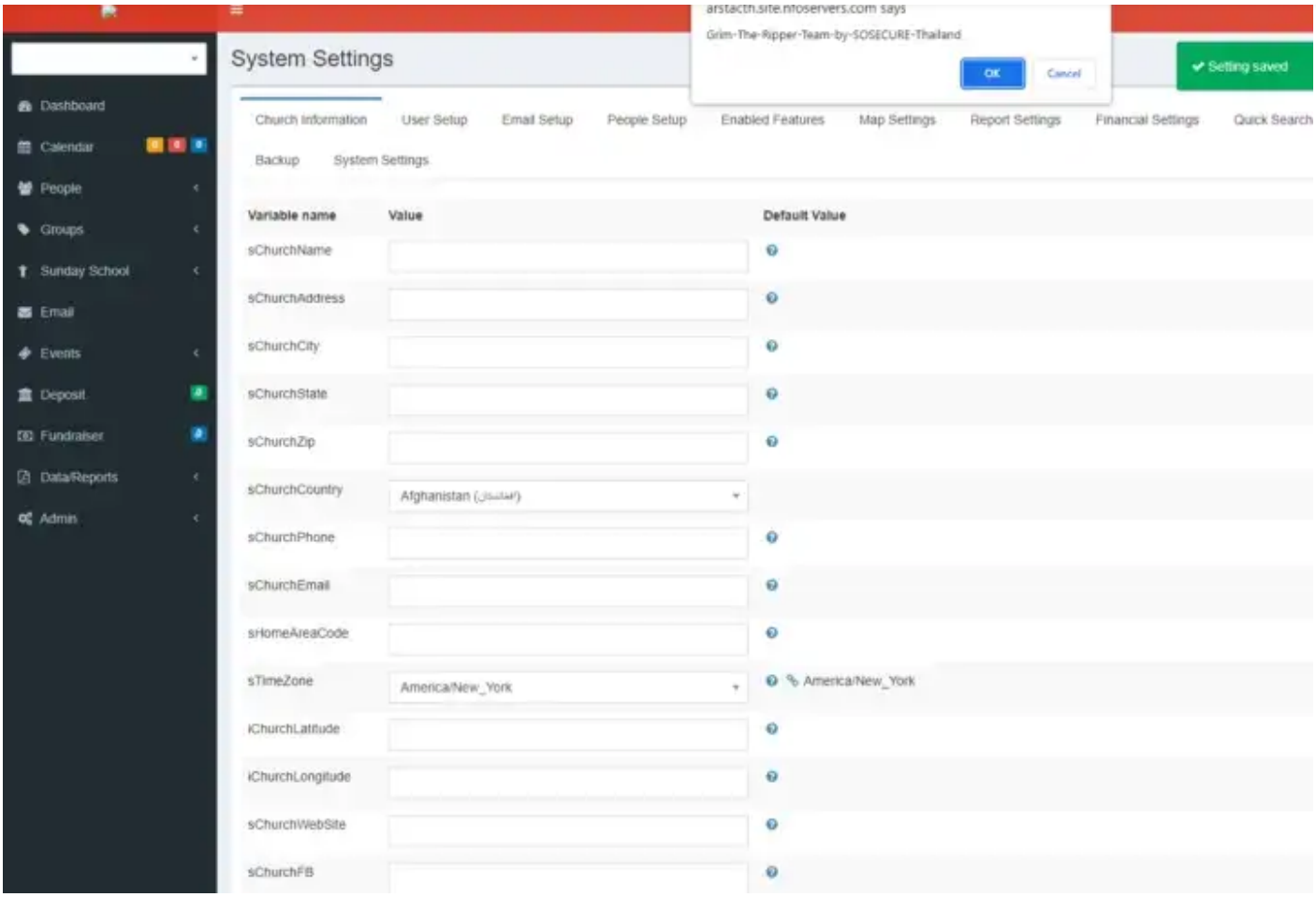
2. Go to the “Admin” as show in the picture and Click on the “Edit General Settings”



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



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