

Tiki Wiki Cms Groupware 21.2
Responsible Disclosure
for CVE-2020-29254
by Maximilian Barz

Summary:

Found Vulnerabilities:

- LFI
- CSRF (CVE-2020-29254)
- Information Exposure

Affected files:

- tiki-edit_templates.php
- tiki-installer.php

Attack Scenarios:

Vulnerability Chain 1: CSRF + LFI resulting in Information Disclosure leading to admin account takeover through phpMyAdmin and remote code execution.

Vulnerability Chain 2: CSRF + LFI resulting in Information Disclosure leading to admin account takeover through unlocked tiki-installer.php and remote code execution.

PoC Videos:

- **TikiWiki 21.2 - Local File Inclusion and Information Exposure**
(<https://youtu.be/MOdzlQrU22Y>)
- **TikiWiki 21.2 - Edit Template CSRF (CVE-2020-29254)**
(<https://youtu.be/Uc3sRBtu50>)
- **TikiWiki 21.2 - Administrator Compromise - Attack Chain 1 PoC**
(<https://youtu.be/YIqpHr5l-lg>)
- **TikiWiki 21.2 - Full System Compromise Attack Chain 2 PoC**
(<https://youtu.be/lK61NYhmqIo>)

All videos are not public and just via their specified URI available

The following vulnerabilities are part of my **responsible disclosure and Bug Bounty Hunt**. If TikiWiki acknowledges the presence of these vulnerabilities I will request CVE numbers for them.

Vulnerabilities and attack scenarios:

Affected File: tiki-edit_templates.php

1. Local (php) File Inclusion:

In TikiWiki 21.2, an user can be given the permission to edit .tpl templates. This feature can be abused to escalate the users privileges by inserting the following piece of smarty code: „{include file='../db/local.php'}“. The code snippet includes TikiWikis database configuration file and displays it in the pages source code. Any other www-data readable file like „/etc/passwd“ can be included as well. The config file displays TikiWikis database credentials in cleartext.

See PoC Video: Local File Inclusion and Information Exposure

Calculated CVSS: 7.0 High

Recommended solution: Disallow including filetypes other than .tpl

2. Cross-Side-Request-Forgery (CSRF)

TikiWiki 21.2 allows to edit templates without the use of a CSRF protection. This could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected system. The vulnerability is due to insufficient CSRF protections for the web-based management interface of the affected system. An attacker could exploit this vulnerability by persuading a user of the interface to follow a maliciously crafted link. A successful exploit could allow the attacker to perform arbitrary actions on an affected system with the privileges of the user. These action include allowing attackers to submit their own code through an authenticated user resulting in local file Inclusion. If an authenticated user who is able to edit TikiWiki templates visits an malicious website, template code can be edited.

See PoC Video: CSRF

Calculated CVSS: 5.0 Medium

CVE: CVE-2020-29254

Recommended solution: Add security ticket like in scheduler feature.

3. Information Exposure

An user who is able to edit template files can use smarty code to include Files like the database configuration file which allows access to TikiWikis Database. The User can authenticate against it and simply give itself admin privileges or compromise the administrator account.

See PoC Video: Local File Inclusion and Information Exposure

Calculated CVSS: 7.5

Recommended solution: Disallow including filetypes other than .tpl

Affected File: tiki-installer.php (unlocked)

Also if the tiki-installer.php page is not locked this vulnerability can be used to authenticate against tiki-installer.php. After that the attacker can simply change the database connection to its own tiki database resulting in a whole compromise of the application as the attacker could add a new user with admin privileges.

It's also possible to change the administrators email adress after logging in to tiki-installer.php. After that its possible to simply reset the administrators password which also results in a whole application compromise.

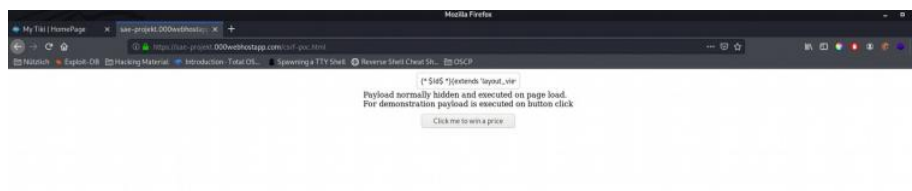
Another Method would be to specify an invalid database ip resulting in Denial of Service.

Demonstration on how these vulnerabilities can be turned into a whole system compromise using attack chains:

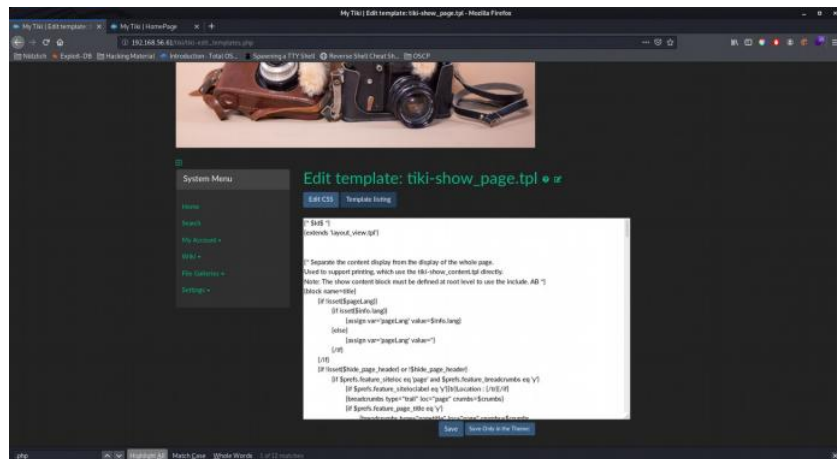
Attack Chain 1: CSRF + LFI resulting in Information Disclosure leading to administrator account takeover through phpMyAdmin and remote code execution.

This scenario demonstrates how an attacker is able to completly compromise TikiWiki 21.2. To make this attack chain work, an administrator has to be tricked into visiting a malicious website while beeing logged in to TikiWiki.

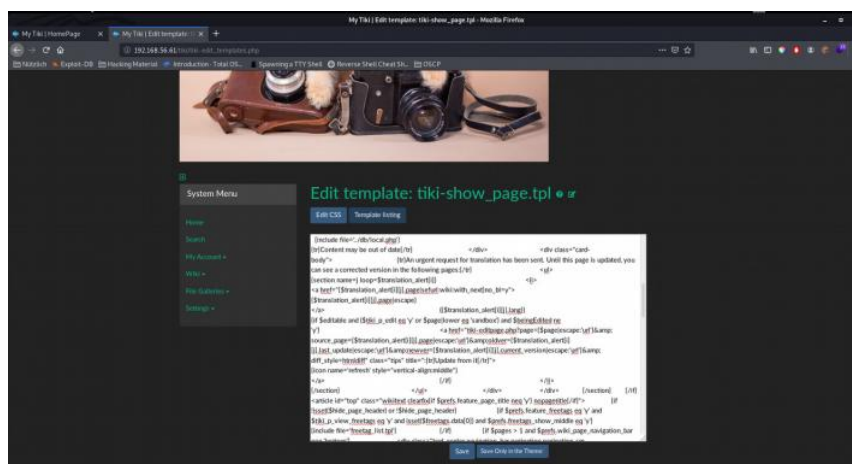
Step 1: The administrator or an user who is able to edit templates has to visit a malicious website controlled by the attacker.



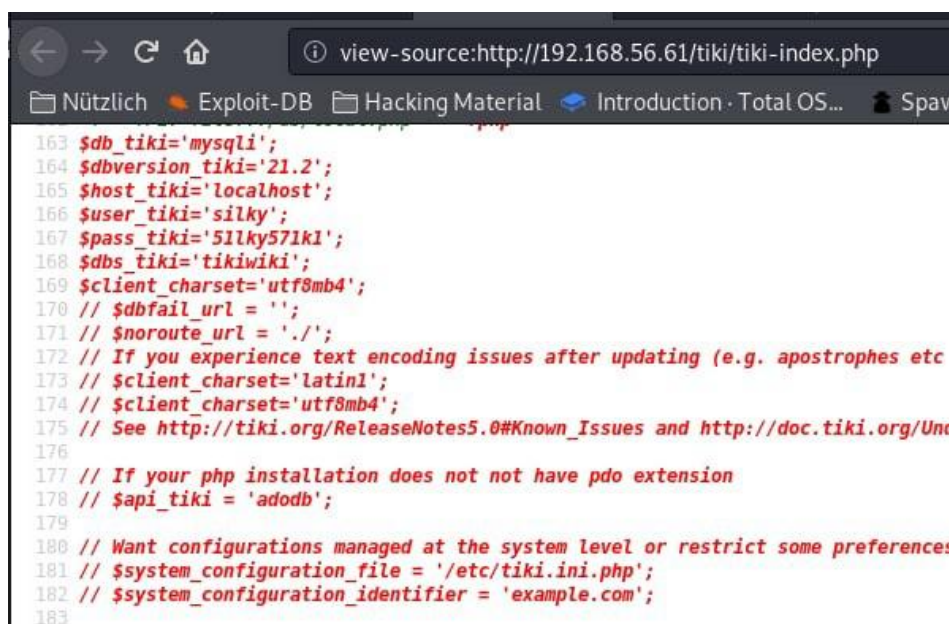
Step 2: Template tiki-show_page.tpl gets automatically edited through CSRF and exposes TikiWikis database credentials in tiki-index.php source code. Victim has not to save the edited template as it is saved automatically. The template stays the same except that a line is added which includes TikiWikis configuration file.



Normal Condition

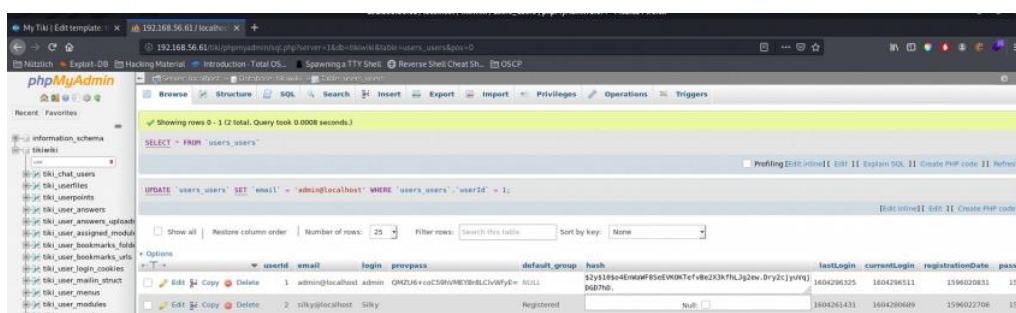


Changed condition



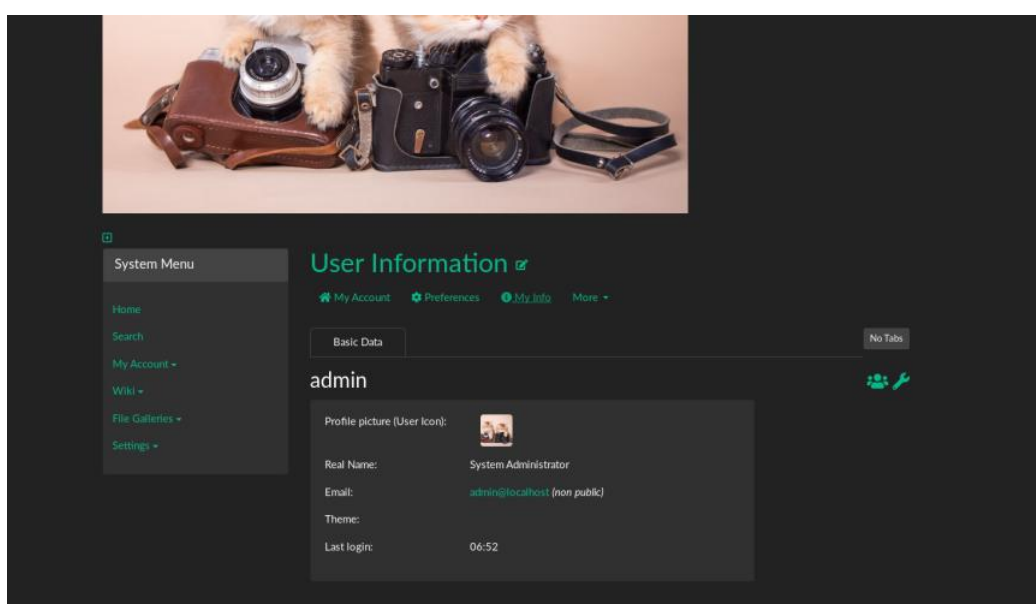
Configuration file is exposed

Step 3: Attacker logs in to phpMyAdmin and changes the administrator passwordhash to one created by himself.



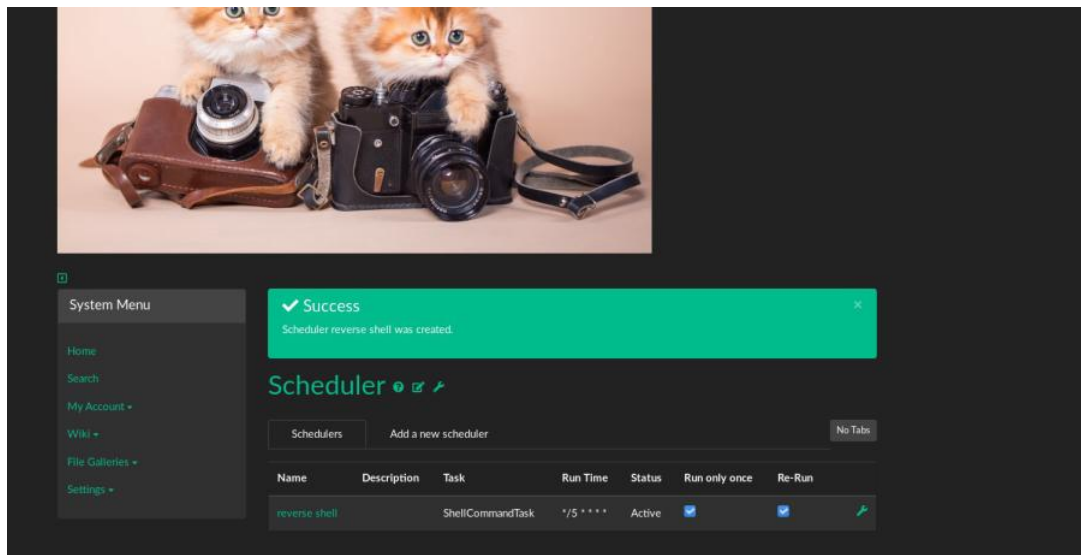
Credentials allow access to database

Step 4: Attacker logs in to TikiWiki as an administrator

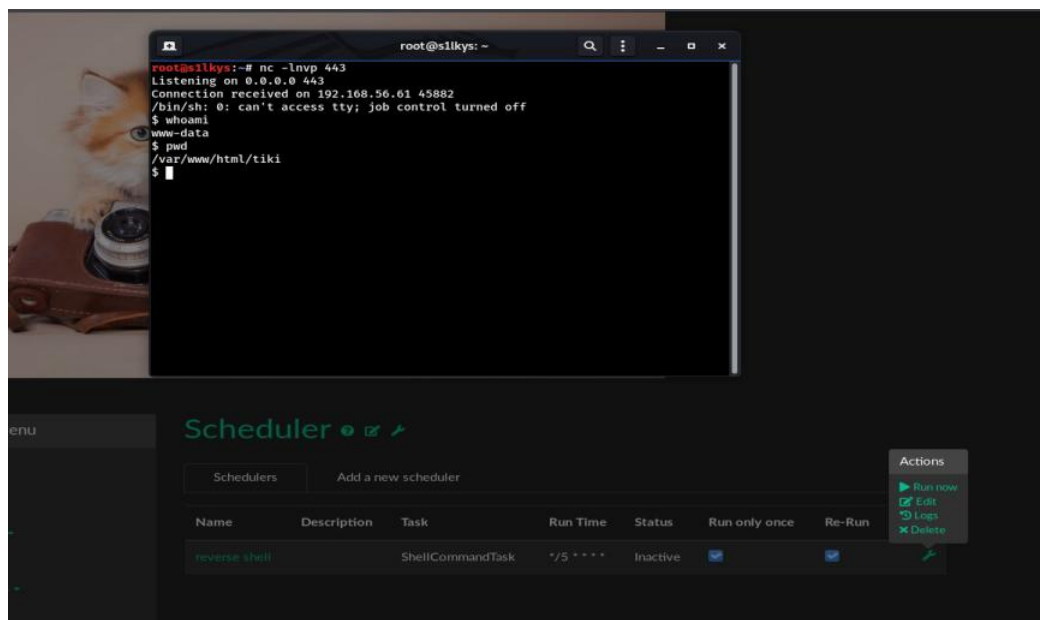


Attacker can log in as admin

Step 5: Attacker creates new scheduler which executes a reverse shell



Scheduler is created



Scheduler executes reverse shell

Impact: Critical

Compromised Systems or accounts:

- MySQL database
- Administrator account
- TikiWiki Application
- TikiWiki Server

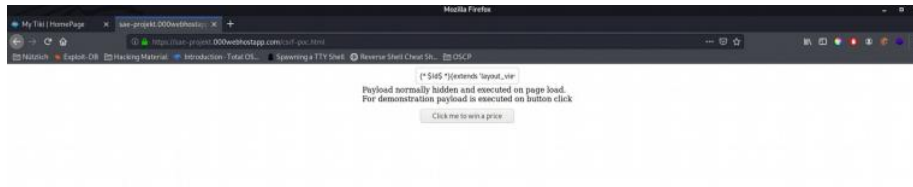
See PoC Video: Attack Chain 1

Maximilian Barz (OSCP)
 Email: mbzra@protonmail.com
 Twitter: S1lky_1337

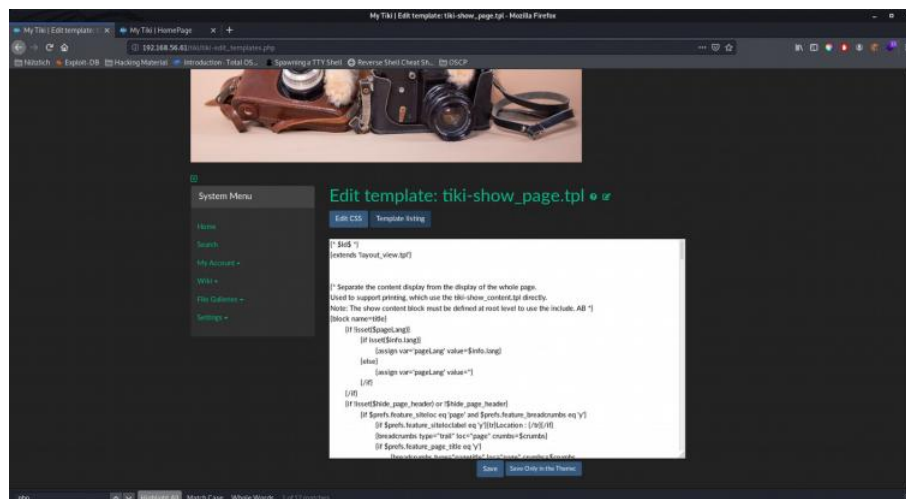
Attack Chain 2: CSRF + LFI resulting in Information Disclosure leading to admin account takeover through unlocked tiki-installer.php and remote code execution.

This scenario demonstrates how an attacker is able to completely compromise TikiWiki 21.2. To make this attack chain work, an administrator has to be tricked into visiting a malicious website while being logged in to TikiWiki.

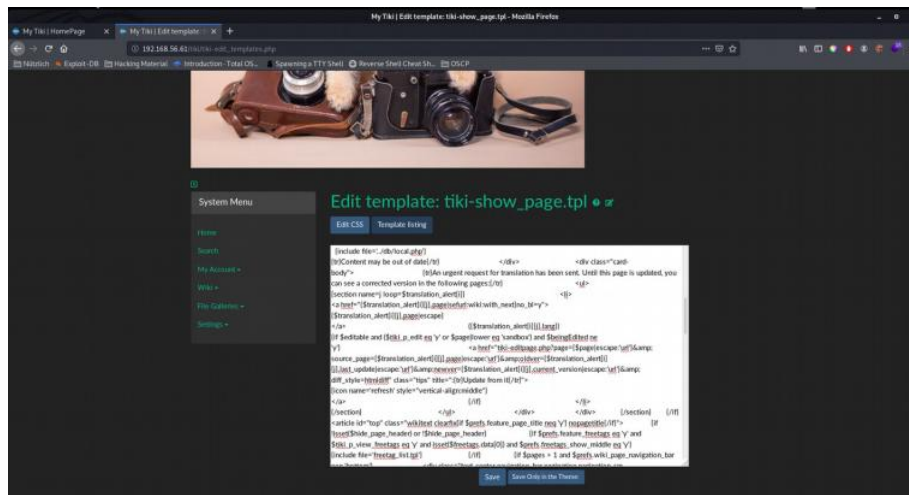
Step 1: The administrator or a user who is able to edit templates has to visit a malicious website controlled by the attacker.



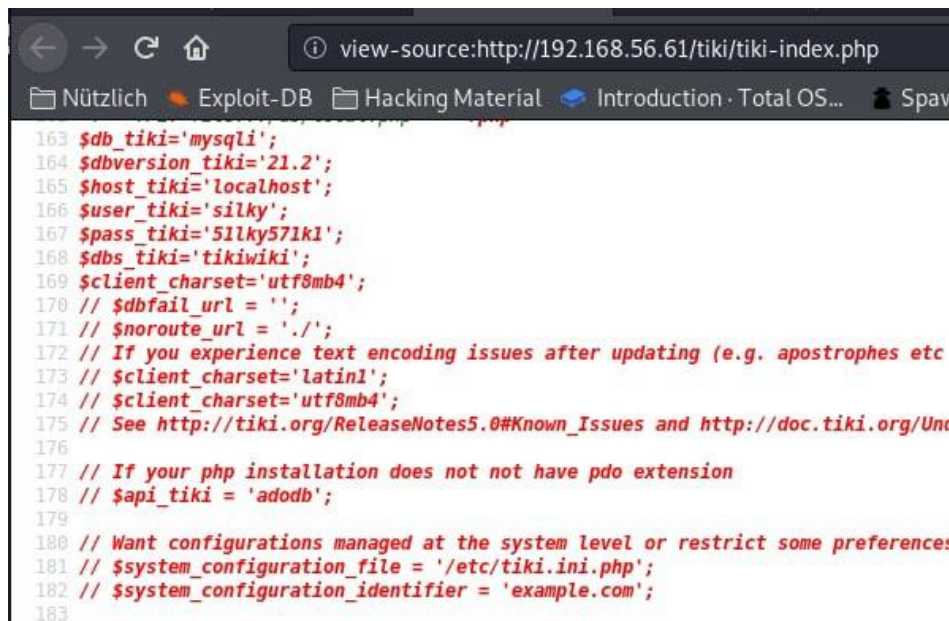
Step 2: Template tiki-show_page.tpl gets automatically edited through CSRF and exposes TikiWiki's database credentials in tiki-index.php source code.



Normal Condition

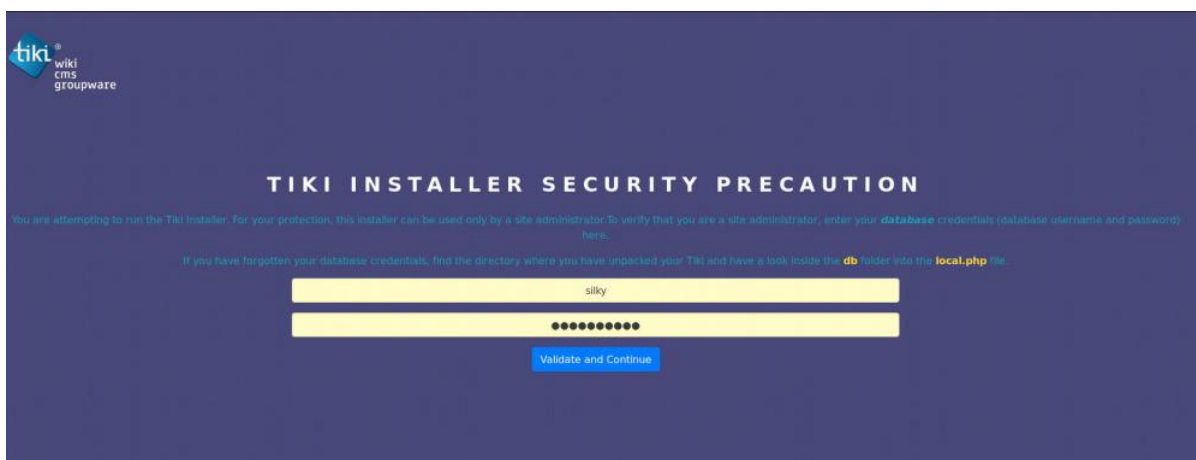


Changed condition



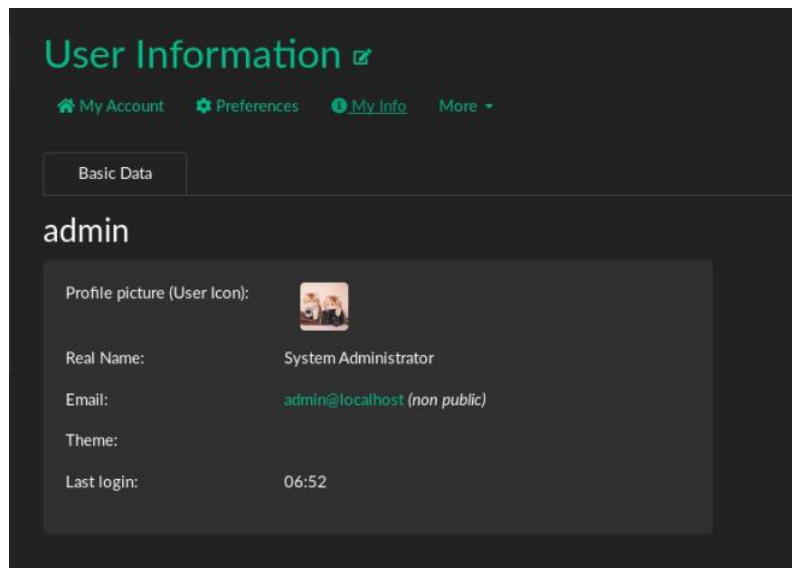
Configuration file is exposed

Step 3: Attacker logs in to tiki-install.php and changes the administrators email address to one of his own by using „Configure the General Settings“.



Authenticate against tiki-installer.php

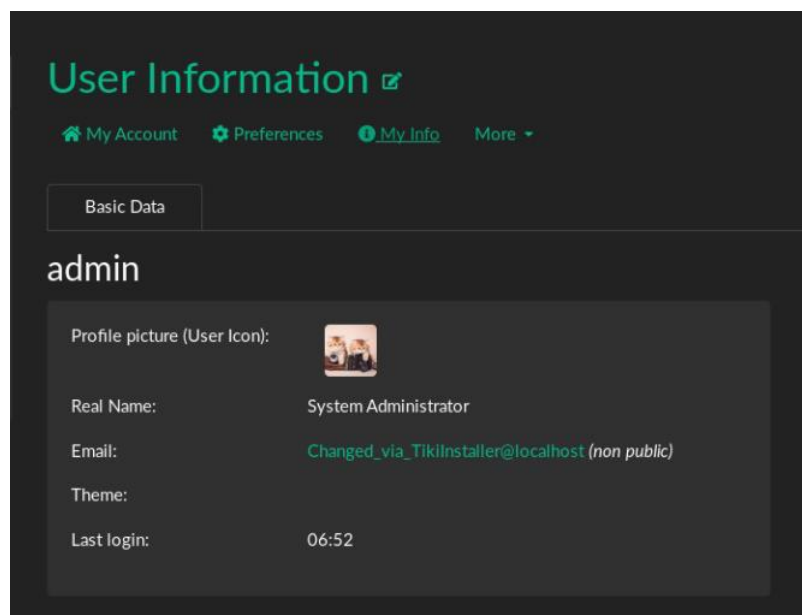
Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337



Email before change



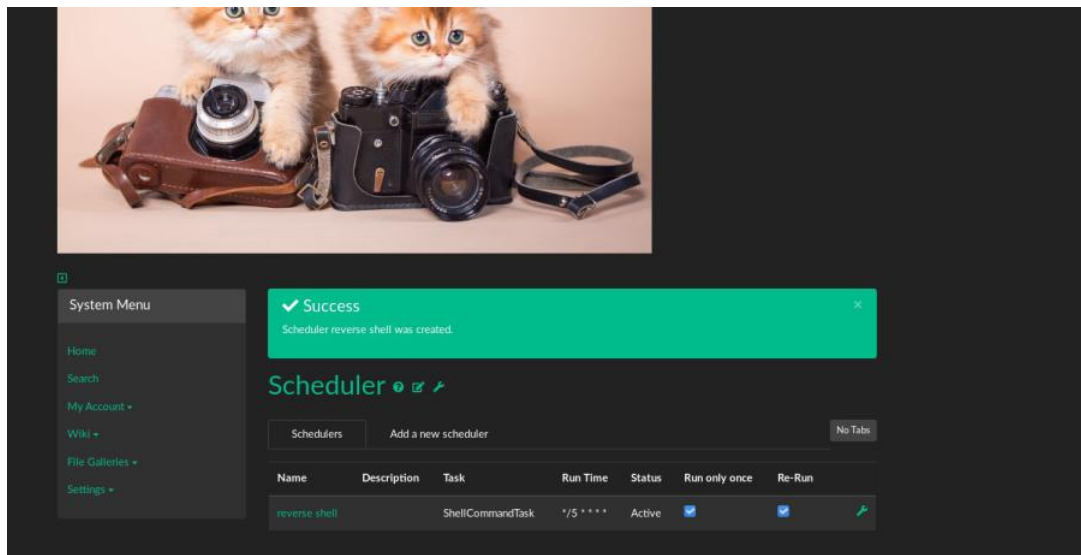
Changing administrators email adress



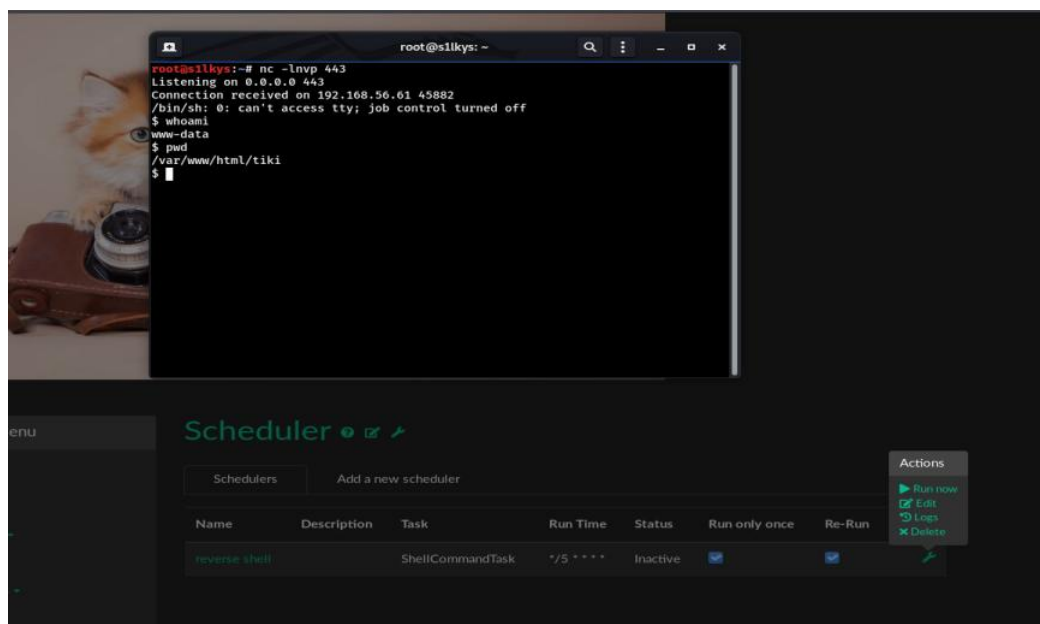
Email after change

Step 4: Attacker resets administrator password by clicking „I forgot my password“ and creates a new password, then logs in to TikiWiki as an administrator.

Step 5: Attacker creates new scheduler which executes a reverse shell



Scheduler is created



Scheduler executes reverse shell

Impact: Critical

Compromised Systems or accounts:

- Administrator account
- TikiWiki Application
- TikiWiki Server

See PoC Video: Attack Chain 2 (Demonstrates the change of administrators email address only)

Maximilian Barz (OSCP)
 Email: mbzra@protonmail.com
 Twitter: S1lky_1337