

[php-myseq-pv-assistance](#) / [doc](#) / [readme.md](#) Copy



 **heseltine** 1 minute ago



174 lines (95 loc) · 7.59 KB

[php-myseq-pv-assistance](#) / [doc](#) / [readme.md](#)

Up [Top](#)

[Preview](#) [Code](#) [Blame](#)

More options ...

SCR4 PV-Assistance Project, Jack Heseltine



Based on php-mysql-bookstore-dev-8 sample project, FHOoe/Hagenberg SCR4 2023.

Test-Login (admin)

user: 'admin'

password: 'admin'

DDEV Instructions

```
ddev import-db --src=db/pv-assistance.sql  
ddev describe  
ddev start  
ddev stop
```



URLs

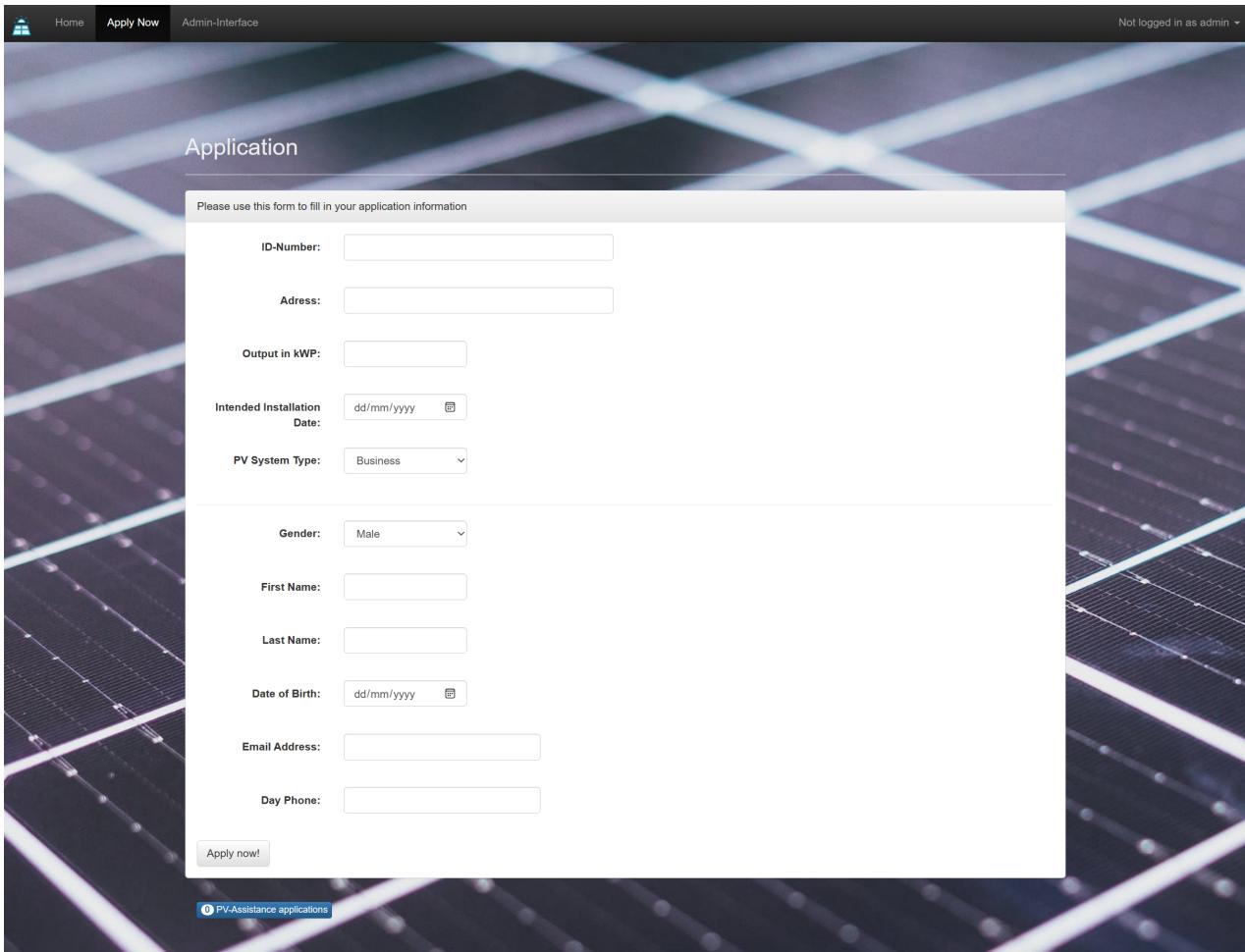
home: <https://pv-assistance.ddev.site/>

phpmyadmin: <https://pv-assistance.ddev.site:8037/>

Idea/Project Description and Architecture

Idea

The core architectural idea is a no-credentials log in for the application part, so it is accessible, and a protected area for Sachbearbeiter. The "Sachbearbeiter" (admin) can log in with their credentials and have access to the protected area. The admin can then create, read, update and delete data from the database.



The screenshot shows a web application interface for a solar panel application. The background features a close-up image of solar panels with white grid lines. At the top, there's a navigation bar with icons for Home, Apply Now, Admin-Interface, and a dropdown for user status. Below the navigation is a title 'Application' and a sub-instruction 'Please use this form to fill in your application information'. The form contains several input fields: ID-Number, Address, Output in KWP, Intended Installation Date (with a date picker icon), PV System Type (Business dropdown), Gender (Male dropdown), First Name, Last Name, Date of Birth (date picker), Email Address, and Day Phone. At the bottom left is a 'Apply now!' button, and at the bottom right is a link to 'PV-Assistance applications'.

The main application-UI is the form for submission, for admins it is a simple UI allowing status updates and data manipulation (accepted or rejected, optionally notes). There is also a token-protected area for getting the latest version of the application, for the applicant.

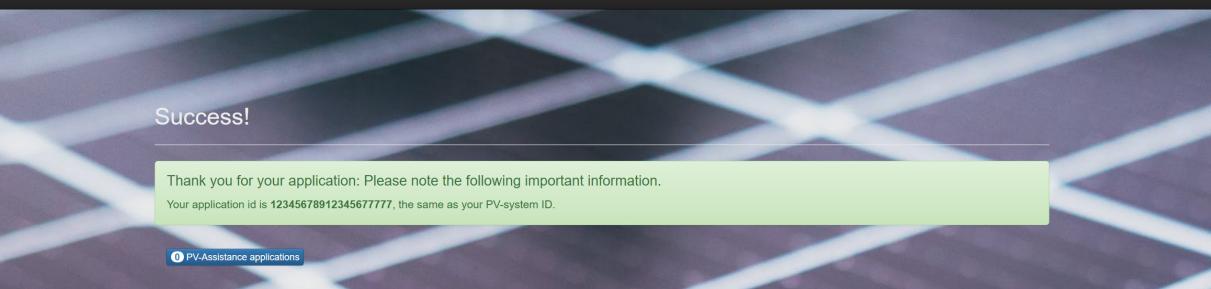
Architecture

The major component is an application form submitted to the Controller (POST-request) to handle input checks server-side, as specified, and either display feedback or a submission confirmation for the application. The DataManager handles writing to the database when all input checks have passed (createUser(), createApplication()): the central element is construction php objects from the query results, and vice versa. These can then also be accessed in the Controller.

Input-Error Case:

A screenshot of a web application interface. At the top, there is a dark header bar with the 'Home' icon, 'Apply Now' button, and 'Admin-Interface' link. On the far right, it says 'Not logged in as admin'. The main content area has a light gray background with a large, faint watermark-style graphic of a road or path. In the center, there is a red rectangular callout box containing four validation error messages: 'ID must be 20 digits long, please check your ID', 'Please enter a valid first name', 'Please enter a valid last name', and 'Please enter a valid email address'. Below this, the word 'Application' is displayed in a large, bold, black font. At the bottom, there is a white input form with the placeholder text 'Please use this form to fill in your application information'.

Success-Case:

 Home Apply Now Review Existing Application Admin 

Everything is also tracked per user and application, especially, including IP address:

			12345678912345678212	2 OTTENSHEIMERSTRASSE 68	0.05	2023-06-08	business	2023-06-13 12:23:13	172.19.0.6	Yh(WM 2949899c36a123...	showRequest0efdbbcba-0407-4c39-9eac-09a040d43c99	In Progress
--	--	--	----------------------	-----------------------------	------	------------	----------	---------------------	------------	----------------------------	--	-------------

Admin log-in:

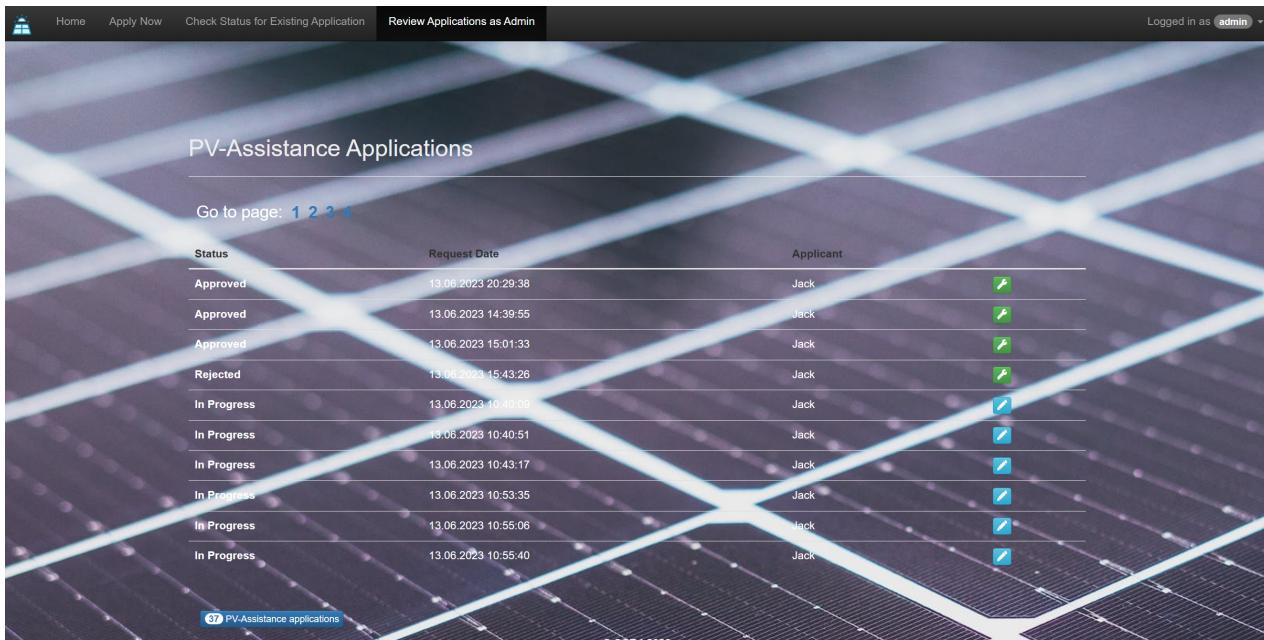
A screenshot of a web application's login interface. The background features a dark purple gradient with white diagonal lines forming an 'X' pattern. At the top, there is a navigation bar with icons for Home, Apply Now, and Check Status for Existing Application, along with an Admin dropdown. Below the navigation bar is a large, bold 'Log In' heading. A central callout box contains instructions: 'Please log in to process applications.' followed by two input fields labeled 'Username' and 'Password', both containing the placeholder text 'try \'admin\''. A 'Login' button is positioned below the password field. At the bottom left, there is a small badge with the number '37' and the text 'PV-Assistance applications'. The bottom right corner displays the text 'SCR4 2023'.

After login an additional header section is available to admins.

Header partial and login actions in the controller/DataManager implement the login functionality for admins. In the logged in state admins have an additional header link that allows them to access the forms for processing. (Admin sign up is out of scope, see existing admin database entries.)

Admin processing:

List view:



PV-Assistance Applications

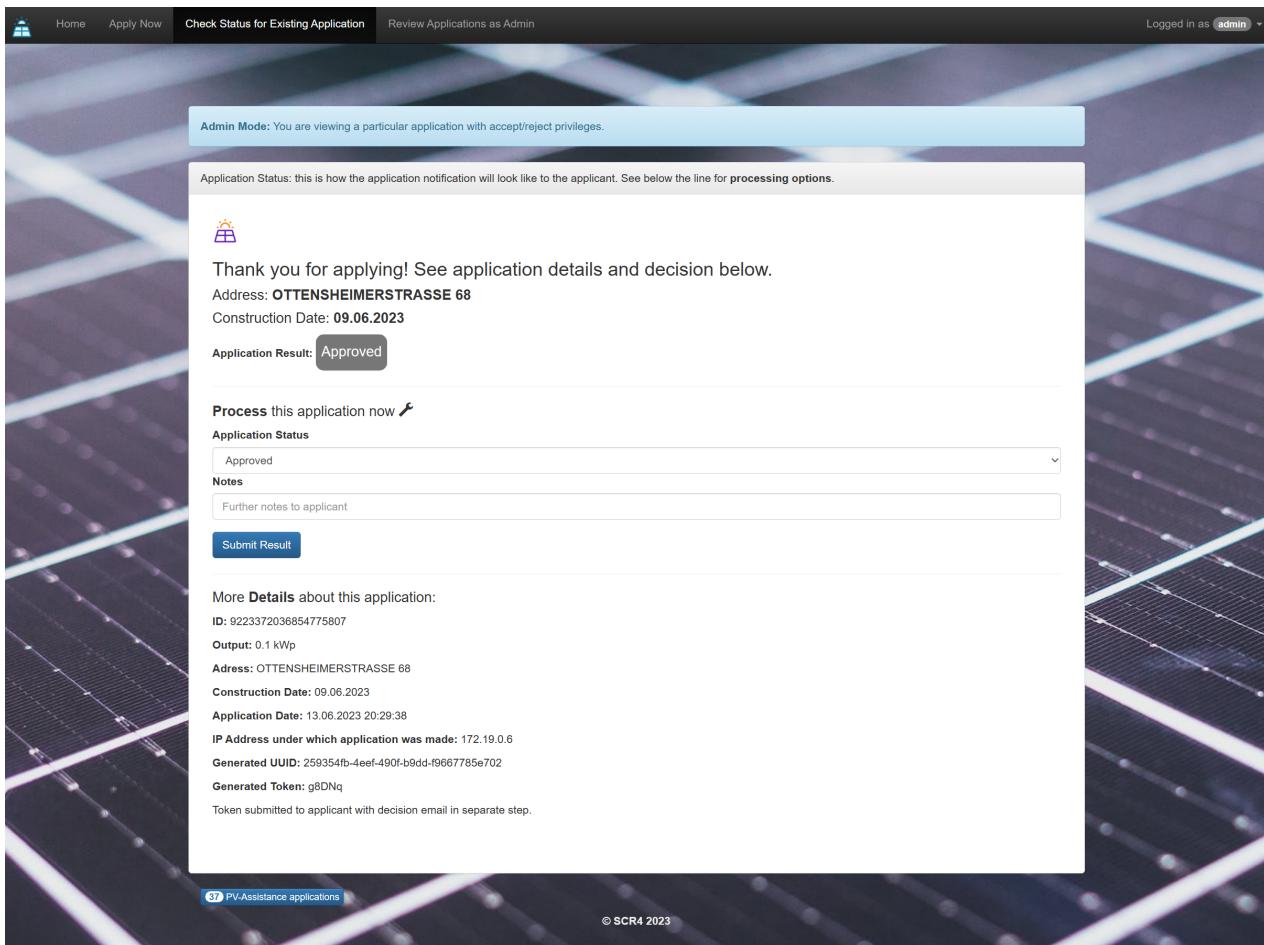
Go to page: 1 2 3 4

Status	Request Date	Applicant
Approved	13.06.2023 20:29:38	Jack
Approved	13.06.2023 14:39:55	Jack
Approved	13.06.2023 15:01:33	Jack
Rejected	13.06.2023 15:43:26	Jack
In Progress	13.06.2023 16:19:09	Jack
In Progress	13.06.2023 10:40:51	Jack
In Progress	13.06.2023 10:43:17	Jack
In Progress	13.06.2023 10:53:35	Jack
In Progress	13.06.2023 10:55:06	Jack
In Progress	13.06.2023 10:55:40	Jack

37 PV-Assistance applications

A click on the edit button links to checkStatus tailored to admins, allowing for token processing and similar. The other side of the same view will be the user side.

Approved case:



Admin Mode: You are viewing a particular application with accept/reject privileges.

Application Status: this is how the application notification will look like to the applicant. See below the line for processing options.

 Thank you for applying! See application details and decision below.
 Address: OTTENSHEIMERSTRASSE 68
 Construction Date: 09.06.2023
 Application Result: Approved

Process this application now 

Application Status

Notes
 Further notes to applicant

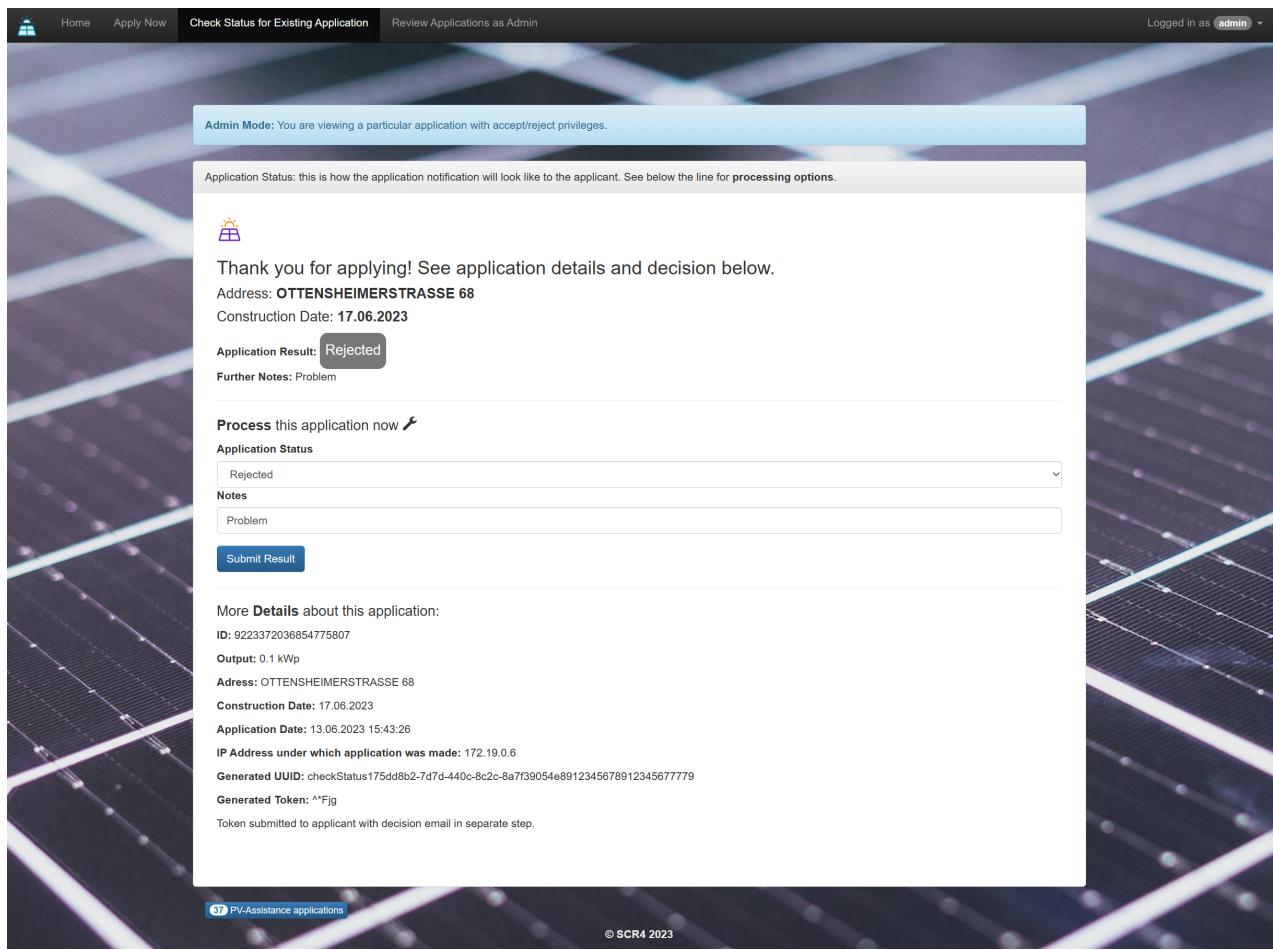
Submit Result

More Details about this application:
 ID: 9223372036854775807
 Output: 0.1 kWp
 Address: OTTENSHEIMERSTRASSE 68
 Construction Date: 09.06.2023
 Application Date: 13.06.2023 20:29:38
 IP Address under which application was made: 172.19.0.6
 Generated UUID: 259354fb-4eeb-490f-b9dd-f9667785e702
 Generated Token: gBDNq
 Token submitted to applicant with decision email in separate step.

37 PV-Assistance applications

© SCR4 2023

Rejected Case including note and db representation:



Admin Mode: You are viewing a particular application with accept/reject privileges.

Application Status: this is how the application notification will look like to the applicant. See below the line for processing options.

 Thank you for applying! See application details and decision below.
Address: OTTENSHEIMERSTRASSE 68
Construction Date: 17.06.2023

Application Result: **Rejected**

Further Notes: Problem

Process this application now 

Application Status

Notes

Submit Result

More Details about this application:
ID: 9223372036854775807
Output: 0.1 kWp
Address: OTTENSHEIMERSTRASSE 68
Construction Date: 17.06.2023
Application Date: 13.06.2023 15:43:26
IP Address under which application was made: 172.19.0.6
Generated UUID: checkStatus175dd8b2-7d7d-440c-8c2c-8a7f39054e8912345678912345677779
Generated Token: ^Fjg
Token submitted to applicant with decision email in separate step.

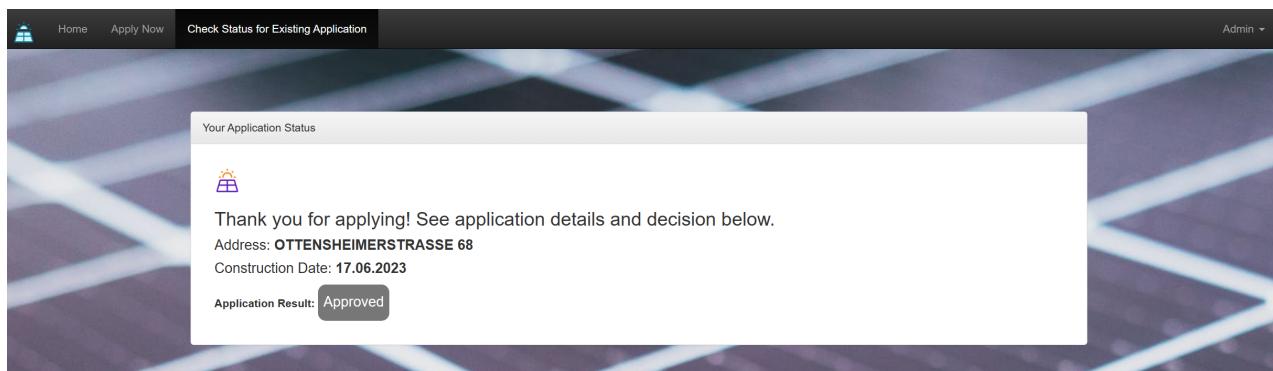
32 PV-Assistance applications © SCR4 2023

OTTENSHEIMERSTRASSE 68	0.1 2023-06-17	business	2023-06-13 15:43:26 172.19.0.6	^Fjg	checkStatus175dd8b2-7d7d-440c-8c2c-8a7f39054e89123...	Rejected Problem
---------------------------	----------------	----------	--------------------------------	------	---	------------------

The user is more limited in their options.

Application display once processed (with result):

(Approved case:)

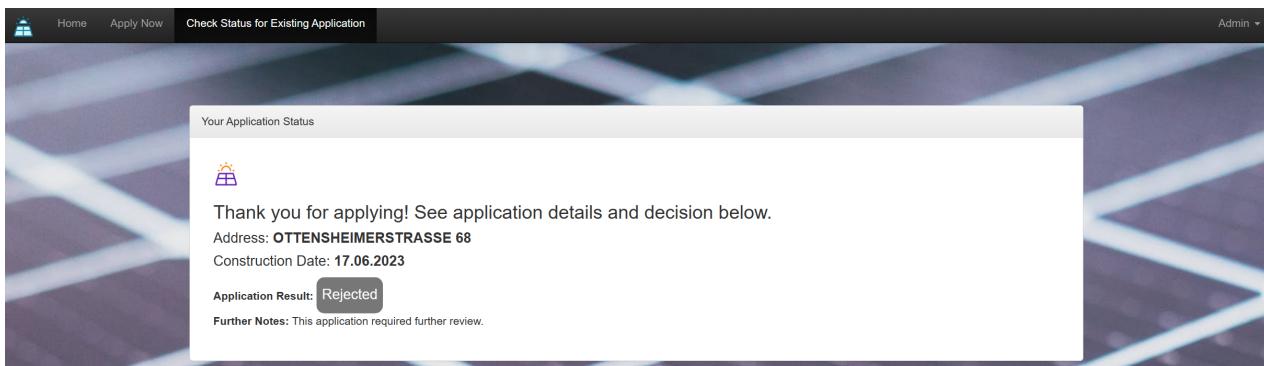


Your Application Status

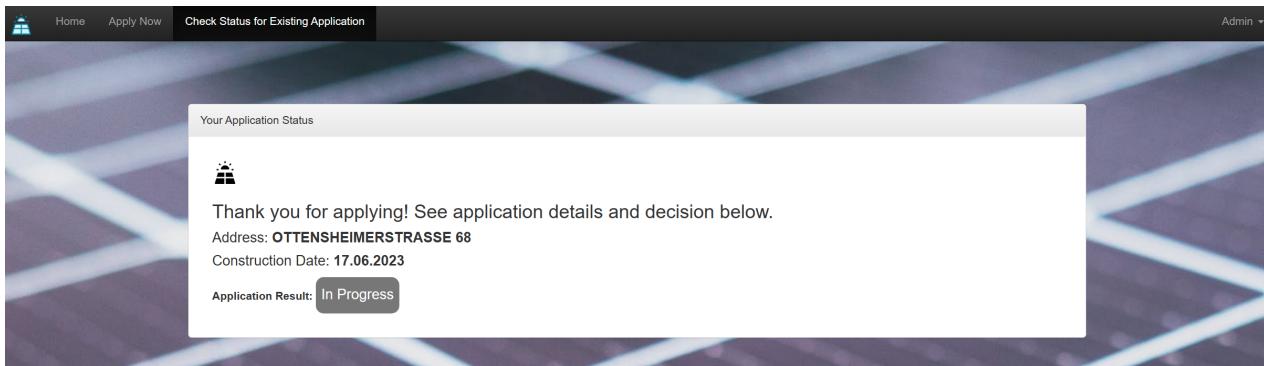
 Thank you for applying! See application details and decision below.
Address: OTTENSHEIMERSTRASSE 68
Construction Date: 17.06.2023

Application Result: **Approved**

(Rejected case:)



For completeness, in progress can also be called and looks like this:



Security: UUID Mechanism

The access URL is encoded in the following snippet.

```
// 32 bits for "time_low"  
mt_rand(0, 0xffff), mt_rand(0, 0xffff),  
  
// 16 bits for "time_mid"  
mt_rand(0, 0xffff),  
  
// 16 bits for "time_hi_and_version",  
// four most significant bits holds version number 4  
mt_rand(0, 0x0fff) | 0x4000,  
  
// 16 bits, 8 bits for "clk_seq_hi_res",  
// 8 bits for "clk_seq_low",  
// two most significant bits holds zero and one for variant DCE1.1  
mt_rand(0, 0x3fff) | 0x8000,  
  
// 48 bits for "node"  
mt_rand(0, 0xffff), mt_rand(0, 0xffff), mt_rand(0, 0xffff)
```



The code generates a version 4 UUID (Universally Unique Identifier) using random numbers. UUIDs are 128-bit identifiers that are typically used to uniquely identify objects or entities in computer systems.

Here's a breakdown of the code:

The first line generates the "time_low" part of the UUID, which consists of 32 bits. It uses `mt_rand(0, 0xffff)` twice to generate two random 16-bit numbers.

The second line generates the "time_mid" part of the UUID, which is another 16 bits. It uses `mt_rand(0, 0xffff)` to generate a random 16-bit number.

The third line generates the "time_hi_and_version" part of the UUID, which is 16 bits as well. It combines a random 16-bit number generated by `mt_rand(0, 0x0fff)` with the version number 4 (represented by the bitwise OR operation `| 0x4000`).

The fourth line generates the "clk_seq_hi_res" and "clk_seq_low" parts of the UUID, which together make up 16 bits. It combines a random 14-bit number generated by `mt_rand(0, 0x3fff)` with the variant bits for DCE1.1 (represented by the bitwise OR operation `| 0x8000`).

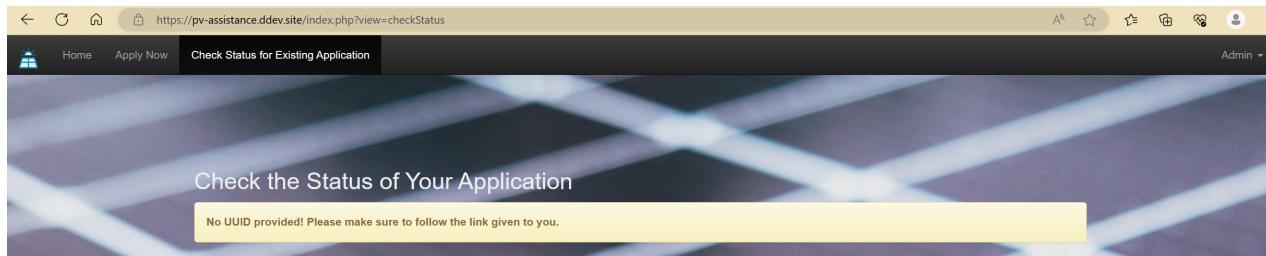
The remaining three lines generate the "node" part of the UUID, which is 48 bits. They use `mt_rand(0, 0xffff)` three times to generate three random 16-bit numbers.

Overall, the code uses the `mt_rand` function to generate random numbers within specific ranges and combines them to form a version 4 UUID with the required format and structure.

Security: Overall Concept

UUID and token provide two factors for security. The interface is:

(No-UUID case:)



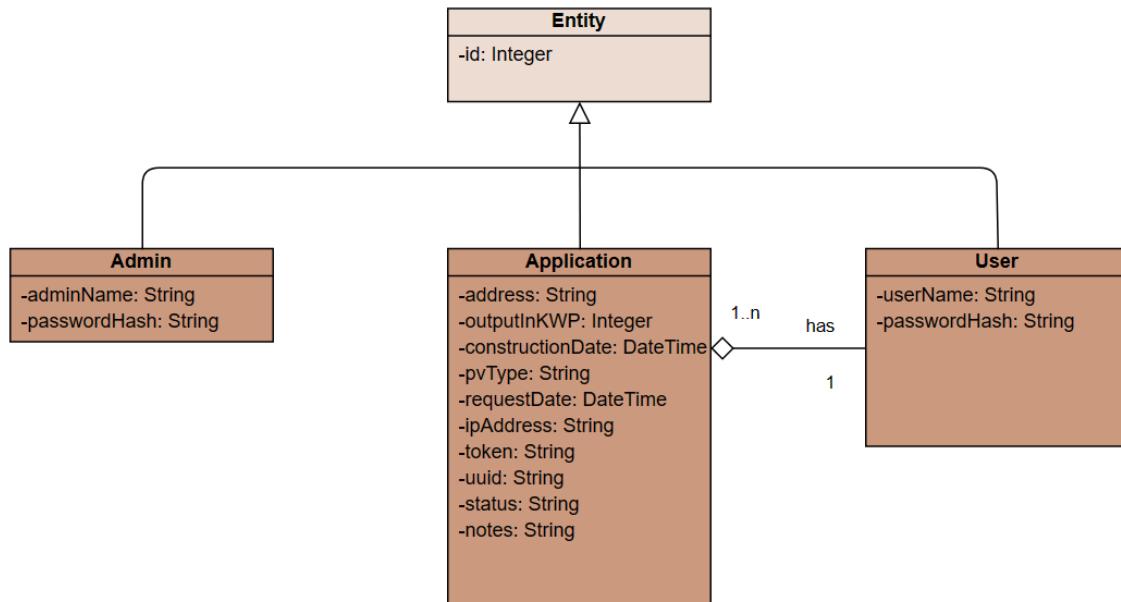
(UUID-link followed correctly:)



As specified, token- and UUID distribution are not implemented here. A simple separation of the two factors when sending (sending at different times) provides a good degree of security.

DB-Structure (UML)

The basic structure reflected in the classes for this project is User for applicants, Admin for application reviewers, Application for applications.



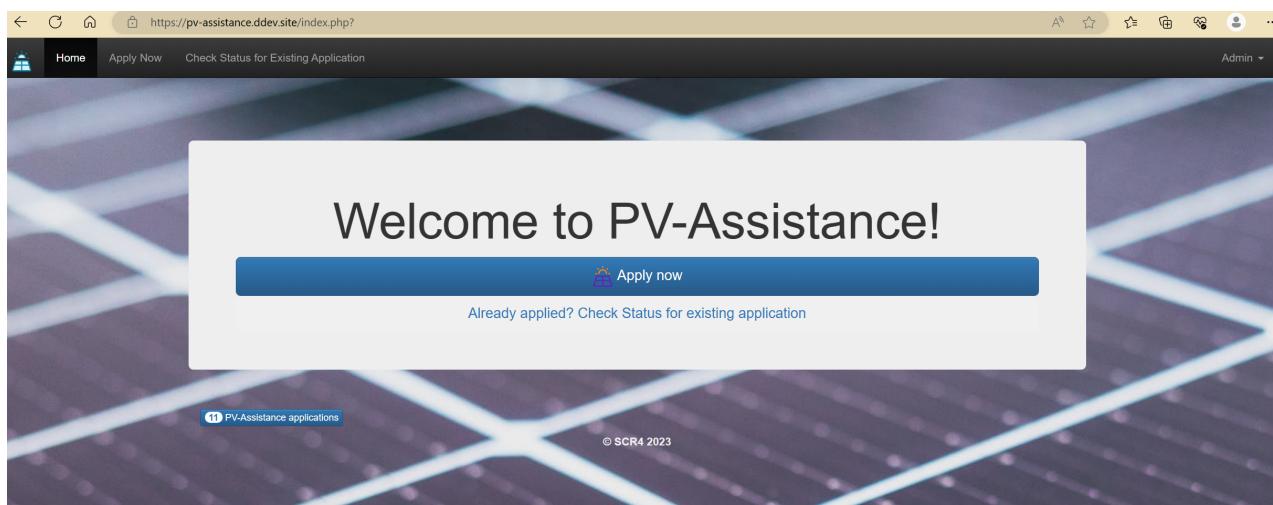
The text-based log is represented in the db, but not in the program class structure.

DB-Structure (SQL)

Test Cases

Major functionality tests were already covered in the preceding Architecture discussion, so I will focus on pen-testing here.

Trying to list applications (by direct link) as non-admin: Redirects to homepage.



Accessing an application without valid UUID has been tested. Valid UUID, but wrong token:

The screenshot shows a web interface titled "Check Status for Existing Application". At the top, there are links for "Home" and "Apply Now", and a user dropdown set to "Admin". A red error message box contains the text "Application not found, please check your ID and token". Below it, a yellow info box says "No UUID provided! Please make sure to follow the link given to you.". A central form is titled "Token-Access-Control" and contains a text input field with the value "test" and a button labeled "Get Status Now". At the bottom left, there's a small blue badge with "11 PV-Assistance applications". The footer includes the copyright notice "© SCR4 2023".

Finally, a log representation, where the logging feature was added at all the sensible junctions.

		<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	id	IPAddress	action	userId	timestamp
		<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	2	172.19.0.6	application with uuid showRequest73767a4f-c23b-4dc...	1	2023-06-15 10:24:36
		<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	3	172.19.0.6	application with uuid checkStatus4643f918-7b8e-48a...	1	2023-06-15 10:33:08
		<input type="checkbox"/>	<input type="checkbox"/> Edit	<input type="checkbox"/> Copy	<input type="checkbox"/> Delete	4	172.19.0.6	new application with uuid 959eb92c-c97a-4449-9678....	1	2023-06-15 10:50:20