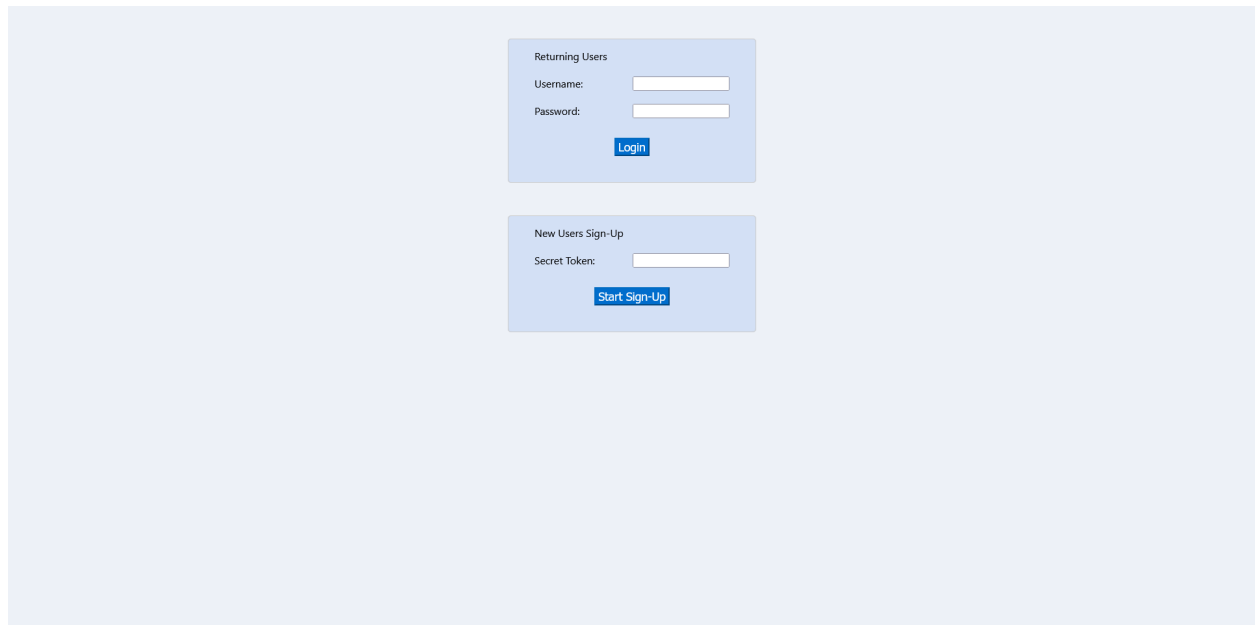
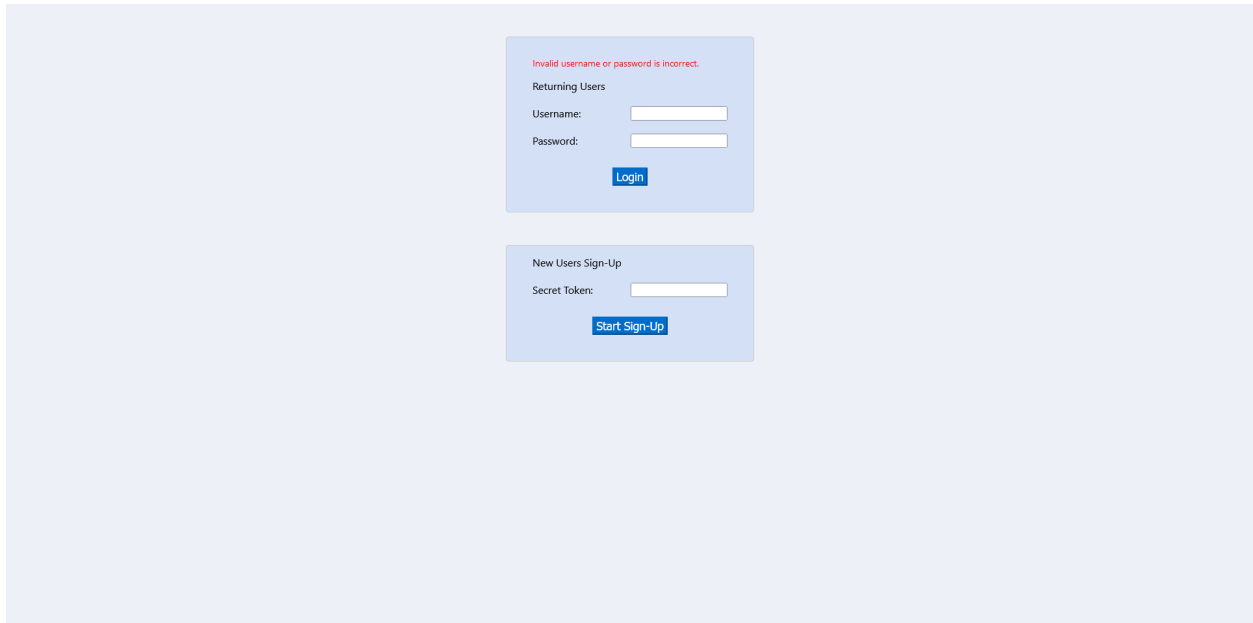


I used some code from a previous feedback site that I had to create in Engineering Secure Software. However, a lot of things had to be rewritten and modified to ensure all functionality was introduced. Several files had to be written from scratch. Most of the HTML and CSS was able to be reused. As such, I apologize if the code is a bit inconsistent in some places.

I wiped the database and reran the configuration script before starting. When the site is first visited, we have the choice to logon or enter the token needed to create an account.

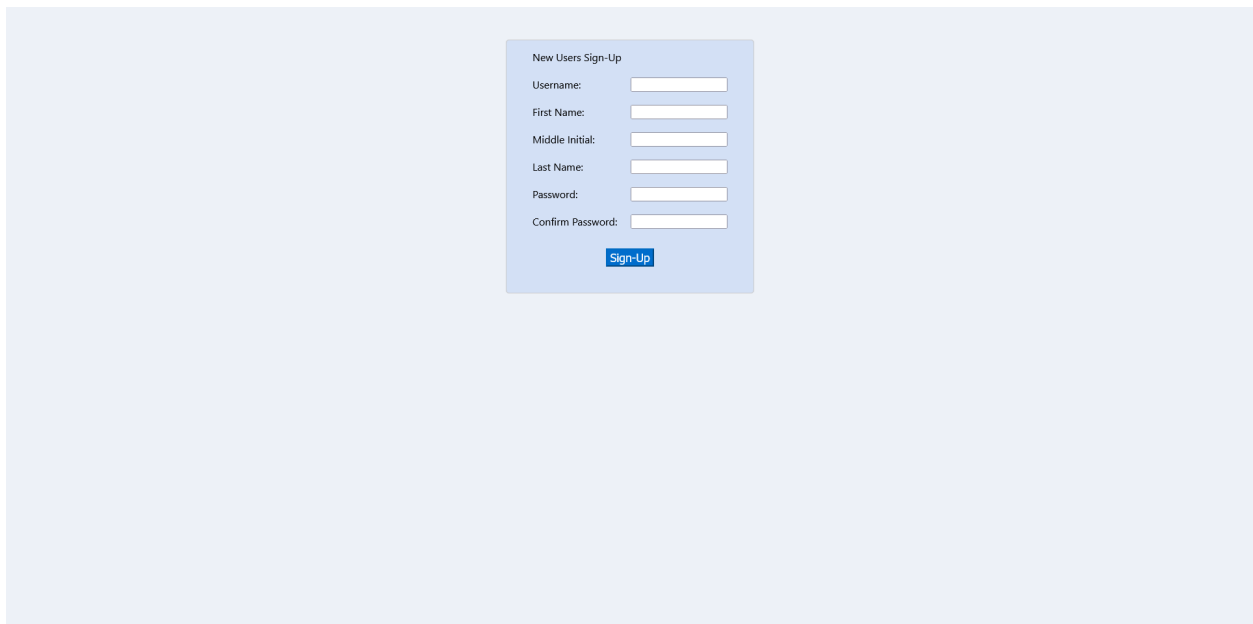
The image shows a web interface with two distinct login/sign-up forms. The top form, titled 'Returning Users', is a light blue box containing labels for 'Username:' and 'Password:', each followed by a white input field. A blue 'Login' button is positioned below the password field. The bottom form, titled 'New Users Sign-Up', is also a light blue box, featuring a 'Secret Token:' label and a white input field, with a blue 'Start Sign-Up' button below it. Both forms are centered on a light blue background.

I enter some random nonsense into the returning users box and hit enter. I get an error message about invalid credentials. Since the user I entered doesn't exist, there won't be an entry into the attempt logons table.



The screenshot shows two forms on a light blue background. The top form is titled "Returning Users" and contains fields for "Username:" and "Password:", followed by a blue "Login" button. Above these fields is a red error message: "Invalid username or password is incorrect." The bottom form is titled "New Users Sign-Up" and contains a single field for "Secret Token:", followed by a blue "Start Sign-Up" button.

After entering the token “WebScienceRules” into the new users sign up form, I am redirected to the correct form.



The screenshot shows a "New Users Sign-Up" form on a light blue background. The form includes fields for "Username:", "First Name:", "Middle Initial:", "Last Name:", "Password:", and "Confirm Password:", followed by a blue "Sign-Up" button.

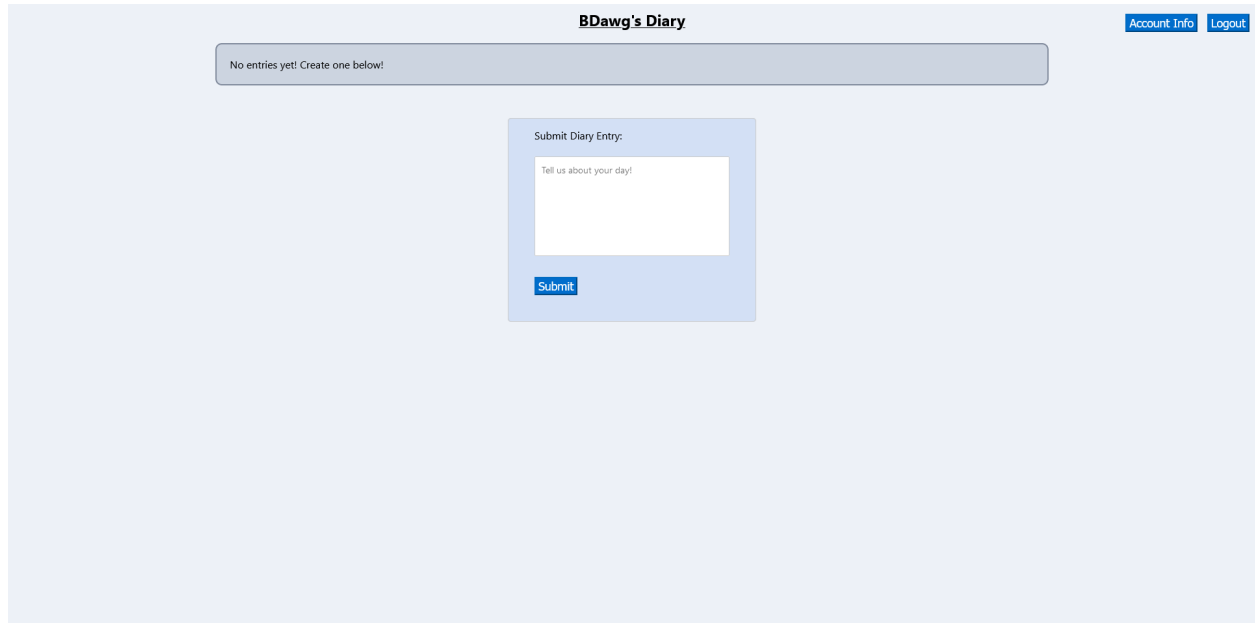
I enter some data and select sign up. I don’t show it here, but I do check that passwords match and show a message if they don’t. I also check that the name isn’t used already. A message is shown to indicate success.

The screenshot shows a light blue background with two white boxes. The top box is titled 'Returning Users' and contains a 'Username:' field with the text 'BDawg', a 'Password:' field with four dots, and a blue 'Login' button. The bottom box contains a green message 'Success! Log in above.', a 'New Users Sign-Up' section with a 'Secret Token:' field, and a blue 'Start Sign-Up' button.

I haven't logged in yet, so if I look at the database, I should see one user and no entries in the diary entries table or logon attempts table.

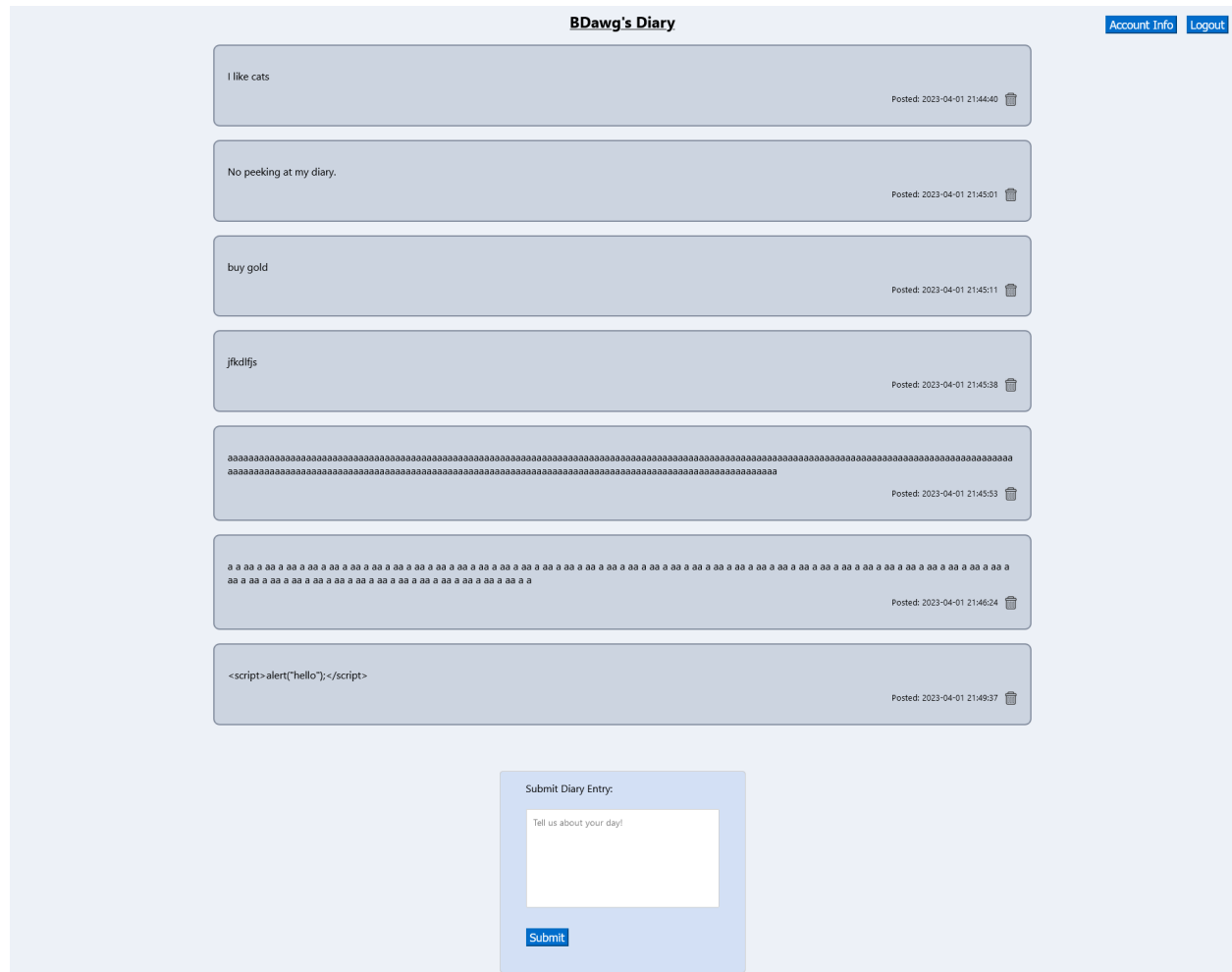
Table	Action	Rows	Type	Collation	Size	Overhead
<input type="checkbox"/> tbl_diary_entries	★ Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_general_ci	32.0 KiB	-
<input type="checkbox"/> tbl_logon_attempts	★ Browse Structure Search Insert Empty Drop	0	InnoDB	utf8mb4_general_ci	32.0 KiB	-
<input type="checkbox"/> tbl_users	★ Browse Structure Search Insert Empty Drop	1	InnoDB	utf8mb4_general_ci	16.0 KiB	-
3 tables	Sum	1	InnoDB	utf8mb4_general_ci	80.0 KiB	0 B

When logged on, I see this. My username is visible as well as a link to the account info (logon history) and a button to logout.

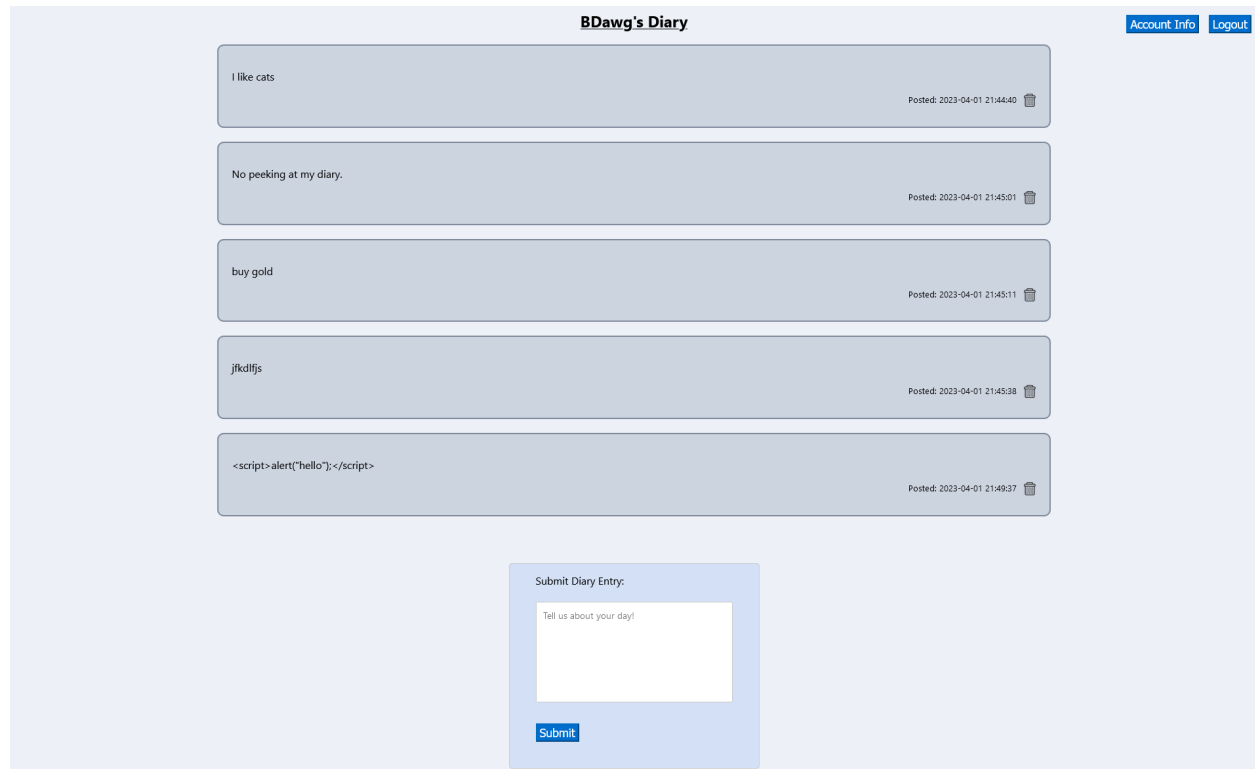


The screenshot shows the 'BDawg's Diary' web application. At the top, there is a header with the title 'BDawg's Diary' and two links: 'Account Info' and 'Logout'. Below the header, a message box states 'No entries yet! Create one below!'. In the center, there is a form titled 'Submit Diary Entry:' with a text area labeled 'Tell us about your day!' and a 'Submit' button at the bottom.

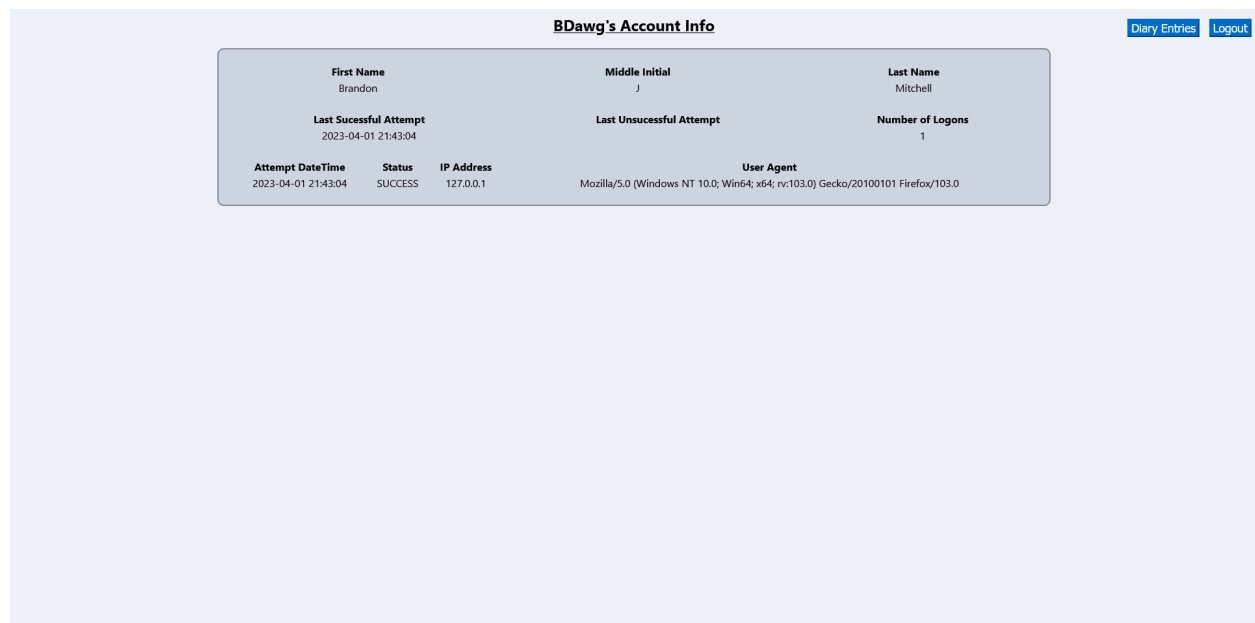
I inserted a bunch of entries. You can't tell in the picture, but the buttons are stuck to the corner and will always be there when you scroll. I also tested inserting some HTML code. Prepared statements are used whenever data is being inserted into a string. The date and time of the post is in the corner (the time on my server doesn't seem to match my computer's time) and a trash bin icon button is used to delete things. It is actually a form and clicking the image submits it.



I delete a couple to make sure the delete functionality works.



I click the account info button and am able to view my login history.



Clicking the diary entries button brings me back to my diary entries.

BDawg's Diary[Account Info](#)[Logout](#)

I like cats

Posted: 2023-04-01 21:44:40

No peeking at my diary.

Posted: 2023-04-01 21:45:01

buy gold

Posted: 2023-04-01 21:45:11

jfkdlfjs

Posted: 2023-04-01 21:45:38

<script>alert("hello");</script>

Posted: 2023-04-01 21:49:37

Submit Diary Entry:

Tell us about your day!

Submit

Clicking the logout button destroys my session and brings me to the landing page so I can sign back in or create another account.

Returning Users

Username:

Password:

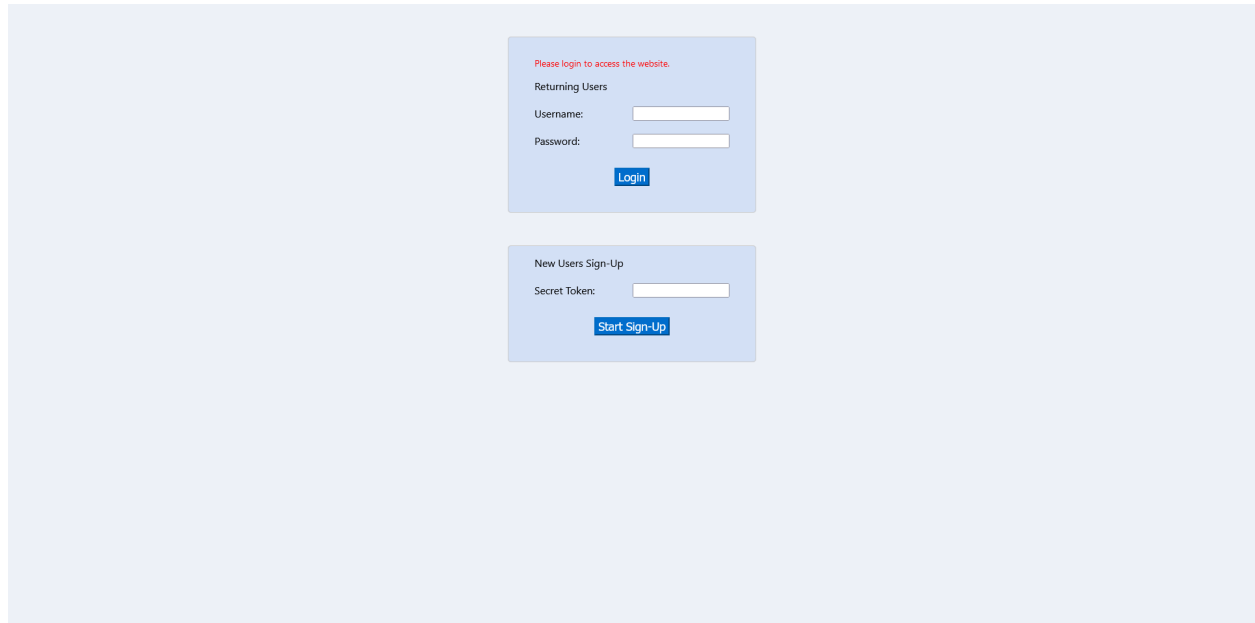
Login

New Users Sign-Up

Secret Token:

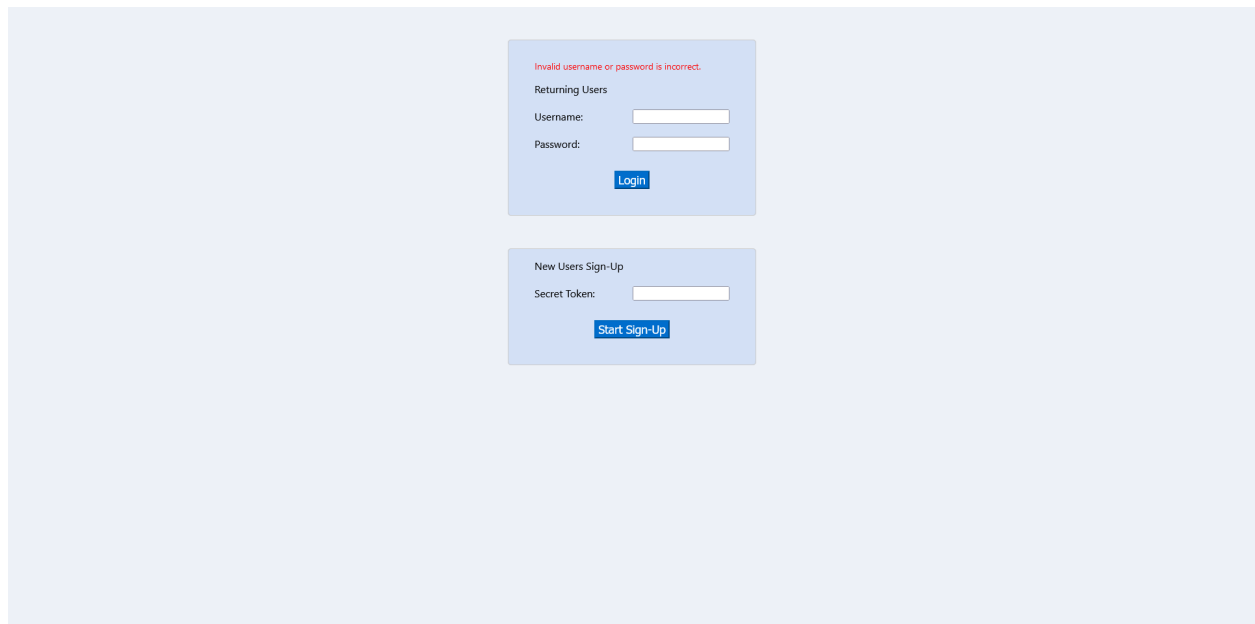
Start Sign-Up

I can verify it logged me out correctly by trying to visit the entries page again. I am redirected back to the landing page with an error message. I also test with the account info page and get the same message.



The screenshot shows two forms on a light blue background. The top form is titled "Returning Users" and contains a red error message "Please login to access the website." Below this, there are input fields for "Username:" and "Password:", followed by a blue "Login" button. The bottom form is titled "New Users Sign-Up" and contains a "Secret Token:" input field, followed by a blue "Start Sign-Up" button.

I go ahead and try signing in again but with an incorrect password. I get a warning and I don't sign in. Behind the scenes, the logon history is updated.



This screenshot is identical to the one above, but the red error message in the "Returning Users" form now reads "Invalid username or password is incorrect." The rest of the form structure, including the "Username:" and "Password:" fields, the "Login" button, and the "New Users Sign-Up" form below it, remains the same.

I log in with the correct information and then check the logon history. We see that there are two new entries: one for an unsuccessful attempt and one for a successful attempt. This makes sense. The last unsuccessful logon is updated. The number of logons is at two. I interpreted it as the number of successful logons, not the total logon attempts, so it shows 2 for the two successful attempts.

BDawg's Account Info

[Diary Entries](#)[Logout](#)

First Name Brandon	Middle Initial J	Last Name Mitchell																
Last Successful Attempt 2023-04-01 22:35:43	Last Unsuccessful Attempt 2023-04-01 22:34:57	Number of Logons 2																
<table><tr><th>Attempt DateTime</th><th>Status</th><th>IP Address</th></tr><tr><td>2023-04-01 21:43:04</td><td>SUCCESS</td><td>127.0.0.1</td></tr><tr><td>2023-04-01 22:34:57</td><td>FAILURE</td><td>127.0.0.1</td></tr><tr><td>2023-04-01 22:35:43</td><td>SUCCESS</td><td>127.0.0.1</td></tr></table>	Attempt DateTime	Status	IP Address	2023-04-01 21:43:04	SUCCESS	127.0.0.1	2023-04-01 22:34:57	FAILURE	127.0.0.1	2023-04-01 22:35:43	SUCCESS	127.0.0.1	<table><tr><th>User Agent</th></tr><tr><td>Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0</td></tr><tr><td>Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0</td></tr><tr><td>Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0</td></tr></table>		User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0
Attempt DateTime	Status	IP Address																
2023-04-01 21:43:04	SUCCESS	127.0.0.1																
2023-04-01 22:34:57	FAILURE	127.0.0.1																
2023-04-01 22:35:43	SUCCESS	127.0.0.1																
User Agent																		
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0																		
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0																		
Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0																		

I go ahead and try creating another user. I put the wrong token in this time to verify it correctly redirects me.

Returning Users

Username:

Password:

Login

Incorrect Token.

New Users Sign-Up

Secret Token:

Start Sign-Up

I go ahead and create another user and then log in. I am unable to see the other user's entries on the entries page and I see the new user's info on the account info page.

Cats's Diary [Account Info](#) [Logout](#)

No entries yet! Create one below!

Submit Diary Entry:

Tell us about your day!

[Submit](#)

Cats's Account Info [Diary Entries](#) [Logout](#)

First Name Cats	Middle Initial C	Last Name Cats
Last Successful Attempt 2023-04-01 22:43:42	Last Unsuccessful Attempt	Number of Logons 1
Attempt DateTime 2023-04-01 22:43:42	Status SUCCESS	IP Address 127.0.0.1
User Agent Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0		

I create a third user with some HTML in their name to verify I am correctly escaping HTML from the user. It appears to show correctly, so the escaping should be working.

<div>cats</div>'s Account Info

Diary Entries

Logout

First Name		Middle Initial		Last Name	
<div>cats</div>		h		<div>cats</div>	
Last Sucessful Attempt		Last Unsuccesful Attempt		Number of Logons	
2023-04-01 22:46:11				1	
Attempt DateTime	Status	IP Address	User Agent		
2023-04-01 22:46:11	SUCCESS	127.0.0.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:103.0) Gecko/20100101 Firefox/103.0		