CISC472 PENTESTING REPORT

by

Calvin Banning

A self-critique of the UX and security for the final project of CISC472. Hosted versions of the project can be found at https://banningcalvin-redchan.glitch.me/ and at https://github.com/banningcalvin/redchan/.

2020

TABLE OF CONTENTS

Chapter

Chapter 1

SECURITY EVALUATION

A pentesting report for the final project of CISC472. Hosted versions of the project can be found at:

https://banningcalvin-redchan.glitch.me/

and at :

https://github.com/banningcalvin/redchan/.

1.1 Trivial Vulnerabilities

These vulnerabilities will not result in data loss, but may result in an adverse user experience. For this project, it is completely understandable that these would be present for testing purposes, but a production environment should have solutions to all of these.

- Users can comment very quickly and overload a post with comments.

1.2 Data Vulnerabilities

In addition to UIDs being openly displayed, examining network output reveals even more data:

1.3 Testing of other vulnerabilities

I briefly tried a variety of common attacks to see if the application was vulnerable:

- Firebase is not vulnerable to SQL injection, and it appears that all data is sent and received from firebase.
- Session management appears to be solid. All of this seems to be followed according to firebase specifications, and trying to break this would be a futile exercise.

1.4 Vulnerability Resolution

The most important vulnerability to patch is how posts are attributed to authors. The developers must stop attribute posts based on auth tokens, rather than a user-supplied UID. Having a Firebase function which assigns the author value in the database rather than allowing the user to pass in an arbitrary value is a quick and secure fix for this.

Next, various steps should be taken to secure this development environment before it moves to production. Identify users with a username rather than a UID, and prevent information like their personal email from being leaked by comment and post data.

Finally, spam attacks can be prevented by adding post timers or a captcha to all registrations, posts and comments, which would prevent users from creating massive volumes of phony accounts, comments, posts, and votes.

Chapter 2

UX QUALITY ASSURANCE

A self-critique of the UX for the final project of CISC472. Hosted versions of the project can be found at:

https://banningcalvin-redchan.glitch.me/

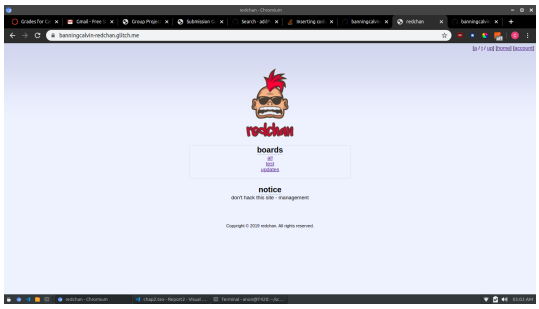
and at :

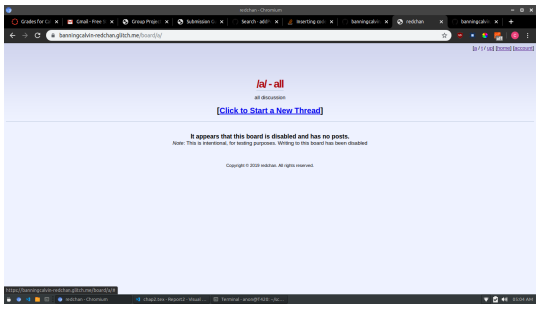
https://github.com/banningcalvin/redchan/.

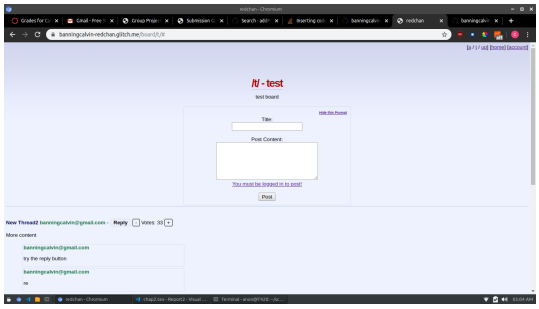
It is important to note that because I created this, some level of bias may be present in that I knew my own design goals and built the design in a way that I was satisfied with. I am not entirely sure how others will interpret the layout or color scheme.

2.1 Overview

On the following pages is a series of screenshots for reference. In order, they are the homepage, the /a/ board, the /t/ board, and the account page.







2.2 Evaluation

The website clearly follows in the design of discussion boards less reputable than Reddit such as 4chan and 2chan. The site is not modern and does not follow modern design styles (as intended), but it does not fail to deliver an enjoyable and intuitive user experience.

The homepage delivers basic information: it offers links to the various boards, a link to the account page, and a message from the site owner. Having a dedicated homepage is justified to act as a sort of directory and noticeboard for the site, and helps give the site some character. Because the user experience is primarily derived from discussion, rather than from consumption, I felt that this character was refreshing.

The boards are straightforward in their purpose and navigation. The styling doesn't seem quite as perfected and uniform as the sites it's modelled after, but it seems to do 'enough'.

The login page isn't as clean as the rest of the site. The logout button is always shown, even when the user is logged out, and the login button is awkwardly situated in the middle of the screen.

Other than that, the only other content on the site is posts. The /a/ board is disabled, but it has a notice which is professionally attached.

2.3 Suggestions

Not all users will share the admiration for this design style. In the same way that Reddit offers old.reddit.com, it might be useful to move this domain to old.redchan.com, and create a new frontend hosted at a different subdomain, which follows modern design fads. It should be understandable that this is out of scope for this project, as other tasks hold higher priority.

It would be wise to tweak the login and logout links to match the style of other buttons and links on the site. Additionally, the logout button should be displayed conditionally depending on the auth state.

On a final pass of the site, I discovered that upvotes were not working as expected. An investigation and patch is pending at the time of this writing.