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 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.

- Users can comment or post very quickly and overload a post with comments.
- User emails are used to identify posts. This presents a potential breach of privacy.
- When logged in, upvotes do not appear, and multiple seem to appear from a single click. (A bug, perhaps?). I recall this system working at one point, so I'll have to investigate what is broken in order to implement an appropriate fix.

1.2 Data Vulnerabilities

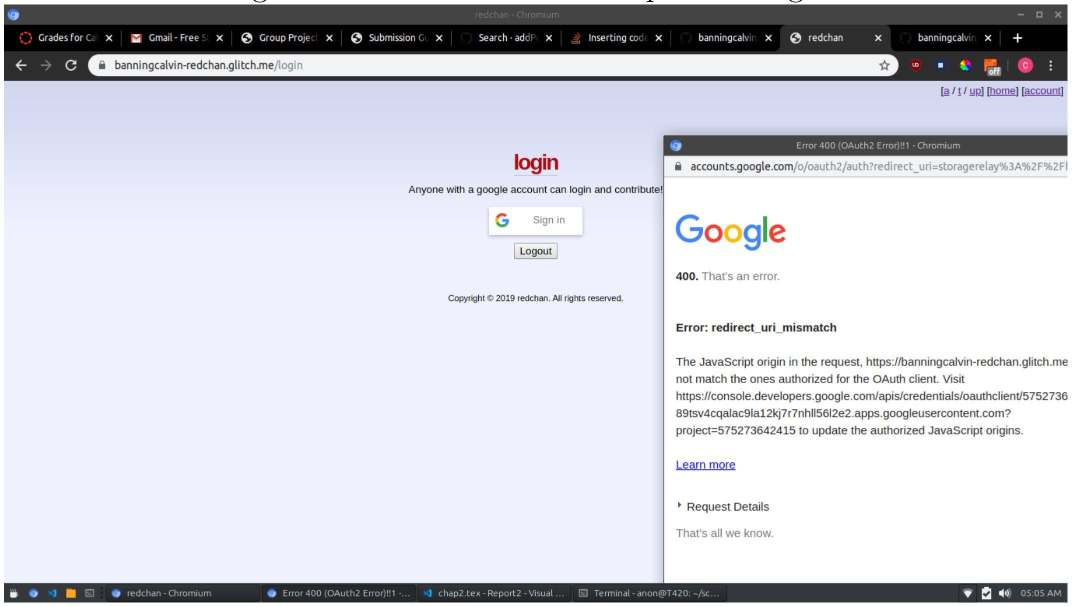
It doesn't seem that there are any major vectors to leak data on the website. The login system could conceivably be fooled by copying over a valid auth token, but because all data is sent via https, I felt that such an attack would be unsuccessful. However, I did think that the way I was storing the token while browsing a page was insecure. If an attacker had access to the cookies on the machine, they could copy them over to another. While a new token is generated on navigation, and it is set to timeout at a reasonable interval, a quick execution could mean that an attacker could potentially steal another user's credentials temporarily.

Other than this, Firebase - which is used as a backend - does not make any content not already shown on the site public, so UID's, etc. are kept private as they should be.

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 because all data is read only as plaintext and the way it is read into and out of Firebase.
- There do not seem to be any XSS vulnerabilities.
- I even found that glitch was not authorized to perform logins:



redchan - Chromium
banningcalvin-redchan.glitch.me/login
[a / t / up] [home] [account]
login
Anyone with a google account can login and contribute!
Sign in
Logout
Copyright © 2019 redchan. All rights reserved.
Error 400 (OAuth2 Error)!!1 - Chromium
accounts.google.com/o/oauth2/auth?redirect_uri=storagerelay%3A%2F%2F
Google

400. That's an error.

Error: redirect_uri_mismatch

The JavaScript origin in the request, https://banningcalvin-redchan.glitch.me
not match the ones authorized for the OAuth client. Visit
https://console.developers.google.com/apis/credentials/oauthclient/5752736
89tsv4cqalac9la12kj7r7nhll56l2e2.apps.googleusercontent.com?
project=575273642415 to update the authorized JavaScript origins.

Learn more

Request Details

That's all we know.

This is a testament to how well authentication is setup.

- Role elevation seemed impossible because of Firebase rules. In order to gain permissions to, say, post on the /up/ board (where you must be a moderator), there is no other way than to have an account. This is because setting the moderator flag can only be done from Firebase. From a UX perspective, this isn't the best method. However, such a utility would be rarely used because moderators would vastly outnumber users, so it is a low-priority problem.

1.4 Vulnerability Resolution

There are three security concerns which ought to be addressed before release. First, users should be identified by an anonymous username, rather than their personal email. This is a simple fix: force users to choose a unique username when logging in for the first time, and associate this with their account. When making posts, lookup the user according to the UID returned by the auth operation, and assign their username to the post. Do not allow the user to pass in a username, as they could pass in any arbitrary name and make it seem as if it were posted by another user.

Second, the upvote system should be fixed. They should appear immediately, and users should only be able to have a power of 1 vote. I think this might be related to how Firebase structures upvotes, and a failure on my part to ensure each vote is associated with a unique UID. Preventing duplicate votes if a UID-vote pair is present would be the quickest fix.

Finally, storing the auth token in a cookie seems to be a moderate security concern. Although this token is always updated on navigation, the fact that it is stored as plaintext, even on a single machine, and only for a short time, means that a compromised machine is an attack surface. Of course, stealing credentials with a keylogger is just as likely and outside the scope of this application's security, but cookie theft through other means is possible. Rather than storing the token in a cookie, simply generate one whenever necessary, and do not save it.

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/

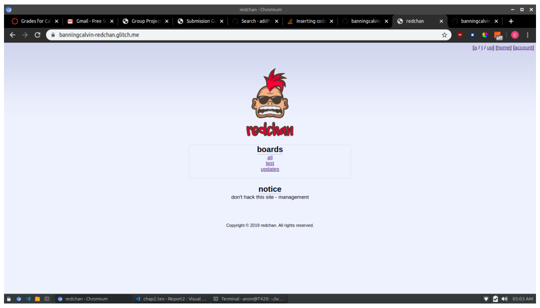
and at :

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

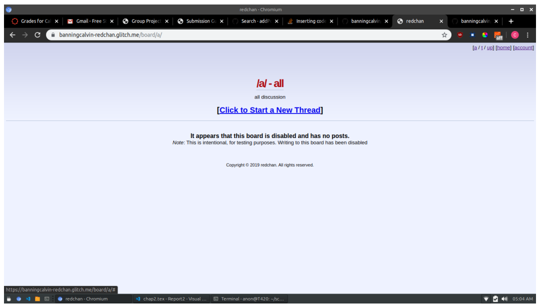
On the following pages is a series of screenshots for reference. In order, they are the homepage, the /a/ board, the /t/ board, and the account page.



redchan - Chromium
banningcalvin-redchan.glitch.me
[a / t / up] [home] [account]
redchan
boards
all
test
updates
notice
05:03 AM

don't hack this site - management

Copyright © 2019 redchan. All rights reserved.

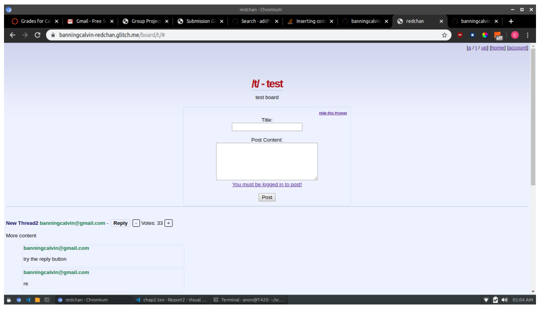


redchan - Chromium
banningcalvin-redchan.glitch.me/board/a/
[a / t / up] [home] [account]
/a/ - all
all discussion
[Click to Start a New Thread]
https://banningcalvin-redchan.glitch.me/board/a/#
05:04 AM

It appears that this board is disabled and has no posts.

Note: This is intentional, for testing purposes. Writing to this board has been disabled

Copyright © 2019 redchan. All rights reserved.


banningcalvin-redchan.glitch.me/board/t/#

[a / t / up] [home] [account]

/t/ - test

test board

Title:

Post Content:

You must be logged in to post!

New Thread2 banningcalvin@gmail.com - Reply - Votes: 33 +

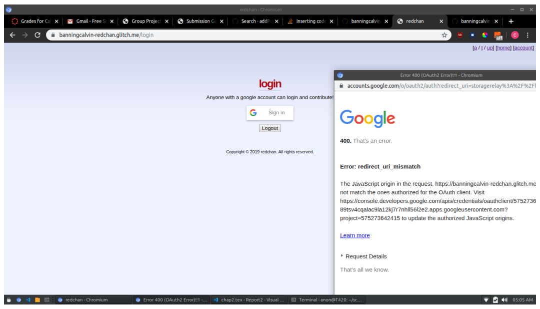
More content

banningcalvin@gmail.com

try the reply button

banningcalvin@gmail.com

re


banningcalvin-redchan.glitch.me/login

[a / t / up] [home] [account]

login

Anyone with a google account can login and contribute!

Copyright © 2019 redchan. All rights reserved.

Error 400 (OAuth2 Error)!!1 - Chromium

accounts.google.com/o/oauth2/auth?redirect_uri=storagerelay%3A%2F%2F

400. That's an error.

Error: redirect_uri_mismatch

The JavaScript origin in the request, https://banningcalvin-redchan.glitch.me not match the ones authorized for the OAuth client. Visit https://console.developers.google.com/apis/credentials/oauthclient/5752736 89tsv4cqalac9la12kj7r7nhll56l2e2.apps.googleusercontent.com?project=575273642415 to update the authorized JavaScript origins.

Learn more

Request Details

That's all we know.

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. See chapter 1 for an overview on this bug and a suggested fix.