Kenneth Woodard

CS366

Nov 15, 2022

Comprehensive Report for Course Project

My project goal was to make a phishing site that could at least trick an elderly person or someone who is not very tech-savvy. The following features were to be expected: a download link of "malware," a file that contains login information after each attempt, redirection to the real site after attempting to login, a TLS certificate to improve the legitimacy of the site, two SQL injections vulnerabilities, and two strategies for drawing victims to the website. I have a MacBook, so I used MAMP to create the site. I started off using the free version of MAMP, but realized after far too long that using MAMP PRO was the way to go. It has much more functionality. MAMP PRO, a simple text editor, and the internet provided every tool I needed to build my phishing site.

Let us start with the features that I implemented successfully. I started off trying to create a phishing version of twitter, but I ran into some issues trying to figure out how to grab the login info upon pushing the login button. This is entirely due to my lack of experience in CSS and HTML. I felt lost, so I ended up making "fakefacebook." There was more help for this available online, so I rolled with it. I copied over the source HTML code for the login page as I did before and got to work again. I was soon able to grab the necessary login data with few obstacles in the way. The password had been encrypted already, so I didn't have to obscure any of the data. I attempted to figure out how to disable this default feature on Facebook's login page, but ended up giving up on it after a while. I know this wasn't required, but curiosity forced my hand.

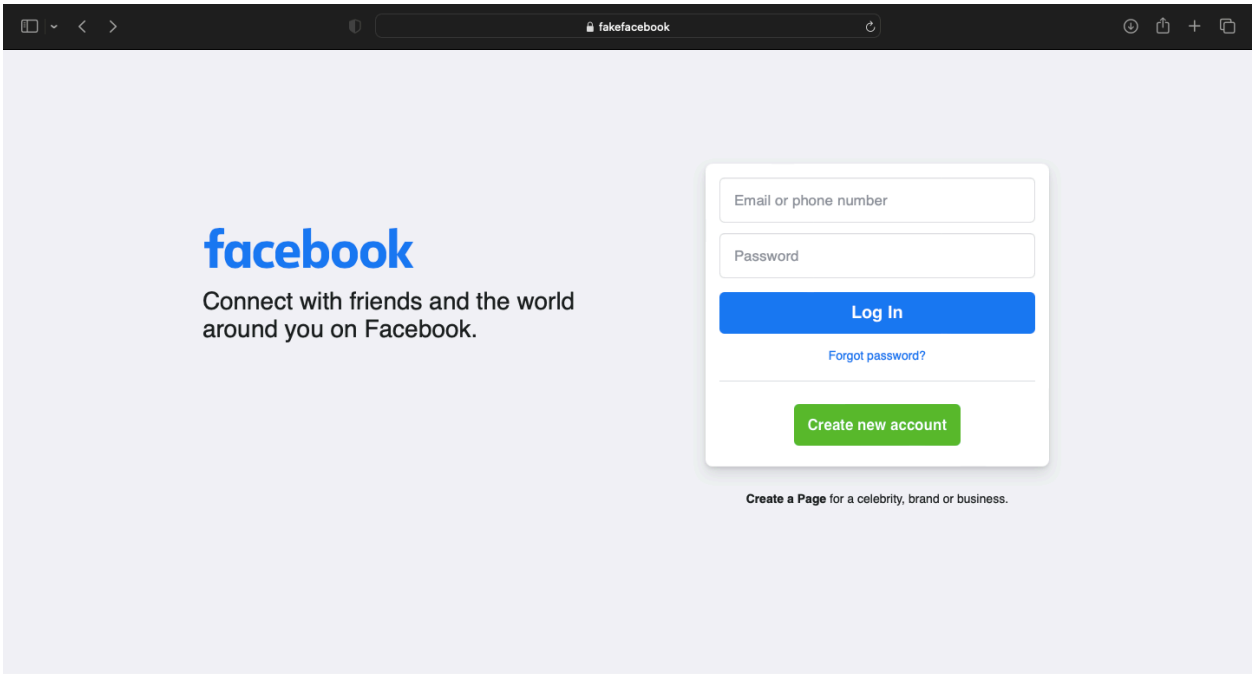
Redirecting back to the real Facebook page upon login wasn't too difficult. The only issue I ran into here was not using the "https://" prefix for the URL in my php file. It's obvious in hindsight, but it wasn't to me at the time. Setting up the TLS certificate was pretty straightforward after I read the link in the course project requirements PDF had done some research. The easiest feature for me to implement was by far the malware download link. I attached the download link to the "Messenger" link on the fugazi Facebook login page. It's just a text file making fun of the victim. Finally, creating methods for tricking victims into clicking the link was pretty straightforward. I made an email for it as well as an instagram post.

The lone feature I failed to implement in the website was the SQL injection vulnerabilities. I presumed it would be difficult when I started this project because I know very little about SQL. Implementing this feature hung me up earlier on. I ended up skipping over it with a plan to come back and fix it, but to no avail. I suppose I just have no idea what I'm doing when it comes to SQL. I understand what SQL injection is, but implementing it was significantly more difficult. I ended up just giving up on it. For sure, I would go into more detail and name specific issues if I wasn't so clueless when it came to this. But figuring what my issues with it really were proved to be difficult as I made pretty close to zero progress on it. This was, far and away, the most difficult and frustrating task in the course project. I imagine that other people at least felt the same way about implanting the vulnerabilities.

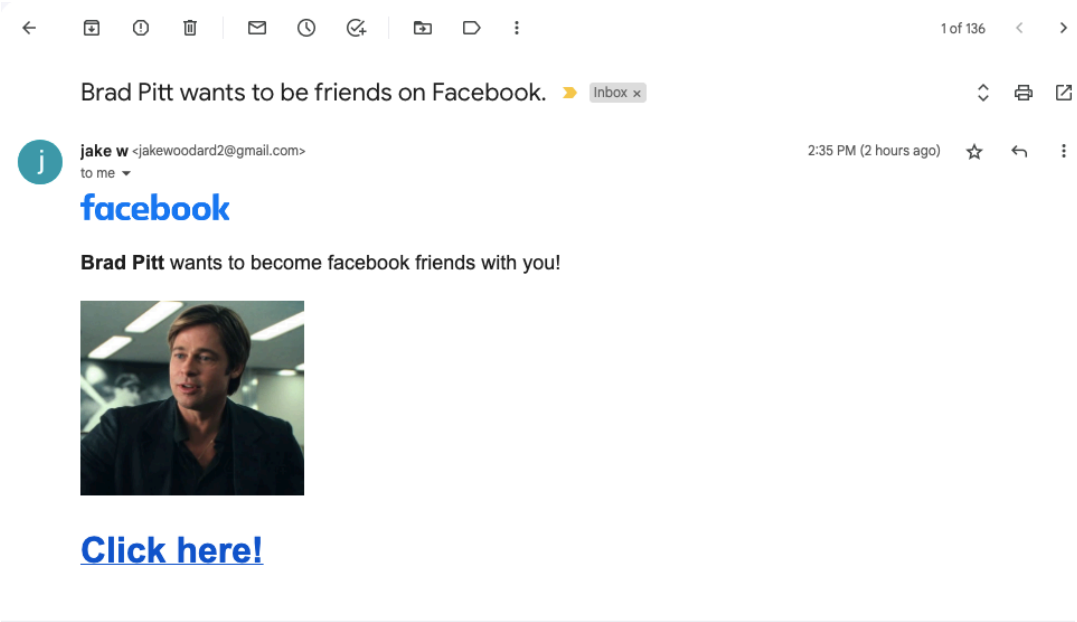
Despite the frustration of feature number four, overall this was an extremely enjoyable and worthwhile course project. I learned a lot about HTML and CSS. While I learned a good bit less about SQL, it was still a valuable experience. If I had more time, I would obviously spend more time on the SQL injection vulnerabilities, but I would also like to do it again for other

websites just to see the differences in design. Here is my video link: https://youtu.be/t1EnxgrvozE Below are some figures detailing my project.

fakefacebook



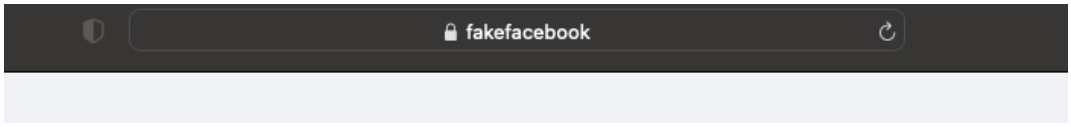
Methods to trick victims

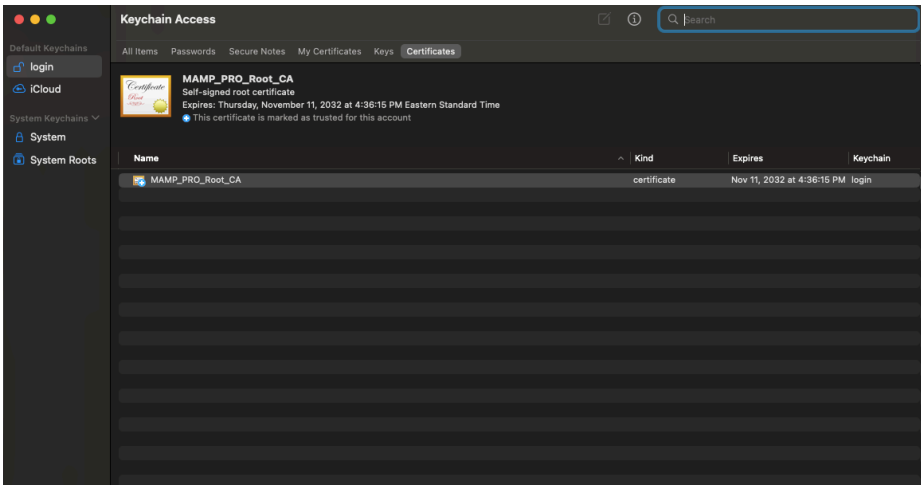


Storing login data

```
11-11-22 09:09:54
jazoest=2809
lsd=AVoF0-EBMkA
email=sup
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1668200994:AatQAGfCVaXp5IeP4LpR7bQgXKq4TyQWU1KGDJZkG7w3MUV+iavfY8C2s6yv28qW/
82U2aYi08JJ2orWATaVm2v7ZiTIFGH6foffNKYsqpbaq+K428ecfqx5bWcjN++t6YVokAm33axJ



14-11-22 04:43:10
jazoest=2809
lsd=AVoF0-EBMkA
email=6154063001
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1668462190:AatQAIcJmYV7oL/
VXWl7hhMJdoPUYOxb9iGeUf+U40XS6SYtm+1Lj+6wC1IwkdWYh6fEnAX4FKZEZLHmsoxNP887Ixpu49ABg+IhU0rehi6g2stcYBstn4HoapHkwtV1nPB6jsRfYQrygtu



14-11-22 05:19:13
jazoest=2809
lsd=AVoF0-EBMkA
email='
login_source=comet_headerless_login
next=
encpass=#PWD_BROWSER:5:1668464353:AatQAN3yb6/8zc8fooYaAcGSolvxiYBFq+9QrvzqKyuumABPbCmsuS0SPcB3FjNkykkrnNhXJLGb3zpcW3v6isd0IkXQk/
tcFxmJCrRFzZuG40/1nlAYkKH7sfGB1ZcvZMwv4ik=
```

Certificates





Malware download link