Week 1 - 2 : SoC - F Society Breachers

Mentee - Navya ( 22b1007 ) Mentor - Shanttanu Oberoi

===================Report==========================

In the first two weeks, I have covered the seven modules of the stanford cs253 course.

First module was an introduction to **web security and its requirements**.

Majorly

1. What is web security?
2. Why is it hard ?

Then I explored the four blogs on **Insides of Modern Web Browser.** It majorly covered how the browser at a broad level works. How it allocates workers for handling different pages and an overview of flow of the things that happen inside a browser.

Then I covered module 2 which was based on DNS and HTTP. Majorly it covered

1. What happens when you type a URL and press enter?
2. What is DNS ?
3. DNS Hijacking
4. What is HTTP?
5. Different headers and error codes in http.
6. Proxy Server

Then I covered Module 3 which was based on the same origin policy. Majorly it covered

1. What is the origin ?
2. What is the need for a same origin policy?
3. Document.domain method and why it is a bad idea.
4. Fragment Identifier Cross Origin communication
5. The PostMessage API
6. Same Origin Policy - Exceptions

Module 4 was mainly based on cookies and sessions.

1. What are cookies?
2. How can they be used to maintain sessions?
3. Signature Schemes
4. What are the possible ways to attack ?

Module 5

1. Session Hijacking
2. Secure and HttpOnly properties of cookies
3. Cross origin cookie exploitation
4. Cross Site Request Forgery
5. Referer header in http and associated privacy issues
6. Issues with referrer - cache-control
7. SameSite feature and it’s variants
8. How long should cookies last?

Module 6

1. Introduction to XSS
2. Reflected XSS and stored XSS
3. Multitude of ways in which code can be injected and the attacker can exploit the vulnerability in the parser.

Module 7

1. Defending Mechanisms
2. Ejs
3. React
4. XSS Auditor
5. Frame Busting
6. Content Security Policy

**Below is the short documentation which I prepared when I was studying these modules.**

**They are a bit informal but I think they further strengthen the fact that I have indeed covered the modules.**

**========================================================================**

Day 1 - Basics - 28 May 2024

Millions of cyber attacks happens throughout world and this number is increasing. Why people do attack ? RANSOMWARE • Mine cryptocurrency • Geopolitical motivations. As such we would like to build robust and secure systems in order to protect the privacy of common people and confidential governmental/institutional data.

What I covered on this day?

1. Lecture 1 slides which basics introduced web security, its importance and challenges.
2. Explored the three modules of “chrome for developers”, in order to get a very high level overview of how a browser works. ( the third module went too much in how the DOC is rendered which I skipped honestly ). Learned about various different processes and how they interact with each other in order to handle errors and user requests.

Questions

1. What is this Origin thing ?
2. When we navigate to some other site in same tab, what happens to the data of the earlier site?
3. What exactly is a service worker?
4. How much knowledge of HTML, CSS, Javascript will be required in this project ?
5. What I have studied till now is not technical. Will I get to learn some intellectual stuff or not?

Day 3 - Same Origin Policy ( May 31, 2024)

Questions:

1. What kind of expectations do sites have from a browser ?
2. If at all they have how they ensure that the client is using write browser ?
3. What kind of interactions happen between two sites? I am not getting how sites can interact with each other.

Day 4 - Understanding HTTP Cookies ( Jun 3, 2024)

Questions:

1. Cookies are also used for tracking the user behaviour. How and what are the privacy issues associated with it?
2. Difficulty in understanding secure and HttpOnly attribute of set-cook

Dag - 5 - Diving into sessions attacks ( Jun 4 , 2024 )

Questions:

1. Why it is good to set the path attribute in set-cookie equal to ?

Day 6 - continuation

1. Who would like to mark there cookies as sameSite = None?