Key SDEV Week 2 Summary

**SDEV AMI VM:**

The SDEV AMI has the following installed components:

Hardware

- AWS EC2 instance - t2.micro, 1GB RAM,

Software

- O/S: AWS: Microsoft Windows Server 2016 Base
- Browser: Firefox
- Java - jre-8u171
- Vulnerability Tools: ZAP_2_7_0_windows
- Notepad++

Notice the SDEV AMI was created using an existing baseline AMI. Essentially, the baseline O/S Windows server platform and the UMUC installed the other tools needed for the course. Be sure you take the time to get this running and be comfortable moving files back and forth from your desktop machine. Remote desktop works with both Mac and Windows machines.

**Web Page Foundations:**

The Mozilla developer site, referenced in this week's reading materials is one of the best HTML, CSS and JavaScript sites out there. Please be sure you review the site and pick up the basics including:

- HTML base tags including <HTML> <Head><Title> <Body>
- HTML tables, images, hyperlinks and forms

Note for this week we aren't submitting the form data. We are just building the forms.

The CSS style sheets and JavaScript we will touch next week but since the emphasis of this course is on security, we won't focus on the mechanics or design of web sites.

**Apache and HTTP:**

To be able to serve up web pages, the server needs to run a web server. In this course, we will be using Apache2. It is popular and fairly robust. HTTP is a protocol allowing the fetching of resources associated with web pages and documents. You can consider the browser running on your desktop as a client, and the Apache web server running on the cloud AMI as the server.

Since HTTP is stateless, other mechanisms (e.g. cookies and sessions) are needed to keep track of a user and their requests. Communication between the client and server occurs using request/response pairs. Popular request types include get and post. They are differentiated by how the data is sent:

- GET: fetches an existing resource with the URL containing all the necessary information the server needs to locate and return the resource.

- POST: creates a new resource with the POST requests carrying a payload that specifies the data for the new resource.

Servers keep track of the requests and log errors and other HTTP information. This log information is critical to cybersecurity as you can clearly see when attacks are attempted. Although other methods attackers use don't log their attempts, analysis of the access logs is always a needed component in a strong cybersecurity initiative.

Error codes from requests are logged and can easily be decoded to indicate the issue. 2xx codes indicate a successful request whereas 4xx and 5xx codes indicate client and server errors, respectively. 1xx code are informational does whereas 3xx codes are redirection indicators.

Throughout this course, we will be reviewing HTTP access on the SDEV AMI server looking for trends and anomalies.