**Course Syllabus  
Web Ecosystem and Vulnerabilities  
Module 2 for Diplomado en CiberSecuridad Ofensiva**Spring 2022

Instructor: Andrew Wilson  
Course Hours & Venue: Online + Hybrid (see email as schedule updates)  
Instructor Office Hours: By Appointment  
Instructor’s WhatsApp: +14803537391  
Email: [andrew.wilson@academicos.udg.mx](mailto:andrew.wilson@academicos.udg.mx)

TA: Jesus Antonio Lopez Luquin  
Email: [diplomado.ciberseguridad@administrativos.udg.mx](mailto:diplomado.ciberseguridad@administrativos.udg.mx)WhatsApp: +52 1 33 3361 3291

**Course Description**

This course will provide a deeper dive into understanding how the web works, vulnerabilities associated with various key technologies, and a primer on many of the common types of technology that you will run into and how you might test them.

**Overall Objectives and Expected Learning Outcomes**

The overarching objective for this course is to provide participants with a strong foundation of web based technologies, understanding the protocols that make the web work, and how modern developers build and deploy code. This will enable module will enable students to understand a web based request from beginning to end, and build stronger web testing skills.

|  |  |
| --- | --- |
| **Deliverables** | **% of Grade** |
| Class Participation | 10 % |
| Quiz | 20 % |
| Labs Completion | 30 % |
| Group Project | 40% |

**Course Grading**

|  |  |
| --- | --- |
| **A+** | **97+** |
| **A** | **93-96** |
| **A-** | **90-92** |
| **B+** | **87-89** |
| **B** | **83-86** |
| **B-** | **80-82** |
| **C+** | **77-79** |
| **C** | **73-76** |
| **C-** | **70-72** |
| **D+** | **67-69** |
| **D** | **65-66** |
| **F** | **Below 65** |

**Class Schedule**

|  |  |  |
| --- | --- | --- |
| **Session / Date** | **Topic** | **Preparation** |
| **Session 1** 23.3.2022 | **Web Proxies 201** | N.A |
| **Session 2** 25.3.2022 | **Web Protocols / Standards** | Tangled Web - Chapter 3 |
| **Session 3**  30.3.2022 | **Browser Fundamentals** | Tangled Web - Chapter 4  Tangled Web - Chapter 1 |
| **Session 4**  1.4.2022 | **HTTP Routing** | Tangled Web - Chapter 2 |
| **Session 5**  6.4.2022 | **Server Basics** |  |
| **Session 6**  8.4.2022 | **API Basics** |  |
| **11.4.2022 - 24.4.2022 - Spring Break (CUCEI)** | | |
| **Session 7** 27.4.2022 | **Front End Patterns** | Intro to Angular / MVC / Front / Page controller |
| **Session 8** 29.4.2022 | **Common Web Deployments** |  |
| **Session 9** 4.5.2022 | **Identity and the Web** | <https://www.secureauth.com/blog/an-introduction-to-saml-security-assertion-markup-language/>  <https://pragmaticwebsecurity.com/talks/introductionoauth.html> |
| **Session 10**  6.5.2022 | **JavaScript Security** | Tangled Web – Chapter 6  Tangled Web – Chapter 9 |
| **Session 11**  11.5.2022 | **Electron Security** | <https://bishopfox.com/blog/reasonably-secure-electron> |
| **Session 12**  13.5.2022 | **Group Presentations** | **Extended class** |

**Required Books**

* [**Tangled**](https://www.amazon.com.mx/Art-Software-Security-Assessment-Vulnerabilities-ebook/dp/B004XVIWU2/ref=tmm_kin_swatch_0?_encoding=UTF8&qid=&sr=) **Web -** [**https://www.amazon.com/-/es/Michal-Zalewski/dp/1593273886**](https://www.amazon.com/-/es/Michal-Zalewski/dp/1593273886)

**Labs List:**

|  |  |  |
| --- | --- | --- |
| **Lab Name** | **Hack The Box** | **Burp Academy** |
| Server Side Request Forgery | ForwardSlash | All Apprentice and Practitioner |
| Http Smuggling |  | Basic CL.TE  Basic TE.CL |
| Auth Flaws |  | Username enumeration via different responses  2FA simple bypass |
| Web Sockets |  | Apprentice |
| HTTP Host Header Attacks |  | [Routing-based SSRF](https://portswigger.net/web-security/host-header/exploiting/lab-host-header-routing-based-ssrf)  [SSRF via flawed request parsing](https://portswigger.net/web-security/host-header/exploiting/lab-host-header-ssrf-via-flawed-request-parsing) |
| OAuth Attacks |  | [OAuth account hijacking via redirect\_uri](https://portswigger.net/web-security/oauth/lab-oauth-account-hijacking-via-redirect-uri)  [Authentication bypass via OAuth implicit flow](https://portswigger.net/web-security/oauth/lab-oauth-authentication-bypass-via-oauth-implicit-flow)  [Stealing OAuth access tokens via an open redirect](https://portswigger.net/web-security/oauth/lab-oauth-stealing-oauth-access-tokens-via-an-open-redirect) |

**Deliverables**

**Team Project**Each student will join a team of no more than 4 students. As a team, you will build and present a basic web application that you will develop. This website can be programmed in any language, using any database as a back end. The website must be a basic “todo” task list which includes:

* Adding, Deleting, and Editing tasks
* Prioritize of tasks
* Reorganize task list
* Tasks must have the following features:
  + Pictures as parts of notes
  + Notes
  + Start / End times
  + Hour Estimate
  + Title

Extra credit will be offered for the following:

* Authentication of users to the application
* Cloud hosting (and show us how you did it)
* An API that allows for the general CRUD features of the application

**Hack the Box Labs**

Students will be assigned into groups, which will be assigned lab times throughout the week using the hack the box system. These labs are to be done individually and not as a group, and each student must complete all of the assigned labs during a week. If a student misses their assigned time, they can work with the TA and get scheduled makeup time to complete the assignments. All labs must be done before the end of the class.

**Quiz**

Students will be given a quiz that will need to be completed in the middle of the course. This will review relevant course material for the first half of the class. The mid-course quiz will be before our break focusing on the first half of the course.

**Attendance Policy**

Unexcused absences will require you to work with other students to get information about what was missed. If you know you are unable to attend a class ahead of time, please contact me or Jesus ahead of time.