## Description and Objective

In 1995, Amazon.com shipped its first book. Also in 1995, a software programmer created a webpage he called Auction Web, now called eBay. Ever since, the internet has been leveraged as a tool for commerce. The increase in popularity of eCommerce has lead to a rise in identity theft, stolen credit cards from online retailers, and online fraud.

This class is designed to teach students how to properly secure a web server, web page, and web application. Students will take an already existing web application and redesign it to be as secure as possible. Students will also design and build an eCommerce site designed with the best security practices. Students will learn how to protect confidential information, including financial and personal data.

Part of security is testing the security and vulnerabilities of the web application. To that end, students will also learn the common techniques for penetrating web applications and web servers. This will give students the techniques to properly test their web applications in their academic and professional careers.

## Concepts

Upon completing this course, students will:
- Understand the fundamentals of web server architecture and security
- Understand the components of securing web applications
- Be able to establish and maintain a set of web servers and services
- Be able to protect confidential information involved in eCommerce

## Prerequisites/Recommended Preparation

One from ITP 325, ITP 301, or CSCI 351

## Instructor

Joseph Greenfield

## Contacting the Instructor

joseph.greenfield@usc.edu | 213-740-4604

## Lecture

4 hrs/week

## Required Textbooks


## Web Site

All course material will be on Blackboard at blackboard.usc.edu
**Grading**

Students will have structured labs throughout the semester, to be conducted during the scheduled lab time. In addition, students will have a comprehensive final project to be completed in the later portion of the semester. The grading breakdown is as follows:

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labs</td>
<td>60%</td>
</tr>
<tr>
<td>Midterm</td>
<td>15%</td>
</tr>
<tr>
<td>Final Project</td>
<td>25%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**Grading Scale**

The following is the grading scale to be used for the final grades at the end of the semester:

- 93% and above: A
- 90% - 93%: A-
- 87% - 90%: B+
- 83% - 87%: B
- 80% - 83%: B-
- 77% - 80%: C+
- 73% - 77%: C
- 70% - 73%: C-
- 67% - 70%: D+
- 63% - 67%: D
- 60% - 63%: D-
- Below 60%: F

**Policies**

- Projects turned in after the deadline will automatically have 5% deducted per day. Projects will not be accepted after 1 week beyond the project's deadline.
- No make-up exams (except for medical or family emergencies) will be offered nor will there be any changes made to the Final Exam schedule.
- It is your responsibility to submit your project on or before the due date. **It is not the responsibility of the lab assistant.** Do **not** turn in anything to your lab assistant!
- All projects will be digitally submitted through blackboard except where specifically specified. Always keep a backup copy of your labs.

**Academic Integrity**

The use of unauthorized material, communication with fellow students during an examination, attempting to benefit from the work of another student, and similar behavior that defeats the intent of an examination or other class work is unacceptable to the University. It is often difficult to distinguish between a culpable act and inadvertent behavior resulting from the nervous tension accompanying examinations. When the
A professor determines that a violation has occurred, appropriate action, as determined by the instructor, will be taken.

Although working together is encouraged, all work claimed as yours must in fact be your own effort. Students who plagiarize the work of other students will receive zero points and possibly be referred to Student Judicial Affairs and Community Standards (SJACS).

All students should read, understand, and abide by the University Student Conduct Code listed in Scampus, and available at: [http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html](http://www.usc.edu/student-affairs/SJACS/nonacademicreview.html)

| Students with Disabilities | Any student requesting academic accommodations based on a disability is required to register with Disability Services and Programs (DSP) each semester. A letter of verification for approved accommodations can be obtained from DSP. Please be sure the letter is delivered to me (or to your TA) as early in the semester as possible. DSP is located in STU 301 and is open 8:30 a.m. – 5:00 p.m., Monday through Friday. The phone number for DSP is (213) 740-0776. |
Course Outline

Week 1 – Review
- Course Overview
- Review of hackers and hacker methodologies
- Network technologies
Reading: Instructor Notes

Week 2 – Web Fundamentals
- HTML
- HTTP
- Client-side scripting
- Server-side scripting
Reading: Instructor Notes
Lab 1: Setting up the web server

Week 3 – Web server architecture
- Windows & Linux
- IIS and LAMP servers
- Network topologies and DMZ
- Hacking these platforms
Reading: Chapter 3
Lab 2: Hacking web servers

Week 4 – Web applications
- Introduction to web applications
- Web application hacking
- Overview of browsers, extensions, and platforms
Reading: Chapter 1
Lab 3: Setting up the web application platform

Week 5 – Infrastructure mapping and profiling
- Scoping the app from a hacker’s perspective
- Platform profiling and mapping
- Application identification and profiling
- Profiling countermeasures
Reading: Chapter 2
Lab 4: Profiling

- 4 -
Week 6 – Web Authentication
- Overview of web authentication
- Hacking passwords
- Digital signatures
Reading: Chapter 4
Lab 5: Hacking Authentication

Week 7 – Web Authorization
- Understanding authorization
- Hacking access control lists
- Session IDs and Cookies
- Hijacking URLs
- Protecting Authorization
Reading: Chapter 5

Week 9 – MIDTERM

Week 10 – Script Hacking and Defensive Coding
- Attack Vectors
- Buffer Overflows
- Input validation
Reading: Chapter 6

Week 11 – Securing Databases and Database Access
- Introduction to SQL
- SQL Injection
- Database Platform Attacks and Security
- Database Encryption
Reading: Chapter 7
Lab 6: SQL Injection

Week 11 – Denial of Service
- DoS attacks
- DoS countermeasures
Reading: Chapter 11
Final Project Assigned

Week 12 – Web Application Management
- WebDAV
- Configurations and Misconfigurations
- Data leakage
Reading: Chapter 9
Lab 7: Proper web server configuration
**Week 13** – Web Client Security
- Web browser hacking and security
- Phishing
- Adware/Spyware
**Reading:** Chapter 10
**Lab 8:** Client Security

**Week 14** – Threat Modeling
- Modeling attack vectors and defense strategies
- Threat and mitigation strategies
- Code review and binary analysis
**Reading:** Chapter 12

**Week 15** – Conclusion
- Conclusion to the course