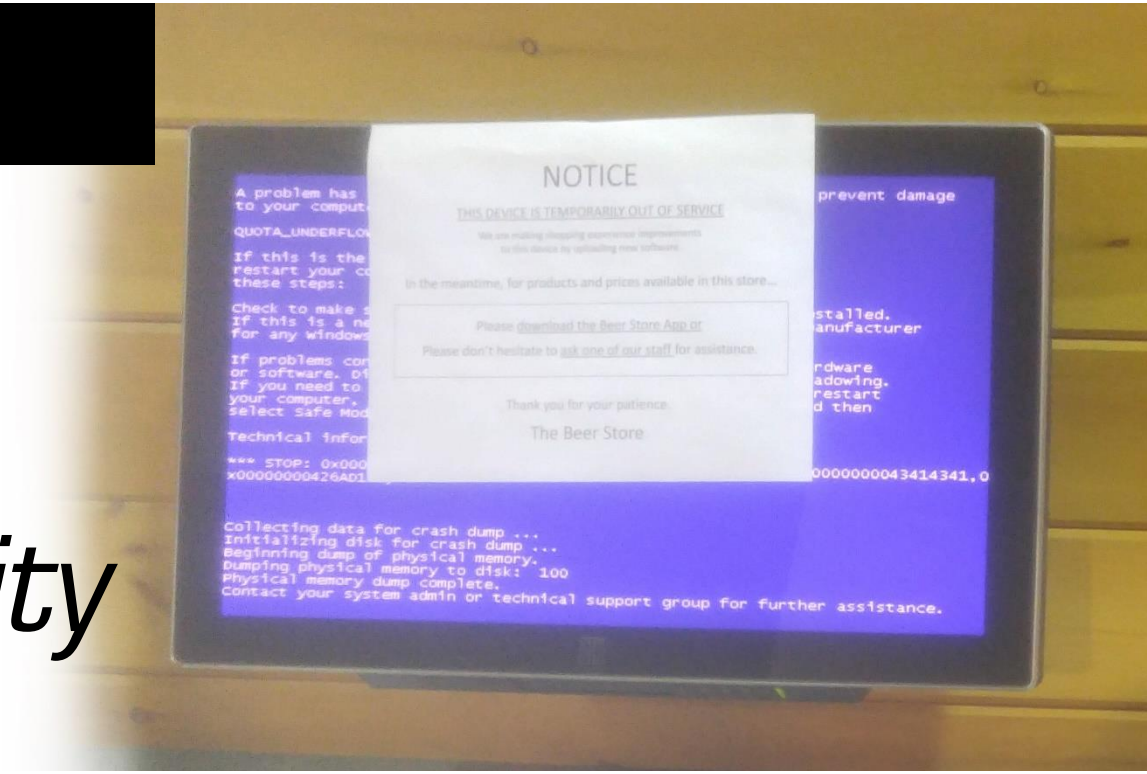
FANSHAWE

INFO-6076



Web Security

Course Introduction

FANSHAWE

Agenda

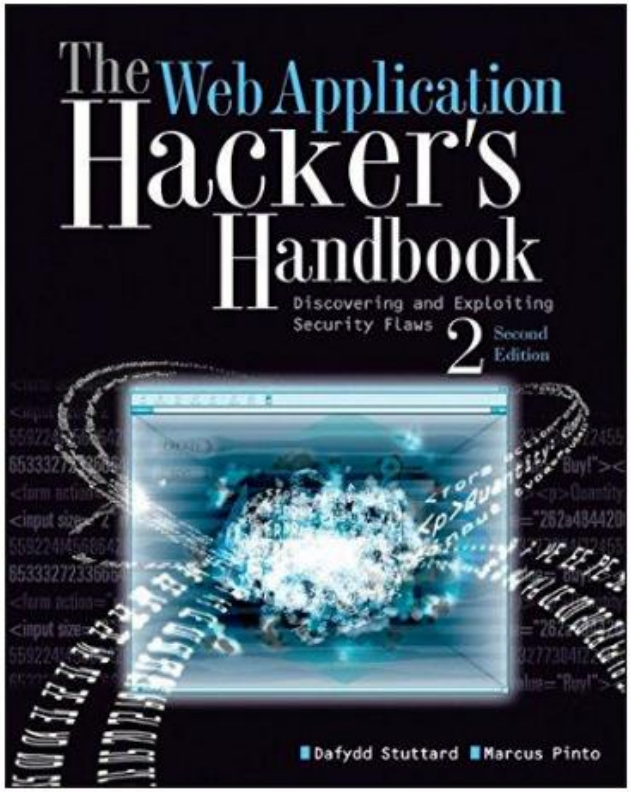
- Course Information
- Components of Web Applications
- Web App Security
- Lab 01 – VM lab set up

Course Information

FANSHAWE

Course Textbook

- This course does not have a required textbook
- The **recommended** textbook is:



The Web Application Hacker's Handbook

ISBN
9781118175248

Contact Information

Email: a_mackiewicz2@fanshaweonline.ca

Email Tips:

- Include the course number in the **subject**:
  INFO-6076 - Question about Test 1
- You must send emails from your @fanshaweonline.ca address
- Please keep your email brief and to the point
- Don't be afraid to use the point form:
  - 1) When do we …
  - 2) How to ..
- Please do not wait until the last minute to send your email!
- Please send emails only in the plaintext format
- Emails will be typically be answered in 24 hours (Monday-Friday)

FANSHAWE

General Information

- The course is assigned **4 hours per week**:
  - A 2-hour lecture/lab followed by a 2-hour lab only session each week
  - There are no lectures or labs on the weeks in which you have a test or exam

The labs will develop essential skills and reinforce the lecture content

FANSHAWE

Course Evaluation Methods

- Tests and Exams: (70%)

There are two tests (weeks 5 & 10) and the final exam

- Details can be found in the CIS

- Labs (30%)

Labs are delivered weekly

- Students must finish and submit the lab by the **deadline** posted on Fanshawe Online
- Only your latest submission will be graded

Test / Exam Format

This is a general guideline:

The majority of your test/exam questions will be in one or more of the following formats:

- Multiple Choice
- Multi-Select
- True False
- Matching/Ordering

There may be short answer questions on the tests/exam

FANSHAWE

Test Dates

Scheduled Test Dates:

Test 01 in Week 05:

- Monday January 30th

Test 02 in Week 10:

- Monday March 13th

Final Exam in Week 15:

- Date/Time/Location to be announced

FANSHAWE

Lab Details

- You need to do the labs yourself
- Do not rely on your fellow student's answers
- Don't share screenshots with other students
- Do not edit/modify screenshots in Photoshop or any other software (you can, however, resize / cut images)
- Make sure your screenshots:
  - ✓ 'fit' into the PowerPoint screen
  - ✓ Include your student information
  - ✓ Are in the correct order

FANSHAWE

Lab Details

- Please follow the lab instructions precisely. Don't skip any steps…
- Before asking any questions, please use 'common sense':
  - Double check that you have all the required software/components running
  - Apply what you've learned from the previous labs
  - Try to resolve the issue yourself instead of looking for an easy answer
- Make sure you have no network/connectivity issues with your VM
  - Shutdown all the other VMs
  - Make sure your VM has the proper network settings (NAT, Bridge mode, etc.)
  - Check network adapter(s) settings; disable wireless/wired adapter(s) not in use
  - Disable Windows/3rd party firewall(s), malware scanners on the host computer
  - Restart OS on the host computer
- Do not expect me to do the lab for you…

  For instance, if you need to find some URL in the lab, please don't ask me to help you find it

FANSHAWE

Lab Details

- You will find all the required files for your labs online through a provided link or on Fanshawe Online

- I will provide you with any download links as required in the lab instructions

FANSHAWE

Topics

- Web Application Enumeration
- Authentication Management
- Web App Penetration Testing
- Access Control
- XSS / CSRF
- Injection Attacks
- The Dark Web / TOR
- Automation
- Web Server Security

FANSHAWE

Components of Web Apps

FANSHAWE

Components of Web Apps

- You should have a good understanding of the different languages that make up Web Applications
- You will need to be able to differentiate between Markup, Scripting, Backend, and Database components

FANSHAWE

Components of Web Apps

- Markup languages
  - SGML
  - HTML
  - XML
  - XHTML
  - CSS
- Scripting Languages
  - JavaScript
  - JS
  - JSON
  - AJAX

FANSHAWE

Components of Web Apps

- Backend (Server Side) Languages
  - PHP
  - Python
  - Perl
  - Ruby
  - ASP
  - .NET

FANSHAWE

Components of Web Apps

- Databases
  - MS SQL
  - MySQL
  - PostgreSQL
  - Oracle
  - MariaDB

FANSHAWE

The Changing landscape of Web Apps

- Web applications have become a lot more complex
  - Importing scripts
  - Linking to analytic servers
  - Advertisements
  - User input
- All of the extra code required for user engagement also creates an opportunity for exploitation

FANSHAWE

The Changing landscape of Web Apps

- As opposed to being static web sites, most are now complex Web applications that require user input
  - Login/Authentication
  - E-Commerce
  - Online Banking
  - Social Media
  - User created content
  - Forums

FANSHAWE

The Changing landscape of Web Apps

- Most web applications now have different interfaces for various platforms
  - Mobile Apps
  - Use HTTP-based APIs

- Business software that used to be accessed through a network computer can now be accessed through web apps
  - Outlook Web Access / Office 365
  - Google Apps

FANSHAWE

Web App Security

FANSHAWE

Web App Security

- Organizations used to rely on perimeter security
- Web applications need to allow user traffic to access them
- This creates a problem because back end servers can be compromised through a web app

Web App Security

- OWASP's Top Ten list keeps evolving
- Certain vulnerabilities change due to various reasons
  - User awareness
  - Developer awareness
  - Browser security
- Problem is that new vulnerabilities arise to replace old ones

Web App Security

- The core security problem lies within user input
- Malicious users can alter data being sent to a server through:
  - Request parameters
  - Cookies
  - HTTP headers
- These can be done using automated tools in addition to manual input manipulation

Web App Security

- SSL does not stop a malicious user from altering the data a server is expecting
  - Hidden HTML form fields
  - Modified session tokens
  - Tampering with parameters
  - Injection attacks

FANSHAWE

Web App Security

- Adding functionality to web applications increases their attack surface
- More lines of code = More potential vulnerabilities
  - Password recovery
  - Username recovery
  - Password hints
  - Etc.

Lab Details

LAB-01: Overview

FANSHAWE

Lab-01: Overview

- Download client and server VM files
- Kali VM prep
- Windows 10 VM prep
- Windows Server 2016 VM prep
- Metasploitable2 Server VM prep
- Ubuntu 18.04 LTS Server VM prep

Wrapping up…

- Questions…?