CNIT 129S: Securing Web Applications

Instructor: Sam Bowne Web Site: **samsclass.info** E-mail: **sbowne@ccsf.edu**

Catalog Description

Techniques used by attackers to breach Web applications, and how to protect them. How to secure authentication, access, databases, and back-end components. How to protect users from each other. How to find common vulnerabilities in compiled code and source code.

Advisory: CNIT 131 and CNIT 120, or comparable familiarity with websites and security concepts.

After successful completion of this course, students will be able to:

- Explain the current state of Web application security
- Analyze basic application functionality
- Secure data stores and back-end components
- Protect users from other users
- Demonstrate common exploits and patch their root causes
- Implement servers and firewalls effectively

Textbook

"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition", by Dafydd Stuttard , Marcus Pinto; ISBN-10: 1118026470

Grades

The number of points you accumulate during the semester determines your final grade. Points come from projects, quizzes, and the final exam. Details are on my web site: **samsclass.info**

Your final letter grade is determined from your total points as shown below:

%	Grade
90% or more	A
80% - 89.99%	B
60% - 79.99%	C
50% - 59.99%	D
49.99% or less	F

This course allows "Pass/No Pass" grading, if that option is requested before the deadline.

Ethics

Security professionals are held to high standards of ethics, like police officers. Lying, copying others' work and passing it off as your own, crude or abusive language, and performing cybercrimes will not be tolerated in this class. Offenders will be punished by losing points, or by immediate expulsion and a final grade of F, at the discretion of the instructor. \

Changes

I reserve the right to change any of these policies as necessary during the semester and will inform you of any changes.