Tufts University
Department of Computer Science
COMP 116: Introduction to Computer Security
Fall 2017
Quiz 2 Practice. Closed Book.

Quiz 2 will cover the following topics:

- Password cracking
- Cross-Site Scripting (XSS)
- SQL injection
- Cookie tampering
- Command injection via Remote Code Execution
- Cross-Site Request Forgery (CSRF)
- Directory traversal
- Static analysis
- Dynamic analysis
- Malware / viruses / worms / backdoors / tini

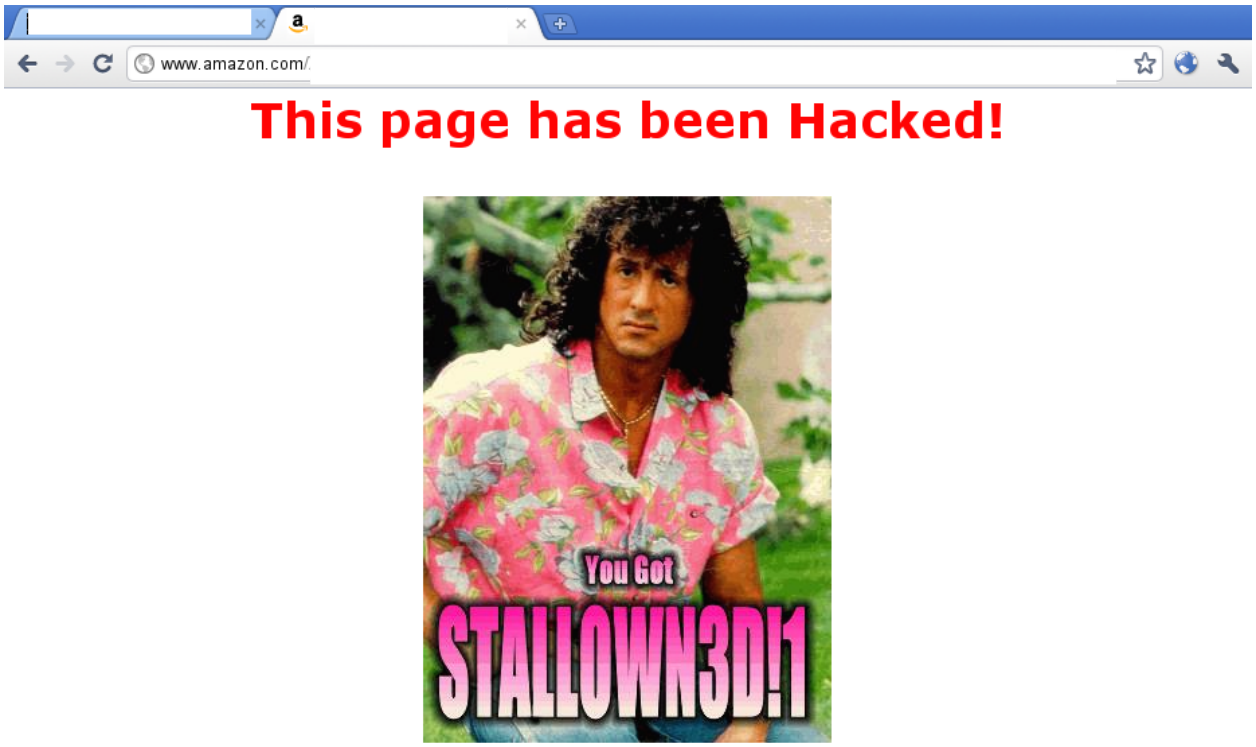
Types of questions on the quiz will include:

- Multiple guess
- Fill-in-the-blank
- True or false
- Really short answer

You will be given at least two real scenarios on the quiz.

Sample Question (actual from fall 2014)

This is a real incident from 2010. Consider the following screenshot:



1 (2 points). What vulnerability on Amazon is responsible for this defacement?

2 (3 points). Briefly describe how can an attacker conduct such defacement on Amazon?

3 (2 points). Briefly describe how an intrusion detection system (IDS; example is what you did in Assignment 2) could monitor or detect such an attack.

4 (2 points). Suppose you were a software engineer at Amazon, how can you patch or defend against this attack?

Answer:

1. Cross-Site Scripting (XSS)
2. Post something that contains JavaScript code to replace the content of the page with picture as seen above (i.e., defacement). That "something" must be entered in a place where content entered will be displayed to everyone who visits a page (e.g., product review). Example of malicious post:
   `<script>document.getElementById("SomeElementHere").innerHTML='<h1>This page has been Hacked</h1><p><img src="http://domain.com/path/to/stallowned.jpg" alt="Hacked"/>'</script>`
3. Look for `<script></script>` or variations of it (e.g., unicoded).
4. Sanitize inputs. That is, remove HTML tags or special characters in post.