**Name**: Marvin Newlin

**Paper**: Detecting SQL Injection and Cross Site Scripting Attacks with Static and Taint Analysis

**Overall Score: (92/100% = 74/80 points)**

**Summary**:

A research paper on using static analysis to detect SQL Injection and Cross Site Scripting.

**Abstract (5/5%):**

101 words. The abstract describes SQL and XSS vulnerabilities and the damage they do. It also mentions that the paper discusses the characteristics of a tool that would improve detection.

**Introduction (12/15%):**

The introduction begins by motivating the need to secure web applications that are vulnerable to XSS and SQLI and then provides a brief overview of format analysis. It then concludes with a single sentence saying, "in this paper we explore a few of the most well-known approaches for formal analysis of SQLI and XSS in web applications and present some avenues for future work." The introduction should cover a bit more of what is in the remainder of the paper.

**Bibliography (5/5%):** 15 references

**Literature Review (50/50%):**

The literature review provides a solid background on SQLI and XSS followed by a review of three different characteristics of analysis: flow sensitivity, content sensitivity, and path sensitivity. The author then proceeds to a thorough review of static analysis tools for detecting SQLI and XSS. He concludes with a table summarizing his findings.

**Methodology (20/25%):**

The author suggests an approach that combines context sensitive but path and flow insensitive. He provides the beginnings of a development plan citing several other works to build on. The only weakness is the test plan which lacks details as well as a dataset to use.