Vulnerability Assessment for Web Applications

Susana Paola Lainez Garcia
susana.lainezgarcia@utdallas.edu

Amy S. Abraham
amy.abraham@utdallas.edu

Kristina Kepic
Kristina.kepic@utdallas.edu

Ebru Celikel Cankaya
ebru.cankaya@utdallas.edu

Department of Computer Science
University of Texas at Dallas
Richardson 75080, TX, USA

Abstract

Considering the everlasting need for security in network platforms, this study investigates various penetration testing tools in the abundance of options when it comes to network security. We present the experimental run results of select penetration testing tools on deliberately vulnerable network traffic, as well as the comparison of those tools. We test three vulnerability assessment tools: ZAP, Vega and Arachni as part of this research in the hope to provide current and practical data for the research community in the field. The selection criteria we adopted were being current, ease of use, reliability (stability), and speed performance. Our results demonstrate that each vulnerability assessment tool depicts its own advantages and disadvantages by being better at one or more criteria than the others, but not prevailing in all.

Keywords: Vulnerability Assessment, Penetration Testing, Web Applications, SQL Injection, Cross-Site Scripting (XSS).

A full manuscript of this abstract may be found at https://jisar.org