

Naxsi performance

Lutz Engels, Dennis Pellikaan
University of Amsterdam

February 22, 2013

1 Introduction

In a time where huge botnets are utilized to attack services, it is ever more important to protect your infrastructure. When taking into account the fact that web services gain more market share it is the web servers that need to be protected. One of those web servers is nginx. Compared to other web servers it is light-weight, which attracts more users in time where power consumption of infrastructure becomes important. Currently (February 2013) it holds 13% market share.¹

In 2011 development of Naxsi (*Nginx Anti Xss & Sql Injection*) started. As the (written out) abbreviation implies it protects nginx from Cross-site scripting (XSS) and Sql injection attacks. To do so it takes the whitelist approach, as to circumvent overly complex and regular expression based rule sets.

This project aims at generating valuable data by conducting performance testing of Naxsi in a number of scenarios.

2 Scope

3 Approach

4 Requirements

5 Planning

References

¹<http://news.netcraft.com/archives/category/web-server-survey/>, February 2013, monthly updated