Naxsi performance

Lutz Engels, Dennis Pellikaan
University of Amsterdam

February 22, 2013

1 Introduction

More and more people will have access to the internet [**?**] and they will have access to many web applications. Commercial companies have access to an ever growing market, but also criminals become more intelligent on how to reach end-users and abuse the web services users are accessing on a daily basis. According to the web survey held by Netcraft in february 2013 [1], the majority of web servers is running Apache and it is followed by Microsoft. However, Nginx is gaining more popularity and it is not only used as a standard web server, but also as a reverse proxy for load balancing purposes. Naxsi is developed as a response to common attacks that often occur the internet. Naxsi is firewall designed to work with Nginx. It works as a DROP-by-default firewall and rules should be added to ACCEPT certain traffic. This concept is also known as whitelisting. Our research will focus on the performance of an Naxsi-Nginx server when it is under heavy load and it has to deal with different attacks.

—

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 [2]

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.

[1] `http://news.netcraft.com/archives/category/web-server-survey/`, February 2013
[2] `http://news.netcraft.com/archives/category/web-server-survey/`, February 2013

2 Scope

Naxsi can be run in learning mode and production mode. Within our research we will focus on the performance of Naxsi in production mode. This means that we will have to find a good learning set for Naxsi to use, which fits are production environment. For our research we will look at a setup as can often be seen by blog hosters:

- MySQL database
- Naxsi-Nginx web server
- Wordpress 3.5.1

3 Approach

- Setup test enviroment
- Gather learning information for Naxsi
- Pre-test functionality
- Performance test with firewall enabled
- Performance test without firewall enabled
- Analyze the data
- Draw conclusions

4 Planning

Week 1	Literature study
Week 2	Performance testing
Week 3	Data analysis
	Fine tuning performance test
Week 4	Writing report
	Preparing presentation

References

A Acronyms and abbreviations