Review

of the Master Certification Work on

«Web-sites Vulnerabilities' Research and Methods of Their Elimination»

by Kedrovskiy Mikhail Anatoliyovych

Work topicality

Nowadays almost every Web-site has vulnerabilities both minute, which do not contain any threat to the site, server or users, and those which endanger not only a Web-site, but also a server and users. As a rule, young and sometimes experienced specialists do not think about the security of the site and its users until the attack occurs.

This problem may be eliminated due to increasing the qualification level of young specialists in such issues:

- Consideration of basic vulnerabilities;
- The way of carrying out attacks by intruders by means of the vulnerabilities;
- Methods of their elimination;
- Methods of their detection;

This work was directed to consider these issues.

Aim of the work

The main goal of this paper is the research of basic vulnerabilities of Websites, methods of their detection and elimination. In order to reveal any vulnerable places, another objective was assigned - Web-interface development to a vulnerabilities' scanner Nikto 2.03.

Assigned tasks

In order to assign the objective, the following tasks have been carried out:

- Web-sites basic vulnerabilities research;
- Methods of their elimination analysis;
- Basic vulnerabilities' scanners research;

- NTUU "KPI" Web-sites vulnerabilities analysis on the basis on newly created scanner;
- Comparison of vulnerabilities' statistics among NTUU "KPI" Websites and Web-sites vulnerabilities according to Positive Technologies data in 2008.

Achievements

Having reached the results in addressing the task, the author presents:

- Analyzed data on NTUU "KPI" Web-sites vulnerabilities;
- Necessity to eliminate as much vulnerabilities as possible;
- Necessity to increase the qualification level of young specialists in the context of security;
- Newly created by the author Web-interface to vulnerabilities' scanner Nikto 2.03.

Scientific novelty of the work

The scientific novelty of the work is presented by the analysis of NTUU "KPI" Web-sites vulnerabilities' data and its comparison with Web-sites vulnerabilities' statistics according to Positive Technologies data from 2008. This fact gives an opportunity to see how the situation has changed since that time. The newly developed parallel scan algorithm for Web-sites scanning in search for vulnerabilities can also be regarded here. It can reduce time which is needed for the mass Web-sites' scanning.

Practical value

On the basis of the new parallel scan algorithm for Web-sites scanning in search for vulnerabilities, a Web-interface to vulnerabilities' scanner Nikto 2.03 was created.

Conclusions

Each site has vulnerabilities, and it is nothing to do with this fact, because it is physically impossible to follow up all vulnerabilities, a fortiori when new methods of intrusion occur. Owing to the vulnerabilities' scanners, one of which is presented by

Nikto-online, the amount of vulnerabilities may be minimized and thereby the security of the site and its users can be increased.

During the research and performing the work the basic vulnerabilities and methods of their elimination were analyzed. Few new techniques of Web- application's development were studied and correlation between them was found.

The author developed a Web-interface to vulnerabilities' scanner Nikto 2.03 in order to research Web-sites' vulnerabilities. This system is pleasant and easy to use. It gives an opportunity to simultaneous scanning of few sites, without spending any users' computer resources. This provides an opportunity for quick and mass scanning of all necessary Web-sites.

The paper consists of 119 pages, 30 pictures, 6 tables, 13 sources.

Key words: SECURITY OF WEB-SITES, VULNERABILITIES OF WEB-SITES, VULNERABILITIES' SCANNER, ELIMINATION OF VULNERABILITIES.