ABSTRACT

The relevance of work

The potential of Grid technology is currently very high. In the short term Grid Computing will become a powerful tool for the development of high technologies in various fields of human life. However, the rapid development of Grid depends on providing end users with simple tools to solve their problems, while hiding the complexities of implementing the system. Creating a convenient and simple Web- portal access to Grid-resources solves this problem. Since Web-portals are Web- applications, they are vulnerable to hacker attacks, therefore the study of mechanisms of their information security and problem-solving to enhance their protection is relevant and important.

The purpose of work

The purpose of this work is to study the mechanisms of information security of the access portal to Grid infrastructure on an example of GridSphere and EnginFrame systems and to enhance their level of protection by identifying vulnerabilities and description of recommendations for their elimination.

Solved problems in the work

In the work such problems had been solved: classification analysis of threats in order to highlight features of each class of threats, the establishment of generalized models of hacking and security Web sites, overview of the basic mechanisms of the security of web projects, preparation of comparative characteristics of some common automated security scanners to select the tools for testing security web portal SDGrid, conducting scanning the security system of CMS GridSphere and EnginFrame and creation the authentication module by MyProxy mechanism for EnginFrame system.

The results of work

The classification of security threats of the Web applications was analyzed and marked: the types of threats, their level of risk, characteristics and scope. Advantages and disadvantages of searching methods of vulnerabilities in Web applications was allocated. Common model of hacking and common model for the protection of websites was created. Was held the comparative features characteristic of some common used automatic security scanners on the basis of the five selected groups of criteria and was marked advantages, disadvantages, and a major specialization of the scanners. The features of the basic mechanisms of the SDGrid portal security based on the GridSphere and EnginFrame systems was considered. The results of scanning SDGrid portal security by the security scanners was submitted. Recommendations for increasing the degree of protection of the portal was formulated. Was created the authentication module by MyProxy mechanism for EnginFrame system.

Scientific novelty

Scientific novelty of the work is to study the mechanisms of information security of the portal access to Grid infrastructure, which based on GridSphere and EnginFrame systems and identifying vulnerabilities in them and increasing levels of their security. Also for the first time was held the comparative characterization of some modern security scanners Nmap, Nessus, Xspider, Shadow Security Scanner and Acunetix Web Vulnerability.

The practical value of the work

The practical value of the work includes identifying vulnerabilities and description of recommendations to address them in the GridSphere and EnginFrame systems, and creating an authentication module by MyProxy mechanism for the EnginFrame system, which provides increased levels of protection and facilitates and easy integration with the Grid infrastructure.

Conclusions

The researching showed that the level of protection systems and GridSphere EnginFrame generally comparable, but the systems has vulnerabilities. GridSphere and EnginFrame systems contains such security mechanisms: authentication by login and password, authentication by certificates (MyProxy), and by Kerberos protocol, supports GSI, HTTPS/SSL, access control and logging system.

GridSphere system is vulnerable to attacks such classes as: "Cross-site scripting" high risk and "Session fixation" medium risk level, the EnginFrame system vulnerable to attacks of a class «XPath injection» of high level of risk. Both systems have different vulnerability class "identification application" low level of risk.

To use the founded security threats high and medium level of risk is difficult and the success of their application depends by the professionalism of the hacker and by negligence of security administrators. With proper administration of the portal, as well as the implementation of recommendations to enhance the level of protection of application data security threats are minimized.

The work on the 133 pages contains 21 tables, 16 illustrations and 1 application. By preparation of work the literature from 25 different sources was used.

The list of keywords: GRID PORTALS, SDGRID PORTAL, SECURITY MECHANISMS OF THE GRID PORTALS, SECURITY SCANNERS, GRIDSPHERE, ENGINFRAME.