РЕФЕРАТ

Актуальность работы

Потенциал технологии Grid в настоящее время очень велик. В ближайшей перспективе Grid должен стать мощным вычислительным инструментарием для развития высоких технологий в различных сферах жизни человека. Однако быстрое развитие Grid напрямую зависит от предоставления конечным пользователям простых средств для решения их задач, скрытие при этом всех сложностей реализации системы. Создание удобного и простого Web-портала доступа к Grid-ресурсам решает эту проблему. Так как Web-порталы являются Web-приложениями, то они уязвимы к хакерским атакам, поэтому исследование механизмов их информационной безопасности, а также решение проблем усиления их защиты является актуальным и важным.

Цель работы

Целью данной работы является исследование механизмов информационной безопасности порталов доступа к Грид-инфрастуктуре на примере систем управления порталом GridSphere и EnginFrame с целью усиления уровня их защиты за счет выявления уязвимостей и описания рекомендаций по их устранению.

Решаемые в работе задачи

В работе решались такие задачи: анализ классификации угроз с целью выделения особенностей каждого класса угроз, создание обобщенных моделей взлома и защиты веб-сайтов, обзор основных механизмов безопасности веб-проектов, составление сравнительной характеристики ряда распространенных автоматических сканеров безопасности с целью выбора инструментальных средств для тестирования системы безопасности веб-портала SDGrid, проведение сканирования системы безопасности CMS GridSphere и EnginFrame, а также создание модуля аутентификации по механизму MyProxy для системы EnginFrame.

Достигнутые результаты

Проанализирована классификация угроз информационной безопасности веб-приложений, в которой выделены: типы угроз, их уровень риска, особенности и область применения. Выделены преимущества и недостатки методов поиска уязвимостей веб-приложений. Разработана обобщенная модель взлома, а также обобщенная модель защиты веб-сайтов. Проведена сравнительная характеристика функциональных возможностей ряда распространенных автоматических сканеров безопасности на основе пяти выделенных групп критериев, отмечены достоинства, недостатки и основная специализация данных сканеров. Рассмотрены особенности основных механизмов безопасности портала SDGrid на базе систем GridSphere и EnginFrame. Представлены результаты сканирования системы безопасности SDGrid портала выбранными сканерами безопасности. Сформулированы рекомендации по увеличению степени защиты портала. Создан модуль аутентификации по механизму MyProxy для системы EnginFrame.

Научная новизна

Научная новизна работы состоит в исследовании механизмов информационной безопасности порталов доступа к Грид-инфрастуктуре на основе систем GridSphere и EnginFrame, выявления в них уязвимостей, а также решения проблем усиления уровня их защиты. Также впервые была проведена сравнительная характеристика ряда современных сканеров безопасности Nmap, Nessus, Xspider, Shadow Security Scanner и Acunetix Web Vulnerability.

Практическая ценность работы

Практическая ценность работы заключается в выявлении уязвимостей и описания рекомендаций по их устранению в системах GridSphere и EnginFrame, а также в создании модуля аутентификации по механизму MyProxy для системы EnginFrame, который обеспечивает усиление уровня ее защиты и способствует удобной интеграции с Грид-инфрастуктурой.

Выводы

Проведенное исследование показало, что уровень защищенности систем GridSphere и EnginFrame в целом соизмерим, однако системы уязвимы к ряду найденных угроз безопасности. Системы GridSphere и EnginFrame содержат такие механизмы безопасности: аутентификация по логину и паролю, аутентификации по сертификатам (MyProxy), а также по протоколу Kerberos, поддержка GSI, HTTPS/SSL, разграничение доступа и системы ведения журналов.

Система GridSphere уязвима к таким классам атак как: «Межсайтовое выполнение сценариев» высокого уровня риска и «Фиксация сессии» среднего уровня риска, а система EnginFrame к атакам класса «XPath injection» высокого уровня риска. Обе системы имеют различные уязвимости класса «Идентификация приложений» низкого уровня риска.

Воспользоваться найденными угрозами безопасности высокого и среднего уровня риска довольно сложно и успех их применения во многом зависит от профессионализма хакера и халатности администраторов безопасности портала. При правильном администрировании портала, а также выполнении рекомендаций по усилению уровня защиты применение данных угроз безопасности сводится к минимуму.

Работа на 133 листах содержит 21 таблицу, 16 иллюстраций и 1 приложение. При подготовке работы использовалась литература из 25 разных источников.

Перечень ключевых слов: ПОРТАЛЫ ДОСТУПА К ГРИД-ИНФРАСТУКТУРЕ, ПОРТАЛ SDGRID, МЕХАНИЗМЫ БЕЗОПАСНОСТИ ПОРТАЛОВ ДОСТУПА К ГРИД-ИНФРАСТУКТУРЕ, СКАНЕРЫ БЕЗОПАСНОСТИ, GRIDSPHERE, ENGINFRAME.