РЕФЕРАТ

Актуальність роботи

Потенціал технології Grid у наш час дуже великий. У найближчій перспективі Grid повинен стати потужним обчислювальним інструментарієм для розвитку високих технологій у різних сферах життя людини. Однак швидкий розвиток Grid напряму залежить від надання кінцевим користувачам простих засобів для розв'язку їх завдань, приховуючи при цьому всі складності реалізації системи. Створення зручного й простого Web-порталу доступу до Grid-ресурсам вирішує цю проблему. Так як Web-портали є Web-додатками, то вони вразливі до хакерських атак, тому дослідження механізмів їх інформаційної безпеки, а також вирішення проблем посилення їх захисту є актуальним і важливим.

Ціль роботи

Метою даної роботи є дослідження механізмів інформаційної безпеки порталів доступу до Грід-інфрастуктури на прикладі систем керування порталом Gridsphere і EnginFrame з метою посилення рівня їх захисту за рахунок виявлення вразливостей і опису рекомендацій з їхнього усунення.

Задачі, що розв'язувалися в роботі

У роботі вирішувалися такі завдання: аналіз класифікації загроз із метою виділення особливостей кожного класу загроз, створення узагальнених моделей злому й захисту веб-сайтів, огляд основних механізмів безпеки веб-проектів, складання порівняльної характеристики ряда розповсюджених автоматичних сканерів безпеки з метою вибору інструментальних засобів для тестування системи безпеки веб-порталу SDGrid, проведення сканування системи безпеки CMS Gridsphere і EnginFrame, а також створення модуля аутентифікації за механізмом Мургоху для системи Enginframe.

Досягнуті результати

Проаналізована класифікація загроз інформаційної безпеки веб-додатків, у якій виділені: типи загроз, їх рівень ризику, особливості і область застосування. Виділені переваги і недоліки методів пошуку вразливостей веб-додатків. Розроблена узагальнена модель злому, а також узагальнена модель захисту веб-сайтів. Проведена порівняльна характеристика функціональних можливостей ряда розповсюджених автоматичних сканерів безпеки на основі п'яти виділених груп критеріїв, відзначені переваги, недоліки й основна спеціалізація даних сканерів. Розглянуті особливості основних механізмів безпеки порталу Sdgrid на базі систем Gridsphere і Enginframe. Представлені результати сканування системи безпеки Sdgrid порталу обраними сканерами безпеки. Сформульовані рекомендації зі збільшення ступеня захисту порталу. Створений модуль аутентифікації по механізму Мургоху для системи Enginframe.

Наукова новизна

Наукова новизна роботи полягає в дослідженні механізмів інформаційної безпеки порталів доступу до Грід-інфрастуктури на основі систем Gridsphere і Enginframe, виявлення в них вразливостей, а також вирішення проблем посилення рівня їх захисту. Також уперше була проведена порівняльна характеристика ряда сучасних сканерів безпеки Nmap, Nessus, Xspider, Shadow Security Scanner і Acunetix Web Vulnerability.

Практична цінність роботи

Практична цінність роботи полягає у виявленні уразливостей і опису рекомендацій з їхнього усунення в системах Gridsphere і Enginframe, а також у створенні модуля аутентифікації за механізмом Мургоху для системи Enginframe, який забезпечує посилення рівня її захисту й сприяє зручній інтеграції із Грід-інфрастуктурою.

Висновки

Проведене дослідження показало, що рівень захищеності систем Gridsphere і Enginframe в цілому однаковий, проте системи вразливі до ряду знайдених загроз безпеки. Системи Gridsphere і Enginframe містять такі механізми безпеки: аутентифікацію за логіном й паролем, аутентифікацію по сертифікатах (Мургоху), а також за протоколом Kerberos, підтримку GSI, HTTPS/SSL, розмежування доступу і системи ведення журналів.

Система Gridsphere уразлива до таких класів атак як: «Міжсайтове виконання сценаріїв» високого рівня ризику і «Фіксація сесії» середнього рівня ризику, а система Enginframe до атак класу «XPath ін'єкція» високого рівня ризику. Обидві системи мають різні вразливості класу «Ідентифікація додатків» низького рівня ризику. Скористатися знайденими загрозами безпеки високого і середнього рівня ризику досить складно і успіх їх застосування багато в чому залежить від професіоналізму хакера й недбалості адміністраторів безпеки порталу. При правильному адмініструванні порталу, а також при виконанні рекомендацій з посилення рівня захисту застосування даних загроз безпеки зводиться до мінімуму.

Робота на 133 аркушах містить 21 таблицю, 16 ілюстрацій і 1 додаток. При підготовці роботи використовувалася література з 25 різних джерел.

Перелік ключових слів: ПОРТАЛИ ДОСТУПУ ДО ГРІД-ІНФРАСТУКТУРИ, ПОРТАЛ SDGRID, МЕХАНІЗМИ БЕЗПЕКИ ПОРТАЛІВ ДОСТУПУ ДО ГРІД-ІНФРАСТУКТУРИ, СКАНЕРИ БЕЗПЕКИ, GRIDSPHERE, ENGINFRAME.