УДК 62-82:658.512.011.56

В. Ш. Гіоргізова-Гай,
кандидат технічних наук
А. В.Сулімов

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ НАДІЙНОГО ДОСПУПУ ДО ГРІД-ІНФРАСТУКТУРИ

Розглянуто питання загальної інформаційної безпеки Грід- порталів. Особливості вибору інструментальних засобів побудови Грід- порталів та пошуку уразливостей у системі їхньої безпеки розглянуто на прикладі експериментального порталу доступу до обчислювальних можливостей і інформаційних ресурсів національної Grid-інфраструктури Україні — SDGrid.

Грід-технології дозволяють об'єднати різні обчислювальні ресурси в єдину розподілену інфраструктуру і забезпечити колективний доступ до них користувачам, які орієнтовані на вирішення певних завдань і є членами відповідних віртуальних організацій. Сьогодні Грід-технології все активніше входять у різні сфери життя суспільства і спрямовані на вирішення не тільки складних науково-технічних завдань, а й власних завдань бізнесу, промисловості, організації сховищ даних тощо.

Доступ до ресурсів та сервісів є одним із найбільш важливих компонентів Грід-системи, що називається User Interface (UI). Йому приділено особливу увагу, тому що він є ключовою сполучною ланкою між Грід-середовищем і кінцевим користувачем.

User Interface зазвичай реалізують у двох видах:

— інтерфейс командного рядка (Command Line Interface — CLI) — командна оболонка Grid Shell;

— графічний інтерфейс (Graphical User Interface — GUI), який за характером реалізації можна розділити на два типи: Java-аплети й програми та Грід-портали (Web-орієнтовані обчислювальні портали).

Очевидними перевагами GUI є надання користувачам простого інтуїтивно зрозумілого засобу, який дозволяє зробити складну інфраструктуру Грід прозорою для вирішення їх прикладних завдань. На додаток до цього GUI у вигляді Грід-порталу дозволяє користувачам отримати доступ до ресурсів та сервісів Грід за допомогою стандартного web-браузера, який у наш час встановлено на кожному комп'ютері.

Проте Web-портали, як і будь-які Web-додатки, вразливі до атак зловмисників. Навіть якщо зловмисник не зможе отримати доступу до самих ресурсів Грід, а тільки до порталу, це зашкодить виконанню основного завдання останнього — надійного обслуговування користувачів. Тому питання, пов'язані з організацією і аналізом інформаційної безпеки Грід-порталів, є досить важливими.

Метою цієї статті є розгляд питань загальної інформаційної безпеки Грід-порталів, особливостей вибору інструментальних засобів їх побудови та пошуку вразливостей у їх системі безпеки на прикладі експериментального порталу доступу до обчислювальних можливостей й інформаційних ресурсів національної Grid-інфраструктури Україні — SDGrid.

Загальна концепція захисту Web-сайту. Класифікацією загроз безпеці Web-додатків займається міжнародна організація Web Application Security Consortium (WASC) [1]. За результатами досліджень, які було проведено 2008 року організацією WASC і компанією Positive Technologies [2], найбільш небезпечними загрозами є такі класи атак: «Міжсайтове виконання сценаріїв», «SQL ін'єкція», «SSI ін'єкція», «LDAP ін'єкція», «XPath ін'єкція», «Переповнювання буфера», «Форматування рядків», «Виконання команд OS». Найбільш поширеними загрозами за даними фірми Positive Technologies є: класи атак «Міжсайтове виконання сценаріїв» і «Впровадження операторів SQL», а також різні варіанти використання вразливостей класу «Виток інформації». Рівні небезпеки загроз обчислювалися за системою Common Vulnerability Scoring System Support (CVSS) і привласнювалися згідно зі стандартом Payment Card Industry Data Security Standard (PCI DSS).

Загальна концепція захисту Web-проекту повинна забезпечувати комплексний захист, який має включати: надійну безпеку інформаційного середовища Web-сер-

вера, системи управління Web-порталу (CMS), інформаційного середовища адміністраторів Web-порталу, а також сторонніх Web-додатків.

До інформаційного середовища Web-сервера можна віднести операційну систему, Web-сервер, середовище програмування, базу даних, засоби захисту Web-сервера. Кожен із цих компонентів може мати власні вразливості, які мають бути враховані як при виборі компонентів, так і при формуванні загальної політики захисту Web-сайту. Система управління порталом повинна мати єдину і надійну систему аутентифікації, надійну систему розмежування прав доступу, надійні механізми шифрування інформації при передачі даних, надійну систему оновлень і ведення журналів, а також надійний контроль за критично небезпечними ділянками коду. Для управління Web-порталом використовуються комп'ютери адміністраторів, які можуть мати свої вразливості і, як правило, входять до складу корпоративної мережі. Для цих комп'ютерів повинен забезпечуватись надійний антивірусний захист, захист від віддалених атак і захист від витоку інформації. Краще, щоб цими заходами була забезпечена вся корпоративна мережа. Сторонні Web-додатки є ніби проектом у проекті, тому їх захист базується на тих самих принципах.

Важливими механізмами забезпечення інформаційної безпеки Web-проектів є: політика безпеки, аудит і протоколювання подій, які необхідно забезпечувати на всіх компонентах комплексного захисту інформаційного середовища Web-сервера, системи управління Web-проектом, інформаційного середовища адміністраторів Web-проекту і сторонніх Web-додатків.

Політика безпеки є комплексом технічних і організаційних заходів, спрямованих на захист системи від несанкціонованих дій відповідно до цілей та вимог, що висуваються до роботи системи. Аудит досліджує політику безпеки об'єкта і допомагає усунути вразливості, виявлені у процесі його проведення. Ефективність процесу аудиту істотно залежить від якості інструментів пошуку вразливостей. Система протоколювання інформації забезпечує надання інформації для виявлення й аналізу проблем безпеки. Вона дозволяє реконструювати послідовність подій, виявити спроби порушення інформаційної безпеки, забезпечити підзвітність користувачів і адміністраторів.

Розглянемо більш детально питання, пов'язані з безпекою CMS і аудитом безпеки порталу, на прикладі експериментального Web-порталу SDGrid (System Development by Grid), який було створено з метою надання доступу користувачам до обчислювальних можливостей і різних інформаційних ресурсів національної Grid-інфраструктури України [3].

Вибір засобів побудови порталу. За даними незалежного опитування, сьогодні майже всі [4] компанії-розробники Web-сайтів використовують для створення своїх проектів CMS (Content management system) — конструктори створення й керування сайтом, наприклад, 1С-Бітрикс, NetCad, Joomla, WordPress, Drupal тощо. Специфіка організації Грід-порталу полягає у спільній реалізації портальних і Грід-технологій. Тому існує цілий ряд CMS-систем, що враховують саме цю специфіку, наприклад, Gridsphere, Uportal, Clarens та багато інших. Завдяки їх використанню розробка, впровадження, підтримка і використання Grid-порталів стає дедалі зручнішою. Ці засоби є достатньо зрілими продуктами, що забезпечують досить високу безпеку створених на їх основі порталів. Сильною стороною сучасних CMS є забезпечення експорту функціональних модулів — портлетів сторонніх розробників, а також створення власних портлетів, але це може негативно вплинути на питання безпеки.

При створенні Web-порталу SDGrid були висунуто такі загальні вимоги:

— універсальний доступ без додаткового ПО з боку клієнта;

— наявність надійних інформаційних сервісів, зокрема про Grid-ресурси;

— використання відкритих стандартів і технологій Grid;

— масштабована і гнучка структура, легкість додавання/видалення додатків порталів, програмних систем Grid, обчислювальних ресурсів, сервісів, користувачів і т. д.;

— підтримка стандартів Global Grid Forum [5];

— реалізація програмного рішення на відкритих стандартах;

— підтримка розподілених клієнтських застосувань і порталів;

Також висуваються такі вимоги до безпеки системи управління порталом:

— підтримка стандарту безпеки Грід Globus Security Infrastructure (GSI);

— використання протоколів HTTPS/SSL, шифрування даних на всіх рівнях;

— надійний механізм аутентифікації;

— єдина система аутентифікації: використання одного облікового запису для доступу до різних ресурсів Grid;

— використовувані інструментальні засоби повинні мати добре супроводження і постійне оновлення.

Портал SDGrid було побудовано на базі CMS Gridsphere 2.1.5 з використанням OGCE 2.2 portlets і GridPortlets 1.4. Проведена розробниками порталу SDGrid порівняльна характеристика безкоштовних Grid-орієнтованих CMS показала, що Gridsphere на сьогодні є найбільш зручною, популярною і поширеною платформою для створення як обчислювальних порталів, так і порталів користувача [6].

Gridsphere і додатковий інструментарій відповідають висунутим вимогам до системи безпеки порталу. Gridsphere і сумісний з нею інструментарій підтримує використання GSI, єдину систему аутентифікації (використання одного облікового запису для доступу до різних ресурсів Grid), HTTPS/SSL, можливість використовувати аутентифікацію за логіном і паролем, а також за протоколом Kerberos [7].

Механізм аутентифікації порталу SDGrid заснований на аутентифікації користувача за логіном і паролем і подальшому отриманні тимчасового проксі-сертифікату у сервера MyProxy для аутентифікації у Грід. Проксі-сертифікат користувач отримує на основі сертифікату, виданого йому центром сертифікації, приватного ключа і пароля passphrase. За допомогою порталу і отриманого проксі-сертифікату користувач авторизується і може посилати завдання у Грід і проглядати результати. Механізм авторизації виконується у контексті аутентифікації. Якщо суб'єкт аутентифіковано, він може бути авторизований відповідно до типу доступу. Gridsphere має вбудовану підтримку контролю доступу (Role Based Access Control), що дозволяє гнучкіше налаштовувати доступ до порталу.

Gridsphere також має вбудовану систему ведення журналів, яка забезпечує аудит подій, що відбуваються в системі.

Крім CMS та інструментарію, який є необхідним для її встановлення, а також доповнює її можливості, до інформаційного середовища сервера порталу входить ПЗ ОС і Web-сервера. У якості операційної системи для порталу було вибрано ОС Fedora Core Linux 8, виходячи з міркувань надійності, захищеності і нативної підтримки JAVA (зокрема JDK). Останнє є важливим, оскільки Gridsphere побудована на JAVA. Як Web-сервер було вибрано Apache HTTP Server 2.2., якому властиві надійність і гнучкість [8].

Проведення аудиту безпеки порталу. Для пошуку загроз інформаційній безпеці Web-додатків існує два методи: ручний пошук (виконуваний людиною) і автоматичний (виконуваний сканером безпеки). До переваг ручного методу належить: універсальність, гнучкість, висока результативність пошуку, але він вимагає великих витрат часу, високої професійної кваліфікації фахівця і при цьому можливі пропуски вразливостей за рахунок людського чинника. Натомість автоматичний метод є вільним від цих недоліків, але він на сьогодні не є універсальним, може припускати помилкові спрацьовування, якість пошуку вразливостей залежить від повноти бази даних сканера і вимагає постійного її оновлення.

Для проведення об'єктивного дослідження системи безпеки порталу SDGrid, спочатку був виконаний автоматичний аналіз безпеки, а потім — ручна перевірка знайдених загроз високого і середнього ступеня небезпеки.

Вибір автоматичних сканерів безпеки проводився на основі огляду ринку сканерів і результатів опитування, проведеного 2008 року порталом Securitylab.ru [9]. Таким чином, були вибрані такі сканери безпеки: Xspider (версії 7.5. (Build 1610) Trial Version), Nessus (версії 4.0.2), Shadow Security Scanner (версії 7.153 (Build 294)), як найбільш популярні, Nmap (версії 5.21) як найбільш відомий і доступний, а також широко рекламований розробниками Acunetix Web Vulnerability Scanner (версії 6.5 (Bulid 20090604)).

Порівняння вибраних сканерів безпеки проводили за їхніми характеристиками, які були заявлені розробниками. Було виділено п'ять груп критеріїв порівняння, які найповніше охоплюють функціональні аспекти вибраних сканерів:

1. Параметри сканування — наявність перевірок на методи ідентифікації вузла мережі, відкритих портів, служб, додатків і операційних систем, атаки класу DOS, найбільш небезпечні атаки на Web- сервери (XSS атаки, SQL, SSI, XPath, LDAP ін'єк-

ції), підтримка різних методів перевірки однієї й тієї ж уразливості, а також додатково: можливість сканування об'єкта за допомогою сервера посередника (proxy), можливість відключення небезпечних перевірок для вузла сканування, включення/відключення окремих перевірок або їх груп, наявність готових шаблонів перевірок, можливість сканування декількох об'єктів у паралельному режимі.

2. Розгортання і архітектура — наявність розподіленої архітектури, наявність командного рядка і графічного інтерфейсу, розмежування доступу.

3. Управління результатами сканування і реагування — опис знайдених уразливостей, варіантів їх використання і рекомендацій з усунення, опис причин помилкових спрацьовувань, форми звітності.

4. Оновлення і підтримка: наявність бази знань, автоматичного оновлення бази, форми підтримки користувачів.

5. Додаткові критерії: інтеграція з системами виявлення атак (IDS), наявність документації і звітів російською мовою.

Загальна порівняльна характеристика сканерів по всіх групах критеріїв подана у табл. 1. Оцінка показує, скільки критеріїв (можливостей) з максимальної кількості у групі підтримує цей сканер.

Таким чином, внаслідок порівняння найбільш важливих критеріїв 1-ї і 3-ї груп (функціональних можливостей), лідирують сканери Nessus і XSpider, непогано зарекомендували себе сканери AWVS і SSS, сканер Nmap отримав найменшу кількість балів головним чином через відсутність використання різних налаштувань і методів.

Таблиця 1. — **Загальна оцінка по всіх групах критеріїв**

Критерій порівняння	Максимум балів	Nmap	Nessus	AWVS	SSS	XSpider
Параметри сканування	15	9	13	9	10	10
Розгортання і архітектура	5	2	5	1	1	1
Управління результатами сканування і реагування	11	0	7	9	7	10
Оновлення і підтримка	4	0	2	2	2	3
Додаткові критерії	3	1	0	1	0	2
Разом балів	38	12	27	22	20	26

Сканування SDGrid порталу проводилося методом «чорної скриньки» на ноутбуку HP Pavilion dv-6850er віддалено через Інтернет по каналу 100Мбит/с. У табл. 2 подана кількість знайдених класів загроз.

Таблиця 2. — **Результати сканування порталу SDGrid**

Критерій порівняння		Nmap	Nessus	AWVS	SSS	XSpider
Час сканування		1 хв	4 хв	47 хв	32 хв	28 хв
Знайдено всього класів загроз		4	2	4	2	4
Ступінь ризику	високий	0	0	1	1	0
	середній	0	0	1	0	1
	низький	4	2	2	1	3

Слід відмітити, що сканери Xspide, AWVS і SSS показали в цілому сумірний час сканування, тоді як Nessus і Nmap працювали на порядок менше. Найшвидше провів сканування Nmap , а найдовше — AWVS.

Знайдені класи загроз безпеці високого і середнього рівнів ризику були перевірені ручним методом пошуку, результати показані у табл. 3. Використовувалася така схема позначень: + (плюс) — сканер визначив загрозу, — (мінус) сканер не визначив загрозу.

Таблиця 3. — **Об'єктивність знайдених класів загроз безпеки високого і середнього ступенів ризику**

Клас знайдених погроз	Nmap	Nessus	AWVS	SSS	XSpider	Ручний пошук
Cross Site Scripting	–	–	+	+	+	Загроза підтверджена
Фіксація сесії	–	–	+	–	–	Загроза підтверджена

Таким чином, сайт виявився вразливим до таких класів атак як: «Міжсайтове виконання сценаріїв» (Cross Site Scripting) високого ступеня ризику і «Фіксація сесії» середнього ступеня ризику. Внаслідок проведеного тестування найкраще зарекомендував себе сканер AWVS, який знайшов найбільшу кількість загроз, що були підтверджені ручним пошуком, показав найдокладніший опис знайдених типів загроз і рекомендацій з їх усунення.

Висновки. Проведене дослідження показало, що механізми безпеки порталу SDGrid в цілому задовольняють висунутим вимогам до безпеки, проте мають ряд уразливостей. Для захисту від класу атак «Фіксація сесії» бажано перейти на 3-ю версію системи GridSphere. Для захисту від класів атак «Міжсайтове виконання сценаріїв» необхідно додати перевірки на коректність очікуваних даних, що отримують із будь-яких джерел, а також провести заміну потенційно небезпечних символів HTML сторінки на їх еквіваленти. Скористатися цими уразливостями досить складно і успіх їх застосування багато в чому залежить від професіоналізму хакера і халатності адміністраторів безпеки порталу.

Знайдені вразливості низького рівня ризику належать до класу «Ідентифікація додатків». Проте ці загрози використовуються на підготовчому етапі атаки для збору інформації про об'єкт, що атакується, тому вони не завдають шкоди порталу, а лише розкривають інформацію про різні додатки.

Захист Web-проекту повинен бути комплексним і включати такі складові інформаційної безпеки, як захищеність CMS-системи, інформаційного середовища Web-сервера (ОС, БД, засобів захисту Web-сервера), а також інформаційного середовища адміністраторів Web-порталу.

Загальний захист портального сервера може також підвищити використання індивідуального міжмережевого екрану у вигляді або апаратного рішення, наприклад, Chek Point FW-1, або більш економічного програмного рішення, наприклад, CYBERWALLPLUS компанії Network-1 Security Solution. Такий екран забезпечить додатковий рівень безпеки за рахунок запобігання відомим типам атак на сервер і своєчасних сповіщень адміністратора безпеки про підозрілу діяльність [10].

Література

1. Офіційний сайт організації Web Application Security Consortium. — Режим доступу: http://www.webappsec.org/.

2. Статистика уразливостей WEB-додатків у 2008 році. — Режим доступу: http://www.ptsecurity.ru/stat2008.asp.

3. *Згуровський М. З.* Створення національної Grid-інфраструктури для забезпечення наукових досліджень / М. З. Згуровський, А. І. Петренко, Г. Д. Кисельов // Інформаційні технології в освіті. — 2009. — № 4. — С. 12–17.

4. Сайт о системах управления сайтом. — Режим доступу: http://cmslist.ru/

5. Overview of the Grid Security Infrastructure. — Режим доступу: http://www.globus.org/security/overview.html

6. *Киселев Г. Д.* Использование платформы GridSphere для создания Grid-порталов / Г. Д. Киселев, А. А. Зеленюк, А. Г. Киевский, Е. В. Оленович // Системный анализ и информационные технологии: материалы 11-й международной научно-технической конференции «САИТ-2009». — К. : НТУУ «КПІ», 2009. — С. 440.

7. Офіційний сайт системи GridSphere. — Режим доступу: http://www.gridsphere.org

8. *Киселев Г. Д.* Построение вычислительного Grid-портала для национальной Grid сети / Г. Д. Киселев, В. А. Матущенко, Р. В. Чепурной // Системный анализ и информационные технологии: материалы 10-й международной научно-технической конференции «САИТ-2008». — К. : НТУУ «КПИ», 2008. — С. 300.

9. Сравнительный анализ сканеров безопасности. Часть 1: тест на проникновение (краткое резюме) [Електронний ресурс]. — Режим доступу: http://www.securitylab.ru/analytics/365241.php

10. Програмные и аппаратные межсетевые экраны [Електронний ресурс]. — Режим доступу: http://www.intuit.ru/department/network/fireWalls