Исследование механизмов информационной безопасности на портале SDGrid в национальной Грид-инфрастуктуре

Сулимов А.В, студент группы ДА42-М
кафедры СП УНК «ИПСА» НТУУ «КПИ»

Цель работы и решаемые задачи

Целью работы является исследование механизмов информационной безопасности портала SDGrid на примере систем управления порталом **GridSphere** и **EnginFrame**.

Решаемые задачи:

- анализ классификации угроз безопасности веб-приложений;
- создание обобщенных моделей взлома и защиты веб-сайтов;
- обзор основных механизмов безопасности веб-порталов;
- составление сравнительной характеристики 5 распространенных сканеров безопасности;
- проведение сканирования систем безопасности CMS GridSphere и EnginFrame;
- формирование рекомендаций по усилению защиты портала SDGrid
- создание модуля аутентификации по механизму MyProxy для демо-версии системы EnginFrame.

Классификация угроз безопасности веб-приложений

- Классификацией занимается международная организация **Web Application Security Consortium** (WASC).
- Этой организацией был создан документ **Web Security Threat Classification** (WSTC) – классификация, которая представляет собой попытку собрать воедино всевозможные угрозы безопасности Web-приложений.
- Согласно данного документа угрозы безопасности веб-приложений делятся на **атаки** и **уязвимости.**
- Документ включает **34** классов атак и **15** классов уязвимостей, которые структурированы в такие разделы: «Аутентификация», «Авторизация», «Логические атаки», «Атаки на клиентов», «Информационное раскрытие», «Выполнение команд» и «Другие».

Обобщенная модель взлома веб-сайта

Обобщенная модель защиты веб-сайта

Методы поиска угроз безопасности веб-приложений

- ***Автоматический***

+ **Экономия времени за счет автоматизации проверок**
+ **Метод не требует профессиональных знаний в информационной безопасности**
+ **Предоставление подробного описания найденных угроз**

— **Универсального алгоритма автоматического поиска в настоящее время не существует**
— **Возможность ложных срабатываний**
— **Необходимость в постоянном обновлении баз данных сканера**

- ***Ручной***

+ **Метод более универсальный**
+ **Вероятность обнаружения уязвимостей значительно больше, чем при автоматичном поиске**
+ **Понимание и контроль за процессами поиска**

— **Большие затрат по времени**
— **Необходимы профессиональные знания в информационной безопасности**
— **Возможность пропуска уязвимости за счет ошибки человеческого фактора**

Выбор сканеров безопасности для проведения тестирования

- ***Xspider*** (версии 7.5. (Build 1610) Trial Version);
- ***Nessus*** (версии 4.0.2);
- ***Shadow Security Scanner*** (версии 7.153 (Build 294));
- ***Nmap*** (версия 5.21);
- ***Acunetix Web Vulnerability Scanner*** (версии 6.5 (Bulid 20090604));

Сравнительная характеристика выбранных сканеров безопасности

по 5 группам критериев функциональных возможностей

Группа критериев	**Nmap**	**Nessus**	**AWVS**	**SSS**	**XSpider**
Развёртывание и архитектура	2	5	1	1	1
Параметры сканирования	11	14	10	11	13
Управление результатами	0	7	9	7	10
Обновление и поддержка	0	2	2	2	3
Дополнительные	1	0	1	0	2
Итого баллов (из 40)	**14**	**28**	**23**	**21**	**29**

Портал SDGrid

- ***GridSphere 2.1.5***
- ***Базовая система портала***
- Является популярной бесплатной Java платформой
- *Отличается:*
  - доступностью;
  - соответствием API стандарту JSR 168;
  - поддержкой разработки и внедрения новых приложений.

- ***EnginFrame 5.0 (Demo)***
- ***Выбрана альтернативой***
- Является платной клиент-серверной системой
- *Отличается:*
  - производительностью;
  - совместимостью с современными протоколами HPC систем;
  - модульностью и гибкостью доступа к Грид-инфрастуктуре.

Основные механизмы безопасности SDGrid портала

Механизмы безопасности	*GridSphere 2.1.5*	*EnginFrame 5.0*
Поддержка аутентификации по логину и паролю	+	+
Поддержка аутентификации по сертификатам (MyProxy)	+	+ (*)
Поддержка аутентификации по протоколу Kerberos	+	+ (*)
Поддержка GSI	+	+
Поддержка HTTPS/SSL	+	+
Поддержка разграничения доступа	+	+
Наличие системы ведения журналов	+	+

* – встроенная поддержка отсутствует в Demo версии системы

Результаты сканирования портала на основе системы GridSphere 2.1.5

Критерии сравнения		Nmap	Nessus	AWVS	SSS	XSpider
Время сканирования		10 мин	4 мин	47 мин	32 мин	28 мин
Найдено всего классов угроз		1	1	3	2	2
Риск угроз	Высокий	0	0	1	1	1
	Средний	0	0	1	0	0
	Низкий	1	1	1	1	1

Класс найденных угроз	Nmap	Nessus	AWVS	SSS	XSpider	Ручной поиск
Cross Site Scripting	—	—	+	+	+	Класс угроз подтвержден
Фиксация сессии	—	—	+	—	—	Класс угроз подтвержден
Идентификация приложений	+	+	+	+	+	Класс угроз подтвержден

Результаты сканирования портала на основе системы EnginFrame 5.0 (Demo)

Критерии сравнения		Nmap	Nessus	AWVS	SSS	Xspider
Время сканирования		10 мин	5 мин	26 мин	22 мин	24 мин
Найдено всего классов угроз		1	2	2	1	1
Риск угроз	Высокий	0	0	1	0	0
	Средний	0	1	0	1	0
	Низкий	1	1	1	0	1

Класс найденных угроз	Nmap	Nessus	AWVS	SSS	XSpider	Ручной поиск
XPath инъекция	—	—	+	—	—	Класс угроз подтвержден
Не безопасная конфигурация сервера	—	—	—	+	—	Класс угроз **не** подтвержден
Обратный путь в директориях	—	+	—	—	—	Класс угроз **не** подтвержден
Идентификация приложений	+	+	+	—	+	Класс угроз подтвержден

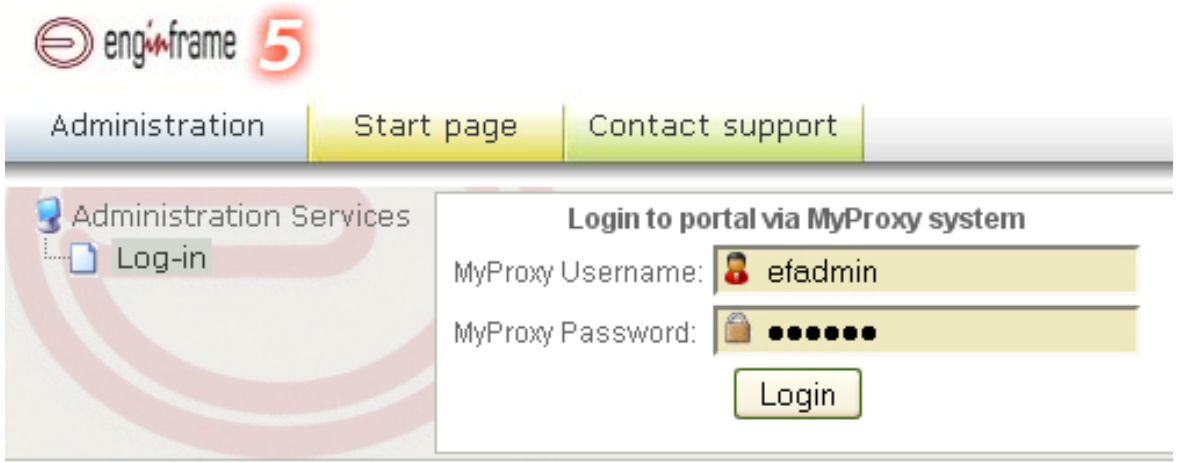
Рекомендации по увеличению степени защиты SDGrid портала (1)

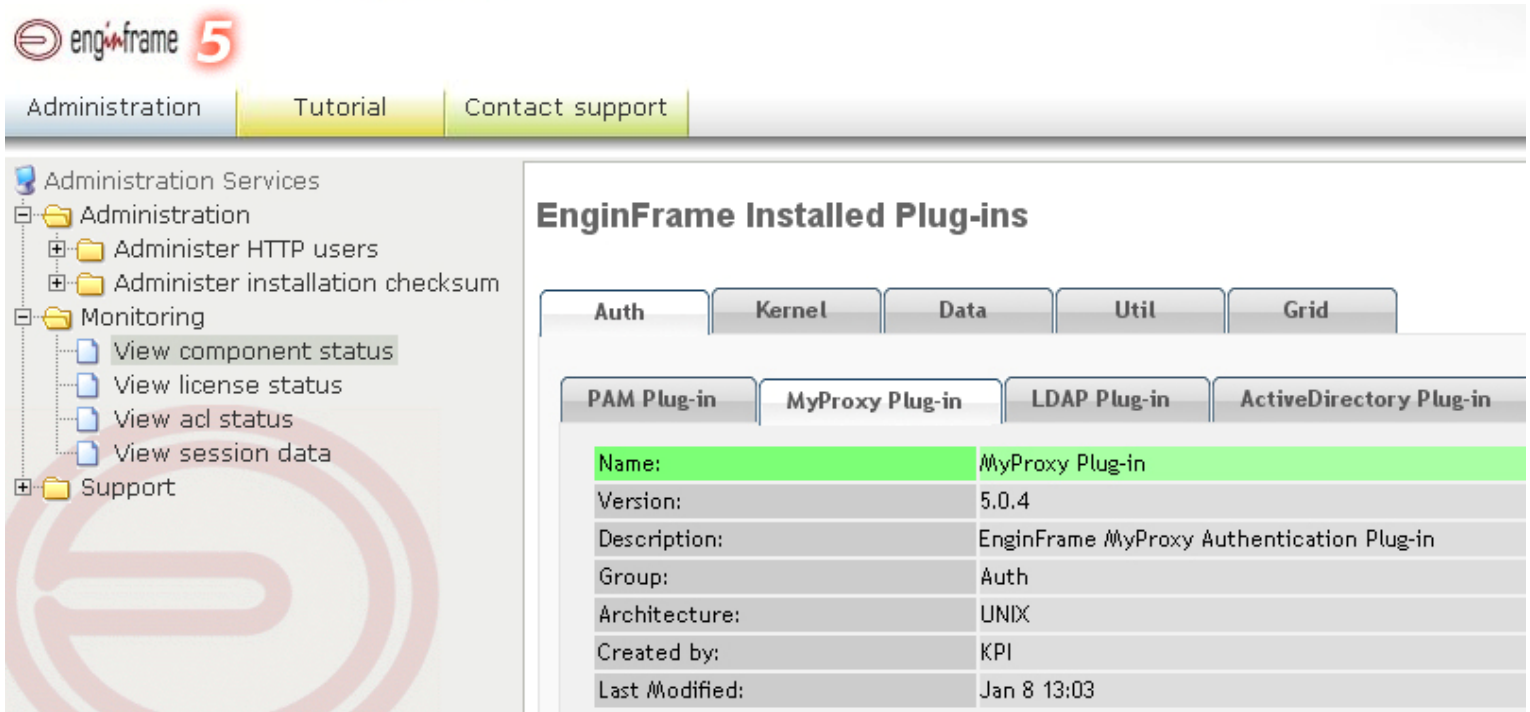
- ***Общие***:
  - Необходимо обеспечить комплексную защиту портала, которая включает надежную безопасность Web-сервера (ОС, БД, средств защиты Web-сервера), системы управления Web-портала (CMS), а также информационной среды администраторов Web-портала и сторонних сторонних Web-приложений
  - Можно использовать специализированный межсетевой экран, например, CyberwallPLUS компании Network-1 Security Solution. Данное решение обеспечит дополнительный уровень безопасности за счет предотвращения известных типов атак на сервер и своевременных оповещений администратора безопасности о подозрительной деятельности.

Рекомендации по увеличению степени защиты SDGrid портала (2)

- для портала на ***GridSphere***:
  - Для защиты от класса атак «Фиксация сессии» желательно перейти на 3-ю версию.
  - Для защиты от классов атак «Межсайтовое выполнение сценариев» необходимо добавить проверки на корректность ожидаемых данных, а также необходимо произвести замену потенциально небезопасных символов HTML страницы.
- для портала на ***EnginFrame***:
  - Для защиты от классов атак «XPath инъекция» необходимо добавить проверки на корректность ожидаемых данных, получаемых из любых источников, а также необходимо произвести замену потенциально небезопасных символов XML.

Модуль аутентификации по прокси-сертификатам для EnginFrame (Demo)





Выводы

- Уровень защищенности систем **GridSphere** и **EnginFrame** в целом соизмерим.
- Обе системы поддерживают основные надежные механизмы безопасности и удовлетворяют поставленным требованиям к безопасности, однако уязвимы к ряду выявленных угроз.
- Воспользоваться найденными угрозами безопасности высокого и среднего уровня риска довольно сложно и при правильном администрировании портала и выполнении рекомендаций их применение сводится к минимуму.