УДК 004.056.738.5

ЗАЩИТА КОНТЕНТА ИНТЕРНЕТ-ПОРТАЛА С ПОМОЩЬЮ СИСТЕМ УПРАВЛЕНИЯ СОДЕРЖИМЫМ (CMS)

Журба А.С.
Научный руководитель – к.т.н. доц. Иванов В.Г.
Харьковский национальный университет радиоэлектроники г.Харьков
Кафедра системотехники
E-mail: legan4ik@i.ua

Аннотация

Журба А.С. Защита контента Интернет-портала с помощью систем управления содержимым (CMS). *В статье рассматривается проблема защиты контента и разграничение прав доступа для информационно-новостного портала о науке и образовании.*

Общая постановка проблемы. Проблема защиты сайтов от различного рода атак (SQL инъекция, межсайтовый скриптинг (XSS), отказ в обслуживании (Denial of Service) и т.д.), а также недостаточная аутентификация и авторизация пользователей всегда актуальны в сети. Веб-сайт – это лицо и одновременно инструмент работы с клиентами для любой компании. В случае выхода его из строя или взломе – фирма может потерять и продажи (например, интренет-магазин) и доверие многих своих клиентов. В связи с эти возникает необходимость защиты своего веб-ресурса от атак и подмены информации на нем.

Вручную администрировать и обеспечивать целостность крупного, динамичного портала пользователю, который вдобавок не имеет глубоких познаний в области информационной безопасности, просто невозможно. Есть несколько решений этой проблемы. Можно выделить два основных: аутсорсинг или разработка своими силами. Первый метод заключается в том, что компания нанимает специалистов в области информационной безопасности, которые и занимаются защитой портала. Некоторую часть работы можно переложить на хостинг-провайдера. Это решение требует серьезных денежных вложений, хотя и обеспечивает высокий уровень защиты. Оно имеет также и недостаток: некоторые организации просто не могут пригласить сотрудников извне, так как защищаемая информация может быть строго конфиденциальна.

Второй метод подразумевает обучение своих сотрудников всем тонкостям сетевой безопасности или же использование готовых систем защиты и управления контентом, которые не требуют дополнительной переквалификации персонала. Последнее гораздо предпочтительнее, так как имеется возможность сэкономить время и деньги компании. Таким образом, самым подходящим вариантом будет применение системы управления содержимым.

Постановка задачи. В настоящее время прослеживается тенденция к автоматизации операций защиты и модерирования контента. Одним из методов решения этой задачи является использование системы управления содержимым (CMS) для администрирования и обеспечения безопасности корпоративных веб-сайтов. Существует множество CMS, которые отличаются функциональной оснасткой, ориентированы на различные нужды, с открытым и закрытым кодом, бесплатные и платные. Большое распространение получили некоммерческие продукты, которые не уступают, а иногда и превосходят, Shareware-разработкам по многим параметрам.

В данной работе анализировались существующие CMS и возможности их расширения для применения к информационно-новостному порталу о науке и образовании, который должен соответствовать следующим условиям:

- многоуровневое разграничения прав доступа для различных пользователей портала;
- защита от SQL и PHP инъекций злоумышленников;

- запрет на многоразовое дублирование сообщений;
- ведение и отправка почтой логов администратору;
- быстрое резервирование восстановление;
- бесплатное распространение управляющей системы;
- удобное обновление для обеспечения лучшей защиты.

Методы решения задачи и результаты. Для решения поставленной задачи был проведен анализ некоторых систем управления контентом, их инструментария и направленности. Наиболее подходящей, учитывая простоту, бесплатность и достаточную ее защищенность, была выбрана CMS Joomla. Ее основные особенности:

- модуль безопасности для многоуровневой аутентификации пользователей/администраторов;
- возможность ограничить доступ к определенным разделам сайта только для зарегистрированных (многоуровневое разграничение прав доступа);
- благодаря хорошей расширяемости можно установить дополнительные модули и плагины, которые смогут еще больше повысить безопасность;
- журналирование;
- удобная система обновлений;
- возможность изменять исходный код для более тонкой настройки системы под разрабатываемый проект;
- Joomla Security Center – бюллетень безопасности, в котором эксперты в области защиты информации публикуют свежие новости, касающиеся проводимых работ, связанных с обеспечением безопасности Joomla. Там же можно сообщить о найденной ошибке, которая непременно будет исправлена в новых версиях.

Необходимо было рассмотреть возможность увеличения существующего уровня безопасности с помощью комплекса сторонних компонентов и модулей. Первоначально был использован дополнительный компонент GuardXT. Он по расписанию может делать анализ файловой системы на уязвимости, регулярно отслеживает изменения файлов, показывает новости безопасности. Кроме того, GuardXT проверяет актуальность версий компонентов выполняет контроль безопасности (конфигурации Joomla, параметры настройки PHP и т.д.). Результаты работы представлены в удобной форме, есть возможность устранить некоторые проблемы прямо из интерфейса компонента. С помощью него были обнаружены некоторые недочеты (проход защиты тайм-аута, отсутствие проверки для JEXEC и т.д.), которые устранились после обновления Joomla до актуальной версии.

Далее был установлен компонент JDefender. С помощью него можно предотвратить SQL, PHP инъекцию, а также запретить flood-атаку. JDefender позволяет почтой отправлять администратору логи и блокировать IP адреса нарушителей. Если же злоумышленник повредил контента портал, то для восстановления информации из резервной копии, которую ранее сделал администратор, будет использоваться плагин LazyBackup 2. Также с его помощью можно создавать по расписанию копии базы данных и отправлять их на несколько электронных адресов.

Выводы.

В результате работы, система наполнения содержимым Joomla была применена для создания, администрирования и защиты информационно-новостного портала о науке и образовании. Таким образом, благодаря комплексу модулей и компонентов, был обеспечен необходимый уровень безопасности. Встроенные средства авторизации и аутентификации защищают контент и административную панель от несанкционированного доступа. При дальнейшей поддержке портала необходимо логично и четко разграничить доступ к ресурсам и админ-панели сайта, делать резервные копии базы данных, а также регулярно обновлять Joomla.