Антон А. Абрамов[1], Виктор С. Горбатов[2], Марина Н. Гришина[3]
[1]ФГУП «Главный научно-исследовательский вычислительный центр» Управления делами Президента Российской Федерации,
г. Москва, 121471, ул. Рябиновая, д. 43, корп. 1
e-mail: genomod@mail.ru, http://orcid.org/0000-0002-4088-6606
[2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, г. Москва, 115409, Россия
e-mail: VSGorbatov@mephi.ru, http://orcid.org/0000-0001-9998-9733
[3]ФГБУ НМИЦ имени академика В.И. Кулакова Министерства здравоохранения Российской Федерации,
ул. Академика Опарина, 4, г. Москва, 117198, Россия
e-mail: m.n.grishina@mail.ru, http://orcid.org/0000-0003-4482-4354

УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ВЕБ-ПОРТАЛА НА ПЛАТФОРМЕ OPEN JOURNAL SYSTEMS

DOI: http://dx.doi.org/10.26583/bit.2018.2.08

Аннотация. В этой статье рассматриваются основные угрозы безопасности веб-порталам, построенным на платформе Open Journal Systems. Платформа Open Journal Systems (далее OJS), изначально разработанная в рамках проекта Public Knowledge Project, является одной из самых популярных открытых платформ для электронных журналов. На 2016 год исходя из данных, которыми располагает проект Public Knowledge Project, насчитывается более 10 тысяч активных журналов, использующих платформу OJS. Для журнала переход на такую продвинутую и сложную платформу, которая позволяет полностью перенести весь рабочий процесс на единый веб-портал, является серьезным шагом и на него идут рецензируемые журналы, входящий в российские и зарубежные системы цитирования, а потому вопрос сохранности содержимого статей до их публикации очень важен для самого журнала, так и для авторов, которые хотят в журнале публиковаться. В этой работе рассматриваются наиболее актуальные угрозы для веб-порталов на платформе OJS, описана частная модель угроз безопасности, а также предложены меры, которые позволяют нейтрализовать эти угрозы.

Ключевые слова: частная модель угроз, модель нарушителя, веб-портал, угрозы информационной безопасности, меры защиты, php, xss, open journal systems.
Для цитирования. АБРАМОВ, Антон А.; ГОРБАТОВ, Виктор С.; ГРИШИНА, Марина Н.. УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ ЭКСПЛУАТАЦИИ ВЕБ-ПОРТАЛА НА ПЛАТФОРМЕ OPEN JOURNAL SYSTEMS. Безопасность информационных технологий, [S.l.], n. 2, p. 86-105, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1113>. Дата доступа: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.08.

Anton A. Abramov[1], Victor S. Gorbatov[2], Marina N. Grishina[3]
[1]Federal State Unitary Enterprise "Main Research Computing Center" of the Administrative Department of the President of the Russian Federation,
Moscow, 121471, Rybinovaya 43
e-mail: genomod@mail.ru, http://orcid.org/0000-0002-4088-6606
[2]National Research Nuclear University MEPHI,
Kashirskoe shosse, 31,Moscow, 115409, Russia
e-mail: VSGorbatov@mephi.ru, http://orcid.org/0000-0001-9998-9733
[3]Federal state budget institution national medical research center named after academician V.I. Kulakova, Ministry of Health of the Russian,
Moscow, 117198, Academica Oparina 4
e-mail: m.n.grishina@mail.ru, http://orcid.org/0000-0003-4482-4354

Information security threats in web-portals on the open journal systems platform

DOI: http://dx.doi.org/10.26583/bit.2018.2.08

Abstract. This article addresses the problem of security threats while working with web portals built on the Open Journal Systems platform. The Open Journal Systems (OJS) platform was originally developed as part of the Public Knowledge Project and it is one of the most popular open-source platforms for web journals today. Based on the data available in the Public Knowledge Project, there were more than 10,000 active journals using the open journal systems platform by the end of 2016. A migration of a journal to such advanced and complex platform helps to handle the entire workflow over a single web portal. Therefore it is an important move and only peer-reviewed journals that are part of Russian and Worldwide citation systems go for it. At the same time the problem of keeping privacy for a manuscript before it is published is very important for these journals and for authors who submit it to the journal. The paper describes the most common threats for the web portals on the OJS platform as well as a particular model of the security threats, and suggests the measures that could help to neutralize these threats.

Keywords: particular threat model, intruder model, web portal, information security threats, protection measures, php, xss, open journal systems.

For citation. ABRAMOV, Anton A.; GORBATOV, Victor S.; GRISHINA, Marina N.. Information security threats in web-portals on the open journal systems platform. IT Security (Russia), [S.l.], n. 2, p. 86-105, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1113>. Date accessed: 26 apr. 2018. doi:http://dx.doi.org/10.26583/bit.2018.2.08.

Введение

Повышение качества существующих и создание современных методов сбора информации, её хранения, обработки и распространения является существенной составляющей процесса развития информационных систем и информационных технологий. Потребность такого совершенствования связана с непрерывным ростом количества электронных документов и их доступностью, что в свою очередь очень затрудняет управление информацией и саму работу пользователя с ней. Для решения этой проблемы специалистами данной области была предложена идея Веб -порталов. Веб -портал является программной средой, которая обеспечивает унифицированный доступ к контенту, расположенному в информационных источниках. Портал структурирует информацию и предоставляет пользователям средства для её поиска. Веб-порталы обрабатывают и хранят огромное количество информации, которая подвержена различным угрозам. Таким образом, появляется острая необходимость в анализе угроз безопасности информации разнообразных веб-ресурсов и веб-порталов, в частности.

Частным случаем использования веб-порталов являются электронные журналы, публикуемые в сети интернет. Одной из наиболее распространенных платформ является платформа Open Journal Systems (далее OJS), изначально разработанная в рамках проекта Public Knowledge Project [1]. На 2016 год, исходя из данных, которыми располагает проект Public Knowledge Project, насчитывается более 10 тысяч активных журналов, использующих платформу Open Journal Systems [2]. На самом деле есть основания полагать, что реальная цифра на порядок выше, т.к. только для России официально насчитывается около 170 журналов, хотя на одной только электронной платформе Elpub, которая базируется на OJS, насчитывается более 260 журналов. OJS разрабатывается как платформа с открытым исходным кодом и дорабатывается мировым сообществом, в том числе активно в этом процессе участвуют и российские разработчики. Для журнала переход на такую продвинутую и сложную платформу, которая позволяет полностью перенести весь рабочий процесс на единый веб-портал, является серьезным шагом и на него идут рецензируемые журналы, входящие в российские и зарубежные системы цитирования, а потому вопрос

сохранности содержимого статей до их публикации очень важен, как для самого журнала, так и для авторов, которые хотят в журнале публиковаться.

В этой работе рассматриваются наиболее актуальные угрозы для веб-порталов на платформе OJS, а также описаны меры, которые позволяют нейтрализовать эти угрозы. Актуальность угроз определялась исходя из специфики работы электронных изданий со своими авторами, рецензентами и редакционной коллегией.

Современные работы, связанные с исследуемой тематикой

Веб-порталы представляют собой достаточно сложную систему, состоящую из множества компонентов, каждый из которых может содержать в себе уязвимости, которые становятся источниками угроз, по средствам которых, злоумышленник может реализовать атаку на веб-портал и нарушить целостность, доступность и конфиденциальность хранимых и обрабатываемых веб-порталом данных. Веб-портал построенный с использованием платформы OJS не является исключением, поэтому разумно взглянуть на современную ситуацию в области безопасности технологий, лежащих в основе OJS. Это позволяет сформулировать определенные требования и рекомендации к используемым компонентам и их конфигурации.

Ключевыми проблемами для большинства порталов являются уязвимости связанные:

- перехватом и подменой трафика между пользователем и сервером;
- исполнением произвольного кода;
- XSS атаками, «межсайтовый скриптинг»;
- загрузкой произвольных файлов;
- открытым доступ к конфигурационным файлам;
- слабым алгоритмом выявления «ботов».

Классическим способом получения данных является перехват траффика в незашифрованном канале, этот способ наиболее актуален если веб-портал использует не защищённый http протокол. Подобные атаки «человек посередине» много раз освещались в литературе и имеют подробное описание, как например в статье А. Малински и др. [3]. В связи с тем, что платформа OJS реализована на языке программирования PHP, то для нее характерны определенные уязвимости, связанные с произвольным исполнением кода и XSS. Методы по выявлению подобных уязвимостей, связанных с особенностями языка PHP хорошо описаны в статье М. Бакерса и др. [4]. В своей статье они представили метод межпроцедурного анализа для приложений PHP, основанный на статистических свойствах кода, который хорошо масштабируется для объемного исходного кода, что актуально в случае с OJS. Похожая работа, но в ключе XSS атак, касающаяся языка PHP, проделана А. Маршадих и З. Зааба и описана в недавней статье [5]. Интересной особенностью этого исследования является то, что помимо простого обнаружения PHP XSS уязвимостей предлагаются и методы устранения найденных уязвимостей, что очень полезно, если учесть тот факт, что исходные коды OJS очень объемны. Вообще тестирование исходных кодов большого объема задача не тривиальная: существует множество подходов для ее решения, в основном работает правило, чем качественнее тестирование, тем большую подготовительную работу требуется сделать. Подготовительные работы могут быть связаны с разбиением исходной системы на отдельные логические блоки, которые выполняют ряд конечных функций, разработка среды для тестирования этих блоков, разработка самих тестов, выполнение тестовых сценариев с протоколированием результатом и, наконец, анализ полученных результатов. Чтобы упростить эту работу применительно к языку программирования PHP, был разработан метод полуавтоматической генерации тестовых примеров, который описан в статье Б. Стивалета и Е. Фонга [6]. Получение доступа к конфигурационным файлам злоумышленником и

возможность манипуляции такими файлами – это серьезная уязвимость для веб-порталов, используя ее возможно получить ключи для прямого подключения к базам данных, с которыми работает веб-портал. Исследования подобного рода для множества различных конфигураций рассматриваются в статье Н. Бен-Ашер и др. [7]. Основной упор в своей работе авторы сделали на построение системы, которая способна менять используемую платформу, т.е. полностью, либо частично заменять стек используемых технологий, в том числе в работе рассматриваются и базовые уязвимости основных платформ. Распространённым способом выявления «ботов» и предотвращения «спам-атак», является reCAPTCHA, однако OJS версии 2.x.x использует первую версию этого алгоритма, его надежность достаточно хорошо изучена и принимая во внимание современные успехи в области компьютерного зрения reCAPTCHA v1 не представляет собой серьезной преграды для современных «ботов». Подробно этот процесс описан в работе Ф. Старка и др. [8]. Помимо прочего авторы предоставляют открытую реализацию алгоритма распознавания символов в CAPTCHA. В области исследования защищенности веб-порталов ведутся серьезные работы с применением передовых наработок, доступных исследователям. Появляются новые, более эффективные методы поиска известных уязвимостей, что существенно облегчает работу для тестирования безопасности веб-порталов и позволяет сформулировать более качественные рекомендации по использованию и настройки составных частей для больших веб-порталов.

Веб-портал и его назначение

Прежде чем перейти непосредственно к исследованию платформы OJS, с точки зрения безопасности, рассмотрим, что из себя представляют веб-порталы и какое место в структуре веб-портала занимает OJS, какие ограничения это накладывает на выбор технологий и прочие особенности построения систем на базе OJS. Веб-портал, в рамках данной статьи, следует рассмотреть, как некую информационную систему, обеспечивающую пользователям единый авторизованный персонифицированный доступ, как к внутренним, так и внешним ресурсам, а также приложениям организации. Веб-порталы классифицируются по специализации информации, целевой аудитории, решаемым задачам и используемым технологиям. Классификация порталов включает следующие основные классы: мегапортал; информационный; корпоративный; коммерческий; горизонтальный; вертикальный; торговый; портал публикации информации; портал приложений; портал управления; портал для совместной работы; портал знаний, - подробная классификация порталов и описание каждого из классов приведено в [9]. Выделим наиболее распространённые виды порталов. Горизонтальные порталы – эти порталы, как правило, предназначены для самой большой аудитории, и включают в себя информацию и услуги, носящие общий характер. То есть они имеют задачу охватить и предоставить как можно больше информации пользователям в разных сферах. Направленность данных порталов тесно связана с деятельностью средств массовой информации. Самыми распространенными мегапорталами являются, например, всем известный Rambler, Yandex, Yahoo! и Mail.ru. Вертикальные порталы также называют нишевыми. Это обычно сайты узкой тематики, которые рассчитаны на определенную целевую категорию пользователей. Вертикальные порталы предоставляют средства, информацию, статьи, исследования, какую-либо статистику по конкретной отрасли. Примерами данного класса порталов являются развлекательные, корпоративные, финансовые, религиозные и образовательные веб-ресурсы. Веб-порталы базирующихся на платформе OJS – это вертикальные порталы знаний.

Можно однозначно сказать, что любой портал включает в себя как минимум три основных функциональных модуля:

- модуль интеграции данных;
- модуль интеграции приложений и сервисов;

- модуль индексирования и поиска.

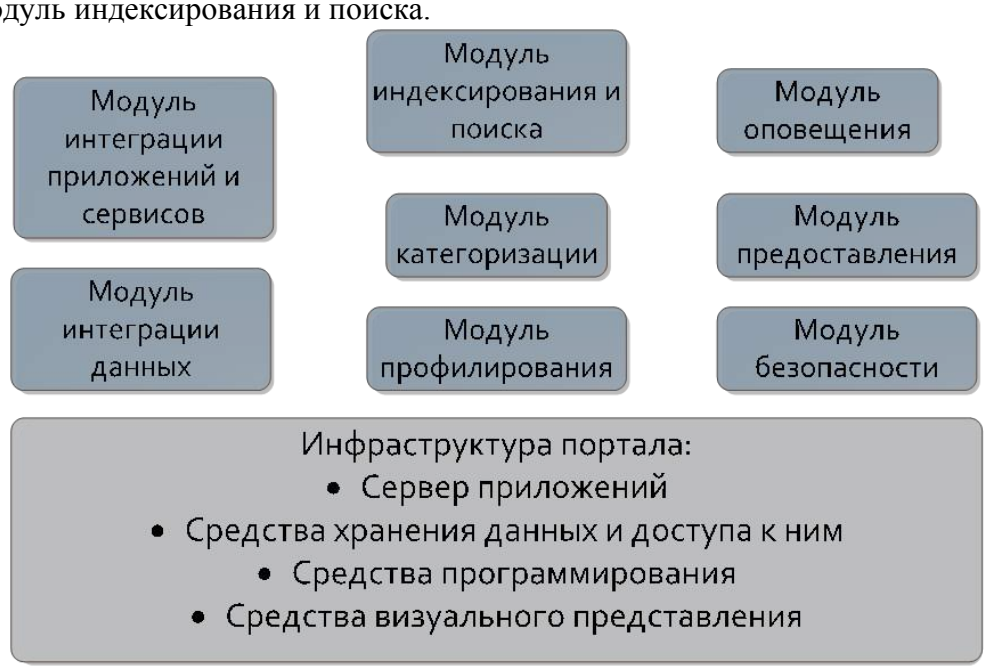

Рис.1. Функциональные модули веб-портала и его инфраструктура
(Fig.1. Functional modules of the web-portal and its infrastructure)

Модуль интеграции данных позволяет использовать средства организации целостного информационного пространства из большого количества различных источников информации. Основной направленностью данного модуля является организация унифицированного доступа к различным источникам информации, таким как: каталогом пользователей, реляционным базам данных, хранилищам документов и электронной почты.

Модуль интеграции приложений и сервисов предоставляет возможность интеграции в веб-портал программных приложений. Кроме того, благодаря данному модулю присутствует возможность расширения функциональности веб-портала за счёт использования сторонних сервисов. Однозначно различить программное приложение и сервис достаточно легко. Главное их отличие заключается в том, что программное приложение является самостоятельным программным продуктом и его использование возможно в рамках других веб-порталов, а сервисы являются частью портала и разрабатываются специально для каждого из них.

Модуль индексирования и поиска предназначен для ускорения поиска нужной информации для пользователя. При использовании этого модуля он сканирует все источники информации, находящиеся в распоряжении веб-портала, а затем индексирует каждый источник. При выполнении поиска после индексирования источников, скорость поиска значительно вырастает, за счёт предварительного отбрасывания большого количества источников, имеющих иной индекс. Это позволяет практически моментально получать релевантные ответы на поисковые запросы пользователей.

Модуль категоризации выполняют функции группировки и структуризации информационного пространства веб-портала. Происходит это путём разделения информационного пространства на информационные подмножества. В свою очередь, информационные пространства состоят из информационных единиц, которые связаны между собой по смыслу. Информационные единицы представляют собой различного рода документы, таблицы из базы данных, и так далее. Связь между информационными единицами обуславливается видом структуры, используемым в рамках веб-портала. Зачастую используются сетевая или иерархическая структура, либо их комбинация. Кроме

того, данный модуль предоставляет функциональность для формирования необходимой структуры.

Модуль профилирования позволяет осуществить явную или неявную персонификацию при использовании пользователем веб-портала. Для выполнения этого в соответствии каждому пользователю создаётся его профиль, который содержит в себе описание предпочтений и/или интересов, а также хранит историю его поисковых запросов. Рассмотрим отличия явной персонификации от неявной персонификации. При явной персонификации пользователю предлагается самостоятельно выбрать для себя способ отображения страниц портала и основную информации для отображения. При неявной персонификации происходит автоматический анализ всех действий пользователя с веб-порталом, на основе которых выделяются его предпочтения. После этого веб-портал, например, может предложить пользователю информацию, которую пользователь не искал, но которая соответствует его интересам.

Модуль оповещения используется для информирования пользователей о всевозможных новостях в портале. Это может быть, например, публикация свежей информации по конкретной, интересующей пользователя, тематике, регистрация новых пользователей, обновление уже прочитанных статей. В основе функционирования этого модуля лежит push-технология, которая для оповещения пользователей может использовать различные средства, например, через электронную почту.

Модуль представления позволяет формировать и изменять способ визуального отображения пользовательского интерфейса веб-портала. Как правило, в модуле используется подход, основанный на предоставления возможности сложения нескольких источников информации, путём комбинирования содержания, в целостное визуальное представление.

Модуль безопасности предназначен для идентификации пользователей при их авторизации на веб-портале, а также создания контекста безопасности при взаимодействии пользователя с функциональностью портала.

Реализация каждого функционального модуля зависит от используемой инфраструктуры веб-портала, к которой относятся: приложения; хранение данных и доступ к ним; средства программирования; средства визуального представления. Следует отметить, что именно от инфраструктуры во многом зависит управляемость, расширяемость и работоспособность веб-портала.

Выявление актуальных угроз на веб-порталы

Все рассмотренные угрозы безопасности веб-ресурсов можно условно разделить на группы.

Первая группа включает в себя недостаточную аутентификацию при доступе к ресурсам. В эту группу входят атаки на основе Подбора (Brute Force), Злоупотребление функционалом (Abuse of Functionality) и Предсказуемое расположение ресурсов (Predictable Resource Location). Основное отличие от недостаточной авторизации заключается в отсутствии проверки прав (или особенностей) уже авторизованного пользователя (например, обычный авторизованный пользователь может получить права администратора, просто зная адрес панели управления, если не производится проверка прав доступа). Эффективно противодействовать таким атакам можно только на уровне логики приложения. Часть атак, например, слишком частый перебор, могут быть заблокированы на уровне сетевой инфраструктуры.

Вторая группа – это недостаточная авторизация. Сюда можно отнести атаки, направленные на легкость перебора реквизитов доступа или использование каких-либо ошибок при проверке доступа к системе. Кроме техник «Подбора» (Brute Force) сюда входит «Угадывания доступа» (Credential and Session Prediction) и «Фиксация сессии»

(Session Fixation). Защита от атак этой группы предполагает комплекс требований к надежной системе авторизации пользователей.

Третья группа охватывает атаки на клиентов, это подмена содержания. Сюда входят все техники изменить содержимое веб-сайта без какого-либо взаимодействия с сервером, обслуживающим запросы — т.е. угроза реализуется за счет браузера пользователя (но при этом обычно сам браузер не является «слабым звеном»: проблемы заключаются в фильтрации контента на стороне сервера) или промежуточного кэш-сервера. Виды атак: «Подмена содержимого» (Content Spoofing), «Межсайтовые запросы» (XSS, Cross-Site Scripting), «Злоупотребление перенаправлениями» (URL Redirector Abuse), «Подделка межсайтовых запросов» (Cross-Site Request Forgery), «Расщепление HTTP-ответа» (HTTP Response Splitting, «Контрабанда HTTP-ответа» (HTTP Response Smuggling), а также «Обход маршрутизациии» (Routing Detour), «Расщепление HTTP-запроса» (HTTP Request Splitting) и «Контрабанда HTTP-запроса» (HTTP Request Smuggling). Значительная часть указанных угроз может быть блокирована еще на уровне настройки серверного окружения, но веб-приложения должны также тщательно фильтровать как поступающие данные, так и ответы пользователя.

Четвертая группа связана с выполнением произвольного кода. Атаки на выполнение произвольного кода являются классическими примерами взлома сайта через уязвимости. Злоумышленник может выполнить свой код и получить прямой доступ к серверу, на котором функционирует веб-портал, отправив определенным образом подготовленный запрос на сервер. Виды атаки, которые реализуют эту угрозу: Переполнение буфера (Buffer Overflow), Форматирование строки (Format String), Целочисленное переполнение (Integer Overflows), LDAP внедрение (LDAP Injection), Mail внедрение (Mail Command Injection), Нулевой байт (Null Byte Injection), Выполнение команд ОС (OS Commanding), Исполнение внешнего файла (RFI, Remote File Inclusion), Внедрение SSI (SSI Injection), Внедрение SQL (SQL Injection), Внедрение XPath (XPath Injection), Внедрение XML (XML Injection), Внедрение XQuery (XQuery Injection) и Внедрение XXE (XML ExternalEntities). Не все из указанных типов атак могут касаться определенного сайта, но корректно они блокируются только на уровне WAF (Web Application Firewall) или фильтрации данных в самом веб-приложении. Все оставшиеся атаки, связанные с ограниченностью серверных ресурсов, можно отнести также в отдельную группу. В частности, это Отказ в обслуживании (Denial of Service) и более точечные атаки — Злоупотребление SOAP (SOAP Array Abuse), Переполнение XML-атрибутов XML Attribute Blowup и Расширение XML-сущностей (XML Entity Expansion). Защита от них только на уровне веб-приложений, либо блокировки подозрительных запросов (сетевое оборудование или веб-прокси). Но при появление новых видов точечных атак необходиом проводить аудит веб-приложений на предмет уязвимости им.

Шестая группа – это угрозы, связанные с отказом веб-портала при достижении определенного количества запросов к его ресурсам в единицу времени, другими словами – это уязвимость к DDoS-атакам. Суть DoS-атаки заключается в том, что злоумышленник пытается сделать временно недоступным конкретный сервер, перегрузить сеть, процессор или переполнить диск. Цель атаки – просто вывести компьютер из строя, а не получить информацию, захватить все ресурсы компьютера-жертвы, чтобы другие пользователи не имели к ним доступа. К ресурсам относятся: память, процессорное время, дисковое пространство, сетевые ресурсы и т. д. Если подобная атака проводится одновременно сразу с большого числа компьютеров, то в этом случае говорят о DDoS-атаке.

Структура платформы OJS

Open Journal Systems (OJS) – это решение с открытым исходным кодом для управления и публикации научных журналов в Интернете. OJS является чрезвычайно

гибкой системой управления и издания журналов, которая может быть загружена бесплатно и установлена на локальный веб-сервер.

Она была разработана, чтобы сократить время и энергозатраты, связанные с канцелярскими и управленческими задачами редактирования журнала, одновременно улучшая учет и эффективность редакционных процессов. Она направлена на улучшение научного и открытого качества публикаций журналов посредством ряда нововведений, в том числе расширения опыта читателей, создания более прозрачных политик журнала и улучшения индексирования [10].

OJS – это система управления журналами / веб-сайтами / публикациями. OJS охватывает все аспекты публикаций онлайн – журналов, начиная с создания веб-сайта журнала, заканчивая задачами эксплуатации, такими, как процесс подачи публикации автором, экспертная оценка, редактирование, публикация, архивирования и индексирования журнала. OJS также помогает управлять аспектами организации журнала, в том числе отслеживанием работы редакторов, рецензентов и авторов, уведомлением читателей и оказанием помощи с корреспонденцией [10].

OJS является гибкой и масштабируемой. Одна установка OJS может поддерживать работу одного или нескольких журналов. Каждый журнал имеет свой собственный уникальный URL-адрес, а также свой собственный внешний вид. OJS может позволить одному редактору управлять всеми аспектами журнала и веб-сайта, или OJS будет поддерживать международную группу редакторов, несущих разную ответственность за несколько разделов журнала. OJS поддерживает принцип расширения доступа. Эта система предназначена не только для оказания помощи в публикации журналов, но и для демонстрирования, как затраты на публикацию журналов могут быть сокращены до уровня, при котором читатели получают «открытый доступ» к содержанию журнала.

Система OJS написана на PHP и может быть запущена на любом веб-сервере с поддержкой данного интерпретатора; в качестве базы данных используется MySQL или PostgreSQL. OJS поддерживает идентификаторы цифровых объектов, что позволяет регистрировать статьи в таких агентствах, как CrossRef, Multilingual European DOI Registration Agency и DataCite. Для вовлечения читателей в процесс создания журнала сообществом Public Knowledge Project был разработан набор инструментов Reading Tools, предоставляющий доступ к смежным исследованиям, тематическим новостям, законодательным актам и другим ресурсам в открытых базах данных. OJS многофункционален: имеется возможность провести информетрический анализ статей, поддерживается электронный кошелёк PayPal. Существует совместимость с системами научных конференций, таких как Easychair и Open Conference Systems. С помощью плагина LatexRender можно подключить возможность интерпретации Tex файлов и их рендеринга. OJS может рассматриваться как электронная библиотека, так как этот продукт обеспечивает доступ к контенту и расширенный поиск по нему (по автору, названию статьи, ключевым словам и др.). OJS позволяет проводить проверку загружаемого материала на плагиат с помощью встроенного модуля, путём поиска заимствований среди утверждений, не являющихся цитатами.

OJS состоит из 4 редакционных стадий: отправление материала, в котором рассматриваются новые заявки (отклоненные, закрепленные за разделом редакторы и т.д.); Рецензирование, в котором проводится экспертная оценка и авторские исправления; литературное редактирование, где прошедшие рецензию и исправления файлы отправляются для литературного редактирования; и публикация, где окончательная версия преобразуется в форматы для публикации (PDF, HTML и т.д.), скорректирована готова к публикации.

Подробная схема редакционного и издательского процессов OJS приведена на рисунке 2.

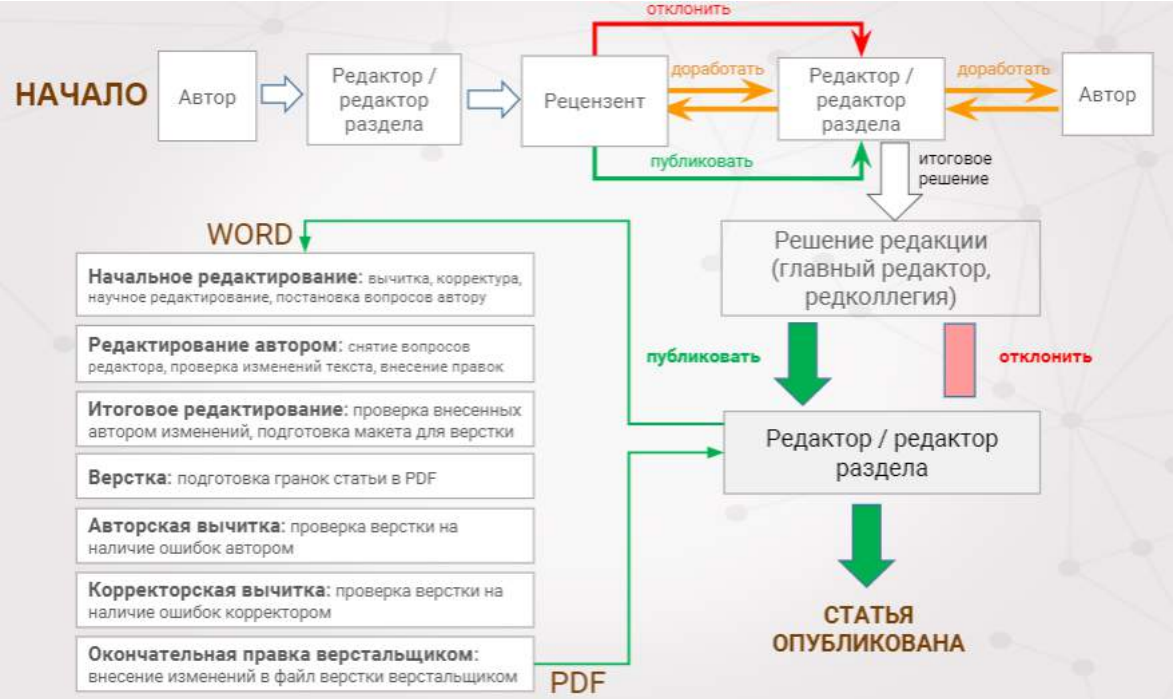

Рис. 2. Схема редакционно-издательского процесса OJS
(Fig. 2. Scheme of the OJS editorial and publishing process)

Структура управления OJS статьями в журнале происходит с помощью четырех редакционных этапов, которые могут выполняться одним или несколькими редакторами.

1. Очередь не назначенных статей: на этом этапе статья назначается одному или нескольким редакторам.

2. Рецензирование статьи: этап охватывает рецензирование и редакционное решение о публикации.

3. Редактирование статьи: этап включает литературное редактирование, верстку и корректуру. Статья закрепляется за определенным выпуском.

4. Содержание: статьи выстраиваются в необходимом порядке и публикуются.

Редакционные роли:

• Менеджер журнала: настраивает журнал и распределяет редакционные роли (может при этом выступать в нескольких ролях).

• Редактор: следит за редакционным процессом; может назначать статьи редакторам разделов, которые управляют рецензированием и редактированием статей; следит за графиком издания журнала.

• Редактор раздела: управляет рецензированием и редактированием принятых к публикации статей.

• Литературный редактор: работает со статьей с целью улучшить грамматику и ясность материала, отправляет автору запросы касательно возможных ошибок, обеспечивает высокое качество стиля статьи и библиографии.

• Верстальщик: преобразует отредактированные статьи в гранки форматов HTML, PDF, и/или PS для последующей публикации.

• Корректор: вычитывает гранки на предмет ошибок правописания и форматирования.

OJS обладает следующими особенностями: OJS может устанавливаться и управляться локально; редакторы настраивают требования, секции, процессы рецензирования, и т.д.; подача публикаций онлайн, двойная слепая рецензия и управление всем контентом; сложное индексирование контента; отзывчивый интерфейс читателя с

поддержкой различных тем; оповещение читателей посредством электронной почты; полная онлайн поддержка; многоязыковая поддержка; открытый код; отсутствие платной лицензии разработчиков

Дополнительные возможности: комментирование статей (анонимное или авторизованное) и администрирование комментариев; возможность проведения открытого рецензирования с публикацией рецензий; публикация тезисов научных работ, в том числе диссертаций, в виде отдельного потока на сайте (не в составе основного контента журнала. Как и любая другая система управления контентом, Open Journal Systems имеет ряд дополнительных модулей (плагинов), которые расширяют ее возможности (основной функционал). Например, существуют плагины, позволяющие индексировать содержимое журнала в Google Scholar и PubMed Central. Плагин подписки реализует поддержку стандартов RSS и Atom. Open Journal Systems соответствует стандартам проекта LOCKSS, что позволяет безопасно собирать, хранить и предоставлять доступ ко всем статьям журнала в долгосрочной перспективе. Часть этих плагинов загружается и устанавливается вместе с системой, т.е. входит в основной дистрибутив. Другая часть создается, дорабатывается и предлагается к использованию сообществом разработчиков.

Уязвимости OJS

Прежде всего, следует уточнить, что под уязвимостью информационной системы понимается любая характеристика информационной системы, использование которой нарушителем может привести к реализации угрозы. Угрозой информационной системе называется потенциально возможное событие, действие, процесс или явление, которое может вызвать нанесение ущерба (материального, морального или иного) ресурсам системы.

Рассмотрим уязвимости платформы Open Journal Systems. Для наглядности, динамика наличия уязвимостей у данной платформы отображена на рис. 3.

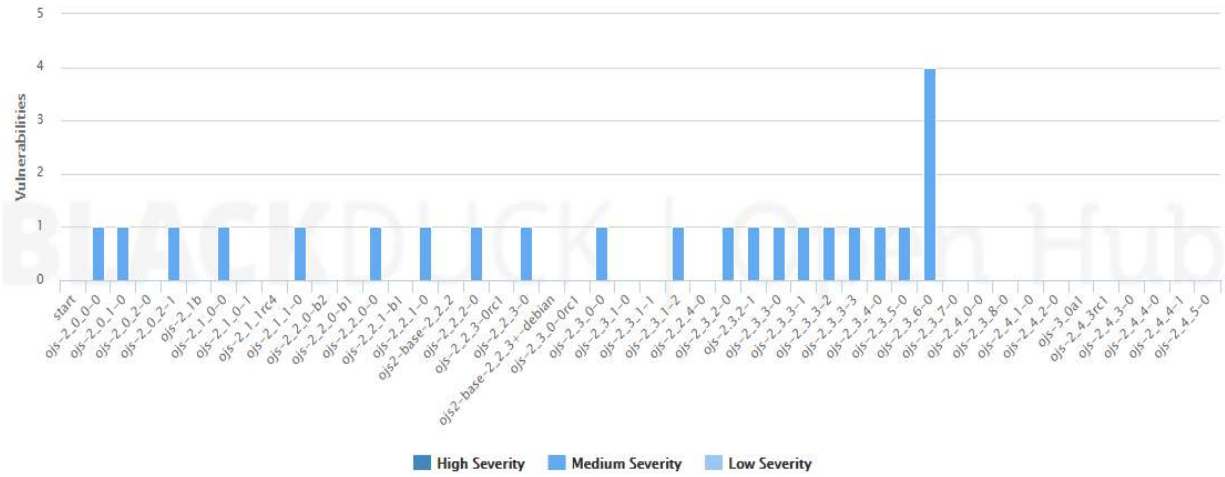

Рис. 3. Диаграмма наличия уязвимостей в зависимости от версии платформы
(Fig. 3. Diagram of vulnerabilities, depending on the version of the platform)

Как видно из диаграммы, наиболее уязвимой версией данной платформы является 2.3.6.0.

В список уязвимостей данной версии входят: произвольное манипулирование файлами в открытых журнальных системах: CVE-2012-1467 (В неё входит «Произвольное удаление файлов», «Переименование произвольного файла»); произвольная загрузка файлов в открытых журнальных системах: CVE-2012-1468; возможность XSS нападение в открытых журнальных системах: CVE-2012-1469. В более поздних версиях все уязвимости устранены. [11]

Частная модель угроз веб-портала на платформе OJS

Приведенная выше структурная модель веб-портала и платформы OJS, позволяет последовательно подойти к построению частной модели угроз безопасности исходя из назначения и внутреннего содержания отдельных модулей системы.

Возможные нарушители по признаку принадлежности к информационной системе делятся на две группы:

Внешние нарушители: клиенты, авторы статей и рецензенты; представители конкурирующих организаций, пользователи сети интернет, которые намеренно предпринимают действия по несанкционированному внедрению в процесс работы веб-портала.

Внутренние нарушители: пользователь системы (администратор, редактор, главный редактор, управляющий журнала); обслуживающий персонал; сотрудники отдела разработки и сопровождения веб-портала.

Исходя из особенностей функционирования портала, допущенные к нему физические лица, имеют разные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам веб-портала в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- Администратор (категория I) отвечает за предварительное конфигурирование и создание журналов на сайте, имеют доступ к некоторым сервисным функциям платформы, таким как очистка кэша данных и шаблонов.
- Управляющий журнала (может быть несколько, если в рамках одного веб-портала функционирует несколько журналов) (категория II) отвечает за функционирование одного конкретного журнала, размещенного на веб-портале. Сюда входят задачи наполнения содержимого сайта информацией, конфигурирование сайта журнала, подключение/отключение/конфигурирование различных плагинов OJS в зависимости от нужд журнала.
- Редакторы и редакторы разделов журнала (категория III) отвечают за редакционный процесс в жизни журнала, они назначают рецензентов, принимают/отклоняют статьи исходя из издательских правил журнала, создают и удаляют выпуски, следят за корректностью ссылок и идентификаторов. Отличие между редактором и редактором раздела существует только внутри больших изданий, там редактор имеет права заниматься редакционным процессом в любом разделе журнала, а редактор раздела, только в строго заданных.
- Зарегистрированные авторы и читатели (категория IV) имеют возможность отправлять статьи в редакцию журнала, просматривать статьи, пользоваться инструментами читателя OJS, комментировать статьи, подписываться на рассылки.
- Рецензенты и верстальщики (категория V) имеют доступ к исходным файлам статей, для рецензентов в зависимости от политики рецензирования статьи могут предоставляться в обезличенном виде (за это отвечают редакторы), верстальщики размечают ссылки в статье и занимаются дополнительным оформлением работы.
- Не зарегистрированные пользователи (категория VI) в зависимости от конфигурации платформы администратором могут иметь доступ аналогичный читателям журнала, либо иметь доступ только к главной странице и новостям журнала.
- Сотрудники, обслуживающие серверы, на которых работают выделенные виртуальные машины и серверы mysql/postgresql, ftp (категория VII) занимаются поддержанием работы всех обслуживающих OJS систем, т.е. систем с использованием которых функционирует платформа. Имеют непосредственный доступ ко всей хранимой и обрабатываемой информации.

- Уполномоченный персонал разработчиков веб-портала, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов портала (категория VIII).

Далее рассмотрим угрозы безопасности, которые могут возникнуть в процессе функционирование веб-портала. При разработке угроз учитывались основные характеристики веб-портала, ресурсы, потенциально подверженные угрозам информационной безопасности, основные каналы реализации угроз безопасности, основные способы реализации угроз безопасности. Описание угроз в своей структуре содержит следующие наименования: название угрозы; возможные источники угрозы; способ реализации угрозы; используемые уязвимости; вид ресурсов, потенциально подверженных угрозе; нарушаемые характеристики безопасности ресурсов; возможные последствия реализации угрозы; рекомендации по нейтрализации угрозы, если имеются.

Основные угрозы безопасности информации веб-портала на платформе OJS

Название угрозы: Несанкционированный доступ к передаваемой информации с использованием программных или программно-аппаратных средств перехвата трафика.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: осуществление перехвата трафика путем использования специализированного ПО или комплекса.

Используемые уязвимости: Особенности протоколов сетей передачи данных и связанные с ними уязвимости.

Вид ресурсов, потенциально подверженных угрозе: Передаваемая и хранимая в системе информация.

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная, либо полная потеря информации, хранимой в системе, искажение этой информации без возможности точного детектирования искаженных частей, частичная/полная дестабилизация работы веб-портала, утечка персональной и конфиденциальной информации.

Атаки, использующие угрозы такого типа могут иметь различные последствия для веб-портала, начиная с отсутствия какого-либо негативного влияния и заканчивая полным прекращением существования веб-портала как такового. Рассмотрим более подробно от чего эти последствия зависят. Наличие рассматриваемой угрозы следует из факта доступности передаваемого трафика третьим лицам, причем для перехвата данных пользователей локальных широковещательных сетей и беспроводных сетей не требуется дорогостоящего оборудования, а в большинстве случае достаточно обычного ПК с установленным специализированным программным обеспечением [3, 12]. Аналогичная ситуация возникает и в мобильных сетях передачи данных, однако с поправкой на необходимость наличия у злоумышленника аппаратной составляющей [13]. Подробно реализация атак описана в статьях [3, 12, 13]. Успех перехвата данных сомнений не вызывает и сам факт перехвата данных, в основном, не влияет на корректность процесса взаимодействия пользователя с веб-порталом. Масштаб последствий зависит от данных, которые сумел получить злоумышленник в ходе перехвата. В случае, когда данные передаются в открытом виде злоумышленник может восстановить перехваченный контекст соединения (так называемые «куки») и работать с веб-порталом от имени «жертвы», причем ему доступен весь функционал, который доступен «жертве» перехвата и не стоит пояснять, что если была перехвачена сессия администратора сайта, то удаление всех журналов с сайта занимает пару кликов. Стратегия с постоянным архивированием содержимого веб-портала в этом случае в полной мере не решает проблемы из-за которой возникает угроза и абсолютно не работает, когда злоумышленник производит точечные модификации данных, которые не влияют на корректность работы портала (например, подменяет рецензию на

статью). Поэтому главной и наиболее эффективной рекомендацией будет использование последних защищенных протоколов передачи данных, т.к. OJS функционирует с использованием протокола http, то логичным будет перейти на его защищенный аналог https с использованием TLS [14].

Название угрозы: Исполнение произвольного кода на стороне клиента или сервера.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: осуществление перехвата трафика путем использования специализированного ПО или комплекса.

Используемые уязвимости: Особенности конкретной реализации взаимодействия составных частей.

Вид ресурсов, потенциально подверженных угрозе: Хранимая и обрабатываемая в системе информация.

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная, либо полная потеря информации, хранимой и обрабатываемой в системе, искажение этой информации без возможности точного детектирования искаженных частей, частичная/полная дестабилизация работы веб-портала, утечка персональной и конфиденциальной информации.

Существует несколько основных атак, которые базируются на возможности выполнения произвольного программного кода или запросов, которые не доступны пользователю. Целью атаки может быть, как другой пользователь системы, так и непосредственно сам веб-портал. Возможность выполнения произвольного кода на PHP для разных версий множество раз обсуждалась и описана во многих статьях, кроме того, существует ряд правил, которых нужно придерживаться разработчикам, чтобы избежать появления подобных уязвимостей. К таким правилам можно отнести использование экранирования спецсимволов в пользовательских запросах, использование различной кодировки для пользовательской части запроса и базовой часть, не использовать «опасные» функции языка PHP (например, eval (string $code), которая выполняет переданную в качестве параметра строку в интерпретаторе). Однако, когда речь идет о взаимодействие нескольких составных частей, то проблемы могут возникать на стыке их взаимодействия. В OJS используется «классический» набор для веб-сайтов PHP, MySQL, HTML. Такой набор хорошо изучен и с точки зрения атакующих и сточки зрения защиты информации [4,15]. Однако для OJS были обнаружены и описаны уязвимости связанные с возможностью выполнения произвольного PHP кода на стороне сервера и XSS атак, для версии 2.3.6 и ниже [16, 17, 18, 19]. Последствия подобных атак могут рознится в зависимости от дополнительных условий, таких как: уровень привилегий с которыми запускается произвольный код, область видимости для этого кода, на какой стороне будет работать код (на сервере веб-портала или на клиентской части «жертвы» атаки). В худшем случае, когда злоумышленник может выполнять свой код на стороне сервера с максимальными привилегиями, его возможности по манипуляциям над процессом работы веб-портала безграничны, однако, стоит сказать, что этот случай соответствует не рекомендованной конфигурации платформы. В случае корректной конфигурации злоумышленник может манипулировать только информацией доступной для записи, а это все загружаемые файлы статей, файлы шаблонов внешнего вида, временные файлы, различные изображения на сайте. При выполнения произвольного кода на стороне клиента злоумышленник по аналогии с предыдущей угрозой может получить доступ к идентификатору сессии пользователя и начать использование веб-портала от имени «жертвы» атаки, последствия в таком случае аналогичны угрозе, рассмотренной выше. В рамках данной работы было дополнительно проверено исправление уязвимостей версии 2.3.6 в последней из версии 2.x.x – это 2.4.8-1 и установлено, что уязвимости отсутствуют. Поэтому для веб-порталов

на платформе OJS рекомендуется использовать версию не ниже 2.4.8. Рекомендации по правам доступа на запись следующие права на запись должны быть только в папках папка public; cache; cache/t_cache; cache/t_compile; cache/_db. Конфигурационный файл рекомендуется настроить в текстовом редакторе и установить права только для чтения на стороне сервера, либо сначала установить права чтение/запись, а после установки и предварительной настройки платформы OJS изменить на «только для чтения».

Название угрозы: Загрузкой произвольных файлов на сервер веб-портала.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Загрузка данных на сервер веб-портала штатными средствами в том числе при их использовании не по назначению.

Используемые уязвимости: Отсутствие индикации загрузки больших файлов, либо большого количества файлов

Вид ресурсов, потенциально подверженных угрозе: Обрабатываемая на веб-портале информация.

Нарушаемые характеристики безопасности ресурсов: Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая требовала записи на диск/базу данных; недоступность веб-портала пока не будет произведена ручная очитка от лишних файлов.

Суть данной угрозы очень проста, т.к. веб-портал на платформе OJS позволяет загружать файлы статей и дополнительных материалов на сервер, то злоумышленник может попробовать загрузить очень большие файлы, либо быстро загружать очень маленькие с целью исчерпания свободного места на диске. Другой вариант – это загрузка больших объемов текста в служебные поля системы, которые сохраняются в базу данных, к таким полям относятся вся информация, связанная с пользователем, заполняемая в «личном кабинете», комментарии к статьям и объявлениям, служебные поля при заполнении формы подачи статьи в редакцию журнала. Атака достаточно тривиальна и не требует от атакующего наличия каких-либо специализированных средств. Хорошим способом защиты будет введение ограничения на максимальный объем загружаемых файлов, ограничение на частоту загрузки данных на сервер, ограничение максимальной длины полей, хранящихся в базе данных, хорошая защита от спама и «ботов».

Название угрозы: Раскрытие содержимого конфигурационных файлов.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Получение доступа к файлу конфигурации OJS.

Используемые уязвимости: Ошибка в конфигурации сервера, на котором функционирует OJS.

Вид ресурсов, потенциально подверженных угрозе: База данных веб-портала

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая хранится в базе данных.

Подобная угроза появляется, когда сервер не достаточно хорошо настроен, по большей части это касается файла .htaccess, который позволяет ограничить доступ пользователей к определенным файлам и папкам сервера, при этом сама платформа OJS (ее исполняемый код) доступ к этим файлам имеет. Файл конфигурации OJS в таком случае можно получить, просматривая доступный файлы и папки через специальную функцию в любом веб браузере, либо попытаться запросить файл с сервера напрямую, зная его имя и местоположение. Получив доступ к содержимому файла злоумышленник получает доступ к информации для входа в базу данных системы и к другой ключевой конфигурационной информации, поэтому последним этапом на пути пользователя в базу данных будет служить межсетевой экран веб-портала, если он не сконфигурирован должным образом, либо отсутствует вообще, то злоумышленник получает полный доступ к информации,

хранящейся в базе данных веб-портала и может производить над ней любые манипуляции. В базе данных OJS хранит всю служебную текстовую информацию, кроме самих файлов статей и других загружаемых файлов. Для предотвращения подобной угрозы следует более тщательно подойти к вопросу конфигурирования OJS и инфраструктуры с которой он взаимодействует (например: с помощью служебного файла .htaccess ограничить пользователям доступ к файлу конфигурации OJS, настроить межсетевой экран между OJS и базой данных таким образом, чтобы он не позволял доступ туда извне.

Название угрозы: Раскрытие содержимого конфигурационных файлов.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Получение доступа к файлу конфигурации OJS.

Используемые уязвимости: Ошибка в конфигурации сервера, на котором функционирует OJS.

Вид ресурсов, потенциально подверженных угрозе: База данных веб-портала

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая хранится в базе данных.

Подобная угроза появляется, когда сервер не достаточно хорошо настроен, по большей части это касается файла .htaccess, который позволяет ограничить доступ пользователей к определенным файлам и папкам сервера, при этом сама платформа OJS (ее исполняемый код) доступ к этим файлам имеет. Файл конфигурации OJS в таком случае можно получить, просматривая доступный файлы и папки через специальную функцию в любом веб браузере, либо попытаться запросить файл с сервера напрямую, зная его имя и местоположение. Получив доступ к содержимому файла, злоумышленник получает доступ к информации для входа в базу данных системы и к другой ключевой конфигурационной информации, поэтому последним этапом на пути пользователя в базу данных будет служить межсетевой экран веб-портала, если он не сконфигурирован должным образом, либо отсутствует вообще, то злоумышленник получает полный доступ к информации, хранящейся в базе данных веб-портала и может производить над ней любые манипуляции. В базе данных OJS хранит всю служебную текстовую информацию, кроме самих файлов статей и других загружаемых файлов. Для предотвращения подобной угрозы следует более тщательно подойти к вопросу конфигурирования OJS и инфраструктуры с которой он взаимодействует (например: с помощью служебного файла .htaccess ограничить пользователям доступ к файлу конфигурации OJS, настроить межсетевой экран между OJS и базой данных таким образом, чтобы он не позволял доступ туда извне [20].

Название угрозы: Исчерпание свободного дискового пространства и вычислительных ресурсов большим числом внешних запросов.

Источники угрозы: пользователи веб-портала категории IV и VI.

Способ реализации угрозы: Использование распределенных или централизованных систем для генерации большого числа реальных запросов к веб-порталу.

Используемые уязвимости: Слабый алгоритм выявления «ботов».

Вид ресурсов, потенциально подверженных угрозе: Данные, обрабатываемые веб-порталом.

Нарушаемые характеристики безопасности ресурсов: Целостность, Доступность

Возможные последствия реализации угрозы: Частичная утрата информации, которая требовала записи на диск/базу данных; недоступность веб-портала пока не будет произведена ручная очитка от лишних файлов на диске и записей в базе данных.

Ключом к появлению этой угрозы служит возможность в автоматическом режиме генерировать корректные с точки зрения взаимодействия пользователя с системой запросы, причем запросы должны быть максимально вычислительно затратные для веб-портала,

чтобы занять его ресурсы. К таким запросам может относиться: регистрация пользователя, написание комментария, отправка статьи на рассмотрение, загрузка файла, сложный запрос в базу данных и т.д. Как правило, человек на формирование такого запроса тратит много больше времени, чем веб-портал его обрабатывает, но когда такие запросы начинают приходить в автоматическом режиме, то система просто перестает справляться и в итоге исчерпывает все доступные ресурсы, что негативно сказывается на качестве работы веб-портала. Решением проблемы, помимо уже рассмотренного ранее ограничения на частоту загрузки данных на сервер, является использование полностью автоматизированного публичного теста Тьюринга для различения компьютеров и людей, известная как CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), это позволяет отбрасывать запросы, которые не могу пройти данный тест (на рисунке 3 представлен пример изображений из теста). Подразумевается, что для человека пройти подобный тест не составляет труда, а вот для компьютера тест – это непреодолимое препятствие. В OJS версии 2.x.x встроен модуль reCAPTCHA v1, который не плохо справлялся со своей задачей, но сейчас не представляет серьёзного препятствия для компьютера. В настоящее время существую системы, которые по разным оценкам достигают точности от 85% до 95% на задаче распознавания букв на генерируемой reCAPTCHA v1 картинке, что сопоставимо с точностью человека [8, 21].

Рис.3. Пример изображений reCAPTCHA v1
(Fig.3. example of reCAPTCHA v1 images)

Решением данной проблемы будет использование reCAPTCHA v2, которая на сегодняшний день широко используется в подавляющем большинстве веб-сайтов, как базовая защита от автоматически генерируемых запросов и достаточно хорошо зарекомендовала себя. Не смотря на значительно возросшую сложность задачи для компьютера, теперь вместо букв нужно определять факт наличия/отсутствия на изображениях или частях одного изображения определенных объектов (пример представлен на рисунке 4). Все же существуют методы, которые позволяют обойти и эту защиту, с меньшей вероятностью, порядка 50-70% и при определенных условиях, требуется достаточно производительная аппаратная платформа и даже при этом условии на обработку одного запроса потребуется прядка 20 секунд [22]. Не смотря на такие существенные успехи использование reCAPTCHA v2 остается оправданным и по сей день. В OJS версии 2.x.x официально отсутствует поддержка reCAPTCHA v2, поэтому в рамках работы по исследованию и доработке платформы была встроена поддержка reCAPTCHA v2 в OJS-2.4.8-1, что является одним из практических результатов проделанной работы.

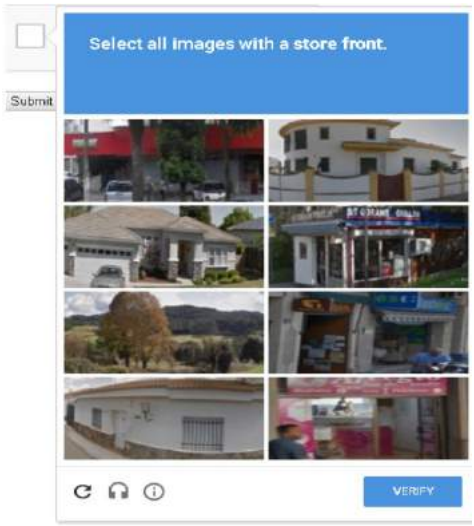

Рис. 4. Пример изображений reCAPTCHA v2
(Fig. 4. example of reCAPTCHA v2 images)

Название угрозы: Несанкционированный доступ к хранимой и обрабатываемой веб-порталом информации.

Источники угрозы: пользователи веб-портала категории VII и VIII.

Способ реализации угрозы: Непосредственное вмешательство в процесс функционирования веб-портала.

Используемые уязвимости: Наличие непосредственного доступа к оборудованию и исходным кодам веб-портала.

Вид ресурсов, потенциально подверженных угрозе: Данные обрабатываемые и харнимые веб-порталом.

Нарушаемые характеристики безопасности ресурсов: Конфиденциальность, Целостность, Доступность

Возможные последствия реализации угрозы: Полная утрата конфиденциальности данных и самих данных, хранимых и обрабатываемых веб-порталом.

Подобного вида угроза возникает как факт того, что веб-порталу необходима аппаратная платформа, на которой он будет работать и если эта платформа находится в неподконтрольной зоне, а доступ к ней имеет неконтролируемый круг лиц, то утрата данных является делом времени. Лицам категории VII и VIII не составляет труда внедрится в процесс работы веб-портала и получить/изменить определенные данные. Поэтому рекомендацией будет размещать веб-порталы только на подконтрольных серверах и доступ, к которым имеет строго ограниченный круг лиц, а если это невозможно, то нужно иметь в виду, что такая угроза имеет место быть информировать об этом пользователей системы и не работать с данными, для которых крайне критична целостность, доступности и конфиденциальность.

Не трудно заметить, что источником для большинства рассмотренных выше угроз служат лица категории IV и VI, т.е. зарегистрированные авторы, читатели и незарегистрированные пользователи, эти две категории представляют наибольший интерес в частной модели угроз, т.к. создатели вертикального, информационного веб-портала знаний не могут контролировать и воздействовать на эти категории пользователей, соответственно появление злоумышленника в этих категориях наиболее вероятно. Кроме того, только для этой категории устранение базовых угроз, которые были перечислены выше не требует колоссальных человеческих и финансовых ресурсов. Лица всех оставшихся категорий должны относится к подконтрольному персоналу и появления там злоумышленника маловероятно. Однако, если это произойдет, то ущерб будет прямо завесить, от полномочий, которыми наделен сотрудник. В случае с I и II категориями

внутренний нарушитель может полностью прекратить существование журнала и веб-портала в целом, от такой угрозы может помочь только периодическое архивирование данных, это поможет восстановить работоспособность веб-портала, но не отменит факта нарушения конфиденциальности статей, находящихся в процессе рецензирования и личных данных пользователей. Лица категории III имеют доступ только к определенным разделам журнала, выпускам и статьям, от их преднамеренного деструктивного воздействия тоже спасает архивирование журнала, но аналогичным образом может быть нарушена целостность и конфиденциальность части данных, хранимых веб-порталом. Лица категории V имеют очень ограниченный функционал и могут только влиять на издательский процесс, но не на работу веб-портала.

Будущие работы

В рамках работ по исследованию и доработке платформы OJS 2.4.8-1 планируется провести дальнейшее тестирование и соответствующую доработку, для устранения обнаруженных недостатков как в обычном функционировании платформы, так и в функционировании систем безопасности. В настоящий момент уже был выявлен и устранен ряд проблем с корректностью работы частей системы, отвечающих за использование защищенного протокола https, платформа переведена под использование reCAPTCHA v2. В соответствии с описанной частной моделью угроз выбраны направления и сценарии для тестирования безопасности системы OJS, в том числе в условиях функционирования на различных программных платформах.

Заключение

В ходе работы были выявлены наиболее характерные угрозы безопасности для веб-порталов, функционирующих на платформе OJS и сформулированы рекомендации по нейтрализации этих угроз. Изучены уязвимости платформы Open Journal Systems, а также возможность типовых атак с их использованием. Приведена статистика уязвимостей всех версий данной платформы, в работе отражены наиболее опасные из них. Так же проведен поиск информации об атаках, совершённых на OJS. За последнее время был известен только один случай попытки злоумышленников провести акт мошенничества, однако компанией была оперативно выработана политика защиты.

С учетом вышесказанного представляется целесообразным использование автоматизированной электронной издательской системы Open Journal Systems в качестве системы управления научным журналом, т. к. она является наиболее динамично развивающейся и хорошо документированной в ней отсутствуют какие-либо непреодолимые проблемы с безопасностью хранимых и обрабатываемых данных. Кроме того, платформа хорошо поддается доработке, что служит существенным плюсом при обнаружении новых уязвимостей, однако требует от разработчика наличия определенных знаний и навыков.

СПИСОК ЛИТЕРАТУРЫ:

1. Public Knowledge Project. History. [Электронный ресурс] URL: https://pkp.sfu.ca/about/history/ (Дата обращения 26.03.2018 г.).
2. Juan Pablo Alperin. How Many Journals Use OJS? - 1 октября 2015 г. [Электронный ресурс] URL: https://pkp.sfu.ca/2015/10/01/how-many-journals-use-ojs/ (Дата обращения 26.03.2018 г.).
3. Maltinsky A., Giladi R., Shavitt Y. On network neutrality measurements (2017) ACM Transactions on Intelligent Systems and Technology, 8 (4), статья № 56 .
4. Backes M., Rieck K., Skoruppa M., Stock B., Yamaguchi F. Efficient and Flexible Discovery of PHP Application Vulnerabilities (2017) Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017, статья № 7961989, pp. 334-349.

5. Marashdih A.W., Zaaba Z.F., Detection and removing cross site scripting vulnerability in PHP web application(2017) Proceedings - 2017 International Conference on Promising Electronic Technologies, ICPET 2017, статья № 8109033, pp. 26-31.
6. Stivalet B., Fong E. Large Scale Generation of Complex and Faulty PHP Test Cases (2016) Proceedings - 2016 IEEE International Conference on Software Testing, Verification and Validation, ICST 2016, статья № 7515499, pp. 409-415.
7. Ben-Asher N., Morris-King J., Thompson B., Glodek W.. Attacker skill, defender strategies and the effectiveness of migration-based moving target defense in cyber systems (2016) Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, pp. 21-30.
8. Stark F., Hazirbas C., Triebel R., Cremers D.. CAPTCHA Recognition with Active Deep Learning, In GCPR Workshop on New Challenges in Neural Computation, 2015.
9. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. «Информационная безопасность открытых систем: Учебник для вузов. Том 1 – Угрозы, уязвимости, атаки и подходы к защите. – М.: Горячая линия – Телеком. 2006. – 536 с.: ст. 117-118.
10. Спирин О.М., Лупаренко Л.А. «Опыт использования программной платформы Open Journal Systems для поддержки научно-образовательной деятельности» - 2017.Т.61 №5. С.196-218.
11. The Open Journal Systems Open Source Project on Open Hub: Security. [Электронный ресурс] URL: https://www.openhub.net/p/ojs2/security?filter%5Bmajor_version%5D=&filter%5Bperiod%5D=&filter%5Bversion%5D=69022&filter%5Bseverity%5D (Дата обращения 29.03.2018 г.).
12. Kavianpour A., Anderson M.C. An Overview of Wireless Network Security (2017) Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, статья № 7987214, pp. 306-309.
13. Khanpara P., Trivedi B. Security in mobile ad hoc networks (2017) Advances in Intelligent Systems and Computing, 508, pp. 501-511.
14. Guo Y., Cao Z., Yang W., Xiong G. A measurement and security analysis of SSL/TLS deployment in mobile applications (2018) Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 209, pp. 189-199.
15. Medeiros I., Beatriz M., Neves N., Correia M. Demonstrating a Tool for Injection Attack Prevention in MySQL (2017) Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017, статья № 8023153, pp. 551-558.
16. CVE-2011-5195. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5195 (Дата обращения 01.04.2018 г.).
17. CVE-2011-5196. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5196 (Дата обращения 01.04.2018 г.).
18. CVE-2011-5197. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5197 (Дата обращения 01.04.2018 г.).
19. CVE-2012-1469. [Электронный ресурс] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1469 (Дата обращения 04.04.2018 г.).
20. Larsson E., Sigholm J. Papering over the cracks: The effects of introducing best practices on the web security ecosystem (2016) International Conference on Information Networking, 2016-March, статья № 7427064, pp. 1-6.
21. Starostenko O., Cruz-Perez C., Uceda-Ponga F., Alarcon-Aquino V. Breaking text-based CAPTCHAs with variable word and character orientation (2015) Pattern Recognition, 48 (4), pp. 1097-1108.
22. Sivakorn S., Polakis I. and Keromytis A. D., "I am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, pp. 388-403. doi: 10.1109/EuroSP.2016.37.

REFERENCES:

[1] Public Knowledge Project. History. [Электронный ресурс] URL: https://pkp.sfu.ca/about/history/ (Дата обращения 26.03.2018 г.).
[2] Juan Pablo Alperin. How Many Journals Use OJS? - 1 октября 2015 г. [Электронный ресурс] URL: https://pkp.sfu.ca/2015/10/01/how-many-journals-use-ojs/ (Дата обращения 26.03.2018 г.).
[3] Maltinsky A., Giladi R., Shavitt Y. On network neutrality measurements (2017) ACM Transactions on Intelligent Systems and Technology, 8 (4), статья № 56 .
[4] Backes M., Rieck K., Skoruppa M., Stock B., Yamaguchi F. Efficient and Flexible Discovery of PHP Application Vulnerabilities (2017) Proceedings - 2nd IEEE European Symposium on Security and Privacy, EuroS and P 2017, статья № 7961989, pp. 334-349.
[5] Marashdih A.W., Zaaba Z.F., Detection and removing cross site scripting vulnerability in PHP web application(2017) Proceedings - 2017 International Conference on Promising Electronic Technologies, ICPET 2017, статья № 8109033, pp. 26-31.

[6] Stivalet B., Fong E. Large Scale Generation of Complex and Faulty PHP Test Cases (2016) Proceedings - 2016 IEEE International Conference on Software Testing, Verification and Validation, ICST 2016, статья № 7515499, pp. 409-415.

[7] Ben-Asher N., Morris-King J., Thompson B., Glodek W.. Attacker skill, defender strategies and the effectiveness of migration-based moving target defense in cyber systems (2016) Proceedings of the 11th International Conference on Cyber Warfare and Security, ICCWS 2016, pp. 21-30.

[8] Stark F., Hazirbas C., Triebel R., Cremers D.. CAPTCHA Recognition with Active Deep Learning, In GCPR Workshop on New Challenges in Neural Computation, 2015.

[9] Zapechnikov S.V., Miloslavskaya N.G., Tolstoy A.I., Ushakov D.V. "Information security of open systems: A textbook for high schools. Volume 1 - Threats, vulnerabilities, attacks and approaches to protection. - M .: Hot line - Telecom. 2006. - 536 pp .: art. 117-118. (in Russian).

[10] Spirin O.M., Luparenko L.A. "Experience of using the Open Journal Systems software platform to support scientific and educational activities" - 2017.T.61 №5. P.196-218. (in Russian).

[11] The Open Journal Systems. Open Source Project on Open Hub: Security. [Web resource] URL: https://www.openhub.net/p/ojs2/security?filter%5Bmajor_version%5D=&filter%5Bperiod%5D=&filter%5Bversion%5D=69022&filter%5Bseverity%5D (Access date 29.03.2018)

[12] Kavianpour A., Anderson M.C. An Overview of Wireless Network Security (2017) Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017, статья № 7987214, pp. 306-309.

[13] Khanpara P., Trivedi B. Security in mobile ad hoc networks (2017) Advances in Intelligent Systems and Computing, 508, pp. 501-511.

[14] Guo Y., Cao Z., Yang W., Xiong G. A measurement and security analysis of SSL/TLS deployment in mobile applications (2018) Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 209, pp. 189-199.

[15] Medeiros I., Beatriz M., Neves N., Correia M. Demonstrating a Tool for Injection Attack Prevention in MySQL (2017) Proceedings - 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2017, статья № 8023153, pp. 551-558.

[16] CVE-2011-5195. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5195 (Access date 01.04.2018)

[17] CVE-2011-5196. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5196 (Access date 01.04.2018)

[18] CVE-2011-5197. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5197 (Access date 01.04.2018)

[19] CVE-2012-1469. [Web resource] URL: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1469 (Access date 04.04.2018)

[20] Larsson E., Sigholm J. Papering over the cracks: The effects of introducing best practices on the web security ecosystem (2016) International Conference on Information Networking, 2016-March, статья № 7427064, pp. 1-6.

[21] Starostenko O., Cruz-Perez C., Uceda-Ponga F., Alarcon-Aquino V. Breaking text-based CAPTCHAs with variable word and character orientation (2015) Pattern Recognition, 48 (4), pp. 1097-1108.

[22] Sivakorn S., Polakis I. and Keromytis A. D., "I am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, pp. 388-403. doi: 10.1109/EuroSP.2016.37.

Поступила в редакцию – 2 марта 2018 г. Окончательный вариант – 27 апреля 2018 г.
Received – March 02, 2018. The final version – April 27, 2018.