ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОСТОВСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ
УНИВЕРСИТЕТ (РИНХ)»
РОСТОВСКОЕ РЕГИОНАЛЬНОЕ ОТДЕЛЕНИЕ
ВОЛЬНОГО ЭКОНОМИЧЕСКОГО ОБЩЕСТВА РОССИИ

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Материалы
VII Всероссийской заочной
Интернет-конференции

20–21 февраля 2018 года

Ростов-на-Дону
2018

ББК 65.9(2Рос)98
П 78

П 78 **Проблемы информационной безопасности**: Материалы VII Всероссийской заочной Интернет-конференции 20–21 февраля 2018 года – Ростов-н/Д, Издательство ООО «АзовПринт», 2018. – 192 с.
ISBN 978-5-6041030-0-5

В издании представлены работы профессорско-преподавательского состава, молодых ученых, магистров и студентов, посвященные проблемам информационной безопасности.

Материалы конференции предназначены для научных сотрудников, преподавателей, аспирантов, магистров и студентов.

Утверждены в качестве материалов конференции редакционно-издательским советом РГЭУ (РИНХ)

ISBN 978-5-6041030-0-5

СОДЕРЖАНИЕ

РАЗДЕЛ 1

ФУНДАМЕНТАЛЬНЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е.А. Витенбург, Е.А. Садовник

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

Процесс построения системы защиты информационной системы (ИС) в предприятия является основополагающим в защите информации ограниченного доступа. При формировании системы защиты необходимо учитывать многие факторы, влияющие на качество защиты информации. Наибольшее значение при проектировании системы защиты информации имеет модель угроз информационной системы [1-2]. Модель угроз формируется для каждой информационной системы предприятия на основе результатов сбора исходных данных, базы данных угроз Федеральной службы по техническому и экспортному контролю (ФСТЭК). На сегодняшний в базе данных угроз ФСТЭК насчитывается более двухсот угроз информационной безопасности. На основе анализа ИС предприятия определены критерии определения актуальных угроз информационной безопасности. Критерии представлены ниже [3]:

- направление деструктивного воздействия;
- способ реализации несанкционированного доступа к защищаемой информации;
- расположение источника угроз.

Для анализа и определения актуальных угроз безопасности информационной системы предприятия, в соответствии с определенными критериями, составлена обобщенная таблица угроз информационной безопасности (таблица 1) [3].

Таблица 1 – Обобщенная таблица угроз безопасности информационной системы предприятия

Критерий	Группа угроз	Подгруппы угроз
Направление деструктивного воздействия	Угрозы нарушения конфиденциальности информации, обрабатываемой в распределенном приложении	

РАЗДЕЛ 5

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.М. Ажмухамедов, О.Н. Выборнова, З.А. Носиров

ПОЛУЧЕНИЕ ЗАКРЫТОЙ ИНФОРМАЦИИ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ

В настоящее время в открытых источниках и специализированных базах данных, доступных в Интернете, представлены большие объемы информации о людях, транспортных средствах, организациях и т.д. При этом нередко в свободном доступе могут быть обнаружены сведения, не желательные для распространения (например, конфиденциальная информация, учетные данные пользователей и т.д.).

Цель статьи: продемонстрировать процедуру сбора и систематизации информации об объекте из открытых источников.

Сбор и обработка информации из открытых источников, в рамках закона и с соблюдением этических норм, может осуществляться в рамках конкурентной разведки. Ее целью является получение максимального объема релевантной информации об объекте исследований, установление взаимосвязей с другими сущностями. В рамках конкурентной разведки обычно осуществляется анализ рынка, проверка контрагентов, определение стратегии и потенциала конкурентов [1].

Источниками информации об организациях могут служить: официальный сайт организации, группы в социальных сетях, сайт государственных закупок, публикации в СМИ, архив вакансий организации и т.д. Для сбора данных в сети Интернет могут быть использованы различные поисковые системы (google, yandex. bing и др.), в том числе специализированные (shodan, censys), поисковики изображений (google-картинки, tineye и др.), а также сервисы проверки контрагентов (например, контур-фокус, СПАРК и т.п.) [2, 3].

Алгоритм проведения конкурентной разведки может различаться в зависимости от поставленных задач, а также имеющихся исходных данных. Рассмотрим пример сбора информации из открытых источников относительно объекта, расположенного в Московской области. Об объекте ничего не известно кроме его местоположения. Примененный в данном случае алгоритм схематически изображен на рисунке 1.

Рисунок 1 – Схема проведения разведки

Объект, расположенный по установленным GPS-координатам, на карте Яндекс.maps не отображается, но на спутниковом снимке он виден. Загрузка данных о местоположении на сервис Викимапия показала, что территория принадлежит государству и на ней расположена воинская часть (в/ч) 33***.

С помощью поисковой системы Google было установлено, что в/ч 33*** является инженерно-технической и входит в состав «Специальных войск Российской Федерации». С помощью сервиса google-картинки были найдены фотографии, связанные с данным объектом, в том числе фотографии в социальных сетях. Часто именно через фотографии происходит утечка конфиденциальной информации (записанные где-то и попавшие в кадр логины, и пароли, фрагменты чертежей, изображения на экране персонального компьютера и т.д.).

Социальные сети на сегодняшний день являются важным элементом современного общества. Они выполняют информационную, коммуникационную, развлекательную и социализирующую функции [4]. В рамках сбора информации об объекте, в результате перехода по ссылке на профиль пользователя социальной сети Вконтакте, служившего в рассматриваемой в/ч, и анализа его записей на стене обнаружены сведения о названии, подчиненности и деятельности в/ч.

Поскольку рассматриваемый объект является государственной организацией, информация по выполнению работ или оказанию услуг для этой организации должна размещаться на веб-сайте госзакупок. В результате

анализа заказов исследуемого объекта были выявлены виды вооружения и специального оборудования, находящегося на территории объекта. Кроме того, поиск аналогичных заявок на участие в открытых аукционах позволил установить похожие объекты в других регионах страны. Состав специального оборудования позволил сделать выводы о задачах, выполняемых на объекте.

Совершенно очевидно, что собранная информация не должна быть в общем доступе и режим конфиденциальности нарушен. С большой долей вероятности можно утверждать, что данный объект обеспечивает специальную связь. А размещение на его территории системы «Периметр» свидетельствует о том, что данный объект является стратегическим.

Исходя из этого, можно сделать вывод, что системное сопоставление и анализ разобщенной информации, полученной из различных открытых источников в сети Интернет, может существенно нарушать режим конфиденциальности. Данный момент необходимо учитывать при проведении работ по обеспечению надежного уровня конфиденциальности.

Библиографический список

1. Конкурентная разведка [Электронный ресурс]. Режим доступа: https://searchinform.ru/resheniya/biznes-zadachi/konkurentnaya-razvedka/
2. Shodan и Censys: опасные гиды по Интернету вещей [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/blog/shodan-censys/11053/
3. Брицов Р.А. Повышение качества информационного поиска за счет совершенствования ранжирования и использования особенностей поведения пользователей // T-Comm. 2016. №2. С.63-66.
4. Ажмухамедов И.М., Мачуева Д.А., Жолобов Д.А. Моделирование процесса распространения информации в социальных сетях // Фундаментальные исследования. 2017. №5. С. 9-14.

А.В. Барабошкина

СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК ГОССОПКА

В статье проводится сравнительный анализ государственной системы обнаружения, предупреждения и ликвидации компьютерных атак. Предстоит разобрать достоинства и недостатки «ГосСОПКИ», рассмотреть нововведения, которое предлагают ведущие специалисты в области информационной безопасности. Разработать концепцию, в которой сочетаются преимущества, а изъяны сведены к минимуму или исключены вовсе.

Потребность в системе «ГосСОПКА» неоспорима, но механизмы обеспечения, которые определены 8-м Центром ФСБ до конца не проработаны и имеют изъяны.

Вопросами о практическом опыте создания центров ГосСОПКА занимался директор Positive Technologies по методологии и стандартизации Дмитрий Кузнецов

Вопросами роли центра мониторинга в концепции ГосСОПКА занимался аналитик фирмы INFOTECS Шапиро Роман.

Все существующие системы обнаружения атак имеют свои недостатки и полностью не защищают от угроз. Данная статья анализирует публичную информацию по ГосСОПКЕ, изучает предложенные концепции по ее реализации.

С каждым годом средства массовой информации предоставляют все больше источников о кибератаках на коммерческие компании и информационные системы гос. организаций. Возрастает количество атак на транспорт, промышленные объекты и связь. В РФ ответом на рост угроз в январе 2013 г. стал указ президентом Владимира Путина о создании в России Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак или ГосСОПКА.

Главные цели, которые вытекают из указа президента, должны быть прогнозирование ситуаций в области обеспечения Информационной безопасности, обеспечение взаимодействия владельцев ИТ-ресурсов при решении задач, связанных с обнаружением и ликвидацией компьютерных атак, с операторами связи и другими организациями, осуществляющими деятельность по защите информации. В список задач системы также входит оценка степени защищенности критической ИТ-инфраструктуры от компьютерных атак и установление причин таких инцидентов.

В марте 2015 года на сайте ФСБ была опубликована выписка из документа "Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" утвержденного Президентом РФ 12.12.2014 № К 1274.

Исходя из документа, система представляет собой единый централизованный территориально-распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган власти, уполномоченный в области обеспечения безопасности критической инфраструктуры РФ и орган власти, уполномоченный в области создания и обеспечения функционирования системы.

Под «средствами» в концепции подразумеваются, главным образом, технологические решения, а под «силами» – специальные подразделения и сотрудники со стороны федерального органа власти, ответственного за систему, а также операторов связи и других организаций, осуществляющих лицензируемую деятельность в сфере защиты информации.

• Требование 7 (t_7): тестировать платежные приложения для устранения уязвимостей и разработки обновлений.

• Требование 8 (t_8): способствовать реализации безопасной сети.

• Требование 9 (t_9): данные держателя карты никогда не должны храниться на сервере, подключенном к Интернету.

• Требование 10 (t_{10}): обеспечить безопасный удаленный доступ к платежному приложению.

• Требование 11 (t_{11}): шифровать конфиденциальный трафик по общедоступным сетям.

• Требование 12 (t_{12}): защитить все не консольные административные доступы.

• Требование 13 (t_{13}): создание руководства по внедрению PA-DSS для клиентов, реселлеров и интеграторов.

• Требование 14 (t_{14}): обозначить требования PA-DSS для персонала и поддерживать учебные программы для персонала, клиентов, реселлеров и интеграторов. [2]

Таким образом, полученные вектора T_1 и T_2 представляют требования для проведения аудита безопасности электронной платежной системы.

Каждому из требований стандартов присваивается значение $t_n = \{0;1\}$, где 0 – это невыполнение требования, а 1 – выполнение данного требования.

Результатом аудита предлагается считать числовое значение $A = |T_1| + |T_2|$, где A – значение результата аудита, которое показывает соответствует ли электронная платежная система стандартам безопасности.

Результат аудита позволяет электронной платежной системе подготовится к проведению периодических аудиторских проверок, а также оценить текущий уровень защищенности системы.

Библиографический список

1. PCI Security Standards Council. Document Library [Электронный ресурс] // URL: https://www.pcisecuritystandards.org/document_library ? category = pcidss & document = pci_dss (дата обращения: 10.01.2018).
2. PCI Security Standards Council. Document Library [Электронный ресурс] // URL: https://www.pcisecuritystandards.org/document_library ? category = pa-dss & document = pa-dss (дата обращения: 10.01.2018).

З.А. Носиров, И.М. Ажмухамедов

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ XSS-УЯЗВИМОСТЕЙ

Среди множества видов угроз информационной безопасности существует категория опасностей, негативные воздействия которых могут провоцировать сами пользователи информационных ресурсов компании, подвергая, таким образом, опасности внутреннюю вычислительную сеть и устройства в нее входящие. Все эти угрозы стали возможны благодаря широкому распространению сети Интернет.

Одним из таких видов опасностей является межсайтовый скриптинг, в англоязычной литературе, называемый – XSS (cross site scripting, x – используется в данной аббревиатуре для краткости, c – не используется, чтобы избежать путаницы с CSS) [2]. С помощью XSS-уязвимостей злоумышленник внедряет вредоносный программный код в веб-страницу, отправляемую сервером клиенту. Данный код может позволить получить доступ к данным авторизации пользователя и использовать ее с целью совершения противоправных действий в отношении защищаемой информации.

Современные средства защиты информации предлагают широкий спектр алгоритмов и программного обеспечения способного предотвращать различные угрозы информационной безопасности. Но у каждого решения есть свои плюсы и минусы. Большинство решений направленных на выявление XSS-уязвимостей веб-приложения не анализируют полную карту веб-сайта. То есть в данных решениях не предусмотрен поиск XSS-уязвимостей в тех областях веб-приложения, которые доступны только после авторизации пользователя на веб-ресурсе.

Исходя из этого, целью работы явилось повышение эффективности защиты веб-приложений от XSS-атак, путем разработки программного обеспечения для детектирования уязвимостей на основе анализа полной карты веб-приложения. Разработанное ПО предоставляет пользователю информацию об уязвимостях исследуемого веб-приложения и формирует отчет с рекомендациями по устранению найденных XSS-уязвимостей.

Для достижения поставленной цели использована методика, основанная на последовательном применении различных алгоритмов обнаружения уязвимостей. Алгоритмы отличаются друг от друга в зависимости от типа обнаруживаемых XSS-угроз. Для разработки программного обеспечения использовался язык программирования Delphi. Разработанное программное обеспечение выявляет следующие виды XSS-уязвимостей:

1) «хранимая (stored) XSS», когда вредоносный код выполняется на сервере;

2) «отраженная (reflected) XSS», пользователю необходимо посетить специально сформированную ссылку;

3) «XSS в DOM-модели», источник проблемы находится в клиентском сценарии, вредоносный код выполняется за счет особенностей объектной модели документов.

Также программа содержит общие методы, осуществляющие следующие вспомогательные операции:

- построение пользовательского интерфейса;
- создание списка анализируемых страниц;
- создание отчета;
- формирование рекомендаций по устранению найденных уязвимостей.

На рисунке 1 представлена диаграмма, иллюстрирующая алгоритм поиска отраженных XSS. Так как данный вид уязвимостей проявляется только при отправке форм, алгоритм провоцирует их отправку методом POST включая в отправляемые элементы значения и получая ответ в виде HTML сообщения.

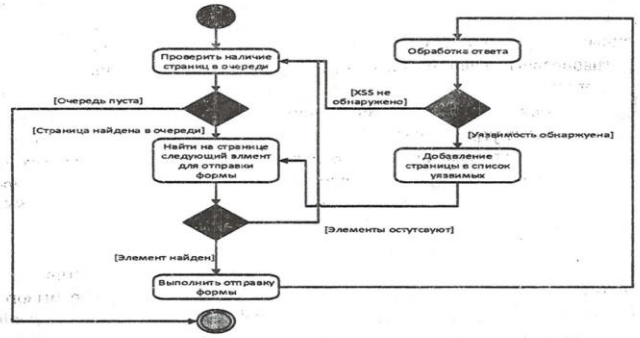

Рисунок 1 – Алгоритм поиска отраженных XSS-уязвимостей.

Пришедшее сообщение затем анализируется на наличие значения уязвимости следующим образом: если пришедший JavaScript код устанавливает значение, хранящееся в объектной модели документа в истинное значение *(document.vulnerable=true)*, то страница помечается как содержащая потенциальную угрозу соответствующего типа, иначе страница помечается как безопасная и не добавляется в итоговый список [1]. Для поиска XSS-уязвимостей, основанных на использовании объектной модели документа – DOM, используется алгоритм, блок-схема которого показана на рисунке 2.

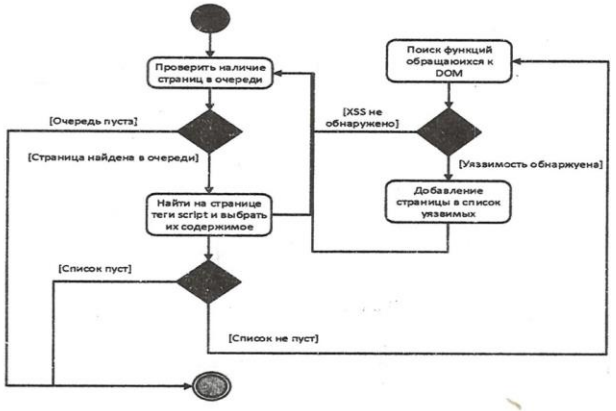

Рисунок 2 – Алгоритм поиска XSS-уязвимостей, эксплуатирующих DOM.

В ходе работы алгоритма осуществляется анализ кода страницы на наличие скриптов спрятанных в HTML тегах. После нахождения содержимого всех скриптов на странице в найденных данных осуществляется поиск вызовов методов объектной модели документа таких как:

- запись чистого HTML;
- прямая модификация модели документа (в том числе события Dynamic HTML);
- прямое выполнение скриптов.

Для реализации поиска хранимых уязвимостей используется алгоритм, блок схема которого показана на рисунке 3. Работа данного алгоритма имеет свои особенности, так как в отличие от отраженных XSS – хранимые уязвимости являются следствием сохранения скрипта в базу данных. Данная операция должна осуществляться с помощью предварительного POST-запроса, чтобы не позволить вредоносному коду внести изменения в базу данных [3]. Алгоритм во многом схож с алгоритмом поиска отраженных XSS-угроз за исключением того, что необходимо производить отправку формы и ждать ответа от сервера.

В случае, если скрипт выполнился, форма и XSS-инъекция запоминается в специальную структуру вместе с прочей информацией о найденной уязвимости. При выполнении скрипта продолжение поиск на данной странице не осуществляется, поскольку при отправке формы, будет осуществляться выполнение скрипта, находящегося в базе данных веб-приложения.

Поэтому данную проверку необходимо запускать повторно после устранения уязвимости.

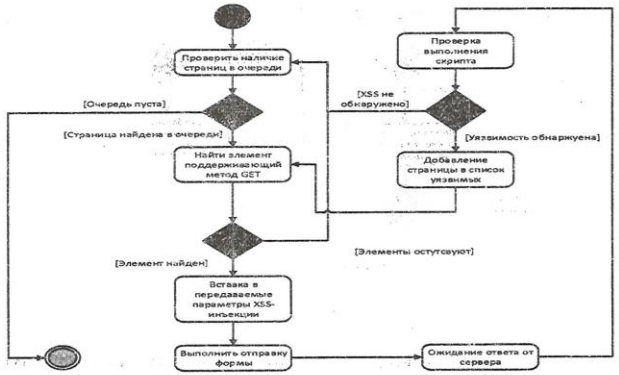

Рисунок 3 – Алгоритм поиска хранимых XSS-уязвимостей.

Формирование отчета о найденных уязвимостях будет доступно после завершения поиска и при наличии записей во внутренней структуре, хранящей найденные угрозы и их описание. Разработанная программа обладает рядом преимуществ перед существующими решения:

- возможность анализа полной карты веб-ресурса;
- выявление всех видов XSS-уязвимостей;
- создание отчета;
- формирование рекомендаций по устранению найденных XSS-уязвимостей.

Использование разработанного ПО значительно облегчит работу веб-разработчиков и тестировщиков.

Библиографический список

1. Brian Goetz. Java theory and practice: Thread pools and work queues. [Текст] / Brian Goetz // IBM. DeveloperWorks. – 2002. – №7. – с. 7.
2. Межсайтовый скриптинг [Электронный ресурс] // Свободная энциклопедия Википедия URL: https://ru.wikipedia.org/wiki/Межсайтовый_скриптинг (дата обращения: 11.01.2018).

3. OWASP Cheat Sheet Series [Электронный ресурс] // OWASP the free and open software security community URL: https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series (дата обращения: 11.01.2018).

Т.А. Омельченко, Т.А. Пахомов

РАЗРАБОТКА АЛГОРИТМА АУДИТА ОПЕРАЦИОННОЙ СИСТЕМЫ МОБИЛЬНОГО УСТРОЙСТВА

Жизнь человека в современном мире не обходится без повседневного использования мобильных устройств. Под мобильными устройствами понимают ряд устройств, который включает в себя смартфоны, планшеты, электронные книги, телефоны, и нетбуки, главной особенностью которых является размер, а также количество выполняемых ими функций.

В узком понятии мобильное интернет-устройство (*Mobile Internet Device, MID*) – класс портативных устройств, предназначенный для доступа в Интернет. [1]

Мобильная операционная система (мобильная ОС) – операционная система для смартфонов, планшетов, КПК или других мобильных устройств. Мобильные ОС сочетают в себе функциональность ОС для персональных компьютеров (ПК) с функциями для мобильных устройств: удаленное администрирование, поддержка VPN, браузеры с flash и java-script, синхронизация почты, заметок, обмен файлами, сенсорный экран, сотовая связь, Bluetooth, Wi-Fi, GPS-навигация, камера, видеокамера, распознавание речи, диктофон, музыкальный плеер, NFC и инфракрасное дистанционное управление. Все это очень удобно, однако рынок средств защиты для подобных устройств развит не достаточно сильно. И основная проблема обеспечения безопасности мобильных ОС связана с многообразием ОС для мобильных устройств и постоянно увеличивающимся количеством их версий в одном семействе.

В 2011 году рынок мобильных устройств, за счет постоянного роста вычислительной мощности и возможностей самих мобильных устройств, впервые обогнал рынок ПК, что привело к появлению новых вопросов и проблем в области обеспечения информационной безопасности.

Мобильные устройства хранят в себе большое количество данных, которые могут быть интересны для злоумышленника (таблица 1):

Согласно отчёту исследовательской фирмы Gartner, 98,4% рынка мобильных ОС занимают iOS и Android. Наиболее распространённой мобильной платформой остаётся Android с долей 80,7%, в то время как iOS владеет 17,7% рынка.

Научное издание

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Материалы VII Всероссийской заочной Интернет-конференции

20–21 февраля 2018 г.

Подписано к печати 24.04.2018 г.
Бумага офсетная. Печать цифровая. Формат 60x84/16.
Объем 8,7 уч.-изд. л. Гарнитура «Таймс».
Тираж 500 экз. Заказ № 444.

Издательство ООО «АзовПирнт»
346780, г. Азов, ул. Привокзальная, 6а, тел.: (86342) 5-37-57

Отпечатано в ООО «АзовПринт»