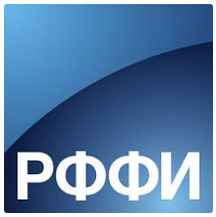

АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
РОССИЙСКИЙ ФОНД ФУНДАМЕНТАЛЬНЫХ ИССЛЕДОВАНИЙ
Факультет математики и информационных технологий

I Международная научно-техническая конференция

«Актуальные вопросы использования технологий анализа данных и искусственного интеллекта»

Материалы Международной научно-технической конференции (молодежная секция)

Астраханский государственный университет, 6-8 ноября 2018 г.

Астрахань – 2018

УДК 004.6+004.8+004.9
ББК 22.19
М 43

I Международная научно-техническая конференция «Актуальные вопросы использования технологий анализа данных и искусственного интеллекта»

I Международная научно-техническая конференция «Актуальные вопросы использования технологий анализа данных и искусственного интеллекта»: Сборник материалов Международной конференции (Астрахань, Астраханский государственный университет, 6-8 ноября 2018 г**.) –** молодежная секция / Под научной редакцией С.В. Окладниковой. – Астрахань: Издатель: Сорокин Роман Васильевич, 2018. – 192 с.

ISBN 978-5-91910-743-9

Сборник материалов молодежной секции Международной конференции посвящен актуальным вопросам использования технологий анализа данных и искусственного интеллекта, относящихся к решению научно-технических, социально-экономических и других классов задач. Представлены исследования в области технологий анализа «больших данных» и методов выявления скрытых зависимостей с использованием современных алгоритмов и программно-технических средств. Конференция проведена в Астраханском государственном университете при финансовой поддержке Российского фонда фундаментальных исследований.

Библиографический список

1. Ильюшин Ю. В., Чернышев А. Б. Устойчивость распределенных систем с дискретными управляющими воздействиями – Известия Южного федерального университета. Таганрог, 2010 – № 12 – С. 166-171.
2. Степанченко И.В. Исследование дискретных систем управления при влиянии ограниченности параметров технических средств – Наука Кубани. Библиотека журнала: Сб. науч. тр. – Краснодар, 2001.
3. Bisgaard, H., O'Callaghan, C., & Smaldone, G. C. Drug delivery to the lung – New York: Marcel Dekker Inc – 2002.
4. IEC 61131-3, International Standard, Programmable controllers – Part 3: Programming languages, Edition 3.0, International Electrotechnical Commission – 2013.
5. Karatkevich A., Bukowiec A., Doligalski M., Tkacz J. Design of Reconfigurable Logic Controllers Studies in Systems – Springer International Publishing Switzerland – 2016.
6. Khoroshevskii V.G., Distributed Computing Systems with Programmable Structure, Vestn. Sib. Gos. Univ. Telekom. Inform. 2(10), 3-41 – 2010.
7. Lewis, R. W. Programming industrial control systems using IEC 1131–3 – IEE Control Engineering Series: IEE. – 1998.
8. Nenashev A.V., Dvurechenskii A.V., Strain Distribution in Quantum Dot of Arbitrary Polyhedral Shape: Analytical Solution – J. Appl. Phys. 107(6) – 2010.
9. Novikov P., Zh. Smagina, D. Vlasov, Space Arrangement of Ge Nanoislands Formed by Growth of Ge on Pit-Patterned Si Substrates – 323(1) – 198–200 – 2011.
10. Silva M. Half a century after Carl Adam Petri's Ph.D. thesis: A perspective on the field – Annual Reviews in Control – 37(2) – 191–219 – 2013.

ДЕТЕКТИРОВАНИЕ XSS-УЯЗВИМОСТЕЙ НА ОСНОВЕ ПОЛНОЙ КАРТЫ ВЕБ-ПРИЛОЖЕНИЯ

Носиров З.А., Астраханский государственный университет, Россия, г. Астрахань, nosirovzafar@outlook.com

Шаров Д.А., Астраханский государственный университет, Россия, г. Астрахань, dmitpiy@inbox.ru

Аннотация. Статья посвящена обнаружению XSS-уязвимостей на основе анализа полной карты веб-приложения. Результаты анализа популярных решений, направленных на обнаружение уязвимостей, показал, что основным недостатком является осуществление поиска уязвимостей только в открытой части веб-ресурса. Это негативно сказывается на уровне защищенности веб-ресурса, так как уязвимость может находиться в закрытой части веб-ресурса, которая доступна авторизованным пользователям. Исходя из этого, целью работы явилось повышение эффективности защиты веб-приложения от XSS путем разработки конкурентоспособного программного обеспечения, осуществляющего поиск XSS на основе анализа полной карты веб-приложения.

Ключевые слова: межсайтовый скриптинг, XSS-атака, внедрение кода, XSS-уязвимость, скриптинг, вредоносный код.

DETECTING XSS-VULNERABILITIES BASED ON A COMPLETE MAP OF WEB APPLICATION

Nasirov Z. A., Astrakhan state University, Russia, Astrakhan, nosirovzafar@outlook.com
Sharov D. A., Astrakhan state University, Russia, Astrakhan, dmitpiy@inbox.ru

Annotation. This article is devoted to the detection of XSS-vulnerabilities based on the analysis of a complete web-application map. The results of the analysis of popular solutions aimed at detecting vulnerabilities showed that the main disadvantage is the implementation of vulnerability search only in the open part of the web resource. This negatively affects the security level of the web resource, since the vulnerability can be in the closed part of the web resource, which is available to authorized users. Based on this, the goal of the work was to increase the effectiveness of protecting the Web application from XSS by developing competitive software that performs the search for XSS based on the analysis of the complete map of the web application.

Keywords: cross site scripting, XSS-attack, code introduction, XSS-vulnerabilities, scripting, exploit.

Введение. Обеспечение информационной безопасности (ИБ) вычислительных систем является одной из приоритетных задач, решаемых любой организацией. Множества угроз ИБ стали возможны благодаря широкому распространению сети Интернет.

При этом десять лет назад большинство веб-приложений были статическими и не имели интерактивных интерфейсов взаимодействия с пользователями. В них почти не было уязвимостей, которые могли бы быть использованы нарушителями. Поэтому многие разработчики игнорировали вопросы безопасности веб-приложений. Однако на сегодняшний день существует большое число динамических веб-сайтов с множеством новых технологий, которые используются в веб-браузерах. Данные технологии позволяют подключать к веб-приложениям различные модули, которые усиливают взаимодействие посетителей с веб-ресурсом.

Однако технологии, функционирующие в динамических веб-сайтах, обеспечивают хорошую платформу нарушителям для внедрения вредоносного кода (SQL-Injection, XSS и т.д.). С помощью внедренного кода нарушитель может получить несанкционированный доступ к данным авторизации пользователей и, выдавая себя за них, совершать противоправные действия. Отсутствие должных мер по соблюдению правил и норм информационной безопасности приводит к появлению угроз, которые можно реализовать с помощью компьютерных атак, эксплуатирующих уязвимости, связанные с внедрением вредоносного кода. Одним из таких видов компьютерных атак 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]. Часто уязвимость, позволяющую реализовать данный тип компьютерной атаки, также называют XSS.

Актуальность. По версии OWASP (открытого проекта обеспечения безопасности веб-приложений), межсайтовый скриптинг является одним из самых распростра-

ненных видов компьютерных атак [3]. Об этом же свидетельствуют и результаты исследования компании Positive Technologies (рис. 1) [4]. XSS занимает около 74% всех компьютерных атак на веб-приложения.

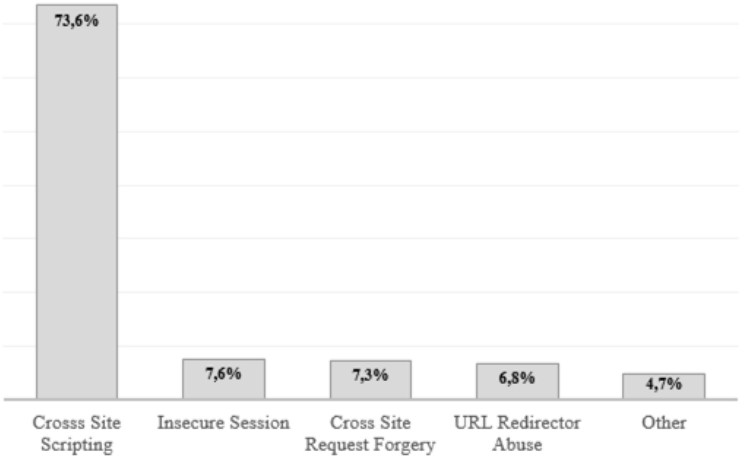

Рисунок 1 – Результаты исследования Positive Technologies

Виды атак, эксплуатирующие XSS уязвимости. Межсайтовый скриптинг – это вид компьютерной атаки, заключающаяся во внедрении вредоносного кода в параметры веб-страницы, отправляемые веб-браузеру пользователя. XSS принято классифицировать по вектору воздействия: «отраженная» (reflected) XSS, «хранимая» (stored) XSS, «XSS основанная на DOM-модели»

Существующее ПО для обнаружения XSS-уязвимостей. Большинство средств обнаружения уязвимостей громоздкие, обладают избыточным функционалом, который может замедлить работу вычислительной системы и увеличить потребление ресурсов. А простые решения «заточенные» только на поиск XSS-уязвимостей также обладают недостатками [1]. Недостатки программ для детектирования XSS связаны с особенностями построения веб-приложений. Большинство веб-приложений предусматривает авторизацию на веб-ресурсе для увеличения привилегий пользователя. То есть авторизованным пользователям будет доступен больший функционал веб-ресурса, чем неавторизованным.

В существующих решениях по детектированию XSS-уязвимостей (таких как XSpider (MAX-Patrol), Nemesida Scanner, Acunetix Online Web Security Scanner и др.) поиск осуществляется только в открытой (не требующей авторизации) части веб-сайта. Это является существенным недостатком, так как XSS-уязвимость может находиться в недоступной для поиска части веб-ресурса.

Постановка задачи. Исходя из выше изложенного, можно утверждать, что разработка программного обеспечения, осуществляющего поиск XSS-уязвимостей на основе анализа полной карты веб-приложения, является весьма актуальной задачей. Это и явилось целью данного исследования.

Решение задачи. Для достижения поставленной цели была использована методика, основанная на последовательном применении наиболее эффективных алгоритмов для обнаружения различных типов XSS-уязвимостей. Функции, реализуемые

разработанным программным обеспечением:

детектирование всех видов XSS-уязвимостей («отраженная XSS», «хранимая XSS» и «XSS основанная на DOM-модели»);

предварительная авторизация в веб-приложении и хранение кука и составление списка всех внутренних URI веб-приложения;

создание отчета о найденных уязвимостях и формирование рекомендаций по найденным уязвимостям.

«Отраженные» XSS-уязвимости проявляются только при отправке форм, разработанный алгоритм провоцирует их отправку методом POST, включая в отправляемые элементы значения и получая ответ в виде HTML сообщения.

Пришедшее сообщение анализируется на наличие уязвимости следующим образом: если пришедший JS-код устанавливает значение, хранящееся в объектной модели документа в истинное значение, то страница помечается как содержащая потенциальную угрозу соответствующего типа.

Для поиска XSS-уязвимостей, основанных на использовании объектной модели документа – DOM, используется алгоритм в ходе выполнения которого 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, работа которого 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. 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 поиска 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.

Отчет предоставляет веб-разработчику полную информацию о тестируемом веб-приложении, а также выдает рекомендации по устранению каждой найденной уязвимости, что значительно облегчает работу по их устранению. Выдача рекомендаций является одним из преимуществ разработанной программы, по сравнению с аналогами.

Сравнение с аналогами. Для оценки разработанного программного обеспече-

ния было проведено его сравнение по основным характеристикам с аналогичными решениями. Результаты сравнения программ, осуществляющие поиск XSS-уязвимостей представлены в таблице 1.

Таблица 1 – Результаты сравнения с аналогами

Характеристики	**XSpider (MAX-Patrol)**	**Nemesida Scanner**	**Acunetix Online Web Security Scanner**	**Разработанное ПО**
Поиск в «закрытой части» ресурса	–	–	–	+
Поиск хранимых XSS	+	+	+	+
Поиск отраженных XSS	+	+	+	+
Поиск DOM XSS	–	+	+	+
Наличие ГИП	+	–	+	+
Формирование рекомендаций	+	–	+	+

Результаты сравнения программ свидетельствуют о том, что разработанное ПО обладает возможностью осуществления поиска уязвимостей в «закрытой части» веб-ресурса. Также одним из важных характеристик является формирование рекомендаций по устранению найденных уязвимостей.

Разработанное ПО и перечисленные аналогичные решения были протестированы на специальном интернет ресурсе, предназначенном для тестирования по поиску XSS-уязвимостей (http://www.insecurelabs.org) (табл. 2).

Таблица 2 – Сравнение результатов тестирования программ

Наименование показателя	**XSpider (MAX-Patrol)**	**Nemesida Scanner**	**Acunetix Online Web Security Scanner**	**Разработанное ПО**
Количество найденных уязвимостей / общее количество	8/8	7/8	8/8	8/8
Затраченное время на поиск (сек.)	35	33	30	28
Среднее время нахождения одной уязвимости (сек.)	4,37	4,71	3,75	3,5

Результаты тестирования программ показали, что разработанное ПО успешно справилось с возложенными на него функциями, при этом было затрачено минимальное количество времени на обнаружение всех XSS-уязвимостей по сравнению с аналогичными решениями.

Выводы. Результаты сравнения и тестирования программ-аналогов свидетельствуют о том, что разработанное ПО имеет ряд преимуществ перед существующими продуктами, а именно:

✓ осуществление поиска XSS в закрытой части веб-ресурса;

✓ нахождение большего количества XSS по сравнению с аналогичными решениями;

✓ минимально затрачиваемое время нахождения XSS-уязвимостей;

✓ формирование рекомендаций по устранению обнаруженных уязвимостей.

Перечисленные преимущества делают разработанную программу конкурентоспособным продуктом, направленным на детектирование XSS-уязвимостей. Разработанная программа повышает эффективность защиты веб-приложения от XSS-атак. В дальнейшем намечается применение технологий искусственного интеллекта для автоматизации поиска веб-уязвимостей.

Библиографический список

1. Джатана Н., Агравал А., Собти К. Пост-эксплуатация XSS: продвинутые методы и способы защиты // SecurityLab.ru [Электронный ресурс]. 12.05.2013. – URL: https://www.securitylab.ru/analytics/440187.php (дата обращения 20.09.2018).
2. Элхади А.М. Полное пособие по межсайтовому скриптингу // SecurityLab.ru [Электронный ресурс]. 2012. – URL: https://www.securitylab.ru/analytics/432835.php?R=1 (дата обращения 25.09.2018).
3. OWASP Top 10 - 2017 The Ten Most Critical Web Application Security Risks // OWASP the free and open software security community [Электронный ресурс]. 2017 – URL: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf (дата обращения 25.09.2018).
4. Positive Research. Уязвимости веб-приложений: пора анализировать исходный код // Positive Research Center [Электронный ресурс]. 08.08.2017 – URL: http://www.blog.ptsecurity.ru/2017/08/web-attacks.html. (дата обращения 20.09.2018).

ПРИМЕНЕНИЕ ОНТОЛОГИЧЕСКОГО МОДЕЛИРОВАНИЯ ДЛЯ КЛАССИФИКАЦИИ СИСТЕМ УПРАВЛЕНИЯ ОБЪЕКТНЫМИ И РЕЛЯЦИОННЫМИ БАЗАМИ ДАННЫХ

Попов П.П., Астраханский государственный университет, Россия, г. Астрахань, pavelpapopov@gmail.com

классификации систем управления объектными и реляционными базами данных.

Проведен сравнительный анализ современных СУБД и их предрасположенность к описанию предметной области.

Ключевые слова: Онтология, онтологическое моделирование, СУБД, объектные СУБД, реляционные СУБД, классификация СУБД.

I Международная научно-техническая конференция

«Актуальные вопросы использования технологий анализа данных и искусственного интеллекта»

Материалы Международной научно-технической конференции (молодежная секция)

Астраханский государственный университет, 6-8 ноября 2018 г.

Издатель: Сорокин Роман Васильевич
414040, Астрахань, пл. К. Маркса, 33, 5-й этаж

Подписано в печать 15.11.2018 г. Формат 60×90/16
Гарнитура Times New Roman. Усл. печ. л. 12,0
Тираж 100 экз.

Отпечатано в Астраханской цифровой типографии
(ИП Сорокин Роман Васильевич)
414040, Астрахань, пл. К. Маркса, 33, 5-й этаж
Тел./факс (8512) 54-00-11, e-mail: RomanSorokin@list.ru