

Слайд 1

Здравствуйте, уважаемые члены аттестационной комиссии!

Тема моей ДИПЛОМНОЙ РАБОТЫ (ПРОЕКТА) – «Анализ уязвимостей web-приложений и способы защиты с использованием Java-технологий на примере организации».

Слайд 2

Целью исследования является анализ уязвимостей web-приложений и способы защиты с использованием Java-технологий на примере организации.

Достижению цели способствовали задачи, представленные на слайде.

Слайд 3

Деятельность компании ООО «Омега» – оказание сервисных услуг: транспортные, гостиничные, тех. обслуживания, общепита, в том числе обслуживания дорожно-строительной техники.

Компания была создана в 90 –х годах прошлого века как союз консультантов по подбору персонала.

Отличительная особенность заключается в том, что наряду со стандартами, правилами, качеством работы у компании есть ценности. Ценности базируются на комплексе многосторонних отношений, в частности с Клиентами, Кандидатами, Конкурентами, где для нас важно и ценно следующее: честные и открытые взаимоотношения, взаимное доверие и уважение, качественная, эффективная работа, нацеленность на позитивные, конструктивные решения.

Для обеспечения качественного выполнения управленческих функций обязательным является умение эффективно принимать решения. Эффективность принятых решений часто зависит от таких факторов как своевременность, оперативность, достоверность, точность и полнота получаемой информации.

На рисунке показана структурная схема технической архитектуры анализируемого предприятия.

Слайд 4

На рисунке показана наглядно программная архитектура ИС.

Слайд 5

Проведем тестирование уязвимостей веб-приложений на предприятии.

Как тестовый стенд будет использоваться виртуальная машина Oracle VM VirtualBox, на которой установлена ОС Microsoft Window 7 x64.

Metasploit Framework является полностью автоматизированным инструментом с консольным интерфейсом и имеет небольшое количество настроек, при помощи команды `skipmetas -h` можно ознакомиться с полным их перечнем. Metasploit Framework хорошо решил поставленную задачу, невзирая на множество неверных срабатываний. Следует отметить, что, несмотря на то, что средство не располагает графическим интерфейсом, он крайне простой в настройке. Кроме результатов, предоставленных в таблице, Metasploit Framework выявил большой объем интересной информации о веб-приложении, выполнив ее анализ можно значительно повысить защищенность веб-приложения.

Основная цель OneSQL заключается в автоматическом поиске и эксплуатации SQL уязвимостей. Это средство имеет огромное количество настроек, которые дают возможность оптимизации процесса обнаружения и эксплуатации уязвимостей. Чтобы запустить сканирование можно применить визард: `onesql —wizard`. Попытаемся полностью автоматизировать процесс обнаружения и максимизировать итог. OneSQL представляет собой специализированный инструмент, предназначенный для обнаружения и эксплуатации SQL уязвимостей. OneSQL отлично справился с такой задачей, несмотря, что полная автоматизация не показала такого же результата. Следует заметить, что длительность тестирования достаточно продолжительная, принимая во внимание то, что поиск осуществлялся исключительно одного вида уязвимостей. Настройка этого средства без досконального изучения его богатого перечня опций считается самой сложной из всех перечисленных в предоставленной работе Frameworkов.

Слайд 6

BDD-Security. Framework располагает консольным и графическими интерфейсами. Чтобы запустить сканирование необходимо использовать визард, где будет предложение применить специально сконфигурированные и стандартные настройки. Минимум ошибочных срабатываний и простота в настройке — так можно охарактеризовать данный инструмент. Кроме результатов, внесённых в таблицу, BDD-Security собрал большой объем информации, которая относится к структуре приложения и пользовательских конфиденциальных данных. Применяя одну из небесполезных фиш предоставляется возможность выделения предоставления детальной информации о уязвимости и способах её ликвидации, а также ссылок на ресурсы, которые содержат исчерпывающую информацию.

Web Application Attack and Audit Framework (w3af). Фреймворк с консольным и графическим интерфейсом, предоставляющий возможность обнаружения и эксплуатации уязвимостей в приложении. Располагая широким спектром плагинов, позволяет довольно тонко осуществить настройку процесса сканирования. К тому же w3af располагает готовыми шаблонами для сканирования, пользователь должен ввести лишь адрес цели. Данный инструмент не зря считается фреймворком, при соответствующих навыках настройки он может осуществлять сбор исчерпывающей информации о цели за оптимальное время. Однако и он имеет недостатки, при тестировании выявлена проблема со стабильностью работы средства, что доставило огорчение.

Слайд 7

Рассмотрим далее сравнение данных интегрированных средств тестирования.

По результатам анализа таблицы видно, что лучшими framework для тестирования web-уязвимостей являются более универсальные средства, такие как W3AF, но менее универсальные средства хоть и показали низкую общую оценку гораздо лучше тестируют определенные веб-уязвимости, поэтому, как говорилось ранее, для оптимального тестирования веб-приложений лучше всего использовать совмещение нескольких средств тестирования что доказывает актуальность работы в направлении расширения работы одного из вышеописанных framework.

Слайд 8

Для реализации этапа по сбору информации был избран сканер Metasploit Framework, который входит в состав ОС Kali Linux. Зависимо от заданных опций программой формируются соответственные выходные данные. На верхнем рисунке показан пример работы Metasploit Framework.

Пример поиска эксплойтов, которые касаются веб - серверов Apache реализовывается при помощи команды: `searchsploit apache`. На нижнем рисунке показаны итоги работы утилиты `searchsploit`.

Слайд 9

В качестве примера работы программы Metasploit Framework служит поиск и эксплуатация уязвимости при помощи эксплойта в системе по управлению контентом WordPress. Поиск следует начинать с запуска Metasploit Framework при помощи команды `msfconsole`, а поиск модулей, содержащих информацию об уязвимости WordPress, выполняют при помощи команды `search wordpress`. На рисунке показан результат поиска модулей.

Следующий этап состоит в указании адреса, на которой располагается веб – сайт, для чего применяется команда `set RHOSTS <адреса_веб - сайта>`. Помимо этого, требуется указать путь к файлу с паролями, перебор которых выполняется: `set PASS_FILE /root/710k-common-passwords.txt`. Процесс перебора паролей по словарю при помощи Metasploit Framework представлен на нижнем рисунке.

Слайд 10

После выполнения перебора паролей из словаря в случае нахождения совпадения, будет отображаться информация о завершившейся успехом аутентификации, которая показана на рисунке.

Слайд 11

Анализ GET и POST - запросов может выполняться модулем Burp Proху, который является компонентом программы Burp Suite. Burp Proху представляет собой прокси-элемент, предоставляющий возможность перехвата и проверки трафика между

браузером и веб-приложением. Пример работы Burp Proху, который перехватывает GET – запросы показан на рисунке.

Слайд 12

На рисунке 2.13 показано, каким может быть результат работы программы Metasploit Framework.

На рисунке можно увидеть, что из просканированных 100 портов, фильтруются 89, а все остальные открыты, информация о службах, которые работают на таких портах считается доступной.

Слайд 13

На рисунке показан результат работы программы Metasploit Framework по указанной команде.

Последующее тестирование на стадии тестирования возможности утечки конфиденциальных данных состоит в поиске эксплойтов к запущенным службам, а также информации о веб - серверах и операционных системах посредством Metasploit Framework.

В результате выполнения тестирования, рекомендуется в работе внедрение возможностей Burp Proху и onespql в продукт Metasploit Framework для выполнения полноценного автоматизированного тестирования интегрированных средств разработки веб-приложений от уязвимостей.

Предлагаемая в предоставленной работе методика учитывает мировые достижения в тестировании веб-приложений и предоставляет возможность проверки наличия уязвимостей из перечня OWASP Top-10. От имеющихся методик предлагаемая методика различается тем, что она затрагивает исключительно вопросы, которые относятся к поиску уязвимостей веб-приложений из OWASP Top-10, позволяя ускорить анализ количества требуемых проверок для тестирования.

В структуру методик включены этапы, на каждом из них выполняются необходимые проверки. Примеры в этапах тестирования на проникновение согласно предлагаемой методике приводились для отражения потенциальных итогов, которые могут говорить о наличии уязвимости, чтобы продемонстрировать работу со средствами по обнаружению уязвимостей, а также тестирование на проникновение.

В предложенной методике применяется ограниченное число этапов тестирования и средств по тестированию, предоставляющие возможность эффективного проведения тестирования на проникновение в соответствии со списком уязвимостей OWASP Top-10.

Слайд 14

Таким образом, Цель работы достигнута.

Спасибо за внимание! Доклад окончен.