МИНИСТЕРСТВО ОБРАЗОВАНИЯ, НАУКИ И МОЛОДЕЖНОЙ ПОЛИТИКИ КРАСНОДАРСКОГО КРАЯ
государственное автономное профессиональное образовательное учреждение Краснодарского края
«Краснодарский информационно-технологический техникум»
Лицензия серия 23Л01 № 0004947 рег. № 08112 от 14.10.2016 г. Гос. аккредитация 23А01 № 0001467 рег. № 03691 от 24.11.2016 г.
350072 г. Краснодар, ул. Московская, 81, тел (861) 252-03-83

ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА

на тему

Анализ защищенности веб-сервера ГАПОУ КК КИТТ

Выполнил Бычук Ю.Р., З-4-9-14В
(Ф.И.О. студента, группа) (подпись)

Выполнил Сахалов Д.А.,З-4-9-14В
(Ф.И.О. студента, группа) (подпись)

Руководитель Морозов Д.А., преподаватель, к.т.н.

Краснодар, 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

На сегодняшний день интернет распространился в каждый дом и по статистике из 300 проверенных сайтов 97% являются уязвимыми к атакам на веб-приложения. В век бурного развития всемирной паутины 75% атак приходится именно на веб-ресурсы. По мнению специалистов, защищённость веб-приложений является одной из самых актуальных тем информационной безопасности. Но, несмотря на печальную статистику, для любого учебного заведения Веб-сайт необходим по ряду причин, будь то привлечение новых студентов, распространение информации и прочее. Так что же делать для того чтобы Веб–сайт учебного заведения приносил прибыль, улыбку и новых студентов? В данном отчёте мы рассмотрим уровень защищённости Веб–сайта ГАПОУ КК КИТТ.

Цель работы:

1. Выделение способов совершенствование защиты Веб – сайта ГАПОУ КК КИТТ.
2. Анализ защищённости Веб – сайта ГАПОУ КК КИТТ.

Объект данной работы является: Информационная безопасность Веб – сервера ГАПОУ КК КИТТ.

Предметом является: аудит защищённости Веб – сервера ГАПОУ КК КИТТ

1 Теоретические основы анализа защищённости веб-сервера

1.1 Основные понятия и определения в области информационной безопасности веб-серверов

Перед началом анализа уязвимостей веб-сайта необходимо рассмотреть соответствующие понятия и определения.

Внешний ресурс - это информационный ресурс, доступный неограниченному кругу лиц через Интернет.

ИБ - Информационная безопасность

ИТ - Информационные технологии

ОС - Операционная система

ПО – Программное обеспечение

СУС - Система Управления Содержимым

База данных – это информационная модель, позволяющая упорядоченно хранить данные о группе объектов, обладающих одинаковым набором свойств.

Сертификат шифрования - цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа.

Эксплоит - программа, которую использует злоумышленник, чтобы получить контроль над целевой системой. Эксплоит доставляет «полезную нагрузку» (вредоносный исполняемый код) до уязвимого приложения.

Фрод - Мошеннические действия

Фишинг – это вид фрода, при котором у целевых пользователей обманным путем выманиваются их парольные данные и прочая важная информация.

Malware - вредоносное ПО.

XSS - атака типа «Межсайтовый скриптинг», чаще всего направлена на перехват чужих Cookies от веб-ресурсов.

Веб-приложения – это вспомогательные программные средства, которые предназначены для автоматизированного выполнения каких-либо действий на Веб-серверах, например удаленное управление компьютером.

Веб-сервер – это сервер, принимающий HTTP-запросы от клиентов и выдающий им HTTP-ответы, как правило, вместе с HTML-страницей, изображением, файлом, медио-протоколом или другими данными.

HTTP – это протокол прикладного уровня передачи данных (изначально – в виде гипертекстовых документов в формате «HTML», в настоящий момент используется для передачи произвольных данных).

Клиент-сервер – это вычислительная или сетевая архитектура, в которой задания или сетевая нагрузка распределены между поставщиками услуг, называемыми серверами, и заказчиками услуг, называемыми клиентами.

Загрузка файлов – термин, применяющийся в отношении данных, передаваемых между двумя вычислительными системами. Обычно применяется в условиях неравноправности систем (например, архитектуре клиент-сервер).

Веб – сайт – это совокупность логически связанных между собой веб-страниц; также место расположения контента сервера.

Веб-страница – это документ или информационный ресурс Всемирной паутины, доступ к которому осуществляется с помощью веб-браузера.

Веб-браузер – это прикладное программное обеспечение для просмотра веб-страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач.

Шелл-код (Запуск оболочки) – это двоичный исполняемый код, который обычно передает управление командному процессору. Также может быть использован как полезная нагрузка Эксплойта, обеспечивающая взломщику доступ к командной оболочке в компьютерной системе.

Межсетевой экран (брандмауэр) – это программный или программно-аппаратный элемент компьютерной сети. Осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Командная оболочка «Интерфейс командной строки» - это разновидность текстового интерфейса между человеком и компьютером, в котором инструкции компьютеру даются в основном путём ввода с клавиатуры текстовых строк (команд).

DOS – Атака – это хакерская атака на вычислительную систему с целью довести её до отказа, то есть создать такие условия, при которых добросовестные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), ибо этот доступ затруднен.

DDOS- атака – такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищенной крупной компании или правительственной организации.

Brute force attack (Полный перебор) – это метод решения математических задач или метод «грубой силы». Относится к классу методов поиска решения исчерпыванием всевозможных вариантов. Сложность полного перебора зависит от количества всех возможных решения задач.

Joomscanner (joomla!) – это одна из самых популярных CMS благодаря своей гибкости, удобству использования, расширяемости и многим другим положительным качествам. Она содержит в себе базу известных уязвимостей. Этот инструмент может помочь веб- разработчикам и веб-мастерам выявить возможные слабости в их веб-сайтах на Jomla!.

SSH (англ. Secure Shell- «безопасная оболочка») – это сетевой протокол прикладного уровня, позволяющий производить удаленное управление ОС и туннелирование TCP-соединений. Особенностью протокола является шифрование всего трафика, включая и передаваемые пароли.

Туннелирование – это процесс, в ходе которого создается защищенное логическое соединение между двумя конечными точками посредством инкапсуляции разных протоколов.

Инкапсуляция – это метод построения модульных сетевых протоколов, при котором логически независимые функции сети абстрагируются от нижележащих механизмов путём включения или инкапсулирования этих механизмов в более высокоуровневые объекты.

IT-уязвимость (Риск) – это любой риск, связанный с использованием информационных технологий.

Парсинг – это принятое в информатике определение синтаксического анализа. Для этого создается математическая модель сравнения лексем с формальной грамматикой, описанная одним из языков программирования. Например, PHP, Perl, Ruby, Python.

CVSS - это открытая схема, которая позволяет обмениваться информацией об IT-уязвимостях. Система оценки CVSS состоит из 3 метрик: базовая метрика, временная метрика и контекстная метрика. Каждая метрика представляет собой число (оценку) в интервале от 0 до 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки.

Информационные технологии – это процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов; приёмы, способы и методы применения средств вычислительной техники при выполнении функции сбора, хранения, обработки, передачи и использования данных, ресурсы, необходимые для сбора, обработки, хранения и распространения информации.

Внешние информационные ресурсы показали невысокую защищенность к воздействиям со стороны Интернет. Критических уязвимостей, которые бы позволили легко и быстро получить доступ во внутреннюю сеть целевой инфраструктуры, обнаружено не было.

Однако, были найдены уязвимости, которые позволяют:

1 Производить атаки типа «отказ в обслуживании» в отношении почтового агента информационного ресурса.

2 Обнаружить административную панель, находящуюся в директории, установленной по умолчанию.

3 Обнаружить СУС следующими способами:

- Ознакомится с логотипами и надписями в административной панели;
- Найти следы СУС в клиентском исходном коде сайта;
- Ознакомится с файлом robots.txt в коревой директории сайта, в котором присутствуют следы СУС;
- Подобрать пароль пользователей методом «Brute Force» на главной странице сайта.
- Подобрать пароль администратора методом «Brute Force» к административной панели.
- Проанализировать структуру сайта и сервера без ограничений (CloudFlare, проверка заголовков браузеров клиентов и т.д.)
- Проанализировать структуру сайта, обнаружить установленные модули и компоненты, проанализировать Javascript ресурса.

1.2 Методика проведения теста на проникновение и установления цели анализа Веб-сайта.

Цель тестирования: проведение комплексного независимого тестирования защищенности Целевой инфраструктуры в соответствии с требованием Заказчика.

В соответствии с договорённостями, заключенными между сторонами, определен следующий состав услуг, оказанных Исполнителями:

1 Тестирование на предмет наличия уязвимостей в подсистеме информационной безопасности внешних информационных ресурсов Заказчика, оценка их критичности, апробирования возможности

эксплуатации данных уязвимостей («Внешнее тестирование на проникновение»).

2 Имитация атак с применением следующих методов в отношении внешних информационных ресурсов заказчика, с целью обнаружения уязвимостей внешних ресурсов и/или получении конфиденциальной информации:

- Brute force;
- Сканирование внешних сетевых адресов Веб-приложения;
- Ручной анализ уязвимостей Веб-приложения организации;
- Анализ защищенности Веб и почтового серверов.

Выделяются следующие этапы при проведении тестирования на проникновение в соответствии с рисунком 1:

- Подготовка к проведению тестирования (проводится на стадии заключения договора)
- Сбор информации;
- Анализ уязвимостей;
- Эксплуатация и активность после эксплуатации;

Рисунок 1 – Жизненный цикл тестирования.

В свою очередь, проведение атаки можно разбить на следующие элементы в соответствии с рисунком 2:

Рисунок 2 – Этапы тестирования на проникновение [1, 2].

2 Анализ защищенности Веб-сервера ГАПОУ КК КИТТ

2.1 Аудит информационной безопасности веб-сайта ГАПОУ КК КИТТ

Цель этапа: наличия уязвимостей и возможности их эксплуатации. Использование авторитетных публичных источников для подтверждения существования уязвимостей и сбора информации об уязвимостях:

1 Подтверждение существование уязвимостей (PoC, exploits):
   - Exploit-db- http://www.exploit-db.com
   - Security Focus – http://www.securityfocus.com
   - Packetstorm – http://www.packetstorm.com
   - Security Reason – http://www.securityreason.com
   - Black Asylum – http://www.blackasylum.com

2 Поиск слабых паролей, словарных паролей, часто используемых паролей;

3 Выполнение аудита осуществлялось при помощи дистрибутива Kali Linux.

Для аудита использовались следующие инструменты:

- Nmap
- Nikto
- Sqlmap
- Uniscan
- SPARTA
- Joomscan
- Searchsploit
- Joomscanner (joomla!)
- - BurpSuite

Применялись следующие методы тестирования

1 Активное:

- С использованием автоматизированных средств на уровне сети;

- С использованием автоматизированных средств на уровне приложения;

2 Пассивное тестирование.

- Проверка существования уязвимостей;
- Планирование атак на основе обнаруженных уязвимостей.

В ходе выполнения анализа системы сайта ГАПОУ КК КИТТ было выявлено несколько уязвимостей, а именно:

1. Административная панель расположена в стандартной директории;
2. Обнаружены демаскирующие элементы в клиентском исходном коде Веб-сайта;
3. Обнаружены демаскирующие элементы в файле «robots.txt», в корневой директории Веб-сайта;
4. Отсутствует проверка заголовков клиентов;
5. Обнаружен открытый доступ к системным директориям Веб-сайта:

– new.kitt.ws/administrator/components
– new.kitt.ws/administrator/modules/
– new.kitt.ws/administrator/components/
– new.kitt.ws/administrator/components/com_joomlaupdate/restore.php
– new.kitt.ws/administrator/components/com_admin/sql/updates
– new.kitt.ws/media/system/js/
– new.kitt.ws/plugins/content/
– new.kitt.ws/media/system/
– new.kitt.ws/media/jui/js/
– new.kitt.ws/media/jui/
– new.kitt.ws/administrator/templates/
– new.kitt.ws/images/2018/
– new.kitt.ws/images/sampledata/

– new.kitt.ws/images/templates/

– new.kitt.ws/media/docs/

– kitt.ws/media/docs/

6. Обнаружено автозаполнение форм входа;

7. Обнаружена уязвимая версия почтового агента информационного ресурса заказчика;

8. Отсутствует SSL-сертификат безопасности для обеспечения безопасного соединения.

9. Пароли передаются от клиента к серверу в открытом виде.

10. Пароли передаются от администратора к серверу в открытом виде.

2.2 Составление рекомендаций для защиты веб-сайта ГАПОУ КК КИТТ

Во время проведения анализа защищенности внешних информационных ресурсов заказчика цель данного тестирования было выполнено. Во время проведения анализа не было выявлено критических уязвимостей, однако, был выявлен ряд уязвимостей представляющих собой угрозы различных степеней важности.

Для обеспечения необходимого уровня безопасности внешних информационных ресурсов был составлен список рекомендаций по устранению выявленных угроз, а именно:

Изменение стандартной директивы, в которой расположена административная панель;

1. Избавиться от демаскирующих элементов в клиентском исходном коде Веб-сайта;

2. Избавиться от демаскирующих элементов в файле «robots.txt» в корневой директории Веб-сайта;

3. Обеспечить проверку заголовков клиентов для защиты от возможной угрозы парсинга;

4. Обеспечить защиту от атак типа «Отказ в обслуживании» (DDoS);

5. Ограничить число неудачных попыток входа как на главной странице, так и в административной панели;

6. Ограничить доступ к системным директориям Веб-сайта:

– new.kitt.ws/administrator/components
– new.kitt.ws/administrator/modules/
– new.kitt.ws/administrator/components/
– new.kitt.ws/administrator/components/com_joomlaupdate/restore.php
– new.kitt.ws/administrator/components/com_admin/sql/updates
– new.kitt.ws/media/system/js/
– new.kitt.ws/plugins/content/
– new.kitt.ws/media/system/
– new.kitt.ws/media/jui/js/
– new.kitt.ws/media/jui/
– new.kitt.ws/administrator/templates/
– new.kitt.ws/images/2018/
– new.kitt.ws/images/sampledata/
– new.kitt.ws/images/templates/
– new.kitt.ws/media/docs/
– kitt.ws/media/docs/

7. Запретить автозаполнение форм входа;

8. Обновить версию почтового агента информационного ресурса заказчика;

11. Установить SSL-сертификат безопасности для обеспечения безопасного соединения.

12. Ограничить передачу паролей от клиента к серверу в открытом виде.

13. Ограничить передачу паролей от администратора к серверу в открытом доступе.

Специалистам ГАПОУ КК КИТТ рекомендуется предпринять меры по скорейшему устранению выявленных угроз.

ЗАКЛЮЧЕНИЕ

Таким образом были рассмотрели теоретические основы анализа защищённости веб-сервера, основные понятия и определения в области информационной безопасности веб-серверов, методику проведения теста на проникновение и установили цели анализа веб-сайта, выбрали средства анализа защещенности веб-сервера, составили рекомендации по совершенствованию системы безопасности для веб-сайта ГАПОУ КК КИТТ.

Все поставленные цели были выполнены и рассмотрены. Во время анализа по выявлению угроз были предоставлены рекомендации по скорейшему их устранению.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Колегов, Д.Н. Лабораторный практикум по основам анализа защищенности веб-приложений: учебное пособие. – Томск: Издательский Дом Томского государственного университета, 2014. – 59 с.

2 Романов, П. Ю. Программное обеспечение компьютерных сетей и web-серверов : учеб. пособие / Г.А. Лисьев, П.Ю. Романов, Ю.И. Аскерко. — М.: ИНФРА-М, 2018. — 145 с.