СОДЕРЖАНИЕ

Введение

В мире миллионы сайтов и интернет сервисов разрабатываются в условиях быстрой разработки. Такой вид разработки позволяет в короткие сроки создавать сайты, онлайн платформы игры и другие приложения. Однако данный подход имеет существенные недостатки.

К недостаткам принято относить ошибки и просчёты в проектировании и реализации интернет приложения. Среди подобный ошибок встречаются: ошибки конфигурации сервера, ошибки работы системы контроля доступа и межсетевых экранов, неактуальный версии программных компонентов, установленных на сервере. Все эти аспекты дают почву для работы злоумышленников, преследующих самые разнообразные цели.

Для предотвращения сбоев в программном обеспечении необходимо проводить тестирования на проникновения, процедуру анализа работоспособности сервера с целью выявления уязвимостей информационной безопасности и их дальнейшего устранения. Подобного рода процедуры приводят к нежелательным тратам денежных средств, особенно если речь идёт о маленьких компаниях, с относительно невысокими бюджетами.

Для тестирования безопасности существуют специальные инструменты, способные обнаруживать некоторые уязвимости. Проводя сканирования подобными инструментами можно найти ошибки и уязвимости, не прибегая к услугам тестировщиков безопасности.

Цель курсовой работы: Создание бесплатной платформы сканирования сайтов для выявления уязвимостей, использующую понятный пользователю интерфейс.

Задачи:

1. Разработать техническое задание для приложения.
2. Провести детальное исследования предметной области.
3. Разработать систему сканирования сайтов.

1 Техническое задание

1.1 Общие сведения

1.1.1 Полное наименование системы и её условное обозначение

Автоматизированная система тестирования сайтов на наличие ошибок и уязвимостей информационной безопасности АС «Гг»

1.1.2 Наименование предприятий (объединений) разработчика и заказчика (пользователя) системы и их реквизиты

Заказчик: Калужский филиал Московского государственного технического университета им. Н. Э. Баумана (КФ МГТУ им. Баумана).

Исполнитель (разработчик): Студент группы ИУК5-42Б КФ МГТУ им. Н. Э. Баумана Хохлов В. М.

1.1.3 Перечень документов, на основании которых создаётся система, кем и когда утверждены эти документы

АС создаётся на основании данного технического задания.

Иных документов, являющихся основанием разработки АС не предусмотрено.

1.1.4 Плановые сроки начала и окончания работы по созданию системы

Плановый срок начала работы _____

Плановый срок окончания работы _____

1.2 Назначение и цели создания системы

1.2.1 Назначение системы

АС «Гг» предназначена для автоматизации проведения тестирования сторонних сайтов на ошибки и уязвимости в программном коде и архитектуре веб приложения, в частности исполнения следующих процессов:

1. Произведение сканирования сайтов на OWASP Top 10 уязвимости;

2. Информирование пользователя о результатах работы.

1.2.2 Цели создания системы

Основными целями создания АС «Г» являются:

1. Получение навыков работы с базами данных, механизмам хранения обработки и передач информации.

2. Получение знаний, касающихся принципов работы реляционных баз данных, контроля доступа к базе данных.

3. Создание бесплатной платформы для проведения тестирования безопасности сайтов.

1.3 Характеристика объекта автоматизации

Объект автоматизации — алгоритмы сканирования веб приложений на наличие уязвимостей и ошибок. Сканирование представляет собой запуск программ для автоматического формирования и отправления запросов на сервера и дальнейший анализ результатов, поступающих от сервера. Сканирование может реализовываться путём использования уже реализованных техник сканирования в виде готовых программ. Подробнее каждый вид сканирования должен быть описан в научно-исследовательской части курсовой работы.

1.4 Требования к системе

1.4.1 Требования к системе в целом

1.4.1.1 Требования к структуре и функционированию системы

Автоматизированная система должна состоять из следующих подсистем:

- Подсистема пользовательского интерфейса
- Подсистема хостинга веб-приложения
- Подсистема контроля доступа
- Подсистема сканирования сайтов

- База данных

Подсистема пользовательского интерфейса должна предоставлять пользователю графический интерфейс для взаимодействия с программой. Пользовательский интерфейс должен быть реализован как веб-сайт.

Подсистема хостинга веб-приложения должна позволять размещать АС на сервере и организовывать доступ к АС, являющейся веб-приложением. Подсистема должна представлять собой веб-сервер nginx или Apache.

Подсистема контроля доступа — часть АС, серверная часть веб-приложения, отвечающая за обработку данных, получаемых от пользователей. Подсистема должна предоставлять доступ к базе данных и подсистеме сканирования сайтов, фильтровать запросы пользователей.

Подсистема сканирования сайта — часть АС, задачей которого является проведение сканирования веб-сайтов и выявление уязвимостей информационной безопасности на сайтах. Подсистема должна соответствовать следующей структуре:

1. Сервис приёма и обработки пакетов для запуска предустановленных программ для сканирования сайтов на наличие уязвимостей ИБ. Реализовать с использованием протокола HTTP(S).

2. Программа для формирования данных, пригодных для записи в базу данных, сформированных на основе предоставляемой сторонними программами сканирования сайтов информации, с возможностью записи данных в базу данных.

3. Сторонние программы установленные с помощью пакетного менеджера или установленные вручную с репозитория — с помощью этих программ производить сканирования сайтов.

База данных должна хранить данные о пользователях АС, результатах сканирования сайтов.

Система должна функционировать в нормальном режиме, являющимся единственным режимом работы АС. Иных режимов для функционирования

системы не предусмотрено. При нормальном режиме работы в АС не возникает ошибок различного рода, выполнение алгоритмов сканирования выполняется успешно.

Система создаётся с целью изучения методов работы с базой данных. Перспективы дальнейшего развития АС и её модернизации существуют.

1.4.1.2 Требования к численности и квалификации персонала системы и режиму его работы

АС должна являться веб приложением с возможностью одновременного использования не более 100 пользователями. К квалификации пользователей, эксплуатирующего АС предъявляются следующее требование: умение работать с компьютером на уровне среднего пользователя. Минимальное понимание предметной области.

К квалификации пользователя-администратора предъявляются следующее требования: умение работать с базой данных, умение работать с компьютером на уровне среднего пользователя.

1.4.1.3 Показатели назначения

АС предназначается преимущественно для тестирование защищенности сайтов, а также получение знаний, умений и навыков работы с БД в рамках выполнения курсовой работы.

АС должна сохранять своё целевое назначение на протяжении всего цикла работы, в независимости от действий пользователей.

1.4.1.4 Требования к надёжности

Система должна отвечать следующим требованиям надёжности:

Отказоустойчивость. Система должна оставаться работоспособной в случае возникновения ошибки в процессе работы модуля сканирования сайтов, получения некорректных данных с клиентской стороне или нагрузки на сервер не более 100 подключений.

Фильтрация трафика. Система не должна предоставлять доступ к конфиденциальным данные, внутренним ресурсам сервера, базе данных в случае получения вредоносного трафика.

Достаточный для нормального функционирования АС уровень надёжности должен достигаться путём:

1. Использование операционной системы, обладающей высокими показателями надёжности;

2. При возникновении сбоев в работе модулей сканирования сайтов требуется делать соответствующие записи в специализированные файлы;

3. Соблюдение рекомендаций OWASP (Открытый проект безопасности веб приложений);

4. Проведение комплекса мероприятий отладки, поиска и исправления ошибок на этапе тестирования и отладки АС.

1.4.1.5 Требования к безопасности

АС не работает с внешними техническими средствами, требующие соблюдения специальной техники безопасности при работе, установке, наладке, техническому осмотру и ремонту. Требований безопасности к АС не предъявляется.

1.4.1.6 Требования к эргономике и технической эстетике

Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав системы, должно осуществляться посредством визуального графического интерфейса (GUI). Интерфейс системы должен быть понятным и удобным, не должен быть перегружен графическими элементами и должен обеспечивать быстрое отображение экранных форм.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа «мышь», клавиатурный режим ввода должен использоваться главным образом при заполнении и/или редактировании текстовых и числовых полей экранных форм.

Система должна обеспечивать корректную обработку аварийных ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна регистрировать соответствующие сообщения в специальный файл.

Экранные формы должны разрабатываться с учётом требований унификации: все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации; для обозначения сходных операций должны использоваться сходные графические значки, кнопки и другие управляющие (навигационные) элементы.

1.4.1.7 Требования к транспортабельности для подвижных АС

Специальных условий для транспортабельности АС не предъявляется: система может транспортироваться на малогабаритных носителях информации (флешка, жёсткий диск) или передаваться по сети Интернет.

1.4.1.8 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы

АС не должна обладать дополнительными техническими средствами, требований к использованию дополнительных технических средств АС не предъявляются.

Допустимая площадь для размещения персонала — площадь, необходимая для размещения одного человека и персонального компьютера (ноутбука). Для корректной работы АС необходимо бесперебойное снабжение электроэнергией устройства, хранящего и выполняющего алгоритмы АС. В качестве устройства хранения информации приложения можно использовать сервер хостинговой компании или персональный компьютер с установленным программным обеспечением.

Требования к эксплуатации АС предъявляются администратору АС:

1. Обновление программных компонентов сервера;

2. Просмотр файлов журналирования работы АС.

3. Конфигурирование веб-сервера и базы данных.

АС может управлять один человек, требований к количеству и квалификации обслуживающего персонала, а также режиму его работы не предъявляются.

АС не должна быть снабжена комплексом запасных изделий и приборов. Требования к составу, размещению и условиям хранения не предъявляются.

1.4.1.9 Требования к защите информации от несанкционированного доступа

АС будет хранить данные, являющиеся персональным данными пользователя, доступ к которым должен быть доступен только аутентифицированным пользователям. Для предотвращения получения несанкционированного доступа к конфиденциальной информации нужно использовать необходимые политики безопасности АС: шифрование, контроль доступа пользователей на стороне сервера.

1.4.1.10 Требования по сохранности информации при авариях

К АС предъявляются требования для обеспечения сохранности данных при сбоях в программе работы сервера. Содержимое базы данных должно копироваться на внешние носители, удалённые хосты или иные запоминающие устройства с периодичностью, необходимой для сохранности 100% информации базы данных.

1.4.1.11 Требования к средствам защиты от влияния внешних воздействий

АС предназначена для работы на стационарных компьютерах, находящихся в условиях отсутствия внешних физических воздействий. Специальных требований к защите информации от влияния внешних воздействий и среде применения не предъявляется.

1.4.1.12 Требования к патентной чистоте

Установка системы в целом, как и установка отдельных частей системы не должна предъявлять требований к покупке лицензий на программное обеспечение сторонних производителей. Допускается использование программ с открытым исходным кодом для ускорения процесса разработки.

1.4.1.13 Требования по стандартизации и унификации

Единообразный подход к решению однотипных задач должен достигаться: единым программно-техническим способом реализации одинаковых функций системы, унификацией компонентов математического, информационного, лингвистического и программного обеспечения, унификацией компонентов технического обеспечения. В графических модулях необходимо использовать единообразные элементы управления и цветовую схему.

1.4.1.14 Дополнительные требования

Дополнительные требования к АС могут быть предъявлены на этапе программной реализации АС. На этапе «формирования требований к АС» дополнительные требования не предъявляются.

1.4.2 Требования к функциям (задачам), выполняемым системой

1.4.2.1 Требования к подсистеме. Перечень функций, задач или их комплексов.

Подсистемы АС должны обладать следующим функционалом:

- Подсистема пользовательского интерфейса
  1. Предоставление графического интерфейса пользователю;
  2. Обработка действий пользователя.
- Подсистема хостинга веб-приложения
  1. Обеспечение бесперебойного доступа к серверу;

2. Обеспечение возможности обслуживания не менее 100 клиентов одновременно.

- Подсистема контроля доступа

  1. Приём, обработка пользовательских запросов;

  2. Фильтрация вредоносного трафика;

  3. Проверка доступа к запрашиваемым ресурсам;

  4. Обеспечение запуска модулей сканирования сайтов;

  5. Обеспечение доступа к базе данных;

  6. Возврат результатов пользовательских запросов в браузер.

- Подсистема сканирования сайтов

  1. Приём, обработка данных подсистемы контроля доступа;

  2. Проведение сканирования сайтов способом, полученным в теле запроса

  3. Формирование строк для записи в таблицу базы данных;

  4. Запись данных в базу данных;

- База данных

  1. Добавление, редактирование, резервное копирование, удаление данных;

1.4.2.2 Требования к качеству реализации каждой функции (задачи или комплекса задач), к форме представления выходной информации, характеристики необходимой точности и времени выполнения, требования одновременности выполнения группы функций, достоверности выдачи результатов

Функции должны полностью выполнять поставленные задачи. Функции не должны аварийно завершать работу системы АС при возникновении ошибок. В случае возникновения ошибки, программный модуль должен корректно завершиться с записью причины завершения в файл.

1.4.3 Требования к видам обеспечения

1.4.3.1 Требования к математическому обеспечению

Требования не предъявляются к математическому обеспечению.

1.4.3.2 Требования к информационному обеспечению

АС должна состоять из модулей, размещаемых на носителе данных. АС должна хранить данные в базе данных. База данных может находиться как на локальном компьютере, так и на удалённом.

АС должна использовать кодировку UTF-8.

Сбор данных в АС должны происходить путём взаимодействия пользователя с подсистемой графического интерфейса. Пользователь последовательно вводит данные, необходимые для дальнейшего использования АС. По нажатии специальной кнопки, данные структурируются, проверяется их корректность. Данные, введённые пользователем, выступают в роли параметров для модулей сканирования сайтов.

Клиент-серверное взаимодействие необходимо реализовать за счет использования протокола HTTP(S). Взаимодействие между БД и сервером (подсистемы контроля доступа) нужно строить с использованием API для доступа к данным БД.

1.4.3.3 Требования к лингвистическому обеспечению

Для реализации компонентов АС необходимо использовать следующие языки программирования:

HTML, CSS, JavaScript — использовать для реализации графического интерфейса пользователя. Также для поддержки веб приложения мобильными устройствами необходимо использовать фреймворк bootstrap.

PHP — реализация серверной логики приложения. Рекомендуется использование фреймворка Laravel.

C++, Python — использовать для реализации подсистемы сканирования сайтов.

1.4.3.4 Требования к программному обеспечению

Для реализации веб-приложения можно использовать любую операционную систему за счёт использования интерпретируемых языков программирования на стороне сервера. Рекомендуется использовать операционную систему Kali Linux, в состав которой входят необходимые инструменты для тестирования безопасности сайтов.

1.4.3.5 Требования к техническому обеспечению

Основным техническим средством, являющимся носителем АС может выступать персональный компьютер. Для корректной работы АС техническое средство должно работать на базе операционной систем Linux, Windows, Mac. Требований к наличию иных комплектующих изделий для использования совместно с АС не предъявляется.

1.4.3.6 Требования к метрологическому обеспечению

Требования к метрологическому обеспечению не предъявляются.

1.4.3.7 Требования к организационному обеспечению

Требования к организационному обеспечению не предъявляются.

1.4.3.8 Требования к методическому обеспечению

Требования не предъявляются.

1.4.3.9 Требования к другим видам обеспечения системы

Требования не предъявляются.

1.5 Состав и содержание работ по созданию (развитию) системы

1. Реализация базы данных. Экспертиза: согласование правильности организации таблиц БД с заказчиком. (Срок __ неделя)

2. Разработка прототипа интерфейса. Экспертиза: согласование прототипа с заказчиком. (Срок __ неделя)

3. Разработка физической и логической схемы АС. Экспертиза: демонстрация проделанной работы заказчику. (Срок __ неделя).

4. Разработка макета АС. Экспертиза: демонстрация проделанной работы заказчику. (Срок __ неделя).

5. Отладка и устранение ошибок программы. Экспертиза: демонстрация готовой к вводу в эксплуатации АС. (Срок __ неделя)

1.6 Порядок контроля и приёмки системы

1.6.1 Виды, состав, объем и методы испытаний системы и её составных частей

Составные части АС должны быть протестированы по окончании стадии разработки программ. Тестирование системы должно включать обнаружение ошибок в ходе выполнения программы, ошибок в результате некорректных действий пользователя, неточностей в работе модулей GUI. При добавлении нового функционала предыдущие тесты должны сохранить работоспособность. Использовать UNIT тесты при тестировании. Проверять соответствие рекомендациям OWASP компонентов АС.

1.6.2 Общие требования к приёмке работ по стадиям

Сдача-приёмка работ производится поэтапно, в соответствии с рабочей программой. После демонстрации работоспособности АС на каждой стадии разработки происходит согласование текущего функционала, после чего разработка переходит на следующую стадию.

1.6.3 Статус приёмочной комиссии

Приёмочная комиссия, организованная КФ МГТУ им. Баумана, осуществляет приёмку работы.

1.7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие

Для ввода АС в действие необходимо выполнение следующих условий:

1. Наличие установленных модулей сканирования сайтов; К модулям сканирования относятся программы с открытым исходным кодом: nmap, dirb, sqlmap, nikto.

2. Наличие установленного веб-сервера Apache или nginx, модулей обеспечения поддержки языков программирования: PHP.

3. Операционная система Linux, Windows, Mac OS.

1.8 Требования к документированию

Требуется предоставить:

1. Техническое задание в соответствии с ГОСТ 34.602-89

2. Расчётно-пояснительную записку, включающую исследовательскую часть, проектно-конструкторскую часть и проектно-технологическую часть. Расчётно-пояснительная записка выполняется с учётом требований, предусмотренных ГОСТ 7.32-2001 и 2.105-95.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ СОСТАВИЛИ

Наименование организации, предприятия	**Должность исполнителя**	**Фамилия, имя, отчество**	**Подпись**	**Дата**

ТЕХНИЧЕСКОЕ ЗАДАНИЕ СОГЛАСОВАНО

Наименование организации, предприятия	**Должность исполнителя**	**Фамилия, имя, отчество**	**Подпись**	**Дата**

Приложения

Перечень принятых сокращений

АС	Автоматизированная система
GUI	Графический интерфейс пользователя
БД	База данных

d