Система контроля защищенности интернет-ресурсов (сайтов) – Веб Безопасность

Руководство системного администратора

Листов 17

Содержание

1. Общие положения

Полное наименование: ПО «Система контроля защищенности интернет-ресурсов (сайтов) – Веб Безопасность».

Сокращенное наименование: ПО «Webbez Scanner».

Перед эксплуатацией ПО необходимо внимательно ознакомиться с комплектом эксплуатационной документации.

В случае обнаружения дефектов технических и программных средств следует обращаться к поставщику ПО.

Настоящий документ должен находиться у должностного лица, ответственного за эксплуатацию ПО.

Данные работы проводятся с целью настройки оборудования для последующей передачи его в эксплуатацию. При невыполнении любого из пунктов (некорректном выполнении) данного руководства работы следует прервать до полного исправления (корректировки) выявленного несоответствия. По результатам работ по каждому пункту вносится запись в журнал работ.

2. Основные технические характеристики

ПО «Webbez Scanner» представляет собой набор решений, направленных на обеспечение функций контроля защищенности информационной системы (далее - ИС), построенной на базе веб-технологий. Использование данной системы позволяет реализовать функции обнаружения, предотвращения и реагирования на попытки несанкционированной активности удаленных и внутренних пользователей компьютерных сетей.

В ПО «Webbez Scanner» реализованы следующие области проверки защищенности ИС, построенных на базе веб-технологий:

– предварительный сбор информации;

– использование поисковых систем для поиска чувствительных данных в информационном пространстве ИС;

– проведение конфигурационного анализа;

– проведение тестов на наличие типовых уязвимостей ИС на базе веб-технологий;

– проверка наличия недостатков в используемых механизмах аутентификации;

– проведение комплексных проверок безопасности используемых веб-технологий;

– поиск стороннего кода;

– выявление фактов непреднамеренного раскрытия чувствительной информации.

1.3 Состав программного обеспечения

ПО «Webbez Scanner» содержит следующие основные функциональные модули:

– веб-интерфейс предназначен для постановки задач и просмотра сгенерированных отчетов пользователем;

– робот – наименьшая структурная единица. Робот представляет собой программный модуль, направленный на выполнение проверки конкретного аспекта безопасности ИС;

– механизм контроля расписания и запуска локальных менеджеров;

– модуль постоянного контроля, который предназначен для периодических проверок заданных ИС;

– демон Daemon (локальный менеджер модуля «Постоянный контроль»), который обеспечивает запуск новых заданий на сканирование, контроль корректности

выполнения ранее запущенных заданий, корректировку глобального расписания, запуск механизма формирования конечного отчета;

– механизм формирования конечного отчета применяется в модуле постоянного контроля для предоставления пользователю результатов в форме pdf-файла;

– база данных MSQL предназначена для хранения данных о доступных роботах, выполняемых проверках, зарегистрированных пользователях и исследуемых ИС;

– робот ar_checker представляет собой программное решение для интеграции с фреймворком Arachni;

– модуль «Экспресс», который предназначен для разовых проверок заданных ИС;

– API-интерфейс модуля «Экспресс» представляет собой полноценный REST-API, который позволяет осуществлять постановку задач и получение результата в составе интегрированных программных комплексов, разрабатываемых ООО «Веб Безопасность»;

– демон apiDaemon (локальный менеджер модуля «Экспресс»), который обеспечивает запуск новых заданий на сканирование, контроль корректности выполнения ранее запущенных заданий, запуск механизма формирования конечного отчета;

– база данных SQLT предназначена для хранения данных о выполняемых проверках, статусе поставленных задач, доступных пакетах модуля экспресс контроля.

1.4 Используемые технологии

ПО «Webbez Scanner» объединяет в себе множество технологий и языков программирования. При проектировании и разработке был сделан выбор в сторону наиболее оптимальных и зарекомендовавших себя решений.

Ниже представлен перечень технологий и языков программирования, используемых в основных элементах комплекса:

1) «Подсистема управления» - веб-фреймворк CodeIgnitor на языке PHP, база данных MySQL;

2) «Модуль постоянного контроля»
   - Демон Daemon - Java;
   - База данных MSQL – СУБД MySQL;
   - Роботы – Perl, Python, PHP;
   - Отчеты роботов – xml-файлы, pdflatex.

3) «Модуль экспресс-тестирования» и «API-интерфейс»
   - Демон apiDaemon - PHP;
   - Роботы – Perl, Python, PHP;
   - api-control – веб-фреймворк CodeIgnitor на языке PHP;
   - api-exec-express – веб-фреймворк CodeIgnitor на языке PHP, база данных SQLite;
   - Отчеты роботов – xml-файлы.

4) «Подсистема сторонних компонентов» - Ruby.

1.5 Назначение и состав роботов входящих в состав изделия

Роботы в ПО «Webbez Scanner» – это наименьшая структурная единица. Роботы представляют собой программные модули, направленные на выполнение проверки конкретного аспекта безопасности ИС. В составе комплекса присутствуют роботы, реализованные на разных языках программирования, перечисленные в предыдущем разделе.

Общий перечень выполняемых проверок представлен в таблице 1.

Таблица 1 – Перечень роботов

1. Сбор информации
1.1 Составление карты сайта
1.2 Получение статусов всех обнаруженных директорий сайта
1.3 Проверка активированных http-методов
2. Работа с поисковыми системами
2.1 Поиск нежелательных данных сайта в поисковой системе Google
2.2 Мониторинг упоминания сайта на хакерских платформах
3. Конфигурационный анализ
3.1 Проверка наличия служебных объектов (по словарю)
3.2 Поиск директорий без индексного файла (листинг директории)
3.3 Поиск резервных копий исполняемых модулей
3.4 Поиск административных и внутренних дочерних доменов
3.5 Проверка цифровых сертификатов
3.6 Анализ файла robots.txt
3.7 Поиск систем администрирования
3.8 Проверка наличия и правильной настройки WebDAV
3.9 Поиск раскрытия номеров кредитных кард
3.10 Поиск доступных систем управления версиями CVS/SVN, GIT, Mercurial
3.11 Поиск распространенных бэкдоров
3.12 Проверка раскрытия email-адресов
3.13 Небезопасное использование cookie
3.14 Проверка использования политики "Strict-Transport-Security"
3.15 Проверка использования защитного механизма "X-Frame-Options"
3.16 Небезопасное использование технологии CORS
3.17 Небезопасное использование кросс-доменной политики
3.18 Небезопасное использование политики клиентского доступа
4. Проверка уязвимостей
4.1 Проверка наличия SQL-инъекций
4.2 Поиск возможности внедрения XSS-векторов
4.3 Проверка устойчивости к несанкционированному подключению файлов
4.4 Поиск возможности для CSRF-атаки
4.5 Проверка наличия SQL-инъекций на основе появления ошибок
4.6 Проверка наличия "слепых" SQL-инъекций на основе дифференциального анализа
4.7 Проверка наличия "слепых" SQL-инъекций на основе анализа временных задержек
4.8 Проверка наличия NoSQL-инъекций на основе появления ошибок
4.9 Проверка наличия "слепых" NoSQL-инъекций на основе дифференциального анализа
4.10 Проверка наличия инъекций исполняемого кода
4.11 Проверка наличия "слепых" инъекций исполняемого кода на основе появления ошибок
4.12 Проверка наличия LDAP-инъекций
4.13 Проверка наличия возможности обхода директорий
4.14 Проверка наличия возможности "расщепления" ответов сервера
4.15 Проверка наличия инъекций команд хостовой ОС
4.16 Проверка наличия "слепых" инъекций команд хостовой ОС на основе анализа временных задержек
4.17 Проверка устойчивости к несанкционированному подключению удаленных файлов
4.18 Проверка наличия возможности неконтролируемого перенаправления пользователя
4.19 Проверка наличия возможности неконтролируемого DOM-перенаправления пользователя
4.20 Проверка наличия XPath-инъекций
4.21 Проверка возможности внедрения XSS-векторов в URL
4.22 Проверка возможности внедрения XSS-векторов в атрибуты html-элементов
4.23 Проверка возможности внедрения XSS-векторов в html-элементы
4.24 Проверка возможности внедрения XSS-векторов в содержимое пользовательских скриптов
4.25 Проверка возможности внедрения XSS-векторов в DOM-модель страницы

4.26 Проверка наличия раскрытия исходного кода приложения
4.27 Проверка устойчивости к атаке "XML External Entity"
5. Слабая аутентификация
5.1 Проверка типовых паролей для basic-авторизации (перебор по словарю)
5.2 Анализ защищенности модулей аутентификации
6. Комплексная проверка
6.1 Определение плагинов и наличие уязвимостей в популярных системах управления содержимым (CMS)
6.2 Поиск сайта в различных "черных" списках
6.3 Проверка устойчивости к DoS-атакам уровня веб-приложения
7. Поиск стороннего кода
7.1 Поиск следов установленных вирусов
8. Раскрытие информации
8.1 Поиск документов без прямых ссылок на сайте

3. Проводимые работы

Перечень проводимых работ, а также ожидаемый результат и действия по факту выполнения или невыполнения приведены в таблице 2.

Таблица 2 – Перечень пуско-наладочных работ

№ п.п.	Выполняемые работы	Ожидаемый результат	Действия по факту выполнения / невыполнения
1	**Подготовительный этап (внешний вид и органы управления)**		
1.1	Произвести мероприятия по технике безопасности: уложить диэлектрический коврик, закрепить антистатический браслет.	Диэлектрический коврик уложен, антистатический браслет закреплен.	**Получен ожидаемый результат:** произвести запись в журнале работ; перейти к следующему пункту плана работ.
1.2	Проверить внешним осмотром смонтированное устройство.	Внешних дефектов видимых поверхностей не выявлено, а именно: отсутствуют следы механических повреждений корпуса, разъемов, органов управления и контроля; в наличии пломбы предприятия-изготовителя; отсутствует повреждение лакокрасочных покрытий.	**Получен ожидаемый результат**: произвести запись в журнале работ; перейти к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ о выявленных недостатках; доклад инженеру-координатору работ о выявленных недостатках (разукомплектованности оборудования, наличии дефектов корпуса); прекращение работ до получения указаний от координатора работ.

1.3	Проверить правильность, соответствие смонтированных коммуникаций рабочей документации, наличие и правильность произведенной маркировки.	Сервер находится в стойке. К нему подключены: кабель Ethernet, кабель питания, KVM-консоль согласно схемам рабочей документации. Кабели промаркированы в соответствии с требованиями «Правил маркировки коммуникаций». Конструктивные элементы и крепления не перекрывают вентиляционные отверстия устройства.	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ; устранение недостатков: выполнить монтаж и маркировку коммуникаций в соответствии с требованиями; доклад инженеру-координатору; при невозможности устранения недостатков - прекращение работ до получения указаний от координатора работ.
1.4	Проверить качество и надежность подключения электропитания и заземления оборудования.	Электропитание подключено к ИБП, протоколы измерений представлены и соответствуют руководящим документам ПУЭ и ПТЭЭП. Проверить: цепь заземления между защитной цепью телекоммуникационного шкафа и устройством проложена проводом,	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ; устранение недостатков: закрепить кабель

		сечением не менее 4 мм^2; усилие затяжки гайки (винта) заземления на корпусе устройства проверено, люфт не обнаружен; с помощью мультиметра произведено измерение разности потенциалов между нулевым проводом и технологической землей на разъеме кабеля электропитания устройства - разность потенциалов между нулевым проводом и технологической землей – 0 В; с помощью мультиметра произведено измерение напряжения между фазой и нулевым проводом на разъеме кабеля электропитания устройства - напряжения между фазой и нулевым проводом составляет ~220 V ± 10% по ГОСТ Р 54149-2010; кабель электропитания плотно вставлен в разъем устройства.	заземления, электропитания; доклад инженеру-координатору; при невозможности устранения недостатков - прекращение работ до получения указаний от координатора работ.
1.5	Удостовериться в наличии электропитания на устройстве путем проверки индикации.	Подача электропитания подтверждается наличием свечения индикатора «Питание».	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ.

			Ожидаемый результат не получен: произвести запись в журнале работ; дополнительно проверить электропитание; произвести доклад инженеру-координатору; при невозможности устранения недостатков - прекращение работ до получения указаний от координатора работ.
2	**Подготовка к настройке**		
2.1	Запустить сервер, путем нажатия кнопки включения на передней панели.	Сервер включился.	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
3	**Настройка конфигурации**		
3.1	Произвести настройку сервера на загрузку ОС с внешнего накопителя, путем установки соответствующего параметра «Boot Priority» в BIOS.	Порядок опроса загрузочных устройств в настройках «Boot Priority» в BIOS изменился.	**Получен ожидаемый результат:** произвести запись в журнале работ;

			переход к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
4	**Сохранение конфигурации**		
4.1	После изменения параметров BIOS необходимо выполнить сохранение произведенных настроек.	Изменения, произведенные в BIOS, сохранились. Сервер загружается с внешнего накопителя.	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
5	**Установка ОС**		
5.1	Вставить компакт-диск с Ubuntu Server 20.04 LTS в CD/DVD-ROM	Сервер загружается с внешнего накопителя. На экране KVM-консоли отображается процесс загрузки сервера с компакт-диска.	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ.

			Ожидаемый результат не получен: произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
5.2	На запросы программы-установщика ОС необходимо задать следующие параметры: Шаг 1. Выбрать язык программы установщика – русский. Шаг 2. Выбор местонахождения – Российская Федерация. Шаг 3. Настройка клавиатуры – Russian. Шаг 4. Раскладка клавиатуры – Russian. Шаг 5. Выбор способа переключения раскладки – Alt + Shift Шаг 6. Настройка сети. Указать необходимые значения IP-адреса, маски подсети, шлюза, DNS-сервера (см рисунок 2). Шаг 6. Ввести имя компьютера – act. Шаг 7. Ввести имя нового пользователя – weeebz. Шаг 8. Ввести пароль нового пользователя – webbez. Шаг 9. Выбрать «не шифровать домашний каталог». Шаг 10. Разметка дисков. Выбрать пункт – «Авто – использовать весь диск». Шаг 11. В качестве дополнительных устанавливаемых пакетов выбрать – «OpenSSH server».	ОС установлена.	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
6	**Установка дополнительных пакетов**		
6.1	Шаг 1. Установить веб-сервер Apache: apt-get install apache2 Шаг 2. Установить интерпретатор PHP5 и необходимые модули: pt-get install php php-cli libapache2-mod-php curl libcurl3 libcurl3-dev php-curl php-gd libjson0 libjson0-dev php-sqlite php-sqlite3 php-mysql Шаг 3. Установить модули Perl: apt-get install libxml-perl libxml-writer-perl libstring-random-perl libmime-perl libdata-random-perl libxml-simple-perl perlbrew Шаг 4. Установить модули Python:	В системе установлен перечисленные компоненты. В процессе установки базы данных mysql ввести логин root и пароль dkDf87_#1	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не получен:**

	apt-get install python-lxml python-mechanize python-pip python-dev libxml2 libxml2-dev libxslt-dev Шаг 5. Установить базу данных sqlite3: apt-get install sqlite3 Шаг 6. Установить модуль PHP для работы с базой данных sqlite3: apt-get install php-sqlite php- Шаг 7. Установить текстовый редактор mc: apt-get install mc Шаг 8. Установить базу данных mysql: apt-get install mysql-server mysql-client php-mysql Шаг 9. Установить базу данных mysql: apt-get install mysql-server mysql-client php-mysql Шаг 10. Установить дополнительные библиотеки perl: perlbrew init perlbrew install perl-5.18.2 pip install MechanicalSoup pip install mechanize perl -MCPAN -e 'install Bundle::Bugzilla' perl -MCPAN -e 'install XML::Writer' perl -MCPAN -e 'install XML::Simple' perl -MCPAN -e 'install String::Random' Шаг 11. Установить socks, proxy сервера и клиенты: apt-get -y install torsocks tor privoxy		произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
7	**Проверка сетевых настроек**		
7.1	Проверить настройку сетевого оборудования. Для этого после установки ОС, в терминале выполнить команду ping 8.8.8.8	Пакеты с данными успешно отправляются и принимаются.	
8	**Конфигурирование ОС**		
8.1	Активация учетной записи root. Шаг 1. Перейти под супер-пользователя путем выполнения команды: sudo su Шаг 2. Задать пароль супер-пользователю: passwd Шаг 3. Активировать удаленный доступ по ssh под супер-пользователем:	Учетная запись root активна. Удалось зайти по ssh под логином root.	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ.

	В конфигурационном файле /etc/ssh/sshd_config значение параметра PermitRootLogin выставить «yes»		**Ожидаемый результат не получен:** произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
9	**Установка СПО**		
9.1	Шаг 1. Копировать в домашнюю директорию архив webbez-API.tar.gz с внешнего накопителя. Шаг 2. Распаковать архив webbez-API.tar.gz: tar –xzf webbez-API.tar.gz Шаг 3. Копировать из него директории «wb20» «webbez-VA» в каталог /var/www: cp –r var_www/* /var/www/	Все компоненты СПО уставлены (На жестком диске появятся папки /var/www/wb20, /var/www/webbez-VA).	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не получен:** произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
10	**Настройка СПО**		
10.1	Шаг 1. Открыть файл «/var/www/api-exec-blank/application/config/config.php» в mcedit и настроить с помощью команды: mcedit /var/www/webbez-VA/webbez20/api-exec-blank/application/config/config.php В поле $config['base_url'] = 'http://ip-адрес-webbez-API/api-exec-blank/'; где «ip-адрес-webbez-API» – это адрес текущего сервера, на котором настраивается сервер webbez (см. рисунок 2). Шаг 2. Открыть файл «/var/www/api-control/application/config/config.php» в mcedit и настроить с помощью команды:	СПО настроено.	**Получен ожидаемый результат:** произвести запись в журнале работ; переход к следующему пункту плана работ. **Ожидаемый результат не**

	mcedit /var/www/wb20/WBapplication/config/config.php В поле $config['base_url'] = 'http://ip-адрес-webbez-API/api-control/'; где «ip-адрес-webbez-API» – это адрес текущего сервера, на котором настраивается сервер webbez (см. рисунок 2). Шаг 3. Изменить владельца скопированной директории с помощью команды: cd /var/www && sudo chown -R www-data:www-data ./* Шаг 4. Копировать файл api из каталога webbez-API в директорию /etc/apache2/sites-available и подключить сайт к серверу Apache cd cp webbez-API/api.conf /etc/apache2/sites-available/lavina.conf a2dissite 000-default.conf a2ensite lavina.conf Шаг 5. Перезагрузить Apache service с помощью команды: service apache2 restart Шаг 6. Прописать ip-адрес управляющего сервера, с которого будут делаться запросы в конфигурационный файл «/var/www/api-control/application/APIDB/servers-ip.ini» с помощью команды: mcedit /var/www/api-control/application/APIDB/servers-ip.ini {"server-main":{"domain":"127.0.0.1/webbez20/","port":"80","protocol":"http","path":"/api-exec-express/index.php/serverexec11/","ip":["ip_адрес_клиента"]}} где «ip_адрес_клиента» – это адрес управляющего сервера, с которого будут производиться запросы (см. рисунок 2). Шаг 7. Прописать демона для созданной директории в автозагрузку с помощью команды: crontab –e 0-59/2 * * * * php /var/www/api-exec-express/application/APIDB/apiDaemon_permament.php 0-59/2 * * * * php /var/www/api-exec-express/application/APIDB/apiDaemon_v1.4.php		**получен:** произвести запись в журнале работ; доклад инженеру-координатору; прекращение работ до получения указаний от координатора работ.
11	**Финальная проверка**		
11.1	Проверить доступность API. Для этого сделать тестовый запрос с сервера, адрес которого прописан в файле servers-ip.ini с помощью команды: curl http://ip-адрес-webbez-API/api-control/index.php/server/list (список доступных серверов)	Ответ, что сервер «server-main» доступен, получен.	**Получен ожидаемый результат:** произвести запись в журнале работ; настройка завершена.

			Ожидаемый результат не получен: произвести запись в журнале работ; устранение неисправностей - проверка корректности вводимой информации согласно руководству; доклад инженеру-координатору; при невозможности устранения недостатков – прекращение работ до получения указаний от координатора работ.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

ПТЭЭП − правила технической эксплуатации электроустановок потребителей;
ПУЭ − правила устройства электроустановок;
СПО − специальное программное обеспечение