**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»

Институт компьютерных технологий и защиты информации

### **КАФЕДРА СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

### **к выполнению лабораторной работы № 1**

на тему

**«**Настройка средств защиты и средств анализа защищенности web-приложений от типовых сетевых атак**»**

Казань 2021

Методические указания к выполнению лабораторной работы по изучению средств защиты и средств анализа защищенности web-приложений от типовых сетевых атак

**Тема:**

Средства защиты и средства анализа защищенности web-приложений от типовых сетевых атак.

**Цель:**

Получить навык работы со средствами защиты и средствами анализа защищенности web-приложений от типовых сетевых атак.

**Программно-аппаратные средства:**

Компьютерная лаборатория с установленным ПО виртуализации VMware Player, ПО анализатор кода Positive Technologies Application Inspector (PT AI), ПО сканер уязвимостей web-приложений Acunetix WVS. На платформе виртуализации работает 2 виртуальные машины:

* Межсетевой экран прикладного уровня Positive Technologies Application Firewall (PT AF);
* Сервер с развернутым уязвимым web-приложением OWASP Mutillidae.

3.2.1 Теоретическая часть

**Средства защиты web-приложений**

Общедоступные web-приложения являются привлекательной мишенью для злоумышленников. Атаки на web-приложения открывают перед ними широкие возможности: доступ к внутренним ресурсам компании, чувствительной информации, нарушение функционирования приложения или обход бизнес-логики – практически любая атака может принести финансовую выгоду для злоумышленника и убытки, как финансовые, так и репутационные – для владельца web-приложения. Кроме того, под угрозой находятся и пользователи web-приложений, поскольку успешные атаки позволяют похищать учетные данные, выполнять действия на сайтах от лица пользователей, а также заражать рабочие станции вредоносным ПО.

Традиционно используемые технологии обеспечения сетевой безопасности определенно играют роль в защите важных для организации web-приложений. Тем не менее, важно понимать, что у них есть ограничения и в одиночку они не могут обеспечить достаточный уровень защиты.

Межсетевой экран, работающий на уровне web-приложений (**Web Application Firewall, WAF**), срабатывает там, где другие технологии обеспечения безопасности прекращают работать, обеспечивая защиту от угроз, действующих на более высоких уровнях стека вычислений. Автоматизированные процессы обучения, дополненные вручную сконфигурированными политиками, приводят к более точному «пониманию» того, как работает каждое защищенное web-приложение, включая все пользовательские характеристики и бизнес-логику. Последовательно обнаруживаемые отклонения представляют собой вредоносный трафик, который автоматически ликвидируется – например блокируется, разрешается с ограничениями или регистрируется – в соответствии с определенными администратором политиками.

К преимуществам WAF относятся следующие способности:

* проверять достоверность вводимой информации, тем самым предотвращая опасные SQL-инъекции, межсайтовый скриптинг и атаки в обход каталога;
* выявлять атаки, фальсифицирующие файлы cookies, сессии или параметры;
* блокировать атаки, использующие уязвимости в пользовательском ПО;
* полностью проверять трафик с SSL-шифрованием на наличие всех типов угроз;
* предотвращать угрозы, использующие логические лазейки в пользовательских бизнес-приложениях;
* обеспечивать защиту от атак типа «отказ в обслуживании» (DoS) и «распределенный отказ в обслуживании» (DDoS) на прикладном уровне;
* динамично маскировать информацию об отклике сервера, которая является потенциально полезной для хакеров;
* обеспечивать комплексную XML-защиту, включая валидацию схем для сообщений SOAP и защиту от инъекций XPath, и идентифицировать/блокировать XML-вложения, скрывающие вредоносный контент;
* обеспечивать соответствие требованию 6.6 стандарта безопасности данных в индустрии платежных карт (Payment Card Industry Data Security Standard (PCI DSS).

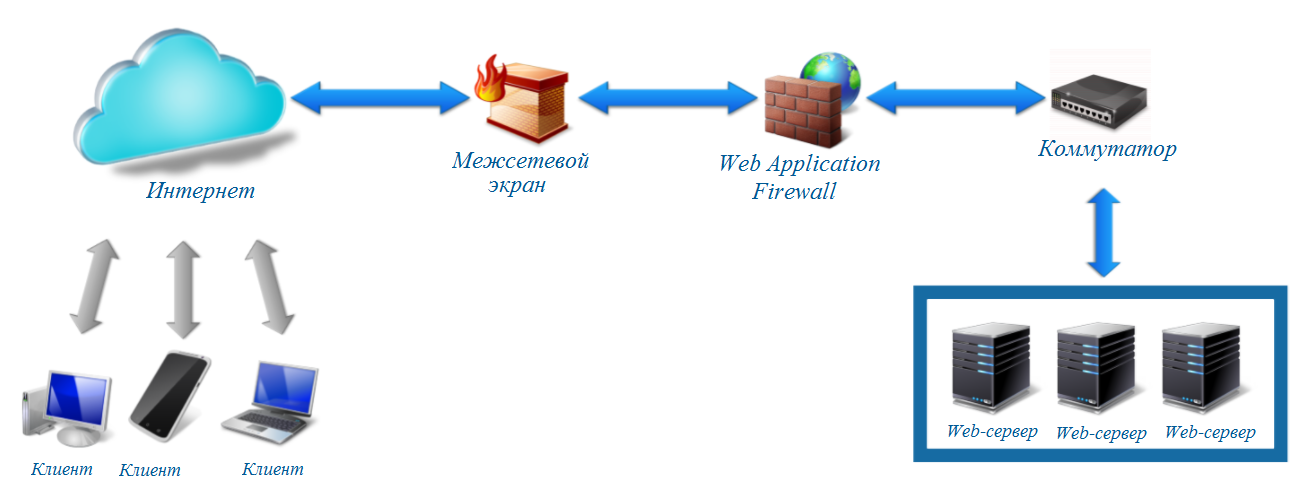
Как правило, WAF размещают в режиме обратного прокси-сервера (трафик проходит через WAF, который активно обнаруживает и предотвращает атаки) перед защищаемыми web-серверами (Рис.3.1). В зависимости от производителя могут поддерживаться и другие режимы работы – например, прозрачный прокси-сервер, мониторинг (маршрутизатор создает копию трафика для WAF, который обнаруживает потенциальные угрозы и предупреждает о них используемые клиентом системы безопасности) или даже автономный режим (WAF изучает системные журналы на предмет наличия в них следов атак, что может быть использовано при расследовании инцидентов).

Рис.3.1. Схема работы WAF в режиме блокирования атак (обратного прокси)

Для обнаружения и предотвращения web-атак и сокращения риска ложных срабатываний WAF применяет две модели безопасности: запрещающую (negative security model) для блокировки известных атак и положительную (positive security model), при которой используется только разрешенный трафик.

В данной лабораторной работе ознакомимся с решением WAF, представленным компанией Positive Technologies – **Positive Technologies Application Firewall (PT AF)**.

**PT AF** использует всестороннюю схему защиты со множеством специализированных модулей и механизмов:

* HMM – самообучающийся модуль для блокировки атак нулевого дня;
* WAF.js – JavaScript-модуль для защиты от атак на стороне клиента (XSS, DOM XSS, CSRF, Clickjacking), запускающийся в браузере пользователя при каждом открытии защищаемой страницы;
* P-Code – модуль, выявляющий уязвимости в исходном коде приложения и автоматически формирующий правила для блокировки атак (виртуальные патчи);
* М-Scan – модуль для автоматического сканирования загружаемых и скачиваемых пользователями файлов на антивирусных ядрах;
* Пассивный сканер – идентифицирует в пассивном режиме компоненты приложений (CMS, фреймворки, библиотеки) для настройки модуля нормализации и обнаружения утечки данных, а также известных уязвимостей на базе словаря CVE;
* ­ Rule Engine – механизм для самостоятельного создания правил, в том числе для всех известных уязвимостей из словаря CVE;
* SOA Firewall – модуль анализа XML для противодействия атакам на распределенные web-сервисы. ­
* Механизм нормализации – переписывает данные и заголовки HTTP-запросов с учетом специфики защищаемого сервера. Это позволяет противодействовать большинству методов обхода межсетевого экрана (HPC, HPP, Verb Tampering и др.).

**Средства анализа защищенности web-приложений**

Анализ защищенности web-приложений позволяет снизить риски информационной безопасности путем своевременного обнаружения и устранения уязвимостей web-приложений.

Средства анализа защищенности web-приложений выполняют анализ и тестирование web-приложений с использованием нескольких методов:

* Static AST (SAST): статическое сканирование безопасности приложений, при котором осуществляется анализ исходного кода web-приложения, как правило, на стадиях его программирования и тестирования;
* Dynamic AST (DAST): динамическое сканирование безопасности приложений, при котором осуществляется анализ рабочего web-приложения;
* Interactive AST (IAST): интерактивное сканирование безопасности приложений, при котором осуществляется анализ приложений с помощью комбинированного подхода (с использованием SAST и DAST).

В данной лабораторной работе ознакомимся с двумя решениями по анализу защищенности web-приложений: с продуктом компании Positive Technologies – **Positive Technologies Application Inspector (PT AI)**, комбинирующим статические, динамические и интерактивные методы (SAST, DAST и IAST) анализа, и с продуктом компании Acunetix – **Acunetix Web Vulnerability Scanner (Acunetix WVS)**, использующим динамический (DAST) метод анализа.

Схема работы продукта **PT AI** представлена на рисунке (Рис.3.2).

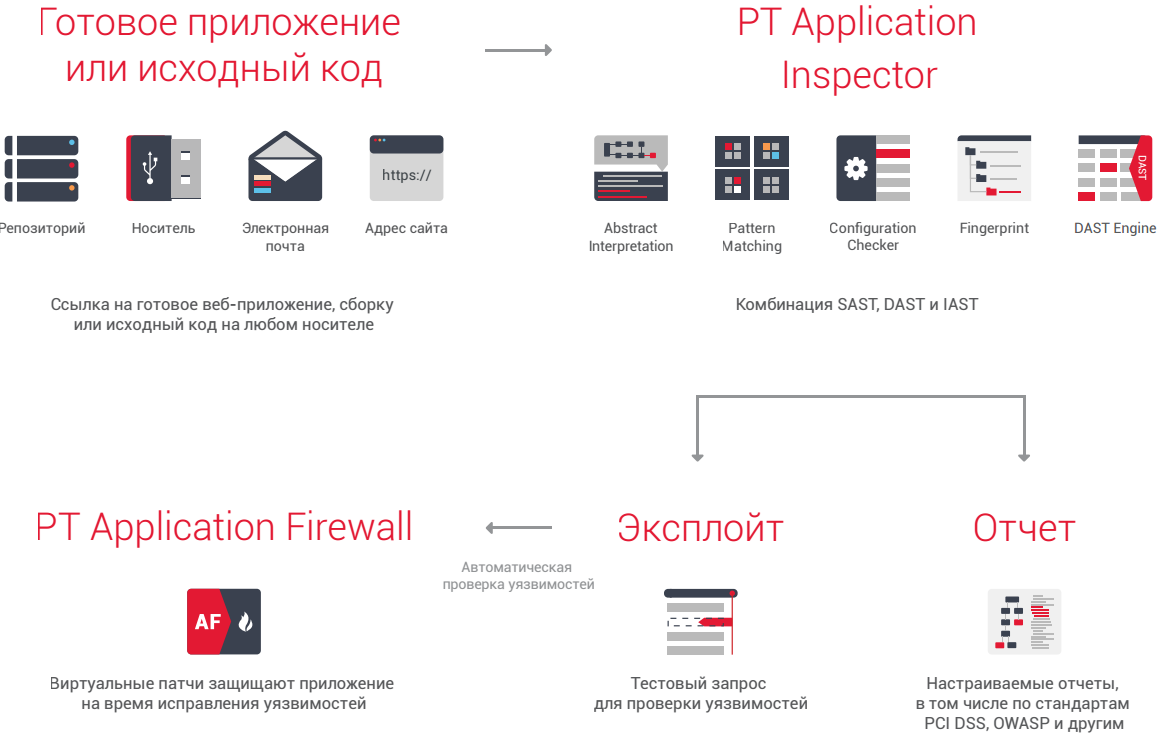


Рис.3.2. Схема работы продукта PT AI

К основным преимуществам продукта **PT AI** можно отнести:

* за счет комбинации DAST, SAST и IAST, анализа контекста и конфигураций серверов и приложений значительно уменьшается число ложных срабатываний, что позволяет радикально снижать затраты экспертов на ручную проверку результатов;
* может анализировать код на самых ранних стадиях разработки, при этом команды контроля качества оповещаются о небезопасном коде до того, как его начнут эксплуатировать, что снижает риски атак и стоимость проверки соответствия стандартам безопасности;
* работает со множеством платформ и языков, включая PHP, Java, .NET, SAP ABAP, HTML/JavaScript и SQL, а также со всеми типами уязвимостей приложений, включая SQLi и XXS;
* функция генерации эксплойтов демонстрирует риски уязвимостей на практических примерах, позволяя ставить четкие задачи для исправления кода;
* адаптация к бизнес-логике приложения позволяет выявлять закладки, оставленные в коде разработчиками или хакерами (выявление признаков НДВ);
* поддерживает интеграцию с системой защитой PT AF: эксплойты, которые генерирует продукт, позволяют межсетевому экрану создавать виртуальные исправления и защищать приложения, пока разработчики будут устранять уязвимости программного обеспечения;
* соответствует требованиям стандарта ЦБ РС БР ИББС-2.6-2014, приказов ФСТЭК № 17 и 21, стандарта PCI DSS.

Продукт **Acunetix WVS** работает следующим образом:

1. **Acunetix WVS** исследует и формирует структуру web-приложения, обрабатывая все найденные ссылки и собирая информация обо всех обнаруженных файлах;
2. Затем программа тестирует все web-страницы с элементами для ввода данных, моделируя ввод данных с использованием всех возможных комбинаций и анализируя полученные результаты;
3. Обнаружив уязвимость, **Acunetix WVS** выдает соответствующее предупреждение, которое содержит описание уязвимости и рекомендации по ее устранению;
4. Итоговый отчет **Acunetix WVS** может быть записан в файл для дальнейшего анализа и сравнения с результатами предыдущих проверок.

В качестве web-приложения для тестирования было выбрано уязвимое web-приложение **OWASP Mutillidae**. OWASP Mutillidae – это бесплатное, с открытым исходным кодом, намеренно уязвимое веб-приложение, предназначенное для тренировки в поиске и эксплуатации различных уязвимостей и тестирования средств защиты и анализа защищенности web-приложений. Проект Mutillidae реализовывает уязвимости, которые описаны в OWASP Top 10. По каждой из уязвимостей из OWASP Top 10 доступно несколько заданий, сопровождающихся подсказками. Также есть возможность переключать уровень защищенности данного web-приложения.

Схема лабораторного комплекса выглядит следующим образом:

Рис.3.3. Схема лабораторного комплекса

**Задание:**

1. Изучить теоретическую часть;
2. Провести атаки на уязвимое web-приложение OWASP Mutillidae;
3. Провести сканирование уязвимого web-приложение OWASP Mutillidae анализатором кода PT AI;
4. Выполнить настройку межсетевого экрана прикладного уровня PT AF;
5. Выполнить виртуальный патчинг, загрузив результаты сканирования на PT AF;
6. Провести атаки на уязвимое web-приложение OWASP Mutillidae для проверки правильности настроек PT AF;
7. Просканировать уязвимое web-приложение OWASP Mutillidae, защищенное межсетевым экраном прикладного уровня PT AF;
8. Сгенерировать отчет по работе межсетевого экрана прикладного уровня PT AF;
9. Подготовить отчет о выполненной работе;
10. Ответить на контрольные вопросы.

3.2.2 Инструкция к выполнению заданий

**Атака на уязвимое web-приложение OWASP Mutillidae**

Проэксплуатировать уязвимость web-приложения OWASP Mutillidae, выполнив атаку типа SQL инъекция на него. Для этого необходимо:

1. Запустить браузер и перейти по адресу <ip-адрес web-приложения>;
2. Перейти на вкладку OWASP 2013 > A1 – Injection (SQL) > SQLi - Extract data > User Info (SQL) (Рис.3.1);

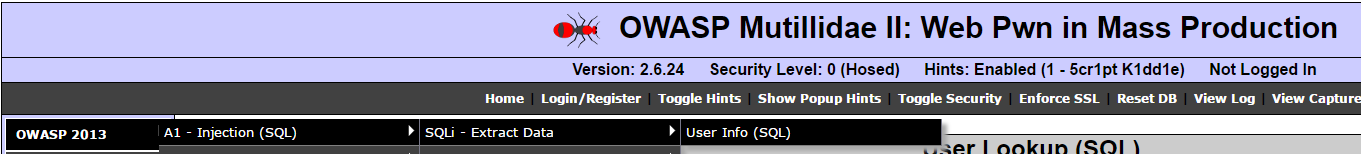


Рис.3.1. Приложение Mutillidae

1. Ввести в поле Name символ «'» и нажать View Account details (Рис.3.2). Обратить внимание на появившееся сообщение об ошибке синтаксиса (Рис.3.3). Это говорит о том, что поле уязвимо к инъекции;
2. Использовать SQL-инъекцию путем расширения условий, ввести в поле Name выражение «**' OR 1=1 #»** и нажать View Account details;
3. Убедиться, что на экран выведена таблица, содержащая учетные данные пользователей (Рис.3.4);
4. Самостоятельно реализовать атаку типа Cross Site Scripting.

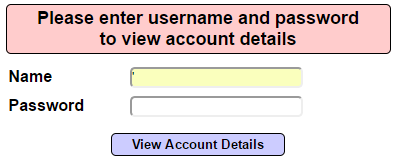


Рис.3.2. Форма авторизации

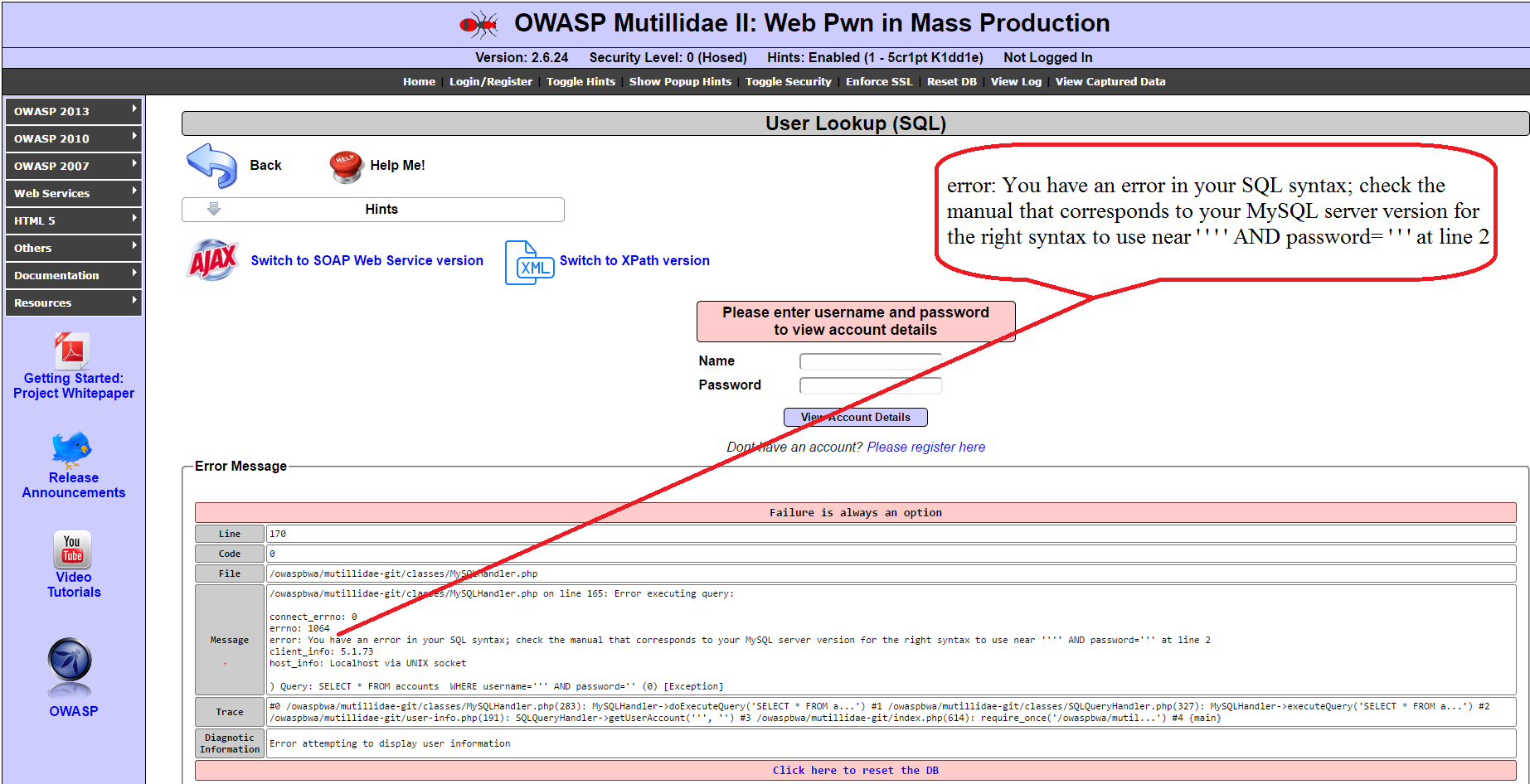


Рис.3.3. Ошибка SQL синтаксиса



Рис.3.4. Таблица учетных данных пользователей

**Сканирование уязвимого web-приложение OWASP Mutillidae анализатором кода PT AI**

1. Запустить PT AI;
2. Нажать кнопку «Проекты» и создать новый проект с названием «Mutillidae» (Рис.3.5);
3. В проекте «Mutillidae» создать новое сканирование, нажав кнопку «Настроить новое сканирование»;
4. В появившемся окне задать настройки сканирования:

* В разделе «Объект сканирования» выбрать каталог, в котором расположены исходные файлы приложения Mutillidae (Рис.3.6);
* В разделе «Основные настройки» выбрать язык приложения и указать ip-адрес web-приложения Mutillidae (Рис.3.6);
* В разделе «Технические настройки сканирования» поставить галочку напротив опции Black-поиска, остальные настройки раздела оставить без изменений (Рис.3.6);

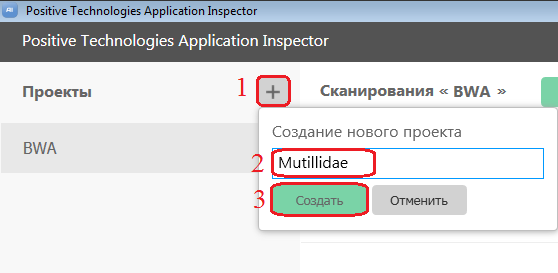


Рис.3.5. Создание нового проекта

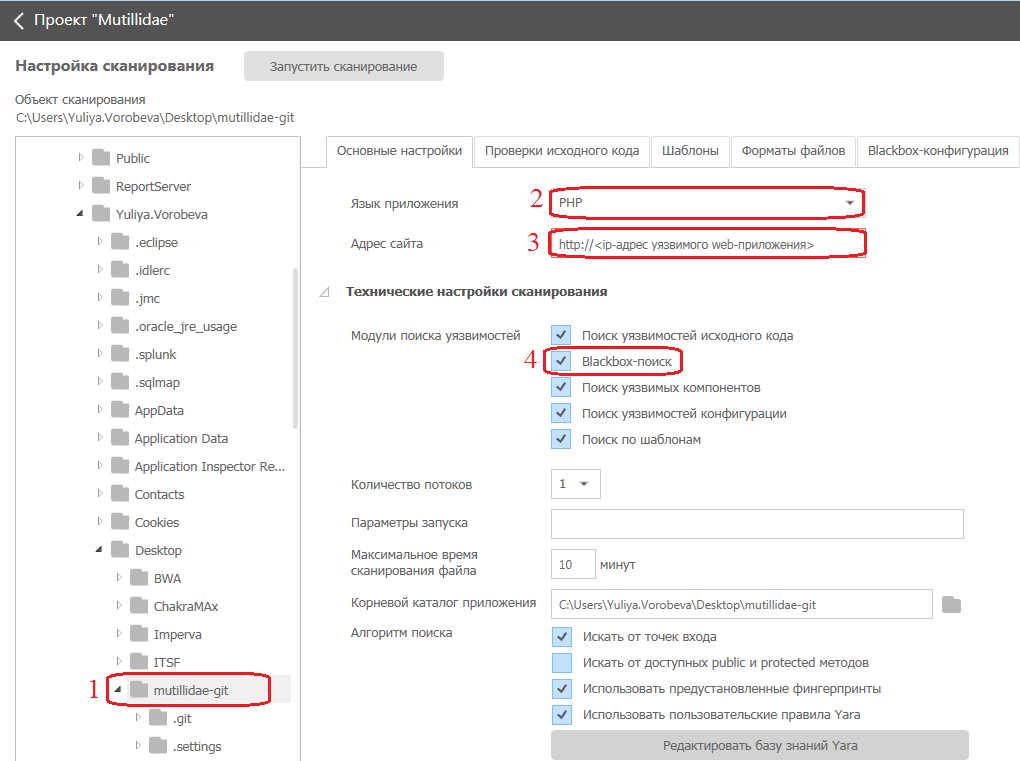


Рис.3.6. Основные настройки сканирования

* Перейти на вкладку «Шаблоны» и поставить галочку «Positive Technologies» для применения всех имеющихся шаблонов (Рис.3.7);

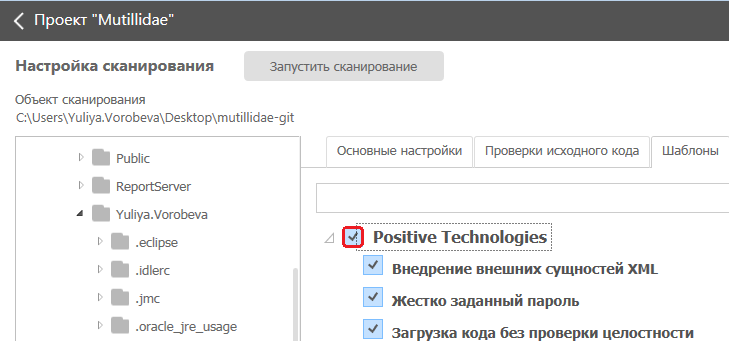


Рис.3.7. Настройки шаблонов сканирования

* Перейти на вкладку Blackbox-конфигурация и указать режим поиска Быстрый (Рис.3.8);

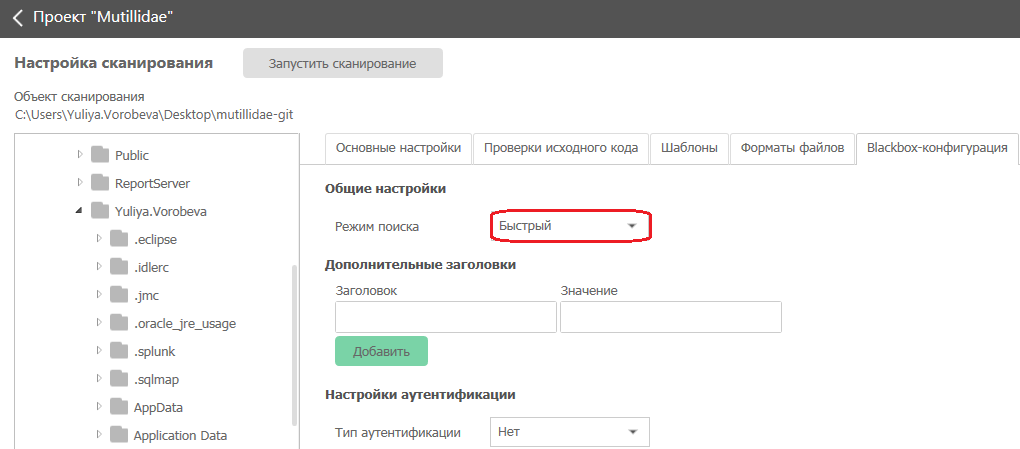


Рис.3.8. Настройка Blackbox-конфигурации сканирования

1. Запустить сканирование, нажав кнопку «Запустить сканирование»;
2. Ознакомиться с результатами сканирования, выгрузить отчет, нажав кнопку «Отчет по результатам сканирования»;
3. Сделать выводы относительно степени уязвимости приложения.

**Настройка межсетевого экрана прикладного уровня PT AF**

1. Войти в локальную консоль PT AF с использованием учетных данных, заданных по умолчанию (имя пользователя – «pt», пароль – «p0s1t1v3»), сменить пароль и произвести первоначальную настройку PT AF.
2. В рамках первоначальной настройки PT AF выполнить базовую настройку сетевых интерфейсов PT AF с использованием конфигурационного скрипта *wsc*:

* Запустить конфигурационный скрипт, набрав в локальной консоли команду:

*sudo wsc*;

* Назначить интерфейсам (eth0, eth1) режим работы командой:

*if mode <interface> static*;

* Назначить интерфейсам (eth0, eth1) правильные IP-адреса и маски подсети (выданные преподавателем) командой:

*if set <interface> inet\_address <addr> inet\_netmask <netmask>*;

* Настроить шлюз по умолчанию командной:

*route add default via <ip-адрес шлюза по умолчанию> dev eth0;*

* Пометить интерфейсы (eth0, eth1) командой mark, для их доступности в web-консоли управления PT AF:

*if mark <interface>*;

* Применить конфигурацию командой:

*config commit*;

* Сохранить конфигурацию для отображения в web-консоли управления PT AF командой:

*config sync.*

1. Подключиться к web-консоли управления PT AF, обратившись по протоколу HTTPS на IP-адрес, назначенный на управляющий интерфейс (eth0) по 8443 порту. Имя пользователя по умолчанию для web-консоли управления PT AF – «admin», пароль – «p0s1t1v3». После подключения необходимо сменить пароль.
2. Настроить режим блокирования атак (обратного прокси):

Шаг 1: создать роль MGMT на вкладке **Конфигурация → Сеть → Алиасы сетевых интерфейсов** (Рис.3.9);

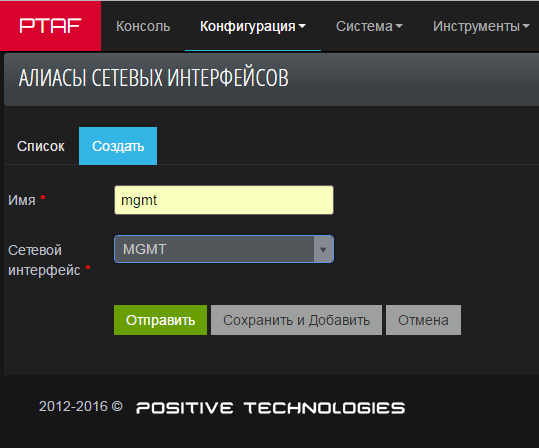


Рис.3.9. Создание роли MGMT

Шаг 2: назначить роль MGMT на управляющий интерфейс (eth0) на вкладке **Конфигурация → Сеть → Шлюзы→ Сеть** (Рис.3.10);

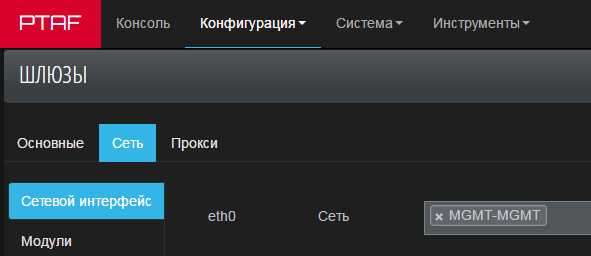


Рис.3.10. Назначение роли MGMT

Шаг 3: создать роль WAN на вкладке **Конфигурация → Сеть → Алиасы сетевых интерфейсов**;

Шаг 4: отредактировать созданную роль WAN, добавив открытые порты, разрешённые для подключения пользователей web-приложения (9999/TCP) (Рис.3.11);

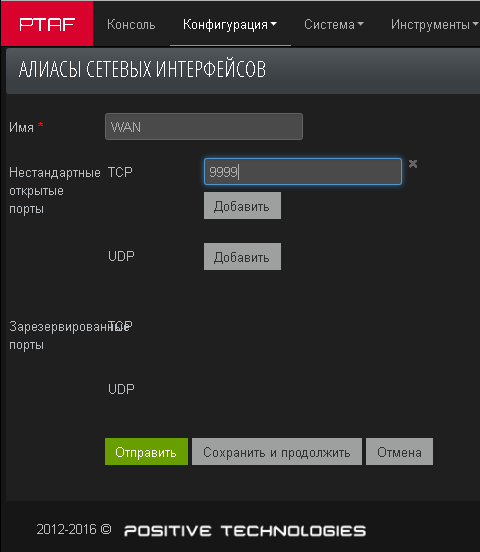


Рис.3.11. Настройка роли WAN

Шаг 5: назначить роль WAN на интерфейс eth1 на вкладке **Конфигурация → Сеть → Шлюзы→ Сеть**;

Шаг 6: создать группу серверов защищаемых web-приложений, на вкладке **Конфигурация → Сеть → Группы серверов**, указав имя группы (Mutillidae) и IP-адрес сервера защищаемого web-приложения (Рис.3.12);

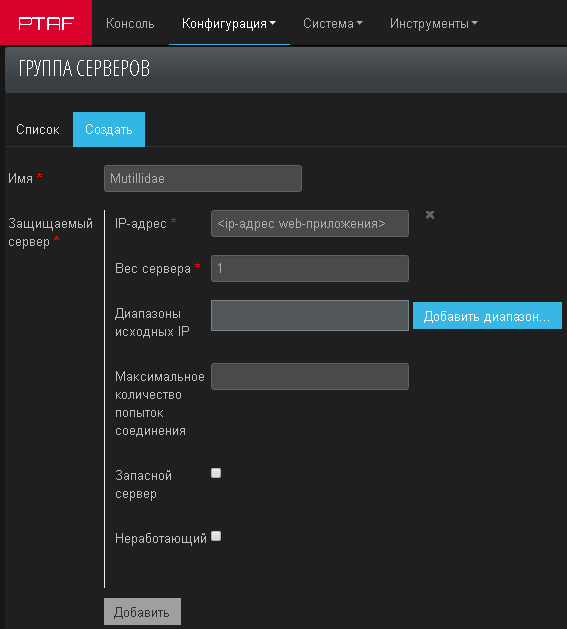


Рис.3.12. Создание группы серверов защищаемых web-приложений

Шаг 7: создать политику для защищаемого web-приложения, на вкладке **Конфигурация → Безопасность → Политики,**  нажав кнопку Создать. В появившемся окне указать имя политики (Mutillidae), шаблон для предустановленных политик (Generic) и ПО защищаемого сервера (PHP/Apache) (Рис.3.13);

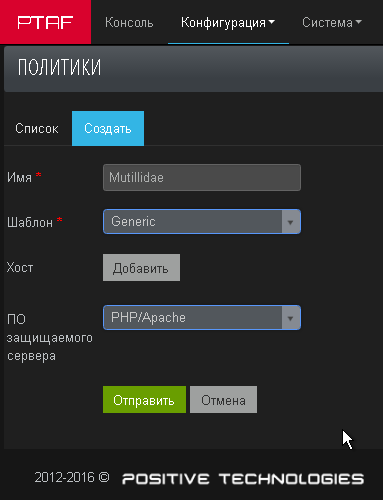


Рис.3.13. Создание политики для защищаемого web-приложения

Шаг 8: отредактировать созданную политику, указав на вкладке Прокси интерфейс, на котором будет открыт порт (WAN), порт, который будет открыт для входящих соединений (9999/TCP); группу серверов защищаемых приложений, на которую будут перенаправляться запросы в режиме работы обратного прокси (Mutillidae). Установить флажок Сервер по умолчанию, чтобы политика обрабатывала запросы на указанный порт и все имена узлов, не заданные в других политиках (Рис.3.14);

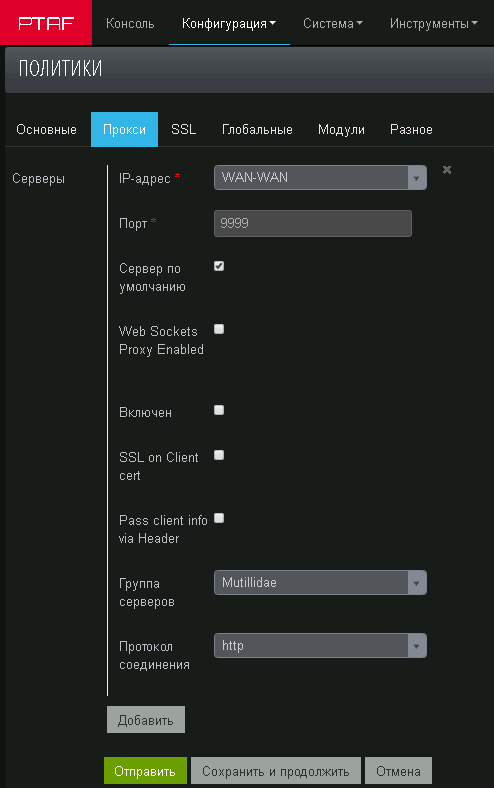


Рис.3.14. Настройка вкладки Прокси

Шаг 9: перейти на вкладку Модули созданной политики и ознакомиться с настройками параметров защитных модулей;

Шаг 10: активировать межсетевой экран, установив флажок Активен на вкладке **Конфигурация → Сеть → Шлюзы → Основные** (Рис.3.15).

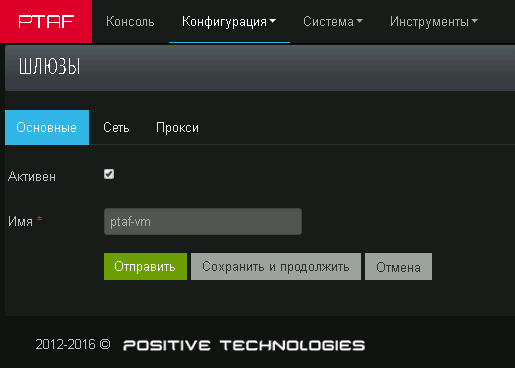


Рис.3.15. Активация межсетевого экрана

1. Убедиться в корректности работы режима обратного прокси, обратившись к web-приложению по адресу <ip-адрес WAN интерфейса>:9999.

**Виртуальный патчинг**

1. Подключиться к web-консоли управления PT AF;
2. Перейти на вкладку **Инструменты → Виртуальный патчинг**;
3. Нажать кнопку Импортировать, чтобы загрузить отчет, полученный ранее в программе PT AI;
4. В появившемся окне «Импортировать отчет Application Inspector» нажмите кнопку Выберите файл, укажите путь к XML-файлу отчета (afreport.xml), укажите политику Mutillidae и нажмите кнопку Импортировать (Рис.3.16);
5. После загрузки файла нажать кнопку Просмотр, ознакомиться с результатом работы виртуального патчинга (Рис.3.17);
6. Проанализировать правила, созданные для закрытия уязвимостей.

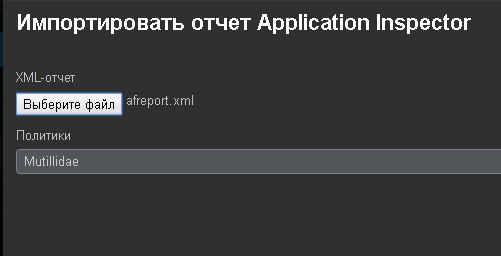


Рис.3.16. Импорт отчета PT AI

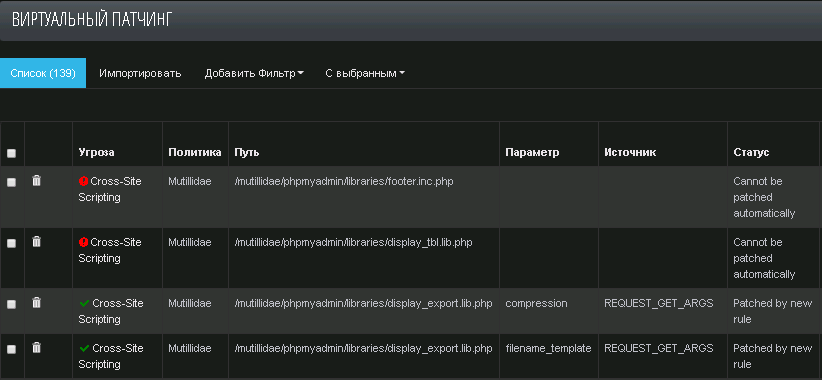


Рис.3.17. Список записей виртуального патчинга

**Атака на уязвимое web-приложение OWASP Mutillidae для проверки правильности настроек PT AF**

1. Выполнить попытку атаки, рассмотренной в 1 задании лабораторной работы;
2. Убедиться в том, что атака была заблокирована межсетевым экраном PT AF (Рис.3.18);



Рис.3.18. Запрос, заблокированный PT AF

1. Подключиться к web-консоли управления PT AF, перейти на вкладку Консоль;
2. В списке ATTACKS найти соответствующее проведенной атаке событие, убедиться, что сработала установленная политика (Mutillidae), ознакомиться с полями события (Рис.3.19);

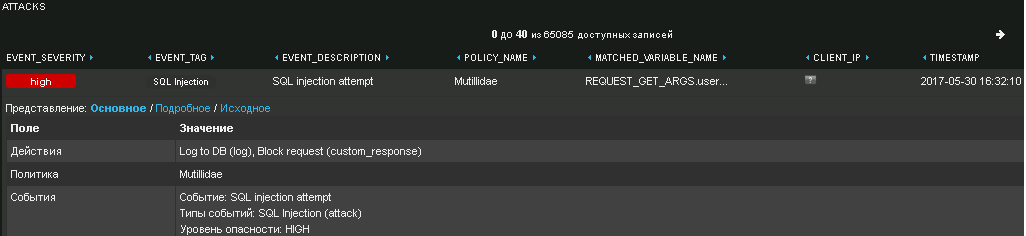


Рис.3.19. Событие, зарегистрированное PT AF

**Сканирование уязвимого web-приложения OWASP Mutillidae, защищенного межсетевым экраном прикладного уровня PT AF**

1. Запустить сканер уязвимостей web-приложений Acunetix;
2. Создать новое сканирование, нажав кнопку New Scan;
3. В появившемся окне Scan Wizard задать настройки сканирования, выбрав тип сканирования «Scan single website» и указав URL web-сайта (https://<ip-адрес WAN интерфейса>:9999/mutillidae) (Рис.3.20);
4. Все остальные настройки оставить по умолчанию без изменений, запустить сканирование;
5. Подключиться к web-консоли управления PT AF, перейти на вкладку Консоль;

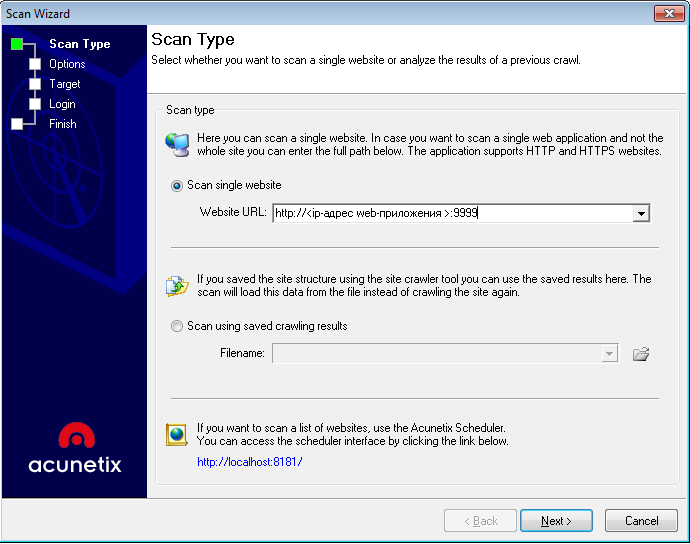


Рис.3.20. Настройки сканирования

1. Проанализировать события, появившиеся в списке ATTACKS (Рис.3.21);

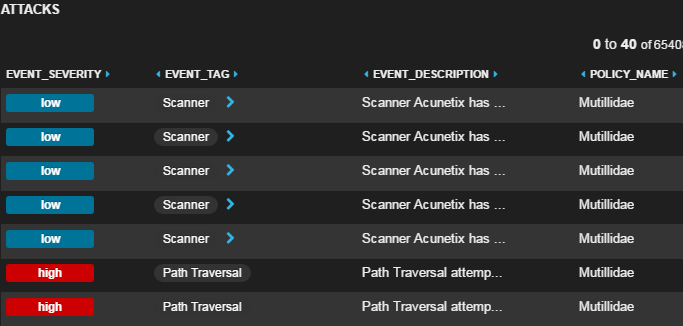


Рис.3.21. События, зарегистрированные PT AF во время сканирования

1. Ознакомиться с инцидентом, появившемся в списке ALERTS (Рис.3.22);

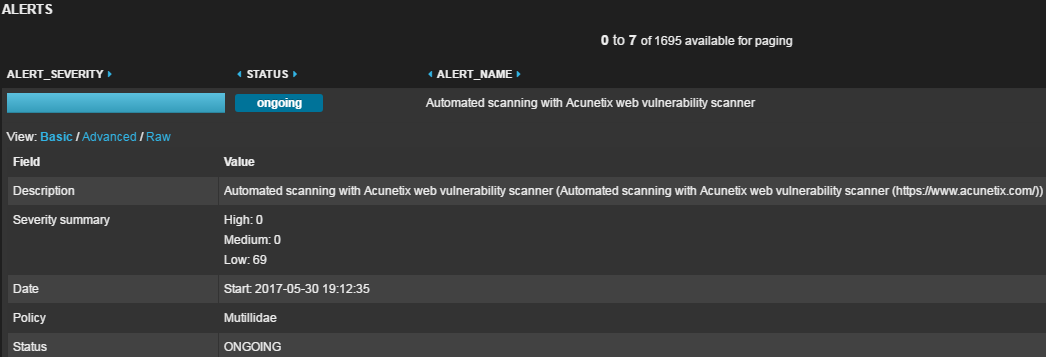


Рис.3.22. Инцидент, зарегистрированный PT AF во время сканирования

1. Проанализировать результаты сканирования сканером уязвимостей web-приложений Acunetix, сделать выводы.

**Генерация отчета по работе межсетевого экрана прикладного уровня PT AF**

1. Подключиться к web-консоли управления PT AF;
2. Перейти на вкладку **Инструменты → Отчеты → Шаблоны отчетов,** нажать кнопку Создать;
3. В появившемся окне задать имя шаблона отчетов (PT\_AF\_lab), выбрать его формат (PDF), указать дополнительные параметры шаблона (по выбору) и нажать кнопку Отправить (Рис.3.23);
4. Перейти на вкладку **Инструменты → Отчеты → Расписание отчетов,** нажать кнопку Создать;
5. В появившемся окне указать время начала генерации отчета (Прямо сейчас), имя отчета (PT\_AF\_Фамилия студента), выбрать период данных (Последний час) и шаблон (созданный ранее PT\_AF\_lab), и нажать кнопку отправить (Рис.3.24);

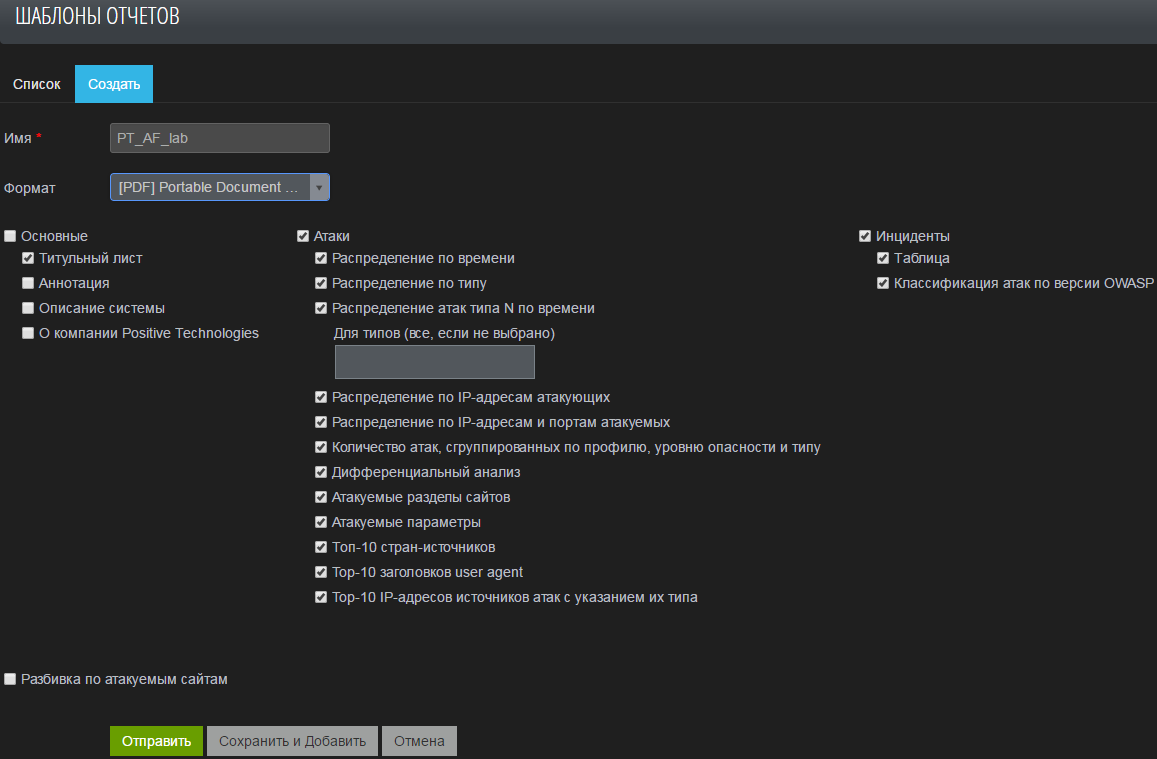


Рис.3.23. Создание шаблона отчетов

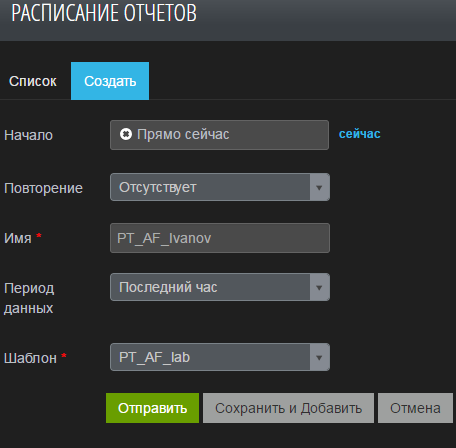


Рис.3.24. Создание расписания отчетов

1. Перейти на вкладку **Инструменты → Отчеты → Отчеты**, найти в каталоге сгенерированный отчет и нажать на его имя, чтобы выгрузить его на диск (Рис.3.25).
2. Проанализировать содержание отчета, сделать выводы об атаках, заблокированных PT AF.

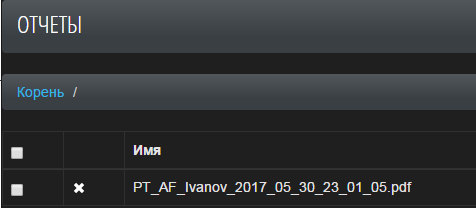


Рис.3.25. Каталог отчетов

3.2.3 Шаблон отчета по лабораторной работе

**Тема:**

Средства защиты и средства анализа защищенности web-приложений от типовых сетевых атак.

**Цель:**

Получить навык работы со средствами защиты и средствами анализа защищенности web-приложений от типовых сетевых атак.

**Выполнил**

Студент гр. № \_\_\_\_\_\_

ФИО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Отчет**

**Атака на уязвимое web-приложение OWASP Mutillidae**

Снимки экрана с результатами проведения атаки типа SQL инъекция и атаки типа Cross Site Scripting.

**Сканирование уязвимого web-приложение OWASP Mutillidae анализатором кода PT AI**

Снимки экрана с результатами сканирования, отчет по результатам сканирования в формате XML, выводы по анализу отчета.

**Настройка межсетевого экрана прикладного уровня PT AF**

Снимки экрана с конфигурацией PT AF.

**Виртуальный патчинг**

Снимки экрана с результатами работы виртуального патчинга, выводы по анализу созданных правил.

**Атака на уязвимое web-приложение OWASP Mutillidae для проверки правильности настроек PT AF**

Снимки экрана с заблокированным запросом и с событием, зарегистрированным PT AF.

**Сканирование уязвимого web-приложения OWASP Mutillidae, защищенного межсетевым экраном прикладного уровня PT AF**

Снимки экрана с результатами сканирования, с инцидентом, зарегистрированным PT AF, выводы по анализу результатов сканирования.

**Генерация отчета по работе межсетевого экрана прикладного уровня PT AF**

Отчет по работе PT AF в формате PDF, выводы по анализу этого отчета.

3.2.4 Контрольные вопросы

1. Какие информационные ресурсы защищает WAF?
2. Какими преимуществами обладает технология WAF?
3. От каких угроз защищает WAF?
4. Какие существуют режимы работы WAF? Их различия.
5. Какой режим работы WAF является преимущественным?
6. Какие модели безопасности используют WAF? Их различия.
7. Какие модули содержит решение PT AF? Их функционал.
8. Какие существуют методы анализа и тестирования web-приложений? Их различия.
9. Какие методы анализа и тестирования web-приложений использует продукт PT AI?
10. Какие методы анализа и тестирования web-приложений использует продукт Acunetix WVS?
11. Какими преимуществами обладает продукт PT AI?
12. Каким образом работает продукт PT AI? Описать схему работы.
13. Для каких целей PT AI интегрируется с PT AF?
14. По какой схеме работает продукт Acunetix WVS?
15. Для чего предназначено уязвимое web-приложение OWASP Mutillidae?
16. Каким уязвимостям подвержено web-приложение OWASP Mutillidae?

3.3 Выводы

В данной главе были представлены методика проведения лабораторной работы по изучению средств защиты и средств анализа защищенности web-приложений от типовых сетевых атак и лабораторный комплекс, на базе которого выполняется данная лабораторная работа. Также приведены методические указания к выполнению лабораторной работы, в которых описаны подробные инструкции по работе с лабораторным комплексом.