**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИЦАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ**

**УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА»**

**(СПбГУТ)**

Факультет Инфокоммуникационных сетей и систем

Кафедра Защищенных систем связи

**ОТЧЕТ ПО УЧЕБНОЙ ПРАКТИКЕ**

Место практики: Mail.ru

Направление/специальность подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

*(код и наименование направления/специальности)*

Студент:

Громов А. А. ИКТЗ-83

*(Ф.И.О., № группы) (подпись)*

Руководитель практики:

Шемякин С. Н.

*(уч. степень, уч. звание, Ф.И.О.) (подпись)*

Оглавление

[Введение 3](#_Toc5)

[Индивидуальное задание 4](#_Toc6)

[Выполнение задания 5](#_Toc7)

[Заключение 10](#_Toc8)

# **Введение**

Производственная практика – практическая часть учебного процесса подготовки квалифицированных рабочих и специалистов, проходящая, как правило, на различных предприятиях в условиях реального производства. Является заключительной частью учебной практики, проходящей в учебном заведении. Во время производственной практики происходит закрепление и конкретизация результатов теоретического учебно-практического обучения, приобретение студентами умения и навыков практической работы по присваиваемой квалификации и избранной специальности или профессии.

Перенос учебного процесса в условия, максимально схожие с обстановкой будущей профессиональной деятельностью студента, – обязательный этап на пути получения высшего образования, обусловленный требованиями госстандартов и регламентированный приказом Минобразования и науки РФ № 1383.

# **Индивидуальное задание**

Ознакомление с уязвимостями на серверной и клиентской стороне веб-приложений.

Ознакомление с процессом исправления, найденных уязвимостей.

Обработка рапортов об уязвимостях в проектах (веб-приложениях, серверной-инфраструктуре, сетевой-инфраструктуре) Mail.ru.

# **Выполнение задания**

1. Первостепенной задачей было изучение организационно-штатной структуры отдела информационной безопасности и общих задач подразделения, а также ознакомление с типами уязвимостей.

Компания Mail.ru Group является крупнейшим игроком на рынке информационных технологий.

SQL injection - один из распространённых способов взлома [сайтов](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B0%D0%B9%D1%82) и программ, работающих с [базами данных](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B7%D0%B0_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85), основанный на внедрении в запрос произвольного [SQL](https://ru.wikipedia.org/wiki/SQL)-кода. Внедрение SQL, в зависимости от типа используемой [СУБД](https://ru.wikipedia.org/wiki/%D0%A0%D0%B5%D0%BB%D1%8F%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%A1%D0%A3%D0%91%D0%94) и условий внедрения, может дать возможность атакующему выполнить произвольный запрос к базе данных (например, прочитать содержимое любых [таблиц](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BD%D0%BE%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_(%D1%80%D0%B5%D0%BB%D1%8F%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BC%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C)), удалить, изменить или добавить [данные](https://ru.wikipedia.org/wiki/%D0%94%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5)), получить возможность чтения и/или записи локальных файлов и выполнения произвольных команд на атакуемом сервере. Атака типа внедрения SQL может быть возможна из-за некорректной обработки входных данных, используемых в SQL-запросах.

XSS ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Cross-Site Scripting — «межсайтовый [скриптинг](https://ru.wikipedia.org/wiki/%D0%A1%D0%BA%D1%80%D0%B8%D0%BF%D1%82)») - тип [атаки](https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D0%BA%D0%B0%D1%8F_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) на [веб-системы](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5), заключающийся во внедрении в выдаваемую веб-системой [страницу](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D1%82%D1%80%D0%B0%D0%BD%D0%B8%D1%86%D0%B0) [вредоносного кода](https://ru.wikipedia.org/wiki/%D0%92%D1%80%D0%B5%D0%B4%D0%BE%D0%BD%D0%BE%D1%81%D0%BD%D1%8B%D0%B9_%D0%BA%D0%BE%D0%B4)(который будет выполнен на [компьютере](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80) пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. Является разновидностью атаки «[Внедрение кода](https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D0%BA%D0%B0%D1%8F_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#%D0%98%D0%BD%D1%8A%D0%B5%D0%BA%D1%86%D0%B8%D1%8F_%D0%BA%D0%BE%D0%B4%D0%B0)». Специфика подобных атак заключается в том, что вредоносный код может использовать [авторизацию](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) пользователя в веб-системе для получения к ней расширенного доступа или для получения авторизационных данных пользователя. Вредоносный код может быть вставлен в страницу как через [уязвимость](https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)) в [веб-сервере](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80), так и через уязвимость на компьютере пользователя.

RCE ([англ.](https://ru.bmstu.wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) Remote Code Execution) – компьютерная уязвимость, при которой происходит удаленное выполнение кода на взламываемом компьютере, сервере и т.п. RCE является максимальной угрозой класса А1 по классификации OWASP. А также это гарантированный способ взлома сайтов и веб приложений. RCE - является одной из самых опасных уязвимостей. Возможность удаленного внедрения кода в серверный скрипт в 100% случаев приводит к взлому ресурса. С помощью RCE злоумышленник сразу получает доступ к серверу атакуемого сайта, размещая на нем веб-шеллы, или любой другой вредоносный код. В практике встречались случаи, когда RCE эксплуатировали боевые скрипты, размещенные на хакерских серверах, которые отслеживали наличие вредоносной составляющей, вирусов шеллов и т.п. на сайте.

*SSRF*-атака — атака на сервер компьютерной сети, в результате которой злоумышленник получает возможность отправлять запросы от имени скомпрометированного хоста. SSRF может быть использована в [DoS](https://encyclopedia.kaspersky.ru/glossary/dos-denial-of-service-attack/)-кампаниях для маскировки реального источника нападения. По сути, взломанное устройство используется киберпреступником в качестве криминального прокси-сервера.

Обход каталогов (или путь обход) атака использует недостаточную проверку безопасности или санитарные имена файлов, поставляемого пользователь, таким образом, что символы , представляющие «траверс к родительскому каталогу» передаются на операционной систему файловой системы API . Уязвимое приложение может быть использовано для получения несанкционированного доступа к файловой системе. Обход каталогов также известен как ***../*** атака (точка, точка, косая черта), перелистывание каталогов и обратное отслеживание. Некоторые формы этой атаки также являются атаками канонизации.

XML External Entity(XXE) это атака, направленная на приложение, которое обрабатывает XML код. OWASP утверждает, что эта возможность этой атаки возникает, когда XML код содержит ссылки на внешние сущности, которые обрабатываются плохо настроенным парсером.

CSRF ([англ.](https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D0%B8%D0%B9%D1%81%D0%BA%D0%B8%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA) cross-site request forgery — «межсайтовая подделка запроса», также известна как XSRF) — вид [атак](https://ru.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D0%BA%D0%B0%D1%8F_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0) на посетителей [веб-сайтов](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%B1-%D1%81%D0%B0%D0%B9%D1%82), использующий недостатки протокола [HTTP](https://ru.wikipedia.org/wiki/HTTP). Если жертва заходит на сайт, созданный злоумышленником, от её лица тайно отправляется запрос на другой [сервер](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5)) (например, на сервер платёжной системы), осуществляющий некую вредоносную операцию (например, перевод денег на счёт злоумышленника). Для осуществления данной атаки жертва должна быть [аутентифицирована](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) на том сервере, на который отправляется запрос, и этот запрос не должен требовать какого-либо подтверждения со стороны [пользователя](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D1%82%D0%B5%D0%BB%D1%8C), которое не может быть проигнорировано или подделано атакующим [скриптом](https://ru.wikipedia.org/wiki/%D0%A1%D1%86%D0%B5%D0%BD%D0%B0%D1%80%D0%BD%D1%8B%D0%B9_%D1%8F%D0%B7%D1%8B%D0%BA).

1. Следующим этапом являлось обучение работы в программе burp suit.

Burp Suite — это интегрированная платформа, предназначенная для проведения аудита веб-приложения, как в ручном, так и в автоматических режимах. Содержит интуитивно понятный интерфейс со специально спроектированными табами, позволяющими улучшить и ускорить процесс атаки. Сам инструмент представляет из себя проксирующий механизм, перехватывающий и обрабатывающий все поступающие от браузера запросы. Имеется возможность установки сертификата burp для анализа https соединений.

Основной функционал основан на следующих модулях:

Proxy — перехватывающий прокси-сервер, работающий по протоколу HTTP(S) в режиме man-in-the-middle. Находясь между браузером и веб-приложением он позволит вам перехватывать, изучать и изменять трафик идущий в обоих направлениях.

Spider — паук или краулер, позволяющий вам в автоматическом режиме собирать информацию о об архитектуре веб-приложения.

Scanner — автоматический сканер уязвимостей (OWASP TOP 10 и т.д.) Доступен в Professional версии, в бесплатной версии только описание возможностей.

Intruder — утилита, позволяющая в автоматическом режиме производить атаки различного вида, такие как подбор пароля, перебор идентификаторов, фаззинг и так далее.

Repeater — утилита для модифицирования и повторной отправки отдельных HTTP-запросов и анализа ответов приложения.

Sequencer — утилита для анализа генерации случайных данных приложения, выявления алгоритма генерации, предиктивности данных.

Decoder — утилита для ручного или автоматического преобразования данных веб-приложения.

Comparer — утилита для выявления различий в данных.

Extender — расширения в BurpSuite. Можно добавлять, как готовые из BApp store, так и собственной разработки.

1. Далее происходило обучение обработке рапортов об уязвимостях из BugBounty программы.

Обработка делится на несколько этапов:

- Определить тип уязвимости.

- Воспроизвести уязвимость.

- Изучить варианты исправления.

- Поставить задачу в jira разработчикам на исправление уязвимости.

- Оценить качество исправления уязвимости.

BugBounty - это программа, предлагаемая некоторыми веб-сайтами и разработчиками программного обеспечения, с помощью которой люди могут получить признание и вознаграждение за нахождение [ошибок](https://ru.wikipedia.org/wiki/%D0%91%D0%B0%D0%B3), особенно тех, которые касаются [эксплойтов](https://ru.wikipedia.org/wiki/%D0%AD%D0%BA%D1%81%D0%BF%D0%BB%D0%BE%D0%B9%D1%82) и [уязвимостей](https://ru.wikipedia.org/wiki/%D0%A3%D1%8F%D0%B7%D0%B2%D0%B8%D0%BC%D0%BE%D1%81%D1%82%D1%8C_(%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D0%B0%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C)). Эти программы позволяют разработчикам обнаружить и устранить ошибки, прежде чем широкая общественность узнает о них, предотвращая злоупотребления. В частности, программы Bug Bounty были реализованы компаниями [Facebook](https://ru.wikipedia.org/wiki/Facebook), [Yahoo!](https://ru.wikipedia.org/wiki/Yahoo!), [Google](https://ru.wikipedia.org/wiki/Google_(%D0%BA%D0%BE%D0%BC%D0%BF%D0%B0%D0%BD%D0%B8%D1%8F)), [Reddit](https://ru.wikipedia.org/wiki/Reddit), [Square](https://ru.wikipedia.org/wiki/Square,_Inc.), [Apple](https://ru.wikipedia.org/wiki/Apple), Mail.ru и [Microsoft](https://ru.wikipedia.org/wiki/Microsoft).

Jira – это программный инструмент для управления проектами, разработанный компанией Atlassian. Jira часто используется в IT-компаниях для формирования списка задач, отслеживания общего прогресса команды и решения возникающих по ходу разработки продукта проблем.

Приложение Atlassian построено по принципам канбан- и скрам-досок, давней практики организации задач. Но эти принципы дополняются массой вспомогательных механизмов, которые добавлялись в приложение исключительно с целью упростить создание новых приложений, добавить в них функции, исправить ошибки и т.п. Также эта система управления проектами исповедует Agile-методику разработки.

1. Завершающими этапами являлась обработка рапортов об уязвимостях и работа по выше описанному процессу.

# **Заключение**

В ходе производственной практики в компании в отделе информационной безопасности были получены новые навыки и усовершенствованы навыки и знания, полученные в университете. Задания, поставленные компанией, были выполнены в полном объеме.