### Report on API Security Vulnerabilities

**1. Exploiting an API Endpoint Using Documentation**

**Описание:** В лабораторной работе было показано, как документация API может раскрывать критически важные функции, которые могут быть использованы злоумышленниками.  
**Предпринятые шаги:**

* Авторизовалась в системе с предоставленными учетными данными.
* Изучила документацию API через тестовые запросы.
* Использовала метод DELETE в интерактивной документации API для удаления целевого пользователя.  
  **Уязвимость:** Открытая документация API позволяла неавторизованное удаление аккаунтов.  
  **Меры защиты:** Ограничить доступ к документации API, внедрить строгую аутентификацию и авторизацию.

**2. Finding and Exploiting an Unused API Endpoint**

**Описание:** Данная лабораторная работа была посвящена обнаружению скрытых API-эндпоинтов, которые могли быть использованы для изменения цен на товары.  
**Предпринятые шаги:**

* Нашла API-запрос, связанный с ценами на товары.
* Изучила доступные HTTP-методы, отправив запрос OPTIONS и PATCH.
* Успешно изменила цену товара на $0.00.
* Оформила покупку товара бесплатно.  
  **Уязвимость:** Неиспользуемые или недокументированные эндпоинты были доступны и подвержены модификации.  
  **Меры защиты:** Регулярный аудит API-эндпоинтов и жесткий контроль доступа.

**3. Exploiting a Mass Assignment Vulnerability**

**Описание:** В данной лабораторной работе использовалась уязвимость массового присвоения, позволяющая изменять параметры скидок и обходить ограничения при покупке.  
**Предпринятые шаги:**

* Выявила скрытые параметры в JSON-структуре запроса.
* Внедрила параметр chosen\_discount в запрос на оплату.
* Изменила значение скидки так, чтобы товар стал бесплатным.  
  **Уязвимость:** Приложение обрабатывало неавторизованные параметры без валидации.  
  **Меры защиты:** Использование белого списка разрешенных параметров и серверная проверка входных данных.

**4. Exploiting Server-Side Parameter Pollution in a Query String**

**Описание:** Использование загрязнения параметров запроса для манипуляции обработкой данных на сервере и получения административного доступа.  
**Предпринятые шаги:**

* Исследовала функционал сброса пароля.
* Добавила дополнительные параметры с использованием URL-кодирования.
* Получила токен сброса и использовала его для смены пароля администратора.
* Авторизовалась под учетной записью администратора и удалила целевого пользователя.  
  **Уязвимость:** Некорректная обработка параметров в URL привела к неавторизованному доступу.  
  **Меры защиты:** Внедрение строгой валидации параметров запросов и отказ от использования клиентской проверки данных.

**5. Exploiting a Hidden API Endpoint**

**Описание:** Обнаружен незащищенный API-эндпоинт, который позволял злоумышленникам изменять цену товара и приобретать его бесплатно.  
**Предпринятые шаги:**

* Проанализировала HTTP-запросы к API товаров.
* Проверила доступные методы, обнаружила возможность изменения цены через PATCH.
* Оформила покупку после изменения стоимости товара на $0.  
  **Уязвимость:** Недостаточно защищенный эндпоинт позволял злоумышленникам манипулировать бизнес-логикой.  
  **Меры защиты:** Ограничить доступные HTTP-методы и проверять права пользователей перед изменением данных.