**Кыргызско-германский проект**

**«Содействие занятости и профессиональному обучению»**

PN: 19.2134.5-001.20

**Техническое задание**

Исполнитель: XX

Период работы *(предварительно)*: с 15.07.2021 по 10.09.2021

**Тема:**

**Аудит на наличие уязвимостей продуктов, разработанных для повышения потенциала партнеров проекта GIZ и их поддержки в сфере инновационных подходов к повышению квалификации и обучению (Министерства здравоохранения и социального развития КР, Министерства образования и науки КР, а также их региональных подразделений)**

**По заказу**

**Германского общества по международному сотрудничеству (GIZ) GmbH**

1. **Введение**

Кыргызско-германский [проект «Содействие занятости и профессиональному обучению»](http://www.giz-employment.kg/), реализуется Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH (Германским обществом по международному сотрудничеству) по поручению Федерального министерства экономического сотрудничества и развития Германии (BMZ).

Цель проекта: cодействие в улучшении перспектив занятости в Кыргызстане, расширении доступа к возможностям трудоустройства и инструментам, способствующим получению профессиональных навыков, отвечающих потребностям рынка труда.

Для достижения этих задач проект работает на разных уровнях в 4 направлениях.

В контексте COVID-19 Проект, в соответствии с потребностями партнерских организаций, поддерживает улучшение цифровой инфраструктуры для дистанционного обучения, а также применяет технические средства, требующиеся для повышения потенциала. В рамках работы по повышению потенциала по коммуникации и продвижению партнеров Проекта (Министерства здравоохранения и социального развития КР, Министерства образования и науки КР, а также их региональных подразделений), в соответствии с потребностями партнеров в данном направлении, Проект продолжает оказывать поддержку в разработке онлайн-курсов по нескольким направлениям: а) мобильной видеосъемке и монтажу, б) навыкам презентации, а также в) навыкам делопроизводства и бизнес-коммуникации. Эти курсы являются частью обучения для специалистов партнерских организаций, а также могут использоваться и для более широкой аудитории в рамках цифровизации профессионального обучения на предназначенных для этих целей платформах партнерских организаций.

1. **Цели задания**

Цель данного задания – аудит по безопасности на наличие уязвимостей продуктов, разработанных для повышения потенциала партнеров проекта GIZ и их поддержки в сфере инновационных подходов к повышению квалификации и обучению (Министерства здравоохранения и социального развития КР, Министерства образования и науки КР, а также их региональных подразделений). Цель испытаний на проникновение (пентестинг) - оценить возможность его осуществления и, в случае если таковые находятся, предложить решение, на основе которых разработчики смогут устранить уязвимости.

Продуктами, которые необходимо протестировать являются: 2 мониторинговых инструмента (веб-приложения), а также 1 обучающая платформа (сделана на Moodle, требуется проверить сервер).

Таким образом необходимо провести анализ вышеупомянутых продуктов с целью выявления и устранения уязвимостей и угроз информационной безопасности, выполнив следующее:

* выявление технических каналов утечки информации и способов несанкционированного доступа к ней;
* исследовать два веб-приложения и одну обучающую платформу на наличие уязвимостей, которые могут спровоцировать неправильную работу, либо полный отказ в обслуживании.

По мере устранения уязвимостей разработчиками необходимо провести вторичный аудит продуктов, чтобы убедиться, что уязвимости устранены.

1. **Основные задачи и план работ исполнителя**

В рамках данного Технического Задания Исполнитель оказывает следующие услуги:

|  |  |  |  |
| --- | --- | --- | --- |
| **№**  | **Задачи** | **Сроки** **(предварительное кол-во дней)** | **Ответственность** |
| 1 | * В ходе тестирования на проникновение решаются следующие задачи:
* Проверяется возможность получения доступа к конфиденциальной информации (включая персональные данные);
* Выявляются уязвимости информационной безопасности и варианты их использования;
* Разрабатываются рекомендации по нейтрализации обнаруженных уязвимостей.
* Помимо вышеупомянутого необходимо проверить на безопасность:
* Доступ к серверу и исходным кодам;
* Уязвимости веб-серверов, а также физического сервера (последнее может быть релевантно для обучающей платформы на Moodle, расположенной в продакшн версии);
* SQL инъекции;
* Межсайтовый скриптинг (XSS);
* Устойчивость приложения и сервера к перебору паролей;
* Получение доступа к системным каталогам.
 | 11 | Исполнитель |
|  | * Согласование методики тестирования согласовывается с заказчиком. За основу берутся практики, принятые в отрасли — например, NIST SP800-115 и OSSTMM (Open Source Security Testing Methodology Manual, в отношении безопасности персональных данных применяется GDPR
 | 3 | Исполнитель |
|  | * После устранения уязвимостей разработчиками исполнителем выполняется проверка действительно ли устранены уязвимости
 | 3 | Исполнитель |
|  | * Предоставить отчёт (в формате Word), содержащий в себе все найденные уязвимости системы безопасности, а также содержащий советы по их устранению для разработчиков. Неотъемлемой частью отчета являются файлы с обнаруженными уязвимостями, предназначенные для работы для разработчиков.
 | 3 | Исполнитель |
|  | **Итого** | **до 20 дней** |  |

1. **Ожидаемые результаты**
	1. Выполненные в оговоренный срок в требуемых форматах задачи с учетом комментариев и запросов Заказчика.
2. **Период выполнения работ и количество рабочих дней**

Задачи должны быть выполнены в течение 20 рабочих дней (или менее) и окончательные версии с отчетами и рекомендациями Исполнитель предоставляет Заказчику по мере завершения работы над ними для комментариев.

Оплата будет выполнена по предоставлении финальных версий всех требуемых материалов с учетом всех комментариев и требований Проекта.

1. **Место проведения работ**

г. Бишкек, Кыргызстан

1. **Поддержка со стороны проекта GIZ**
* Концептуальная поддержка Исполнителя
* Проведение установочной встречи
* Предоставление необходимых материалов и информации (корпоративные требования, стандартные названия Проекта на русском и кыргызском языке, логотипы и проч.)
* Предоставление доступов и ссылок на тестируемые продукты
* Предоставление комментариев
* Окончательное утверждение и прием материалов
1. **Отчетность**

Промежуточные результаты в виде выполненных работ будут предоставлены Исполнителем не позднее 20 августа 2021 г. (предварительно). Окончательное завершение работы не позднее 10 сентября 2021г.

1. **Прочее**
* Все материалы, разработанные в рамках данного Технического Задания и подписанного договора, являются собственностью проекта GIZ и его партнеров и не могут быть переданы третьим лицам.
* GIZ оставляет за собой право переводить, тиражировать тренинговые материалы и отчет в полном и сокращенном виде с обязательной ссылкой на исполнителя/исполнителей.
* Все материалы, разработанные в рамках данного Технического Задания, должны быть подготовлены в формате GIZ (с логотипом, шрифт и т.д.) и в формате, позволяющем редактирование. Исполнитель получит дополнительную информацию по требованиям к отчетной продукции.
1. **Требования к кандидатам**
* Наличие портфолио с выполненными работами подобных форматов: определение уязвимостей на обучающих системах (Moodle), а также веб-приложений.
* Наличие сертификатов, подтверждающих повышение квалификации в области подготовки по информационной безопасности и/или тестирования на проникновение.
* Высшее образование в сфере компьютерных наук, информационно-коммуникационных технологий, или смежной области.
* Опыт работы в сфере информационной безопасности не менее 2 лет.
* Опыт проведения тестирования на проникновение сети, приложений и систем.
* Навык документирования и коммуникации результатов.
* Грамотность (литературный русский язык, знание кыргызского языка будет преимуществом).
* Умение предложить решения и рекомендации по устранению выявленных уязвимостей.
* Опыт работы с учетом требований по защите персональных данных, согласно GDPR.

Утверждено

Толгонай Кудайбергенова

Руководитель проекта

Подготовлено

Назик Мамедова

Младший специалист по мониторингу и оценке