«Согласовано»
Заведующий центра
Компитенции Сетевые
технологий и дизайн
Ахасов Е.Б
«30» 03 2026г.

«Утверждаю»
Заместитель директора по
учебной работе
Баяхметов М.К.
«30» 03 2026г.

Конкурсное задание

Демонстрационного экзамена

по компетенции Кибербезопасность

Module A, B

Адаптировали:

Главный эксперт Тасмағанбет Д.А.

worldskills Kazakhstan

Конкурсное задание

Демонстрационного экзамена

по компетенции Кибербезопасность

Module A

Адаптировали:

Главный эксперт Тасмағанбет Д.А.

Оглавление

Введение

Конкурсное задание в рамках модуля 1 направлено на проверку практических навыков в области веб-безопасности при работе с тестовой уязвимой веб-средой DVWA (Damn Vulnerable Web Application). Участникам необходимо продемонстрировать понимание уязвимостей типа SQL-инъекция и XSS (Stored и Reflected), а также способы их эксплуатации.

Инструкции для участников

Внимательно ознакомьтесь со следующими инструкциями!

- Ознакомьтесь с заданием полностью до начала выполнения.
- Не разглашайте материалы другим участникам.
- Время на выполнение: 2 часа (из общего 4-часового экзамена).
- Рабочая среда: DVWA с уровнем безопасности Low.
- Используйте браузер и Burp Suite (при необходимости).
- Сделайте скриншоты каждого результата и опишите действия.

Оборудование, инструменты и требуемые материалы

Ожидается, что все конкурсные задания могут быть выполнены Студентами на том оборудовании и материалах, которые указаны в инфраструктурном листе *(Определение: Инфраструктурный лист - это оборудование, механизмы, установки и материалы, поставляемые принимающей страной - он не включает инструменты и материалы, которые должны быть предоставлены конкурсантами и/или экспертами)*.

Материалы, оборудование и инструменты, запрещенные на конкурсной площадке

Во время выполнения конкурсного задания студентам запрещается использовать и носить при себе: мобильные телефоны, наушники и различную носимую электронику (за исключением назначенного медицинского оборудования, в таком случае, участник должен иметь справку подтверждающую это, в противном случае эксперты выносят коллегиальное решение).

Описание проекта и заданий

- Задание 1: SQL Injection (уровень Low)

Перейдите в раздел "SQL Injection".
Цель: Получить список всех пользователей через SQL-инъекцию.
Сохраните скриншот результата и укажите использованный SQL-запрос.

- Задание 2: Stored XSS

Перейдите в раздел "Stored XSS".
Цель: Внедрить скрипт:
<script>alert('XSS')</script>
Подтвердите срабатывание скрипта с помощью скриншота.

- Задание 3: Reflected XSS

Перейдите в раздел "Reflected XSS".
Цель: Внедрите отражённый скрипт, добившись отображения alert.
Опишите используемую уязвимую точку и результат атаки.