1. **Паспорт Образовательной программы**

«Защищенная веб разработка» «WEB APPLICATION SECURITY ANALYSIS (ADVANCED)**»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | 15**.**10.2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Образовательная автономная некоммерческая организация дополнительного профессионального образования "Высшая школа информационных технологий и безопасности" (ОАНО ДПО «Выштех») |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 7703434727 |
| 1.4 | Ответственный за программу ФИО | Богомолов Егор Антонович |
| 1.5 | Ответственный должность | Лидер направления |
| 1.6 | Ответственный Телефон | +79776758474 |
| 1.7 | Ответственный Е-mail | e.bogomolov@hackeru.com |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | «Защищенная веб разработка» (Далее WEB APPLICATION SECURITY ANALYSIS (ADVANCED) |
| 2.2 | Ссылка на страницу программы | https://hackeru.pro/universitet-20-35/professii-universitet-20-35/university2035 |
| 2.3 | Формат обучения | Онлайн |
|  | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | Подтверждаем наличие возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа. |
| 2.4 | Уровень сложности | Базовый |
| 2.5 | Количество академических часов | **72** академических часа |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоемкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | Не менее 50 % трудоемкости учебной деятельности отведено практическим занятиям и выполнению практических заданий в режиме самостоятельной работы. |
| 2.6 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | 29900 |
| 2.7 | Минимальное количество человек на курсе | 30 |
| 2.8 | Максимальное количество человек на курсе | 100 |
| 2.9 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 80 |
| 2.10 | Формы аттестации | Практические задания в рамках курса |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

Наиболее полное и содержательное описание программы, которое включает:

1) общую характеристику компетенций, качественное изменение которых осуществляется в результате обучения или которые формируются в результате освоения образовательной программы;

2) описание требований и рекомендаций для обучения по образовательной программе;

3) краткое описание результатов обучения в свободной форме, а также описание востребованности результатов обучения в профессиональной деятельности.

Ограничение по размеру: не менее 1000 символов

Программа повышения квалификации "WEB APPLICATION SECURITY ANALYSIS (ADVANCED)" направлена на формирование профессиональных компетенций в области анализа защищенности веб-приложений и сайтов. Анализ защищенности веб-приложений применяется в самых разных областях - продуктовая безопасность, аудит безопасности, оценка защищенности программных продуктов, разработка программного обеспечение и так далее.

Для успешного освоения программы обучающимся необходимо владеть базовыми компетенциями цифровой грамотности, в том числе навыками владения ПК на уровне среднего или продвинутого пользователя; начальные знания в области работы сетей и протоколов прикладного уровня, программирования на любом языке программирования, а также знаниями основ безопасности в сфере ИТ.

Результаты обучения по программе будут востребованы при решении следующих профессиональных задач: аудит безопасности веб-приложений, в том числе приложений дистанционного банковского обслуживания, электронной коммерции, социальных сервисов и любых других приложений созданных с применением веб-технологий; анализа безопасности архитектуры и бизнес-процессов веб-приложения на этапе создания приложения их формулирования бизнес-требований, оценка защищенности принятых мер по обеспечению безопасности веб-приложений и многие другие.

1. ШАБЛОН ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ (ДПО)

**Образовательная автономная некоммерческая организация дополнительного профессионального образования "Высшая школа информационных технологий и безопасности" (ОАНО ДПО «Выштех»)**

ИНН: 7703434727 ОГРН: 1177700018210

127204, г. Москва, Долгопрудненское шоссе, д. 3, этаж 2, пом. VII, комн.22Г

УТВЕРЖДАЮ:

Исполнительный директор

ОАНО ДПО «ВЫШТЕХ»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.И. Поддубный-Тумаларян

«15» октября 2020 г.

**Дополнительная профессиональная программа повышения квалификации**

**«Защищенная веб разработка» («WEB APPLICATION SECURITY ANALYSIS (ADVANCED)»)**

72 час.

Москва, 2020 год

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Программа повышения квалификации "WEB APPLICATION SECURITY ANALYSIS (ADVANCED)" направлена на освоение (совершенствование) профессиональных компетенций в области "Анализа защищенности веб-приложений" по направлению развития цифровой экономики "Кибербезопасность и защита данных".

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. особенности проведения анализа защищенного веб-приложения;

2.1.2. распространенные уязвимости веб-приложений.

2.2. Умение (способность к деятельности)

2.2.1. обнаруживать и эксплуатировать основные уязвимости серверной части веб-приложений;

2.2.2. обнаруживать и эксплуатировать основные уязвимости клиентской части веб-приложений.

2.3.Навыки (использование конкретных инструментов)

2.3.1. эксплуатация уязвимостей веб-приложений;

2.3.2. использование инструментов анализа и автоматизированных систем для проведения оценки защищенности веб-приложений.

**3.Категория слушателей** (возможно заполнение не всех полей)

* 1. Образование: среднее профессиональное и/или высшее образование
  2. Квалификация: не ниже 4
  3. Наличие опыта профессиональной деятельности: разработчики программного обеспечения, руководители служб и подразделений в сфере информационно-коммуникационных технологий, программисты приложений, специалисты аналитических служб, системные и сетевые инженеры.

**4.Учебный план программы «**WEB APPLICATION SECURITY ANALYSIS (ADVANCED)**»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Знакомство с базовыми технологиями веба | 4 | 2 | 1 | 1 |
| 2 | Устройство современных веб-приложений и сбор информации | 4 | 1 | 2 | 1 |
| 3 | Уязвимости OS Command injection, SQL Injection, SQL Injection | 8 | 4 | 2 | 2 |
| 4 | Аутентификация и менеджмент сессий | 4 | 2 | 1 | 1 |
| 5 | Онлайн и оффлайн брутфорс | 4 | 2 | 1 | 1 |
| 6 | Уязвимость:  Path traversal  File Upload  Broken Access Control  Server-side template injection | 20 | 12 | 4 | 4 |
| 7 | Небезопасная десериализация | 4 | 2 | 1 | 1 |
| 8 | Небезопасное сравнение и приведение типов в PHP | 4 | 2 | 1 | 1 |
| 9 | Уязвимость Server Side Request Forgery. Уязвимость XML External Entity | 12 | 2 | 1 | 1 |
| 10 | Безопасность клиентской части веб-приложений | 4 | 2 | 1 | 1 |
| 11 | Финальное занятие | 4 | 1 | 2 | 1 |
| **Итоговая аттестация** | |  | **Указывается вид (экзамен, зачет, реферат и т.д.)** | | |
|  | | 72 | **Лабораторная работа** | | |

**5.Календарный план-график реализации образовательной программы**

**«**WEB APPLICATION SECURITY ANALYSIS (ADVANCED)**»** в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоемкость (час)** | **Сроки обучения** |
| **1** | Знакомство с базовыми технологиями веба | 4 | 1 день ( 1 день) |
| **2** | Устройство современных веб-приложений и сбор информации | 4 | 2 день (2 день) |
| 3 | Уязвимости OS Command injection, SQL Injection, SQL Injection | 8 | 2 дня (3-4 день) |
| 4 | Аутентификация и менеджмент сессий | 4 | 1 день (5 день) |
| 5 | Онлайн и оффлайн брутфорс | 4 | 1 день (6 день) |
| 6 | Уязвимость:  Path traversal  File Upload  Broken Access Control  Server-side template injection | 20 | 5 дней (7-11 день) |
| 7 | Небезопасная десериализация | 4 | 1 день (12 день) |
| 8 | Небезопасное сравнение и приведение типов в PHP | 4 | 1 день (13 день) |
| 9 | Уязвимость Server Side Request Forgery. Уязвимость XML External Entity | 12 | 3 дня (14-16 день) |
| 10 | Безопасность клиентской части веб-приложений | 4 | 1 день (17 дней) |
| 11 | Знакомство с базовыми технологиями веба | 4 | 1 день (18 день) |
| **Всего:** | | 72 | 18 дней |

**6.Учебно-тематический план программы «** WEB APPLICATION SECURITY ANALYSIS (ADVANCED) **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Знакомство с базовыми технологиями веба | 4 | 2 | 1 | 1 |  |
| 2 | Устройство современных веб-приложений и сбор информации | 4 | 1 | 2 | 1 |  |
| 3 | Уязвимости OS Command injection, SQL Injection, SQL Injection | 8 | 4 | 2 | 2 | Итоговое тестирование |
| 4 | Аутентификация и менеджмент сессий | 4 | 2 | 1 | 1 |  |
| 5 | Онлайн и оффлайн брутфорс | 4 | 2 | 1 | 1 |  |
| 6 | Уязвимость:  Path traversal  File Upload  Broken Access Control  Server-side template injection | 20 | 12 | 4 | 4 | Итоговое тестирование |
| 7 | Небезопасная десериализация | 4 | 2 | 1 | 1 |  |
| 8 | Небезопасное сравнение и приведение типов в PHP | 4 | 2 | 1 | 1 |  |
| 9 | Уязвимость Server Side Request Forgery. Уязвимость XML External Entity | 12 | 2 | 1 | 1 | Итоговое тестирование |
| 10 | Безопасность клиентской части веб-приложений | 4 | 2 | 1 | 1 | е |
| 11 | Финальное занятие | 4 | 1 | 2 | 1 | Контрольная работа |

**7. Учебная (рабочая) программа повышения квалификации «**WEB APPLICATION SECURITY ANALYSIS (ADVANCED)**»**

Занятие 1 (4 часа)

Знакомство с базовыми технологиями веба.

* HTTP, HTML, Javascript, CSS.
* Знакомство с Burp Suite

Занятие 2 (4 часа)

Устройство современных веб-приложений и сбор информации

* Структура веб-приложений
* Статическое и динамическое содержимое
* Сессии
* Сбор информации
* Краулинг и дирбастинг

Занятие 3 (4 часа)

Уязвимости OS Command injection

* Описание уязвимости OS Command injection
* Примеры обнаружения и эксплуатации Reverse shell

Занятие 4 (4 часа)

Уязвимость SQL Injection

* Обзор языка SQL
* Описание уязвимости SQL injection
* Вектора эксплуатации: bypass, union-based
* Обзор имеющихся информационных ресурсов по уязвимости SQL injection

Занятие 5 (4 часа)

Уязвимость SQL Injection

* Вектора эксплуатации уязвимости SQL injection: error-based, boolean-blind, time-based.
* Использование sqlmap для автоматической эксплуатации уязвимостей SQL injection
* Рекомендации для разработчиков для исключения уязвимости SQL injection

Занятие 6 (8 часов)

Аутентификация и менеджмент сессий

Онлайн брутфорс

* Аутентификация
* Хранение паролей
* Сессионный менеджмент
* patator - инструмент для онлайн брутфорса

Занятие 7 (4 часа)

Оффлайн брутфорс

* hashcat
* Определение типа хэша
* Обсуждение словарей
* Работа с правилами hashcat
* Брутфорс по маске

Занятие 8 (4 часа)

Уязвимость Path traversal

Уязвимость File Upload

Атака Local File Read

* Причины возникновения и способы эксплуатации Path traversal.
* Уязвимость FIle Upload.
* Веб-шеллы для PHP ASMX(IIS) JSP
* Рекомендации для разработчиков

Занятие 9 (4 часа)

Уязвимость Broken Access Control

* Уязвимость Insufficient Function Level Access Control
* Уязвимость Insecure Direct Object Reference
* Обнаружение.
* Автоматизированное обнаружение с помощью плагинов BURP Suite
* Рекомендации для разработчиков

Занятие 10 (4 часа)

Уязвимость Server-side template injection

Логические ошибки

* Описание шаблонов и их предназначения, примеры
* Примеры эксплуатации уязвимости для нескольких шаблонизаторов
* Обзор репозитория на payload all the things
* Примеры логических ошибок
* Особенности строгого и не строго сравнения в PHP.
* Автоматическое приведение типов.
* Описание возникающих из за этого уязвимостей
* Рекомендации для разработчиков

Занятие 11 (4 часа)

Небезопасная десериализация

* Описание сериализации и её предназначения
* Описание уязвимости небезопасной десериализации
* Разбор примеров для Java и PHP
* Обзор программного обеспечения ysoserial и phpggc
* Рекомендации для разработчиков

Занятие 12 (4 часа)

Уязвимость Server Side Request Forgery

Уязвимость XML External Entity

* Описание атаки SSRF и примеры её эксплуатации
* XML и внешние сущности
* Вектора эксплуатации XXE:
* Отказ в обслуживании
* Local File read,
* SSRF.
* Рекомендации для разработчиков

Занятие 13 (4 часа)

Same Origin Policy

CSRF

* Описание клиентской безопасности веб-приложений
* Обзор Same Origin Policy
* Разбор атаки Cross-site Request Forgery и практика по её реализации
* Обзор методов защиты от CSRF

Занятие 14 (4 часа)

CORS

XSS

* - Обзор Cross-Origin Resource Sharing
* - Обзор типов XSS
* - Контексты внедрения XSS
* - Практика обнаружения XSS

Занятие 15 (4 часа)

XSS - эксплуатация

* Кража Cookie
* Deface
* CSRF bypass
* XSS с помощью загрузки файлов

Занятие 16 (4 часа)

CSP

* Content Security Policy и как оно защищает от XSS
* Некоторые техники обхода CSP
* Другие заголовки безопасности протокола HTTP
* Обсуждение собеседований

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1 | Знакомство с базовыми технологиями веба. | Исходный код веб страниц, протокол HTTP, атаки на веб-приложения с использованием протокола HTTP | Ученикам предстоит ознакомиться с содержимым исходных кодов клиентской части веб-приложений и научиться их изучать; разобраться в протоколе HTTP прикладного уровня стека TCP/IP и научить использовать его чтобы взаимодействовать с веб-приложением а также изучить первые простые атаки на веб-приложения. |
| 2 | Устройство современных веб-приложений | Устройство современных веб-приложений и сбор информации | Учащимся предстоит научиться определять стек используемых технологий в веб-приложении и собирать информации оставленную разработчиками в ходе создания приложения. |
| 3 | Уязвимости OS | Уязвимости инъекции команд | Учащимся предстоит изучить новый подвид уязвимостей инъекции и на практике разобраться в особенностях эксплуатации этих уязвимостей а также изучить рекомендации по устранению таких уязвимостей. |
| 4 | Аутентификация и менеджмент сессий | Поиск флагов на <https://www.root-me.org/> | Учащиеся на общедоступной платформе проверяют свои навыки взлома. |
| 5 | Онлайн и оффлайн брутфорс | Запуск атак на подбор паролей | Учащимся предстоит самостоятельно произвести атаку на подбор паролей и определить тип кеша. |
| 6 | Уязвимости | Подбор веб-шел | Учащимся предстоит самостоятельно подобрать веб-шел. |
| 7 | Небезопасная десериализация | Подбор векторов в случае использования популярных библиотек | Учащимся предстоит подбор векторов в случаи использования популярных библиотек.  Поиск флагов на [https://w3challs.com](https://w3challs.com/) |
| 8 | Небезопасное сравнение и приведение типов в PHP | Изучение агрегатора [https://ctftime.org](https://ctftime.org/) | Учащиеся изучат агрегатор <https://ctftime.org/> |
| 9 | Уязвимость  Server Side Request Forgery | Уязвимости инъекции команд | Учащиеся попробуют обнаруживать и эксплуатировать SSRF |
| 10 | Безопасность клиентской части веб-приложений | Исследование карьерных возможностей | Учащиеся попробуют себя в поиске уязвимостей за вознаграждение: <https://www.hackerone.com> <https://bugcrowd.com> |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 3. Уязвимости OS |  |  | * OS Command injection относятся к следующему пункту OWASP Top 10, * Что такое валидация? * С помощью какой подкоманды можно выполнить bash? * Отделить одну команду от другой в bash можно с помощью символа * Рекомендуемый набор флагов для приема соединений с помощью nc |
| 6.Уязвимости Path traversal |  |  | * Веб-шелл - это? * Информация о переменных среды может быть обнаружена в следующем файле: * Нулевой байт может быть использован атакующим для того чтобы: * Обертка для содержимого тела запроса * Уязвимость, при которой атакующий может обращаться к файлам вне ожидаемой директориях: |
| 9. Уязвимости Server Side Request Forgery |  |  | * HTTP-заголовок, говорящий веб-серверу, о том что в этом TCP-соединении будет еще один запрос * SSRF-атака при генерации PDF может быть успешной при использовании следующего вектора * Выберите корректный вектор атаки XXE * Обращение к сущности `name` в XML делается так * Символы переноса строки \r\n в URL кодировке |

**8.2.**  О**писание показателей и критериев оценивания, шкалы оценивания**

Шкала итогового тестирования по темам/модулям

|  |  |  |  |
| --- | --- | --- | --- |
| Критерии | Шкала | Описание | Уровень сформированности компетенции |
| зачтено | 91%-100% баллов за тестирование | Обучающийся успешно выполнил тест по теме | Профессиональный уровень |
| зачтено | 76%-90% баллов за тестирование | Обучающийся успешно выполнил тест по теме | Продвинутый уровень |
| зачтено | 61%-75% баллов за тестирование | Обучающийся успешно выполнил тест по теме | Базовый уровень |
| не зачтено | 50%-60% баллов за тестирование | Обучающийся не выполнил успешно тестирование, необходимо повторное назначение теста и консультация преподавателя | Начальный уровень |
| не зачтено | 0%-49% баллов за промежуточное тестирование и практическую работу | Обучающийся не выполнил успешно промежуточное тестирование, необходимо повторное назначение теста и консультация преподавателя | Не владеет, компетенция не сформирована |

Шкала оценивания для выходной диагностики

|  |  |  |  |
| --- | --- | --- | --- |
| Критерии | Шкала | Описание | Уровень сформированности компетенции |
| зачтено | 91%-100% верных ответов на вопросы итогового теста  Успешно выполнено не менее 80% практических заданий курса | Обучающийся успешно выполнил итоговый тест | Профессиональный уровень |
| зачтено | 76%-90% верных ответов на вопросы итогового теста | Обучающийся успешно выполнил итоговый тест | Продвинутый уровень |
| зачтено | 61%-75% верных ответов на вопросы итогового теста | Обучающийся успешно выполнил итоговый тест по теме | Базовый уровень |
| не зачтено | 50%-60% верных ответов на вопросы итогового теста | Обучающийся не выполнил успешно итоговый тест необходимо повторное назначение теста и консультация преподавателя | Начальный уровень |
| не зачтено | 0%-49% верных ответов на вопросы теста | Обучающийся не выполнил успешно итоговый тест | Не владеет, компетенция не сформирована |

Шкала оценивания практических заданий

|  |  |  |  |
| --- | --- | --- | --- |
| Критерии | Шкала | Описание | Допуск к итоговой аттестации/выходной диагностики |
| зачтено | 50%-100% верных ответов по всем практическим заданиям программы | Обучающийся успешно выполнил практические задания | Да |
| не зачтено | 0%-49% верных ответов по всем практическим заданиям программы | Обучающийся не выполнил успешно практические задания в нужном объеме | Нет  Необходимо повторное выполнение заданий и консультация преподавателя |

**8.3.**  **Описание процедуры оценивания результатов обучения**

К итоговой аттестации допускаются слушатели, выполнившие не менее 50% всех практических заданий и сдавшие итоговые тесты по отдельным темам (60% верных ответов по каждому тесту по теме), предусмотренные учебной программой.

В ходе итогового электронного тестирования слушателю предлагается ответить на 20 вопросов. Тестирование считается успешно завершённым, если слушателем даны верные ответы на не менее чем 60% вопросов теста.

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Фамилия, имя, отчество (при наличии) | Место основной работы и должность, ученая степень и ученое звание (при наличии) | Фото в формате jpeg | Отметка о полученном согласии на обработку персональных данных |
| 1 | Богомолов Егор | Head of Security at HackerU Russia  Более двухсот успешных проектов в области анализа защищенности и тестирования на проникновение информационных систем в таких компаниях, как "Информзащита", "Бизон" и "Валарм"  Эксперт по вопросам защиты мобильных и веб-приложений, защищенности корпоративных сетей, анализа кода на предмет информационной безопасности.  Спикер и ведущий воркшопов на конференциях и security-митапах: Party Hack, Security Expresso Romania, Positive Hack Days 9, OffZone 2019, DefCon Group 4799 Meetup, OWASP Moscow Meetup  Участник и призер множества CTF-турниров. Участник BugBounty программ Yandex и HackerOne  Сертификаты: Kaspersky Academy, Cybersecurity Fundamentals Certification, Offensive Security Certified Professional |  | + |

**9.2.Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Иммерсивный метод обучения  Проблемно-развивающие методы  Исследовательский метод  Частично-поисковый метод  Метод контроля и самоконтроля  Самостоятельная работа по освоению теоретического материала  Решение кейсовых задач  Промежуточный контроль (тесты по темам для промежуточной аттестации)  Итоговый контроль (итоговое тестирование по курсу) | The Web Application Hacker's Handbook  [https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting-ebook/dp/B005LVQA9S](https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting-ebook/dp/B005LVQA9S/)  The Tangled Web: A Guide to Securing Modern Web Applications  <https://www.amazon.com/Tangled-Web-Securing-Modern-Applications/dp/1593273886>  http://pentestmonkey.net/category/cheat-sheet/sql-injection (http://pentestmonkey.net/category/cheat-sheet/sql-injection) |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| <https://portswigger.net/web-security>  https://www.jdoodle.com/execute-sql-online  <http://sqlfiddle.com>  http://rextester.com/l/sql\_server  <https://sqliteonline.com/> | OWASP Testing Guide <https://github.com/OWASP/wstg/tree/master/document>  <https://www.root-me.org/en/Challenges/Web-Server/PHP-Command-injection> |

**9.3.Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Теоретический компонент | Операционная система семейств Windows, Mac Os, Linux.  Браузер:  • Firefox 64  • Chrome 61  • Safari 11  • Opera 57  Рекомендуемые программы:  1. ОС: Windows/Linux/MacOS  2. Docker Desktop: https://www.docker.com/products/docker-desktop  3. python3: https://www.python.org/downloads/  4. php: https://www.php.net/downloads  5. Burp Suite CE: https://portswigger.net/burp/communitydownload  Рекомендуется от 128 кбит/сек исходящего потока.  Рекомендуется от 256 кбит/сек входящего потока. |
| Дополнительные теоретические материалы | Операционная система семейств  Windows, Mac Os, Linux.  Браузер:  • Firefox 64  • Chrome 61  • Safari 11  • Opera 57  Рекомендуется от 128 кбит/сек исходящего потока.  Рекомендуется от 256 кбит/сек входящего потока. |
| Аттестационный компонент | Операционная система семейств Windows, Mac Os, Linux.  Браузер:  • Firefox 64  • Chrome 61  • Safari 11  • Opera 57  Рекомендуется от 128 кбит/сек исходящего потока.  Рекомендуется от 256 кбит/сек входящего потока. |
| Практический компонент | Операционная система семейств Windows, Mac Os, Linux.  Браузер:  • Firefox 64  • Chrome 61  • Safari 11  • Opera 57  Рекомендуемые программы:  1. ОС: Windows/Linux/MacOS  2. Docker Desktop: https://www.docker.com/products/docker-desktop  3. python3: https://www.python.org/downloads/  4. php: https://www.php.net/downloads  5. Burp Suite CE: https://portswigger.net/burp/communitydownload  Рекомендуется от 128 кбит/сек исходящего потока.  Рекомендуется от 256 кбит/сек входящего потока. |

**VI.Иная информация о качестве и востребованности образовательной программы** (результаты профессионально-общественной аккредитации образовательной программы, включение в системы рейтингования, призовые места по результатам проведения конкурсов образовательных программ и др.) (при наличии)

**V.Рекомендаций к программе от работодателей**: наличие не менее двух писем и/или подтверждения на цифровой платформе Государственной системы предоставления ПЦС от работодателей о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики с указанием востребованности результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы

К паспорту прилагаются рекомендации от работодателей в формате .pdf

**VI.Указание на возможные сценарии профессиональной траектории граждан** по итогам освоения образовательной программы (в соответствии с приложением)

|  |  |
| --- | --- |
| Цели получения персонального цифрового сертификата | |
| текущий статус | цель |
| Развитие компетенций в текущей сфере занятости | |
| работающий по найму в организации, на предприятии | сохранение текущего рабочего места |
| работающий по найму в организации, на предприятии | развитие профессиональных качеств |
| работающий по найму в организации, на предприятии | повышение заработной платы |
| работающий по найму в организации, на предприятии | смена работы без изменения сферы профессиональной деятельности |

**VII.Дополнительная информация**

**VIII.Приложенные Скан-копии**

1. Рекомендательные письма

2. Скан утвержденной образовательной программы

3. Скан утвержденного паспорта образовательной программы

4. Паспорт образовательной программы в формате word

Исполнительный директор

ОАНО ДПО «ВЫШТЕХ» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ О.И. Поддубный-Тумаларян

«15» октября 2020 г.