**1.** **Паспорт Образовательной программы**

**«**Security Champion**»**

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

**1.** **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | ОАНО ДПО «ВЫШТЕХ» |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 7703434727 |
| 1.4 | Ответственный за программу ФИО | Афанасьев Иван Сергеевич |
| 1.5 | Ответственный должность | Преподаватель Учебного центра ОАНО ДПО «ВЫШТЕХ» |
| 1.6 | Ответственный Телефон | 89164367860 |
| 1.7 | Ответственный Е-mail | i.afanasiev@hackeru.com |

**2.** **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Security Champion |
| 2.2 | Ссылка на страницу программы | https://hackeru.pro/universitet-20-35/professii-universitet-20-35/university2035 |
| 2.3 | Формат обучения | Онлайн |
|  | Подтверждение от ООО 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 | Продвинутый |
| 2.5 | Количество академических часов | **72** академических часа |
|  | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | Не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и выполнению практических заданий в режиме самостоятельной работы:  36 ак. часов практических занятий, в том числе:  15 практических заданий на программирование (см. п. 7) |
| 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 рублей    Программа обучения является уникальной на рынке, ввиду отсутствия |
| 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 | новая программа |
| 2.10 | Формы аттестации | итоговое тестирование |
|  | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | кибербезопасность |

**3.** **Аннотация программы**

В соответствии с профессиональным стандартом «Информационная безопасность», программа повышения квалификации "Security Champion" направлена на формирование профессиональных компетенций в области "Обеспечение информационной безопасности программного обеспечения". Обеспечение безопасности программных продуктов применяется в самых разных областях - розничная торговля, банковское дело, страхование, телекоммуникации, техника, интернет вещей, промышленность, 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; компетенции в области алгоритмизации, в том числе знаниями и умениями в области программирования, базовыми знаниями в области языков программирования для веб (Python, Golang, JavaScript), а также знаниями основ процессов разработки программных тестирования, включающих проектирование, тестирование и последующую эксплуатацию программных продуктов.

В процессе обучения по программе обучающимся рекомендуется прослушать и конспектировать все видеуроки, выполнять по каждой теме практические задания с автоматизированной проверкой и проработать самостоятельно дополнительные материалы, после этого необходимо выполнить тесты по каждой теме и, для успешного завершения обучения, выполнить итоговый тест (не менее 60% верных ответов).

Обучающиеся в результате освоения программы: будут знать основные концепции информационной безопасности, концепты безопасной разработки, требования, которые предъявляются для обеспечения защищенности - ГОСТ, приказы ФСТЭК, отраслевые документы; техники тестирования безопасности программных продуктов - нагрузочное, фаззинг, тестирование на проникновение; техники тестирования Web-приложений на уязвимости, наиболее частые виды атак на приложения - OWASP Top 10; порядок составления модели угроз, модели нарушителя; инструменты для автоматизированного поиска уязвимостей - OWASP Dependency Check, SonarQube, PyBandit, Burp Suite, w3af; решения контроля защищенности - WAF, IDS, SIEM.

Результаты обучения по программе будут востребованы при решении следующих профессиональных задач: методологическое обеспечение безопасности программных продуктов; применение инструментальных средств обеспечения защищенности ПО.

**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**

**“**Security Champion”

72 час.

**Москва, 2020**

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Программа повышения квалификации "Security Champion" направлена на освоение (совершенствование) профессиональных компетенций в области "Обеспечение информационной безопасности программного обеспечения" по направлению развития цифровой экономики "Информационная безопасность".

Программа повышения квалификации "Security Champion" также формирует профессиональные компетенции для решения прикладных задач в области защиты программного обеспечения.

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. моделирование угроз – STRIDE, DREAD, ISO 2700x;

2.1.2. статические анализаторы кода – PyBandit, SonarQube;

2.1.3. инструменты защиты периметра - IDS, SIEM, WAF;

2.1.4. техники тестирования кода - fuzzing, pentesting;

2.1.5 виды уязвимостей Web-приложений - Injection, Broken Access Control, Directory Traversal, XXE;

2.1.6. основные концепты безопасной разработки.

2.2. Умение (способность к деятельности)

2.2.1. анализ веб-приложений,

2.2.2. использовать методологии моделирования угроз;

2.2.3. использовать инструменты защиты ПО.

2.3.Навыки (использование конкретных инструментов)

2.3.1. тестирование на проникновение для анализа Web-приложений;

2.3.2. написание правил для WAF;

2.3.3. разворачивать и использовать SonarQube для анализа исходных кодов.

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

3.1. Образование: среднее профессиональное и/или высшее образование

3.2. Квалификация: не ниже 4

3.3. Наличие опыта профессиональной деятельности: разработчики программного обеспечения, руководители служб и подразделений в сфере информационно-коммуникационных технологий, программисты приложений, специалисты аналитических служб, специалисты DevOps, специалисты по защите информации.

3.4. Предварительное освоение иных дисциплин/курсов /модулей: необходимы знания в области информатики, теории сетей в объёме первого курса вуза.

**4.Учебный план программы «Security Champion»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Введение в продуктовую безопасность | 4 | 2 | 1 | 1 |
| 2. | Программные средства защиты | 4 | 2 | 1 | 1 |
| 3. | Уязвимости веб-приложений | 64 | 32 | 16 | 16 |
| **Итоговая аттестация** | |  | **Итоговое тестирование** | | |
|  | | **72** | Итоговое тестирование | | |

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

(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Введение в продуктовую безопасность | 16 | 4 дн (1-4 день) |
| **2** | Программные средства защиты | 18 | 5 дней (5-9день) |
| 6 | Уязвимости веб-приложений | 38 | 10 дней (9 -18 день) |
| **Всего:** | | 72 | **18 дней** |

**6.Учебно-тематический план программы «** Security Champion **»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Модуль 1. Введение в продуктовую безопасность | 16 | 8 | 4 | 4 | тест |
| 1.1 | Введение в информационную безопасность | 4 | 2 | 1 | 1 |  |
| 1.2 | Оценка рисков безопасности приложения | 4 | 2 | 1 | 1 |  |
| 1.3 | Разработка безопасного кода | 4 | 2 | 1 | 1 |  |
| 1.4 | Практики защиты кода | 4 | 2 | 1 | 1 |  |
| 2. | Модуль 2.  Программные средства защиты | 18 | 12 | 3 | 3 | тест |
| 2.1 | Статический анализ кода | 6 | 4 | 1 | 1 |  |
| 2.2 | Динамический анализ приложений | 6 | 4 | 1 | 1 |  |
| 2.3 | Инструменты для защиты окружения | 6 | 4 | 1 | 1 |  |
| 3. | Уязвимости веб-приложений | 38 | 22 | 8 | 8 |  |
| 3.1. | Уязвимости веб-приложений | 4 | 2 | 1 | 1 |  |
| 3.2. | Устройство современных веб-приложений и сбор информации | 4 | 2 | 1 | 1 |  |
| 3.3. | Уязвимости OS Command injection | 4 | 2 | 1 | 1 |  |
| 3.4. | Уязвимость SQL Injection | 8 | 6 | 1 | 1 |  |
| 3.5. | Аутентификация и менеджмент сессий. Онлайн брутфорс. Оффлайн брутфорс | 6 | 4 | 1 | 1 |  |
| 3.6. | Уязвимости path traversal, file upload, local file read | 4 | 2 | 1 | 1 |  |
| 3.7. | Broken Access Control | 4 | 2 | 1 | 1 |  |
| 3.8. | CORS. XSS | 4 | 2 | 1 | 1 |  |
|  | Итоговая аттестация | 2 |  |  | 2 | Итоговое тестирование |

**7. Учебная (рабочая) программа повышения квалификации «** Security Champion**»**

Модуль 1. Введение в продуктовую безопасность (16 часов).

Тема 1.1 Введение в информационную безопасность (4 часа)

Содержание темы:

* Основные понятия информационной безопасности (кратко)

Тема 1.2 Оценка рисков безопасности приложения (4 часов)

Содержание темы:

* Модели STRIDE и DREAD
* Стандарты ГОСТ/ISO и NIST в части требований к защищенности ПО

Тема 1.3 Разработка безопасного кода(4 часа)

Содержание темы: Основные уязвимости программного кода

Тема 1.4 Практики защиты кода (4 часа)

Содержание темы:

- Обработка ошибок

- Защита API

- Криптография

- Токенизация

- Обработка исключений

- Санитизация ввода

Модуль 2. Программные средства защиты (18 часов)

Тема 2.1. Статический анализ кода (6 часов)

Содержание темы:

- Виды анализаторов исходных кодов

- Развертывание и применение SonarQube

- Анализ зависимостей кода и чистоты лицензий

Тема 2.2. Динамический анализ приложений (6 часов)

Содержание темы:

- Инструменты анализа уязвимостей BurpSuite, w3af, OWASP ZAP

- Фаззинг

- Нагрузочное тестирование

Тема 2.3. Инструменты для защиты окружения (6 часов)

Содержание темы:

- WAF

- Мониторинг инфраструктуры

Модуль 3. Уязвимости веб-приложений (38 часов)

Тема 3.1. Уязвимости веб-приложений (4 часов)

Содержание темы:

* Основные веб-технологии: HTTP, URL, HTML, Javascript, CSS
* Ознакомиться с основными тегами HTML
* Протоколы HTTP
* Программное обеспечение Burp Suite

Тема 3.2. Устройство современных веб-приложений и сбор информации (4 часа)

Содержание темы:

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

Тема 3.3. Уязвимости OS Command injection (4 часа)

Содержание темы:

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

Тема 3.4. Уязвимость SQL Injection (8 часов)

Содержание темы:

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

Тема 3.5. Аутентификация и менеджмент сессий. Онлайн брутфорс. Оффлайн брутфорс. (6 часов)

Содержание темы:

* Аутентификация
* Хранение паролей
* Сессионный менеджмент
* patator - инструмент для онлайн брутфорса
* hashcat
* Определение типа хэша
* Обсуждение словарей
* Работа с правилами hashcat
* Брутфорс по маске

Тема 3.6. Уязвимости path traversal, file upload, local file read. (4 часа)

Содержание темы:

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

Тема 3.7. Broken Access Control (4 часа)

Содержание темы:

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

Тема 3.8. CORS. XSS (4 часа)

Содержание темы:

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

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| 1 | Тема 1.1. Введение в информационную безопасность | Обучение коллег в качестве Security Champion | Составить план занятия для коллег-разработчиков с основными понятиями информационной безопасности. |
| 2 | Тема 1.2 Оценка рисков безопасности приложения | Составление модели угроз | Практическое задание на отработку умения создавать модель угроз.. Для выполнения данного задания необходимо составить текстовое описание возможных угроз для представленного веб-приложения и сделать диаграмму на основе приложения на выбор - ThreatDragon, Microsoft Threat Modeling Tool, SeaSponge. |
| 3 | Тема 1.4 Практики защиты кода | Составление рекомендаций по исправлению кода | Практическое задание на отработку умения нахождения ошибок в коде.  Среди найденных ошибок по темам, необходимо описать ошибки и предложить варианты исправления для разработчиков. |
|  | Тема 2.1 Статический анализ кода | Развертывание и использование SonarQube | Практическое задание на отработку умения развертывать инструменты и пользоваться ими. Необходимо развернуть на локальной машине SonarQube, настроить сканер и просканировать DVWA(Damn Vulnerable Web Application) |
|  | Тема 2.2 Динамический анализ приложений | Написание собственного фаззера на Python | Необходимо написать скрипт, который будет осуществлять перебор значений и проверять устойчивость сервиса для больших входных данных |
|  | Тема 2.3 Инструменты для защиты окружения | Развертывание modsecurity | Необходимо развернуть в локальном окружении modsecurity |
|  | Тема 3.1. Уязвимости веб-приложений |  | Выполнить соответствующее задание с root-me.org |
|  | Тема 3.2. Устройство современных веб-приложений и сбор информации |  | Выполнить соответствующее задание с root-me.org |
|  | Тема 3.3. Уязвимости OS Command injection |  | Выполнить соответствующее задание с root-me.org |
|  | Тема 3.4. Уязвимость SQL Injection |  | Выполнить соответствующее задание с root-me.org |
|  | Тема 3.5. Аутентификация и менеджмент сессий. Онлайн брутфорс. Оффлайн брутфорс. |  | Выполнить соответствующее задание с root-me.org |
|  | Тема 3.6. Уязвимости path traversal, file upload, local file read. |  | Выполнить соответствующее задание с root-me.org |
|  | Тема 3.7. Broken Access Control |  | Выполнить соответствующее задание с root-me.org |
|  | Тема 3.8. CORS. XSS |  | Выполнить соответствующее задание с root-me.org |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |
| --- | --- | --- |
| **№ модуля** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| 1.1. | Тестирование модуль 1 | 1.Главная причина внедрения безопасности в процесс разработки ПО:   1. неавторизованное раскрытие информации 2. защита корпоративного бренда и репутации 3. защита от хакеров, которые могут изменить работу ПО 4. оградить разработчиков от выпуска ПО, которое может содержать дефекты   2. Стойкость ПО к атакам, которые могут привести к изменению или дублированию данных относится к:   1. Конфиденциальности 2. Целостности 3. Доступности 4. Аутентификации   3. Основная причина, по которой показатели доступности ПО должны быть частью процесса безопасности:   1. ошибки в ПО могут привести к бизнес-потерям 2. разработчикам необходимо обучиться процедурам непрерывности бизнеса 3. тестирование доступности сервисов часто игнорируется 4. хакеры любят осуществлять атаки типа “отказ в обслуживании” (DDoS)   4. В случае, когда пользователь банка пытается зайти в устройство, от него требуется ввести код из токена. Какой в данном случае применяется тип аутентификации?:   1. Нечто, чем мы обладаем 2. Двухфакторная аутентификация 3. Нечто, что является частью нас самих 4. Нечто, что мы знаем   5. Какому из следующих принципов безопасного дизайна наиболее соотвествует многофакторная аутентификация:   1. Разделения обязанностей 2. Глубинной защиты 3. Полной проверки 4. Открытого дизайна |
| 1.2 |  | 1. Требование принятия конечным пользователем пользовательского соглашения “as-is” является примером:   1. Избегания риска 2. Смягчения риска 3. Переноса риска 4. Принятием риска   2. Стоимость актива равна 200$, фактор риска - 56%. Ежегодная частота возникновения - 1,2. Необходимо вычислить ожидаемые ежегодные потери:   1. 13378 2. 13440 3. 14082 4. 12896   3. Управление рисками ИБ регулируется следующим стандартом:   1. ГОСТ Р ИСО/МЭК 27005-2010 2. ГОСТ Р ИСО/МЭК 27003-2012 3. ГОСТ Р ИСО/МЭК 27033-4-2014 4. ГОСТ Р ИСО/МЭК 15408-1-2008   4. Какой из нижеперечисленных стандартов применяется для регламентирования работы организаций, которые собирают, обрабатывают и/или хранят данные банковских карт?   1. FIPS 201 2. ISO/IEC 15408 3. NIST SP 800-64 4. PCI DSS |
| 2. | Статика, динамика инструменты.  Тестирование модуль 2 | 1. Какого из нижеприведенных методов сканирования не существует:   - IAST  - DAST  - SAST  - MAST   1. Какой из нижеперечисленных инструментов не является анализатором исходных кодов (SAST):   - Microfocus Fortify  - Checkmarx  - Burp Suite  - PyBandit   1. Необходимо анализировать сторонние зависимости исходных кодов с целью:   - избегать уже исследованных уязвимостей в библиотеках  - избежать zero-day уязвимостей  - обеспечить соответствие стандартам разработки  - избежать необходимости проводить тестирование на проникновение   1. Главной целью тестирования на отказоустойчивость ПО явлчяется определение:   - точки в которой ПО перестанет работать  - сможет ли ПО самостоятельно восстановиться для работы в нормальном режиме  - наличие и эффективность механизмов смягчения рисков  - того, как blackhat может обойти механизмы контроля доступа   1. Какой из следующих компонентов архитектуры Java главным образом предназначен для проверки консистентности типов, безопасности и отсуствия вредоносных инструкций в коде   - Сборщик мусора  - загрузчик классов  - верификатор байткода  - Java Security Manager   1. Подпись исполняемого кода может обеспечить все нижеперечисленное, кроме:   - защита от фальсификации кода  - подтверждение источника кода  - права выполнения для кода  - аутентификация пользователей   1. Главное преимущество статического анализа кода заключается в:   - анализе поведения кода в среде выполнения  - более легком выявлении ошибок в бизнес-логике  - проведении анализа в продакшн среде, или максимально схожем окружении  - ошибки и уязвимости могут быть найдены на ранних этапах жизненного цикла продукта |
| 3. | Тестирование. Модуль 3 | 1. Ниже приведено содержимое HTTP запроса. Чем является `user` в этом запросе:  ```  POST /files/download?user=admin HTTP/1.1  Host: yandex.ru:5050  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:74.0) Gecko/20100101 Firefox/74.0  Accept: application/json, text/javascript, \*/\*; q=0.01  Accept-Language: en-US,en;q=0.5  Accept-Encoding: gzip, deflate  Connection: close  Referer: http://localhost:5000/panel  ```  - HTTP заголовком  - именем параметра  - путем к ресурсу  - методом HTTP  2. Строка `dXNlcjp1c2VyCg==` скорее всего закодирована с помощью:  - URL-кодирования  - хэш-функции  - base64  - HEX-кодирования  3. При запуске dirsearch словарь передается в параметре:  - -d  - -x  - -u  - -w  4. OS Command injection относятся к следующему пункту OWASP Top 10:  - A1  - A2  - A3  - A5  5.При эксплуатации SQL инъекции с помощью техники Error based атакующий:  - Вызывает критическую ошибку и падение сервера СУБД  - Выводит полезную для него информацию в сообщение об ошибке, отображаемое веб-приложением  - Вызывает ошибку SQL, приводящую к тому, что веб-приложение принимает его за администратора  - Объединяет информацию из двух таблиц в одну  6.Выберите вектор для обхода аутентификации.  SQL запрос:  `SELECT \* FROM users WHERE username='<username\_input>' and password='md5(<password\_input>)'`  , тут мы контролируем '<username\_input>, <password\_input> тоже контролируем, но от него вычисляется md5-хэше перед подстановкой в запрос:  - username\_input=or 1='1  + username\_input=' or 1=1 --  - username\_input=' and 1=1 --  - username\_input=' where 1=1 --  7. Уязвимость, при которой атакующий может обращаться к файлам вне ожидаемой директориях:  - File Upload  - Archive issue  + Path Traversal  - LFI  8. Нулевой байт может быть использован атакующим для того чтобы:  + отбросить добавляемую веб-приложением строку  - заставить веб-приложение вывести ошибку  - загрузить файл в произвольную директорию  - вызвать переполнение буфера |

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

Шкала оценивания промежуточного и итогового тестирования

|  |  |  |
| --- | --- | --- |
| Критерии | Шкала | Описание |
| зачтено | Обучающийся успешно выполнил входной тест: 50%-100% верных ответов на вопросы теста | Потенциальный обучающийся успешно выполнил входной тест и может быть допущен к обучению по программе |
| не зачтено | Обучающийся не выполнил успешно входной тест: 0%-49% верных ответов на вопросы теста | Потенциальный обучающийся не выполнил успешно входной тест и не может быть допущен к обучению по программе |

**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)** | **Ссылки на веб-страницы с портфолио (при наличии)** | **Фото в формате jpeg** | **Отметка о полученном согласии на обработку персональных данных** |
| **1** | Афанасьев Иван | Application Security Specialist | [**https://hackeru.pro/o-nas/**](https://hackeru.pro/o-nas/) **подраздел Преподаватели.**  [**https://drive.google.com/file/d/1KlASoxe6kXbAZMcLwUCSloIH0NN3KGhM/view?usp=sharing**](https://drive.google.com/file/d/1KlASoxe6kXbAZMcLwUCSloIH0NN3KGhM/view?usp=sharing)  **6 лет практического опыта в сфере ИБ. Изучал подходы к ИБ с точки зрения бизнеса,**  **занимался наполнением базы знаний Windows для сканера MaxPatrol. Налаживал процессы**  **управления уязвимостями и безопасной разработки, участвовал в разработке архитектуры**  **безопасности банковских продуктов, проводил обучение безопасной разработке для**  **заказчиков.** |  | да |

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

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Проблемно-развивающие методы  Исследовательский метод  Объяснительно-иллюстративный метод  Частично-поисковый метод  Метод контроля и самоконтроля  Самостоятельная работа по освоению теоретического материала  Самоконтроль через ответы на вопросы по видеолекциям и выполнение практических заданий для самоконтроля  Промежуточный контроль (тесты по темам для промежуточной аттестации)  Итоговый контроль (итоговое тестирование по курсу)  Консультативная поддержка преподавателя и менторов в режиме онлайн. | 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 | 1. Операционная система семейств Windows, Mac Os, Linux. 2. Браузер:   • Firefox 64  • Chrome 61  • Safari 11  • Opera 57   1. Рекомендуемые программы: 2. 1. ОС: Windows/Linux/MacOS 3. 2. Docker Desktop: https://www.docker.com/products/docker-desktop 4. 3. python3: https://www.python.org/downloads/ 5. 4. php: https://www.php.net/downloads 6. 5. Burp Suite CE: https://portswigger.net/burp/communitydownload 7. Рекомендуется от 128 кбит/сек исходящего потока. 8. Рекомендуется от 256 кбит/сек входящего потока. |
| Дополнительные теоретические материалы | 1. Операционная система семейств 2. Windows, Mac Os, Linux. 3. Браузер:   • Firefox 64  • Chrome 61  • Safari 11  • Opera 57   1. Рекомендуется от 128 кбит/сек исходящего потока. 2. Рекомендуется от 256 кбит/сек входящего потока. |
| Аттестационный компонент | 1. Операционная система семейств 2. Windows, Mac Os, Linux. 3. Браузер:   • Firefox 64  • Chrome 61  • Safari 11  • Opera 57   1. Рекомендуется от 128 кбит/сек исходящего потока. 2. Рекомендуется от 256 кбит/сек входящего потока. |
| Практический компонент | * VirtualBox / VMWare / Parallels * Docker, Docker-compose * Kubernetes * Vulners scanner * W3af * PyBandit * Sonar * Burp Suite * Python3 * PHP * SQLMAP * Tenable Nessus * Dependency Сheck * Apache & Nginx * Sublime Text 3 * Android Studio * MobSF * Drozer |

**ПАСПОРТ КОМПЕТЕНЦИИ**

**Дополнительной профессиональной образовательной программы повышения квалификации**

**«**Security Champion**»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. | Наименование компетенции | | Выполнение работ для формирования профессиональных компетенций в области анализа защищенности веб-приложений и сайтов | |
| 2. | Указание типа компетенции | общекультурная/  универсальная |  | |
| общепрофессиональная |  | |
| профессиональная |  | |
| профессионально-специализированная | Да | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | | 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.  Уметь решать профессиональные задачи:  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. | |
| 4. | Дескриптор знаний, умений и навыков по уровням | | Уровни сформированности компетенции  обучающегося | Индикаторы |
|  | | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | Знает:  - о протоколах, работающих в сети Интернет  - о том, как работают веб-приложения  - о протоколе HTTP и его устройстве  Умеет:  Работать с веб-приложениями на уровне отдельных запросов к ним и модификации параметров через инструменты разработчика.  Владеет:  Навыками изучения систем в виде абстракций, взаимодействующих в сети или на уровне клиент-серверной модели в веб-приложениях.  Навыками написания простейших скриптов на любом языке программирования. |
|  | | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределённости, сложности.) | Знает:  Устройство протокола HTTP и протокола HTTPS с использованием TLS;  Устройство PKI (Public Key Industry);  Устройство современных веб-приложений и фреймворков, с использованием которых они разрабатываются.  Умеет:  Разрабатывать собственные веб-приложения и отлаживать их код на любом языке программирования.  Отлаживать работу произвольных веб-приложений.  Изучать работу веб-приложения и составлять карту вызовов методов веб-приложения и его файловой структуры.  Владеет:  Навыками анализа веб-приложений.  Знаниями о ряде типовых уязвимостей веб-приложений.  Навыками эксплуатации малого ряда типовых уязвимостей веб-приложений. |
|  | | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | Знает:  Особенности разработки современных веб-приложений, их общую структуру и подходы к их реализации.  Основы несколько языков программирования и шаблоны проектирования приложений для них.  Знает множество типовых уязвимостей, возможности их эксплуатации, а также понимает ущерб, который они могут реализовать.  Умеет:  Быстро анализировать техническую документацию.  Умеет в короткий срок разворачивать стенд для отладки веб-приложений и восстанавливать реализацию веб-приложения по информации об используемым приложением стеке технологий.  Эксплуатировать уязвимости и знает о том, как закрепляться в скомпрометированных системах.  Владеет:  Продвинутым пониманием о том, как определять используемые в приложении фреймворки, языки программирования и технологии. Знает их основные уязвимости, условия их небезопасной конфигурации, и знает, как эксплуатировать данные особенности для демонстрации наличия уязвимостей. |
|  | | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействующими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | Знает:  Особенности реализации большинства популярных фреймворков и языков программирования.  Знает редкие детали технологий и программного обеспечения позволяющие эксплуатировать уязвимости в случаях, когда тривиальные методы эксплуатации бесполезны.    Умеет:  Обнаруживать не типовые уязвимости и уязвимости «нулевого дня» в программном обеспечении.  Эксплуатировать самые продвинутые техники атак в различных системах, в том числе уязвимости языков низкого уровня (т.н. «бинарные уязвимости»).  Владеет:  Навыками эксплуатации из областей сторонних от области веб-технологий. Богатой технической эрудицией и опытом выполнения проектов по анализу защищенности приложений и различного программного обеспечения. |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | | Для формирования данной компетенции слушатель должен владеть:  • компетенциями цифровой грамотности, в том числе навыками владения ПК на уровне среднего или продвинутого пользователя; | |
| 6. | Средства и технологии оценки | | Итоговое тестирование по модулям | |

**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.