Статья · Развлечения

Где учиться пентесту, обзор площадок для практики навыков этичного хакера

Ярослав Ковальчук · Product Manager · Hackerone
Ярослав Ковальчук · Product Manager · Hackerone · 1 ноября 2021 в 10:00

Реклама
Разработка графических интерфейсов с использованием библиотеки wxPython и утилиты wxGlade. Курс для начинающих. Для тех, кто хочет научиться писать свои кроссплатформенные приложения на Python. Скидка 15% по промокоду «habr» — от цифр частного бизнеса к сфере, где вы зарабатываете.
Erlang/OTP: Серверные приложения. Курс для начинающих. Для тех, кто хочет научиться писать свои серверные приложения на Erlang/OTP. Скидка 15% по промокоду «habr» — от цифр частного бизнеса к сфере, где вы зарабатываете.
Реклама скрыта для пользователей с рейтингом выше 0.

Всем привет! Сегодня мы поговорим, какие бывают виды и форматы баг-баунти, что такое Hacker One и Bug Bounty, как выглядит и зачем нужен сертификат, а также расскажем, как выбрать подходящую для себя платформу и начать свой путь в этичном хакинге.

Структура рисунков

Сначала разберемся, что вообще такое баг-баунти и что оно из себя представляет. Определение звучит сложновато: «Программа, в рамках которой сообщают о багах Вашим компаниям».

- **Баг-баунти** — это поиск уязвимостей в системе Bug Bounty, которые выполняют хейкеры — «белые шляпы» и предоставляют отчеты. Обычно вознаграждение зависит от критичности уязвимости, а также от того, насколько сложно было ее найти. Для каждой компании доверяется ограниченное количество хейкеров, которые выполняют задания. Такие программы можно запустить на своей инфраструктуре, а можно воспользоваться сервисами, которые предоставляют инфраструктуру, а также помогают с организацией и проведением.
- **Приватные программы** — это поиск уязвимостей в системе Bug Bounty, которые выполняют хейкеры — «белые шляпы» и предоставляют отчеты. Обычно вознаграждение зависит от критичности уязвимости, а также от того, насколько сложно было ее найти. Для каждой компании доверяется ограниченное количество хейкеров, которые выполняют задания. Такие программы можно запустить на своей инфраструктуре, а можно воспользоваться сервисами, которые предоставляют инфраструктуру, а также помогают с организацией и проведением.
- **Приватные пентесты** — это поиск уязвимостей в системе Bug Bounty, которые выполняют хейкеры — «белые шляпы» и предоставляют отчеты. Обычно вознаграждение зависит от критичности уязвимости, а также от того, насколько сложно было ее найти. Для каждой компании доверяется ограниченное количество хейкеров, которые выполняют задания. Такие программы можно запустить на своей инфраструктуре, а можно воспользоваться сервисами, которые предоставляют инфраструктуру, а также помогают с организацией и проведением. Такие программы можно запустить на своей инфраструктуре, а можно воспользоваться сервисами, которые предоставляют инфраструктуру, а также помогают с организацией и проведением.
- **Приватные пентесты** — это поиск уязвимостей в системе Bug Bounty, которые выполняют хейкеры — «белые шляпы» и предоставляют отчеты. Обычно вознаграждение зависит от критичности уязвимости, а также от того, насколько сложно было ее найти. Для каждой компании доверяется ограниченное количество хейкеров, которые выполняют задания. Такие программы можно запустить на своей инфраструктуре, а можно воспользоваться сервисами, которые предоставляют инфраструктуру, а также помогают с организацией и проведением. Такие программы можно запустить на своей инфраструктуре, а можно воспользоваться сервисами, которые предоставляют инфраструктуру, а также помогают с организацией и проведением.

Полностью готовые на свободные системы и имеют полные сервисы, так по запросу, обработчики, которые выполняют задания.

Hack The Box

Hack The Box — это обобщенный термин, который объединяет несколько сервисов и платформ. Сервисы, которые предоставляют Hack The Box, выполняют задания, которые выполняют хейкеры, при выполнении заданий. Сервисы предоставляют, что задания могут быть разными, а также могут быть разными по сложности. Задания выполняются на своей инфраструктуре, а также могут быть выполнены с помощью сервисов, которые предоставляют инфраструктуру, а также помогают с организацией и проведением.

Скриншоты с сервиса Hack The Box

Основная цель, что Hack The Box предоставляет для исследования своей инфраструктуры, а также для Red Teamов — это сервис Pro Labs. Сервис Pro Labs предоставляет возможность для исследования и изучения