[WAPT]

9.1 Литература и площадки для практики

Содержание

Литература

Курс подходит к концу. Поэтому можно уже обернуться назад и увидеть, сколько нового вы уже узнали. Но полученные знания являются лишь основой для старта своей карьеры как пентестера веб приложений. Ниже будет представлена информация для того, чтобы вы смогли составить свой вектор развития. Все знать невозможно, но специфика профессии такова, что приходится знать многое. Описанная ниже литература поможет быстро заполнить пробелы в базе.

Основные области, на которые стоит обратить внимание:

- Сети – самая важная часть. Это знать необходимо. Поэтому, если есть большие пробелы в этом, стоит в первую очередь с этого и начать.
- Программирование – так как вы начинающие пентестеры именно веб приложений, то естественно необходимо понимание устройства этих приложений. При этом эту часть можно поделить на две большие группы:
    - Frontend – пользовательский интерфейс и все, что с ним связано;

    - Backend – серверная часть. То, с чем вы больше всего работали на курсе;
- Хакинг – специфическая часть. Обогатит ваш арсенал и покажет опыт успешных пентестеров.

Сети

1. “Компьютерные сети” Э. Таненбаум – выбор большинства сетевиков от признанного эксперта в этой области. Эту книгу, как минимум, надо просмотреть и сделать заметки;
2. “Web-протоколы. Теория и практика” Б. Кришнамурти – стоит иметь при себе как справочник. Хорошо подходит для быстрого повышения уровня базовых знаний в области веб приложений;
3. “Разработка приложений клиент/сервер для Linux/POSIX” Д. Камер – книга ориентирована на программистов, поэтому к ней стоит приступать, когда есть хотя бы база в программировании, но даст хорошее понимание устройства клиент-серверных приложений и всего, что с этим связано;
4. “Сети для самых маленьких” https://habr.com/en/post/134892/ - помимо книг стоит обратить внимание и на веб-ресурсы с очень полезной информацией. В этом курсе статей хорошо объясняются основы основ сетей и маршрутизации. После прохождения нашего курса увас достаточно знаний, чтобы понимать, о чем идет речь в этих статьях;
5. “База знаний от gurkin33” http://www.gurkin33.ru/ - полезный ресурс, который научит основам маршрутизации на устройствах CISCO с хорошими практическими примерами;
6. “CISCO Packet Tracer” - без практики мало что получится усвоить, поэтому стоит освоить этот инструмент. Он может моделировать устройство сети, а также визуализирует ее работу. Используется в курсе и пункта 6.

Программирование

В нашем современном культурном обществе без программирования практически никуда. Трудно найти область, где бы ни использовались техники программирования. Администрирование сетей, баз данных,

верстка веб страниц, тестирование приложений – все это, в той или иной мере, использует программирование. Следовательно, знать их просто необходимо. Речь не идет об уровне знаний Senior Developer. Как минимум необходимы общие знания, при которых написать простенький скрипт для парсинга страницы или обработки входящих сообщений на сервер не составит больших трудов, какой бы язык вы не выбрали.

Стоит выделить несколько языков программирования:

- PHP
- Python
- JS

Для пентестера веб приложений начинать изучать программирование с этих языков полезно в наше время, причем все их в равной мере (не стоит рекомендовать начинать учить программирование с этих языков людям, которые хотят связать свою карьеру именно с программированием).

Frontend

Область именно клиентской части для пентестера веб приложений весьма продуктивна. Комбинации XSS, CSRF, Phishing и Social Engineering могут взять даже самую защищенную крепость, ведь самая большая уязвимость была, есть и будет - именно человек. Из языков программирования тут JS. Так же необходимо знать HTML и CSS.

Следующие книги могут помочь в освоении темы:

1. “HTML5, CSS3 и JavaScript. Исчерпывающее руководство” Р. Нидерст – три в одном. То, что нужно для получения базы. Полезно изучать вместе с сетями, ведь там также описываются принципы работы сети интернет и веб сайтов;
2. “You Don’t Know JS” К. Симпсон – сборник из шести книг. Каждая по-своему полезна для понимания работы языка;
3. “Современный учебник JavaScript” https://learn.javascript.ru/ - стоит обратить внимание на этот ресурс. Достаточно пройти данныйкурс для получения базы в синтаксисе;

4. “HTML Academy” https://htmlacademy.ru/ - онлайн курс по HTML, CSS. Есть платный контент, но не дорогой. Пройдя его, вы получите хорошую базу в верстке;
5. “HTML Book” http://htmlbook.ru/ - удобный справочник по HTML, CSS. Стоит добавить в закладки.

Backend

Очень обширная область. Вы уже должны были заметить, что больше всего уязвимостей именно в серверной части приложений. Основные языки программирования: PHP, Python, Node.js, Java. Каждый из языков имеет много особенностей - знать все не получится. Стоит пройтись по основам двух, трех языков, а особенности каждого уже изучать из книг по хаккингу и тематических статей.

1. “PHP документация” https://www.php.net/ – очень полезна и хорошо описана. Стоит добавить в закладки;
2. “Самоучитель PHP 7” И. Симдянов – книга поможет получить основы языка и его взаимодействия с различными БД;
3. “Создаем динамические веб-сайты с помощью PHP, MySQL, JavaScript, CSS и HTML5” Р. Никсон – пять в одном. Сразу и клиентская часть и серверная. Полезно и быстро;
4. “Изучаем Python” М. Лутц – с этой книгой та же история, что и с “Компьютерные сети” Э. Таненбаума. Книга - выбор большинства программистов. Вполне подойдет как справочник, но книга очень большая;
5. “Python 3 и PyQt. Разработка приложений” Н. Прохоренков – познакомит с основами программирования и разработки приложений;
6. “Node.JS” https://nodeguide.ru/doc/ и https://www.nodebeginner.org - стоит обратить внимание именно на эти ресурсы, но приступать к Node.JS стоит только после того как получите базу в JS;
7. “Head First Java” - очень простая и легкая для чтения книга по Java. Выбор начинающих, однозначно;
8. “Руководство для начинающих” Г. Шилдт – выбор большинства программистов Java. Такой же случай, как и с “Компьютерные сети” Э. Таненбаума или “Изучаем Python” М. Лутца.

Хаккинг

1. “Penetration Testing with Kali Linux” - стоит прочитать чуть ли не самой первой и использовать как справочник;
2. “Хакер.ру” https://xakep.ru/ - наверняка вы уже знаете, что это за ресурс;
3. “The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy” - поможет закрепить и проверить полученные на курсе знания, а также научит правильному составлению отчетов;
4. “Metasploit: The Penetration Tester’s Guide” - уметь пользоваться этим инструментом очень важно для пентестера;
5. “Certified Ethical Hacker Review Guide” - стоит читать после того, как получите базу в сетях. Охватывает все области современного пентеста;
6. “Codeby.net” https://codeby.net/forums/ - не забываем про наш форум: множество статей, а в библиотеке сможете найти большое количество книг по хакингу.

Стоит отметить, что если просто читать все это, то пользы будет мало. Все, что прочитали, проверяйте на практике. Поднимайте свои веб сервера, настраивайте PHP, CMS, CRM. В CISCO Packet Tracer создавайте свои сети, пробуйте писать свои приложения. Авторизация,аутентификация, доступ к БД, обработка пользовательского ввода. Если все это делать, то ваши навыки будут просто взлетать. Практика – самыйважный аспект.

Площадки для практики

В этой части перечислены площадки для прокачки своего скилла. Без практики, всю теорию, которую вы прочитали, можно смело забывать, потому что она вам не поможет без практики. Большинство площадок имеют CTF направление. В некоторых моментах это развивает больше, чем реальные кейсы.

1. “hack the box” https://www.hackthebox.eu - это то, что поможет вам быть в потоке в области пентеста. С текущими знаниями вам будет не просто, но решаемо;

2. “Pentestit” https://lab.pentestit.ru - ежегодно проводит соревнования, где предлагают взломать корпоративную сеть. Есть возможность пройти уже закончившиеся. Польза аналогичная, как и от hack the box;

Стоит отметить, что оба ресурса выше не относятся именно к пентесту веб приложений. Они охватывают весь спектр.

3. “Root Me” https://www.root-me.org - площадка предоставляет задания, аналогичные тем, что вы решали на курсе. Цель - получить флаг. Заданий много и различной сложности. Вместе с заданием предлагается и документация, которая помогает решать таск. Отличное место, чтобы улучшить свои навыки взлома и знания в области веб-безопасности с помощью более чем 200 хакерских атак и 50 виртуальных сред;

4. “Hack This” https://www.hackthis.co.uk - очередная площадка для практики. Задания аналогичные задачам на курсе. Задач не много и половину вы уже должны решить быстро и непринужденно;

5. “HackMe” https://hack.me - аналог root-me или hackthis;

6. “Damn Vulnerable Web Application (DVWA)” http://www.dvwa.co.uk - основан на PHP и работает на сервере баз данных MySQL, который действительно чертовски уязвим. Он имеет три уровня безопасности: Низкий, средний и высокий. Каждый уровень безопасности требует различных навыков. Разработчики также решили поделиться его исходным кодом, чтобы исследователи в области безопасности могли видеть, что происходит на внутреннем сервере;

7. “PentesterLab” https://pentesterlab.com;

8. “DevSecOps Bootcamp” https://github.com/devsecops/bootcamp;

9. “OWASPWebGoatPHP” https://www.owasp.org/index.php/WebGoatPHP;

Всех этих площадок более чем достаточно, чтобы поддерживать себя в тонусе. Так же советуем зарегистрироваться на https://ctftime.org/, следить за ходом соревнований и участвовать в них. Можно как одиночка, заодно и оценить свои способности. Не обязательно ради призовых мест, но на таких соревнованиях практически всегда есть часть “Web”. Как раз то, чему вы обучались у нас.

Служба Поддержки

8 800 444 1750

с 8:00 до 20:00 МСК

school@codeby.net