ПЛАН ВКАТЫВАНИЯ В INFOSEC/BUG BOUNTY.

В целом при полном выполнении этих пунктов в теории можно успешно вкатиться в Infosec/bug bounty. При этом список избыточен, но должен дать стабильную базу.

Точно есть талантливые хакеры, которые не имея никаких описанных ниже знаний, шли по пути "поставил бурп, начал хакать, через год вошел в топ 100 на hackerone". Но это скорее исключение чем правило.

В подпунктах Optional указаны необязательные вещи, которые можно отложить на потом, для дальнейшего изучения, когда уже вкатился.

Идти стоит сверху вниз, хотя какие-то вещи, типа чтения книг по инфосек, и прохождение курса по SQL, можно делать параллельно.

CODING.

- Learn Python The hard way
- https://www.codecademy.com/learn/learn-python

Уже после хорошего понимания Питона:

- Создаем и подниммаем свой сайт на Джанго (фреймворк в Питоне для веба), можно сделать за вечер, пройдя любой курс на youtube по запросу build site on django
- https://www.codecademy.com/learn/learn-html?composer_curriculum_redirect=web +
- https://www.codecademy.com/learn/introduction-to-javascript +
- https://www.codecademy.com/learn/learn-sql +
- Start ruby
- Start jango
- Php course

Optional:

- Learn Python 3 the Hard Way
- Learn More Python 3 the Hard Way
- Black Hat Python: Python Programming for Hackers and Pentesters
- Gray Hat Python: Python Programming for Hackers and Reverse Engineers
- http://www.learn-php.org/
- https://www.codecademy.com/learn/learn-java
- https://tour.golang.org

Один основной язык программирования, в теории не важно какой. На практике по совокупности доступных материалов и легкости освоения конечно Питон 2. Остальные языки подтянуть по мере надобности.

Ничего лучше в плане обучения чем Learn Python The hard way, я еще не видел. И сам язык, и автотесты, и даже объяснение работы веб приложений. Плюс отполировать курсом с Codecademy.

Курсы по JS и HTML пробежать, просто для базового понимания устройства страницы и того как работают XSS. Курсы Java/php уже сильно потом, когда вкатился в тему, надо на базовом уровне уметь читать все языки.

Многие курсы с Codecademy можно пройти за один выходной. SQL - обязательно, базовый курс для понимания того как оно вообще работает, хотя на практике все юзают SQLmap.

Но тот кто умеет тестить SQLinj руками, имеет преимущество. Питон- обязательно писать код хотя бы минут по 30 в день, можно идти дальше по упражнениям из книг, можно писать мелкие утилиты для багхантинга. Если просто прочитать LPTHW, и больше не писать код через несколько месяцев забудется почти все. Потом стоит присмотреться к go, он набирает популярность во всех сферах, особенно в infosec.

TOOLS:

- Burp suite. https://www.youtube.com/watch?v=AVzC7ETqpDo
- SQLmap
- dirsearch
- nmap

- Sublister

Optional:

- Burp Advanced course: https://www.youtube.com/watch?v=VhdcOSxa80w

Тулзов море, это базовые, в какой-то момент сам выберешь что именно стоит юзать, часть уже переписана на go, и работает эффективнее. По каждому можно найти курс/видео на youtube либо просто почитать readme.

REGEX/COMMAND LINE.

- Command line crash course (Zed Shaw)
- https://regexone.com/

Регулярки, хотя бы на уровне понимания того что значат символы $,^,*,.,\. В дальнейшем они+sed очень помогут в обработке данных после сканирования.

READING:

- OWASP Top 10 2017 https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf
- OWASP Testing Guide v4 https://www.owasp.org/index.php/OWASP_Testing_Project
- Web Hacking 101
- Breaking into Information Security
- The Web Application Hacker's Handbook: Discovering and Exploiting
- Mastering Modern Web Penetration Testing (Prakhar Prasad)

Optional:

- The Tangled Web: A Guide to Securing Web Applications
- The Mobile Application Hacker’s Handbook
- Network Security Assessment: Know Your Network 158 - Chris Mcnabb has produced 2 editions before this one and this serves as an update to the 2nd edition bringing together different techniques for network enumeration and fingerprinting.

- The Hacker Playbook 2159 - A practical guide which follows a similar methodology to the Infrastructure section of this book.
- Metasploit: The Penetration Tester's Guide 160 - A little bit dated now however still useful for understanding how metasploit works and the different features available at your disposal.
- Penetration Testing: A Hands on guide to hacking 161 - This lends its hand to the hacker
- playbook 2 however gives a deeper overview of the different aspects within penetration testing.
- Bash Pocket Reference 171
- PowerShell Pocket Reference 172
- Red Team Field Manual 173
- Blue Team Field Manual 174

COURSES INFOSEC

- https://www.hacker101.com/
- HackerOne course
- OSCP

Optional:

- all courses from offencive security
- metasploit free sourse offensive security
- MIT infosec
- https://serversforhackers.com

TRAINING GROUNDS:

- XSS Game
- BWAPP
- https://www.hackthissite.org/
- DWWA
- OWASP webgoat
- metasploitable
- Челлендж h1
- Hackthebox

Optional:

- http://google-gruyere.appspot.com/
- OWASP Security Shepherd
- https://security.stackexchange.com/questions/3592/what-hacking-competitions-challenges-exist

WEB APPLICATIONS FOR LEARNING ON

- Damn Vulnerable Web Application (DVWA) 175
- OWASP Web Goat 176
- OWASP List of Vulnerable Web Applications 177
- PentesterLab - A Collection of Exercises to Learn Testing 178
- VulnHub - Not specifically all web app learning but some great VMs to play with 179
- CTFTime 180 - Not exactly web applications, however capture the flag events can be a great

Way to grow your skillsets

- Over The Wire 181

В идеале пройти все, на всех уровнях сложности.

BB PLATFORMS:

- Hackerone
- BugCrowd

Optional:

- Synack
- Zerocopter
- Hackenproof
- Firebonty
- Cobalt.io
- Openbugbounty

TWITTERS/BLOGS:

- https://twitter.com/Jhaddix (Обязательно к прочтению для любого баунтихантера https://twitter.com/Jhaddix/status/1000504088398778368)
- https://twitter.com/avlidienbrunn
- https://twitter.com/seanmeals
- https://twitter.com/fransrosen
- https://twitter.com/arneswinnen
- https://twitter.com/gerben_javado
- https://twitter.com/itscachemoney
- https://twitter.com/thedawgyg
- https://twitter.com/NahamSec
- https://twitter.com/orange_8361
- https://twitter.com/filedescriptor
- https://twitter.com/albinowax
- https://twitter.com/kinugawamasato

- https://blog.zsec.uk/
- https://zseano.com/
- https://github.com/ngalongc/bug-bounty-reference (!!! - собрано большинство стоящего прочтения, самое лучшее со всех блогов)

Интересных твиттеров и блогов около сотни, но это основные.

CTF:

- https://www.hackthebox.eu/
- https://picoctf.com/

Optional:

- https://ctftime.org/ (тут есть ссылки на все CTF)

Вообще, пункт необязательный, но почти все багхантеры так или иначе участвуют в CTF. Хотя есть и те которые считают что это не нужно.

CRYPTO:

- https://cryptopals.com/
- Cryptography I
- Cryptography II
- Стоит пройти picoctf, хотя бы для понимания того что это такое.

ПРОЧИТАТЬ ВСЕ РЕПОРТЫ ТОП-ХАКЕРОВ ИЗ ТОП-100