Please don't hesitate to contribute to this repo!

Bug Bounty Beginner's Roadmap

Hi! I'm **Ansh Bhawnani**. I am currently working as a Security Engineer and also a part time content creator. I am creating this repository for everyone to contribute as to guide the young and enthusiastic minds for starting their career in bug bounties. More content will be added regularly. Keep following. So let's get started!

NOTE: The bug bounty landscape has changed since the last few years. The issues we used to find easily an year ago would not be easy now. Automation is being used rigorously and most of the "*low hanging fruits*" are being duplicated if you are out of luck. If you want to start doing bug bounty, you will have to be determined to be consistent and focused, as the competition is very high.

Introduction

- **What is a bug?**
    - Security bug or vulnerability is “a weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, OR availability.
- **What is Bug Bounty?**
    - A bug bounty or bug bounty program is IT jargon for a reward or bounty program given for finding and reporting a bug in a particular software product. Many IT companies offer bug bounties to drive product improvement and get more interaction from end users or clients. Companies that operate bug bounty programs may get hundreds of bug reports, including security bugs and security vulnerabilities, and many who report those bugs stand to receive awards.
- **What is the Reward?**
    - There are all types of rewards based on the severity of the issue and the cost to fix. They may range from real money (most prevalent) to premium subscriptions (Prime/Netflix), discount coupons (for e commerce of shopping sites), gift vouchers, swags (apparels, badges, customized stationery, etc.). *Money may range from 50$ to 50,000$ and even more.*

What to learn?

- **Technical**
    - **Computer Fundamentals**
        - https://www.comptia.org/training/by-certification/a (https://www.comptia.org/training/by-certification/a)

    - https://www.youtube.com/watch?v=tIfRDPekybU (https://www.youtube.com/watch?v=tIfRDPekybU)
    - https://www.tutorialspoint.com/computer_fundamentals/index.htm (https://www.tutorialspoint.com/computer_fundamentals/index.htm)
    - https://onlinecourses.swayam2.ac.in/cec19_cs06/preview (https://onlinecourses.swayam2.ac.in/cec19_cs06/preview)
    - https://www.udemy.com/course/complete-computer-basics-course/ (https://www.udemy.com/course/complete-computer-basics-course/)
    - https://www.coursera.org/courses?query=computer%20fundamentals (https://www.coursera.org/courses?query=computer%20fundamentals)
- **Computer Networking**
    - https://www.youtube.com/watch?v=0AcpUwnc12E&list=PLkW9FMxqUvyZaSQNQslneeODER3bJCb2K (https://www.youtube.com/watch?v=0AcpUwnc12E&list=PLkW9FMxqUvyZaSQNQslneeODER3bJCb2K)
    - https://www.youtube.com/watch?v=qiQR5rTSshw (https://www.youtube.com/watch?v=qiQR5rTSshw) -https://www.youtube.com/watch?v=L3ZzkOTDins
    - https://www.udacity.com/course/computer-networking--ud436 (https://www.udacity.com/course/computer-networking--ud436)
    - https://www.coursera.org/professional-certificates/google-it-support (https://www.coursera.org/professional-certificates/google-it-support)
    - https://www.udemy.com/course/introduction-to-computer-networks/ (https://www.udemy.com/course/introduction-to-computer-networks/)
- **Operating Systems**
    - https://www.youtube.com/watch?v=z2r-p7xc7c4 (https://www.youtube.com/watch?v=z2r-p7xc7c4)
    - https://www.youtube.com/watch?v=_tCY-c-sPZc (https://www.youtube.com/watch?v=_tCY-c-sPZc)
    - https://www.coursera.org/learn/os-power-user (https://www.coursera.org/learn/os-power-user)
    - https://www.udacity.com/course/introduction-to-operating-systems--ud923 (https://www.udacity.com/course/introduction-to-operating-systems--ud923)
    - https://www.udemy.com/course/linux-command-line-volume1/ (https://www.udemy.com/course/linux-command-line-volume1/)
    - https://www.youtube.com/watch?v=v_1zB2WNN14 (https://www.youtube.com/watch?v=v_1zB2WNN14)
- **Command Line**
    - **Windows:**
        - https://www.youtube.com/watch?v=TBBbQKp9cKw&list=PLRu7mEBdW7fDTarQ0F2k2tpwCJg_hKhJQ (https://www.youtube.com/watch?v=TBBbQKp9cKw&list=PLRu7mEBdW7fDTarQ0F2k2tpwCJg_hKhJQ)
        - https://www.youtube.com/watch?v=fid6nfvCz1I&list=PLRu7mEBdW7fDlf80vMmEJ4Vw9uf2Gbyc (https://www.youtube.com/watch?v=fid6nfvCz1I&list=PLRu7mEBdW7fDlf80vMmEJ4Vw9uf2Gbyc)

      - https://www.youtube.com/watch?v=UVUd9_k9C6A (https://www.youtube.com/watch?v=UVUd9_k9C6A)
    - **Linux:**
      - https://www.youtube.com/watch?v=fid6nfvCz1I&list=PLRu7mEBdW7fDlf80vMmEJ4Vw9uf2Gbyc (https://www.youtube.com/watch?v=fid6nfvCz1I&list=PLRu7mEBdW7fDlf80vMmEJ4Vw9uf2Gbyc)
      - https://www.youtube.com/watch?v=UVUd9_k9C6A (https://www.youtube.com/watch?v=UVUd9_k9C6A) -
      - https://www.youtube.com/watch?v=GtovwKDemnI (https://www.youtube.com/watch?v=GtovwKDemnI)
      - https://www.youtube.com/watch?v=2PGnYjbYuUo (https://www.youtube.com/watch?v=2PGnYjbYuUo)
      - https://www.youtube.com/watch?v=e7BufAVwDiM&t=418s (https://www.youtube.com/watch?v=e7BufAVwDiM&t=418s)
      - https://www.youtube.com/watch?v=bYRfRGbqDIw&list=PLkPmSWtWNIyTQ1NX6MarpjHPkLUs3u1wG&index=4 (https://www.youtube.com/watch?v=bYRfRGbqDIw&list=PLkPmSWtWNIyTQ1NX6MarpjHPkLUs3u1wG&index=4)
  - **Programming**
    - **C**
      - https://www.youtube.com/watch?v=irqbmMNs2Bo (https://www.youtube.com/watch?v=irqbmMNs2Bo)
      - https://www.youtube.com/watch?v=ZSPZob_1TOk (https://www.youtube.com/watch?v=ZSPZob_1TOk)
      - https://www.programiz.com/c-programming (https://www.programiz.com/c-programming)
    - **Python**
      - https://www.youtube.com/watch?v=ZLga4doUdjY&t=30352s (https://www.youtube.com/watch?v=ZLga4doUdjY&t=30352s)
      - https://www.youtube.com/watch?v=gfDE2a7MKjA (https://www.youtube.com/watch?v=gfDE2a7MKjA)
      - https://www.youtube.com/watch?v=eTyI-M50Hu4 (https://www.youtube.com/watch?v=eTyI-M50Hu4)
    - **JavaScript**
      - https://www.youtube.com/watch?v=-lCF2t6iuUc (https://www.youtube.com/watch?v=-lCF2t6iuUc)
      - https://www.youtube.com/watch?v=hKB-YGF14SY&t=1486s (https://www.youtube.com/watch?v=hKB-YGF14SY&t=1486s)
      - https://www.youtube.com/watch?v=jS4aFq5-91M (https://www.youtube.com/watch?v=jS4aFq5-91M)
    - **PHP**
      - https://www.youtube.com/watch?v=1SnPKhCdlsU (https://www.youtube.com/watch?v=1SnPKhCdlsU)

        - https://www.youtube.com/watch?v=OK_JCtrrv-c (https://www.youtube.com/watch?v=OK_JCtrrv-c)
        - https://www.youtube.com/watch?v=T8SEGXzdbYg&t=1329s (https://www.youtube.com/watch?v=T8SEGXzdbYg&t=1329s)

Where to learn from?

- **Books**
    - Web Application Hacker's Handbook: https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470 (https://www.amazon.com/Web-Application-Hackers-Handbook-Exploiting/dp/1118026470)
    - Real World Bug Hunting: https://www.amazon.in/Real-World-Bug-Hunting-Field-Hacking-ebook/dp/B072SQZ2LG (https://www.amazon.in/Real-World-Bug-Hunting-Field-Hacking-ebook/dp/B072SQZ2LG)
    - Bug Bounty Hunting Essentials: https://www.amazon.in/Bug-Bounty-Hunting-Essentials-Quick-paced-ebook/dp/B079RM344H (https://www.amazon.in/Bug-Bounty-Hunting-Essentials-Quick-paced-ebook/dp/B079RM344H)
    - Bug Bounty Bootcamp: https://www.amazon.in/Bug-Bounty-Bootcamp-Reporting-Vulnerabilities-ebook/dp/B08YK368Y3 (https://www.amazon.in/Bug-Bounty-Bootcamp-Reporting-Vulnerabilities-ebook/dp/B08YK368Y3)
    - Hands on Bug Hunting: https://www.amazon.in/Hands-Bug-Hunting-Penetration-Testers-ebook/dp/B07DTF2VL6 (https://www.amazon.in/Hands-Bug-Hunting-Penetration-Testers-ebook/dp/B07DTF2VL6)
    - Hacker's Playbook 3: https://www.amazon.in/Hacker-Playbook-Practical-Penetration-Testing/dp/1980901759 (https://www.amazon.in/Hacker-Playbook-Practical-Penetration-Testing/dp/1980901759)
    - OWASP Testing Guide: https://www.owasp.org/index.php/OWASP_Testing_Project (https://www.owasp.org/index.php/OWASP_Testing_Project)
    - Web Hacking 101: https://www.pdfdrive.com/web-hacking-101-e26570613.html (https://www.pdfdrive.com/web-hacking-101-e26570613.html)
    - OWASP Mobile Testing Guide :https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide
- **Writeups**
    - Medium: https://medium.com/analytics-vidhya/a-beginners-guide-to-cyber-security-3d0f7891c93a (https://medium.com/analytics-vidhya/a-beginners-guide-to-cyber-security-3d0f7891c93a)
    - Infosec Writeups: https://infosecwriteups.com/?gi=3149891cc73d (https://infosecwriteups.com/?gi=3149891cc73d)
    - Hackerone Hacktivity: https://hackerone.com/hacktivity (https://hackerone.com/hacktivity)
    - Google VRP Writeups: https://github.com/xdavidhu/awesome-google-vrp-writeups (https://github.com/xdavidhu/awesome-google-vrp-writeups)
- **Blogs and Articles**
    - Hacking Articles: https://www.hackingarticles.in/ (https://www.hackingarticles.in/)
    - Vickie Li Blogs: https://vickieli.dev/ (https://vickieli.dev/)

    - Bugcrowd Blogs: https://www.bugcrowd.com/blog/ (https://www.bugcrowd.com/blog/)
    - Intigriti Blogs: https://blog.intigriti.com/ (https://blog.intigriti.com/)
    - Portswigger Blogs: https://portswigger.net/blog (https://portswigger.net/blog)
- **Forums**
    - Reddit: https://www.reddit.com/r/websecurity/ (https://www.reddit.com/r/websecurity/)
    - Reddit: https://www.reddit.com/r/netsec/ (https://www.reddit.com/r/netsec/)
    - Bugcrowd Discord: https://discord.com/invite/TWr3Brs (https://discord.com/invite/TWr3Brs)
- **Official Websites**
    - OWASP: https://owasp.org/ (https://owasp.org/)
    - PortSwigger: https://portswigger.net/ (https://portswigger.net/)
    - Cloudflare: https://www.cloudflare.com/ (https://www.cloudflare.com/)
- **YouTube Channels**
    - **English**
        - Insider PHD: https://www.youtube.com/c/InsiderPhD (https://www.youtube.com/c/InsiderPhD)
        - Stok: https://www.youtube.com/c/STOKfredrik (https://www.youtube.com/c/STOKfredrik)
        - Bug Bounty Reports Explained: https://www.youtube.com/c/BugBountyReportsExplained (https://www.youtube.com/c/BugBountyReportsExplained)
        - Vickie Li: https://www.youtube.com/c/VickieLiDev (https://www.youtube.com/c/VickieLiDev)
        - Hacking Simplified: https://www.youtube.com/c/HackingSimplifiedAS (https://www.youtube.com/c/HackingSimplifiedAS)
        - Pwn function :https://www.youtube.com/c/PwnFunction
        - Farah Hawa: https://www.youtube.com/c/FarahHawa (https://www.youtube.com/c/FarahHawa)
        - XSSRat: https://www.youtube.com/c/TheXSSrat (https://www.youtube.com/c/TheXSSrat)
        - Zwink: https://www.youtube.com/channel/UCDl4jpAVAezUdzsDBDDTGsQ (https://www.youtube.com/channel/UCDl4jpAVAezUdzsDBDDTGsQ)
        - Live Overflow :https://www.youtube.com/c/LiveOverflow
    - **Hindi**
        - Spin The Hack: https://www.youtube.com/c/SpinTheHack (https://www.youtube.com/c/SpinTheHack)
        - Pratik Dabhi: https://www.youtube.com/c/impratikdabhi (https://www.youtube.com/c/impratikdabhi)

Join Twitter Today!

World class security researchers and bug bounty hunters are on Twitter. Where are you? Join Twitter now and get daily updates on new issues, vulnerabilities, zero days, exploits, and join people sharing their methodologies, resources, notes and experiences in the cyber security world!

PRACTICE! PRACTICE! and PRACTICE!

- **CTF**
    - Hacker 101: https://www.hackerone.com/hackers/hacker101 (https://www.hackerone.com/hackers/hacker101)

  - PicoCTF: https://picoctf.org/ (https://picoctf.org/)
  - TryHackMe: https://tryhackme.com/ (https://tryhackme.com/) (premium/free)
  - HackTheBox: https://www.hackthebox.com/ (https://www.hackthebox.com/) (premium)
  - VulnHub: https://www.vulnhub.com/ (https://www.vulnhub.com/)
  - HackThisSite: https://hackthissite.org/ (https://hackthissite.org/)
  - CTFChallenge: https://ctfchallenge.co.uk/ (https://ctfchallenge.co.uk/)
  - PentesterLab: https://pentesterlab.com/referral/olaL4k8btE8wqA (https://pentesterlab.com/referral/olaL4k8btE8wqA) (premium)

- **Online Labs**

  - PortSwigger Web Security Academy: https://portswigger.net/web-security (https://portswigger.net/web-security)
  - OWASP Juice Shop: https://owasp.org/www-project-juice-shop/ (https://owasp.org/www-project-juice-shop/)
  - XSSGame: https://xss-game.appspot.com/ (https://xss-game.appspot.com/)
  - BugBountyHunter: https://www.bugbountyhunter.com/ (https://www.bugbountyhunter.com/) (premium)
  - W3Challs : https://w3challs.com/ (https://w3challs.com/)

- **Offline Labs**

  - DVWA: https://dvwa.co.uk/ (https://dvwa.co.uk/)
  - bWAPP: http://www.itsecgames.com/ (http://www.itsecgames.com/)
  - Metasploitable2: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/ (https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)
  - BugBountyHunter: https://www.bugbountyhunter.com/ (https://www.bugbountyhunter.com/) (premium)
  - W3Challs : https://w3challs.com/ (https://w3challs.com/)

Bug Bounty Platforms

- **Crowdsourcing**

  - Bugcrowd: https://www.bugcrowd.com/ (https://www.bugcrowd.com/)
  - Hackerone: https://www.hackerone.com/ (https://www.hackerone.com/)
  - Intigriti: https://www.intigriti.com/ (https://www.intigriti.com/)
  - YesWeHack: https://www.yeswehack.com/ (https://www.yeswehack.com/)
  - OpenBugBounty: https://www.openbugbounty.org/ (https://www.openbugbounty.org/)

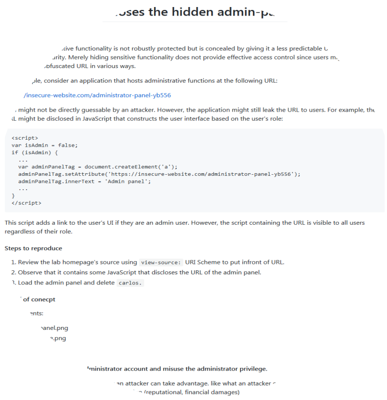
- **Individual Programs**

  - Meta: https://www.facebook.com/whitehat (https://www.facebook.com/whitehat)
  - Google: https://about.google/appsecurity/ (https://about.google/appsecurity/)

Bug Bounty Report Format

- **Title**
    - The first impression is the last impression, the security engineer looks at the title first and he should be able to identify the issue.
    - Write about what kind of functionality you can able to abuse or what kind of protection you can bypass. Write in just one line.
    - Include the Impact of the issue in the title if possible.
- **Description**
    - This component provides details of the vulnerability, you can explain the vulnerability here, write about the paths, endpoints, error messages you got while testing. You can also attach HTTP requests, vulnerable source code.
- **Steps to Reproduce**
    - Write the stepwise process to recreate the bug. It is important for an app owner to be able to verify what you've found and understand the scenario.
    - You must write each step clearly in-order to demonstrate the issue. that helps security engineers to triage fast.
- **Proof of Concept**
    - This component is the visual of the whole work. You can record a demonstration video or attach screenshots.
- **Impact**
    - Write about the real-life impact, How an attacker can take advantage if he/she successfully exploits the vulnerability.
    - What type of possible damages could be done? (avoid writing about the theoretical impact)
    - Should align with the business objective of the organization

Sample Report



oses the hidden admin-pa

ctive functionality is not robustly protected but is concealed by giving it a less predictable U
urity. Merely hiding sensitive functionality does not provide effective access control since users m
obfuscated URL in various ways.

ple, consider an application that hosts administrative functions at the following URL:

/insecure-website.com/administrator-panel-yb556

might not be directly guessable by an attacker. However, the application might still leak the URL to users. For example, the
L might be disclosed in JavaScript that constructs the user interface based on the user's role:

```
<script>
var isAdmin = false;
if (isAdmin) {
  ...
  var adminPanelTag = document.createElement('a');
  adminPanelTag.setAttribute('https://insecure-website.com/administrator-panel-yb556');
  adminPanelTag.innerText = 'Admin panel';
  ...
}
</script>
```

This script adds a link to the user's UI if they are an admin user. However, the script containing the URL is visible to all users regardless of their role.

Steps to reproduce

1. Review the lab homepage's source using `view-source:` URI Scheme to put infront of URL.
2. Observe that it contains some JavaScript that discloses the URL of the admin panel.
3. Load the admin panel and delete `carlos.`

of conecpt

ents:

anel.png

.png

ministrator account and misuse the administrator privilege.

an attacker can take advantage. like what an attacker
(reputational, financial damages)

Some additional Tips

1. **Don't do bug bounty as a full time** in the beginning (although I suggest don't do it full time at any point). There is no guarantee to get bugs every other day, there is no stability. Always keep multiple sources of income (bug bounty not being the primary).
2. **Stay updated**, learning should never stop. Join twitter, follow good people, maintain the curiosity to learn something new every day. Read writeups, blogs and keep expanding your knowledge.
3. Always see **bug bounty as a medium to enhance your skills**. Money will come only after you have the skills. Take money as a motivation only.
4. **Don't be dependent on automation**. You can't expect a tool to generate money for you. Automation is everywhere. The key to success in Bug Bounty is to be unique. Build your own methodology, learn from others and apply on your own.
5. Always try to escalate the severity of the bug, **Keep a broader mindset**. An RCE always has higher impact than arbitrary file upload.
6. It's not necessary that a vulnerability will be rewarded based on the industry defined standard impact. The asset owners **rate the issue with a risk rating**, often calculated as *impact * likelyhood* (exploitability). For example, an SQL Injection by default has a Critical impact, but if the application is accessible only inside the organization VPN and doesn't contain any user data/PII in the database, the likelyhood of the exploitation is reduced, so does the risk.
7. **Stay connected to the community**. Learn and contribute. There is always someone better than you in something. don't miss an opportunity to network. Join forums, go to conferences and hacking events, meet people, learn from their experiences.
8. **Always be helpful**.