بِسۡمِ ٱللَّهِ ٱلرَّحۡمَٰنِ ٱلرَّحِيمِ

GcodexGcodex➔ Telegram

 # 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.youtube.com/watch?v=tIfRDPekybU

- https://www.tutorialspoint.com/computer_fundamentals/index.htm

- https://onlinecourses.swayam2.ac.in/cec19_cs06/preview

- https://www.udemy.com/course/complete-computer-basics-course /

- 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=qiQR5rTSshw

-https://www.youtube.com/watch?v=L3ZzkOTDins

- https://www.udacity.com/course/computer-networking--ud436

- https://www.coursera.org/professional-certificates/google-it-support

- 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=_tCY-c-sPZc

- https://www.coursera.org/learn/os-power-user

- https://www.udacity.com/course/introduction-to-operating-systems--ud923

- https://www.udemy.com/course/linux-command-line-volume1 /

- 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=fid6nfvCz1I&list=PLRu7mEBdW7fDlf80vMmEJ4Vw9uf2Gbyc_

- https://www.youtube.com/watch?v=UVUd9_k9C6A

- **Linux:**

- https://www.youtube.com/watch?v=fid6nfvCz1I&list=PLRu7mEBdW7fDlf80vMmEJ4Vw9uf2Gbyc_

- https://www.youtube.com/watch?v=UVUd9_k9C6A -

- https://www.youtube.com/watch?v=GtovwKDemnI

- https://www.youtube.com/watch?v=2PGnYjbYuUo

- https://www.youtube.com/watch?v=e7BufAVwDiM&t=418s

- 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=ZSPZob_1TOk

- https://www.programiz.com/c-programming

- **Python**

- https://www.youtube.com/watch?v=ZLga4doUdjY&t=30352s

- https://www.youtube.com/watch?v=gfDE2a7MKjA

- https://www.youtube.com/watch?v=eTyI-M50Hu4

- **JavaScript**

- https://www.youtube.com/watch?v=-lCF2t6iuUc

- https://www.youtube.com/watch?v=hKB-YGF14SY&t=1486s

- https://www.youtube.com/watch?v=jS4aFq5-91M

- **PHP**

- https://www.youtube.com/watch?v=1SnPKhCdlsU

- https://www.youtube.com/watch?v=OK_JCtrrv-c

- 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

- Real World Bug Hunting: 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

- Bug Bounty Bootcamp: 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

- Hacker's Playbook 3: https://www.amazon.in/Hacker-Playbook-Practical-Penetration-Testing/dp/1980901759

- OWASP Testing Guide: https://www.owasp.org/index.php/OWASP_Testing_Project

- Web Hacking 101: 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

- Infosec Writeups: https://infosecwriteups.com/?gi=3149891cc73d

- Hackerone Hacktivity: https://hackerone.com/hacktivity

- Google VRP Writeups: https://github.com/xdavidhu/awesome-google-vrp-writeups

- **Blogs and Articles**

- Hacking Articles: https://www.hackingarticles.in/

- Vickie Li Blogs: https://vickieli.dev/

- Bugcrowd Blogs: https://www.bugcrowd.com/blog /

- Intigriti Blogs: https://blog.intigriti.com/

- Portswigger Blogs: https://portswigger.net/blog

- **Forums**

- Reddit: https://www.reddit.com/r/websecurity/

- Reddit: https://www.reddit.com/r/netsec/

- Bugcrowd Discord: https://discord.com/invite/TWr3Brs

- **Official Websites**

  - OWASP: https://owasp.org/

  - PortSwigger: https://portswigger.net/

  - Cloudflare: https://www.cloudflare.com/

- **YouTube Channels**

  - **English**

    - Insider PHD: https://www.youtube.com/c/InsiderPhD

    - Stok: https://www.youtube.com/c/STOKfredrik

    - Bug Bounty Reports Explained: https://www.youtube.com/c/BugBountyReportsExplained

    - Vickie Li: https://www.youtube.com/c/VickieLiDev

    - Hacking Simplified: https://www.youtube.com/c/HackingSimplifiedAS

    - Pwn function :https://www.youtube.com/c/PwnFunction

    - Farah Hawa: https://www.youtube.com/c/FarahHawa

    - XSSRat: https://www.youtube.com/c/TheXSSrat

    - Zwink: https://www.youtube.com/channel/UCDl4jpAVAezUdzsDBDDTGsQ

    - Live Overflow :https://www.youtube.com/c/LiveOverflow

  - **Hindi**

    - Spin The Hack: https://www.youtube.com/c/SpinTheHack

    - Pratik Dabhi: https://www.youtube.com/c/impratikdabhi

PRACTICE! PRACTICE! and PRACTICE!

- **CTF**

  - Hacker 101: https://www.hackerone.com/hackers/hacker101

  - PicoCTF: https://picoctf.org/

  - TryHackMe: https://tryhackme.com/ (premium/free)

  - HackTheBox: https://www.hackthebox.com/ (premium)

- VulnHub: https://www.vulnhub.com/

- HackThisSite: https://hackthissite.org/

- CTFChallenge: https://ctfchallenge.co.uk/

- PentesterLab: https://pentesterlab.com/referral/olaL4k8btE8wqA (premium)

- **Online Labs**

- PortSwigger Web Security Academy: https://portswigger.net/web-security

- OWASP Juice Shop: https://owasp.org/www-project-juice-shop/

- XSSGame: https://xss-game.appspot.com/

- BugBountyHunter: https://www.bugbountyhunter.com/ (premium)

- W3Challs : https://w3challs.com/

- **Offline Labs**

- DVWA: https://dvwa.co.uk/

- bWAPP: http://www.itsecgames.com/

- Metasploitable2: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

- BugBountyHunter: https://www.bugbountyhunter.com/ (premium)

- W3Challs : https://w3challs.com/

 # Bug Bounty Platforms

- **Crowdsourcing**

- Bugcrowd: https://www.bugcrowd.com/

- Hackerone: https://www.hackerone.com/

- Intigriti: https://www.intigriti.com/

- YesWeHack: https://www.yeswehack.com/

- OpenBugBounty: https://www.openbugbounty.org/

- **Individual** **Programs**

  - Meta: https://www.facebook.com/whitehat

  - Google: 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

JavaScript file discloses the hidden admin-panel path

Description

In some cases, sensitive functionality is not robustly protected but is concealed by giving it a less predictable URL: so called security by obscurity. Merely hiding sensitive functionality does not provide effective access control since users might still discover the obfuscated URL in various ways.

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

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

This might not be directly guessable by an attacker. However, the application might still leak the URL to users. For example, the URL 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.`

Proof of conecpt

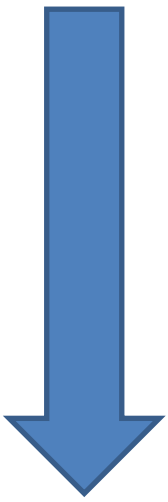
Attachments:

1. admin-panel.png
2. view-source.png

Impact

An attacker can takeover administrator account and misuse the administrator privilege.

- You can explain more about how an attacker can take advantage. like what an attacker can do and what type of damages could be possible against the organization (reputational, financial damages)



@دي كل المصادر يا إخوتي الى جمعتها وتذاكر منها وبإذن الله تعالى ستصل إلى مرادك

*لا تنسونى من دعائكم بالتوفيق وأن يصلح الله لي أمورى ووفقكم الله جميعاً وجعلنا عوناً لبعضنا البعض.

٢٠٢٢