**Assignment-1 CSE3002**

**Name: Viraj Punjani**

**Student id: 20625630**

**Task 1   
Ethical analysis:  
  
Answer 1:**

**Scenario 1 for Alex: Scope Creep**

1. **Documentation**: Alex should thoroughly document the discovered vulnerability in the database, including its nature, potential impact, and any relevant details.
2. **Communication with the Client**: Alex should immediately inform the client about the discovered vulnerability that falls outside the scope of the test. Clearly explain the situation and its potential implications for the client's security posture.
3. **Recommendations**: Provide recommendations to the client on how to address the vulnerability. This may include suggesting further testing or remediation measures specifically targeting the database.
4. **Seek Authorization**: Alex should request explicit authorization from the client to investigate the vulnerability further within the scope of the current engagement. Clearly outline the additional resources and time required for this task.
5. **Document Authorization**: Once authorization is obtained, document it explicitly in writing to ensure clarity and transparency regarding the expanded scope of the penetration test.

**Scenario 2 for Alex: Exploiting Vulnerabilities**

1. **Assess Severity**: Evaluate the severity of the vulnerability and its potential impact on the client's systems and data. Consider factors such as ease of exploitation and potential consequences.
2. **Client Notification**: Promptly inform the client about the critical vulnerability discovered during the penetration test. Clearly explain the nature of the vulnerability and its potential risks to the client's business operations.
3. **Demonstrate Severity**: Rather than actively exploiting the vulnerability, demonstrate its severity through controlled means. Provide the client with a proof of concept or simulated scenario showcasing the potential impact of the vulnerability.
4. **Recommend Mitigation**: Offer recommendations to the client on how to mitigate the vulnerability effectively. This may involve patching systems, updating configurations, or implementing additional security controls.
5. **Authorization for Further Action**: If the client wishes to explore the vulnerability further or conduct additional testing, obtain explicit authorization before proceeding. Document all actions taken and permissions granted to ensure compliance with ethical and legal standards.

**2.1 Task 1**Answer a) Jeff Bezos

Answer b) Parked on the ground near Yuba County Airport ([**MYV**](https://celebrityprivatejettracker.com/airport-iata-myv/)), California, Marysville for about three months.

**2.2. Task 2**

**Find out if the following IP address have ever been reported for malicious use**.

a) 202.95.6.34

**Which Internet Service Provider uses the IP address?**

Answer: RackIP Consultancy Pte. Ltd.

**What is the usage type?**

Answer: Dara center/Web Hosting/Transit

**Which country does the IP belong?**

Answer: Singapore

**What is the reverse DNS address?**

Answer: No dns

**What is the recent activity of this IP Address?**

Answer: There is no recent activity with this Ip address

**2.3. Task   
Find following details of this photo.**

**Geo Location: Coordinates or Maps link.** Answer: 37°43'09.0"S 145°03'10.2"E

**Name of the person who took this photo:**   
 Answer: Wayne eddy.

**When was this photo uploaded:**   
 Answer: June 2018

**Link for this exact photo source:**

Answer: <https://maps.app.goo.gl/BNEyea5zcXfyDerQ9?g_st=ic>

**2.4. Task 4**

You have to conduct OSINT tasks on Latrobe.edu.au and report the following information.

**Website Platform Used (Content Management System-CMS):** Answer: WordPress

**Is WAF being used on the website? If yes, what is it?** Answer: Cloudflare

**Find if there is any ftp port is open or not. Can you login? Take a screenshot and include it in the report.**

Answer: No Ftp port is not open.

**Find out at least 10 IP addresses used by Latrobe.**

131.172.0.10/16

131.171.0.9/16

131.171.0.8/16

131.171.0.7/16

131.172.0.6/16

131.172.0.5/16

131.172.0.4/16

131.172.0.3/13

131.172.0.2/16

131.172.0.1/16  
131.172.0.0/16

**Prepare a list of subdomains of Latrobe.edu.au.**

[accommodation.latrobe.edu.au](http://accommodation.latrobe.edu.au/)  
  
[adminmagento.latrobe.edu.au](http://adminmagento.latrobe.edu.au/)  
  
[agents.latrobe.edu.au](http://agents.latrobe.edu.au/)  
  
[api.latrobe.edu.au](http://api.latrobe.edu.au/)  
  
<https://ba-explorer-tst.latrobe.edu.au/>  
  
<https://store.latrobe.edu.au/>  
  
<https://ojs.latrobe.edu.au/ojs/>  
  
<https://choose.latrobe.edu.au/>  
  
<https://consultation.latrobe.edu.au/s/>  
  
[employer-connect.latrobe.edu.au](http://employer-connect.latrobe.edu.au/)

**Answer 4.1 Image:**always\_look\_for\_details!  
  
**Answer 4.2 Image:**

latrobe\_flag2