**SCHOOL OF CYBERSECURITY**

NAME: OBASI CHARLES CHIDOZIE

ID: VEPH/20B/CY053

TASK: TASK 20D (LESSON 20)

# **Technical Cyber security Report**

# 

# **Analysis Using VirusTotal for Domain Threat Assessment**

# 

# **By**

# **Cyber Security Personnel : OBASI CHARLES CHIDOZIE**

**Date : 16/04/2025**

**Stakeholders : VEPHLA SECURITY TEAM**

**REPORT OUTLINE**

Outline of all pages within technical report

1. Executive Summary
2. Background and Objectives
3. Methodology

3.1 Tool Configuration

3.2 Execution Process

3.3 Monitoring and Analysis

1. Findings and Analysis

4.1 Indicators of Compromise (IOCs)

4.2 Behavioral Analysis

4.3 Risk and Impact Assessment

1. Recommendations

5.1 Immediate Remediation Actions

5.2 Long-Term Mitigation

1. Conclusion

Appendix: Additional Data

## **1. Executive Summary**

* **Overview:**

The analysis with VirusTotal was conducted as part of a malware investigation to assess the behavior of 3 domain urls 17ebook.com, aladel.net and clicnews.com during a routine security scan. The tool successfully utilized virustotal.com url scanning platform, sandbox and threat intelligence functionality to provided insights into possible threats and vulnerabilities like malware, and phishing and potential indicators of compromise assosciated with the domains, thereby allowing the incident response team to take immediate action.

* **Key Findings:**
  + **17ebook.com** was flagged by 11 out of 96 vendors, with six identifying it as malicious and five associating it with phishing.
  + **aladel.net** was flagged by 9 out of 96 vendors and linked to phishing, malware delivery, and suspicious redirections.
  + **clicnews.com** showed minimal detection (0/96) but was still flagged as suspicious and potentially linked to compromised sites.

## **2. Background and Objectives**

* **Project Context:**The project aimed to assess the security posture of the 3 mentioned domains and to identify any malicious and phishing activity that could compromise the infrastructure. VirusTotal was employed as a tool to analyze the behavior of the suspected domains identified through the internal threat detection system and threat intelligence team.
* **Objective of the Tool Use:**VirusTotal was utilized to examine the behavior of the suspicious domain urls by running it in a sandbox environment to track for presence of malware, phishing and other vulnerabilities and Indicators of Compromise.

## **3. Methodology**

### **3.1 Tool Configuration**

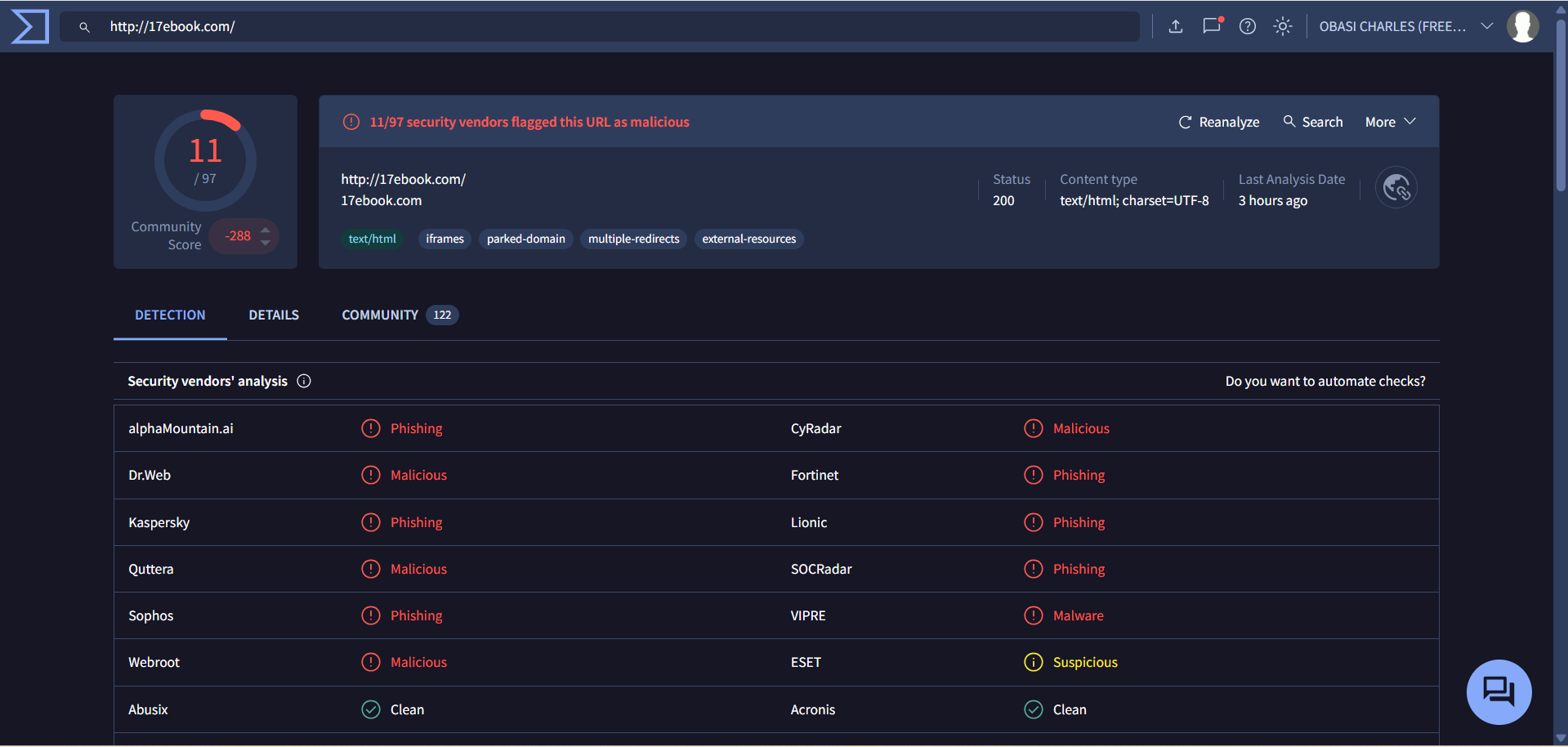
* **VirusTotal.com Configuration:** 
  + 1. VirusTotal web interface was used to perform the domain URL analysis.
    2. Upload the suspicious domain url to the sandbox for analysis.

****

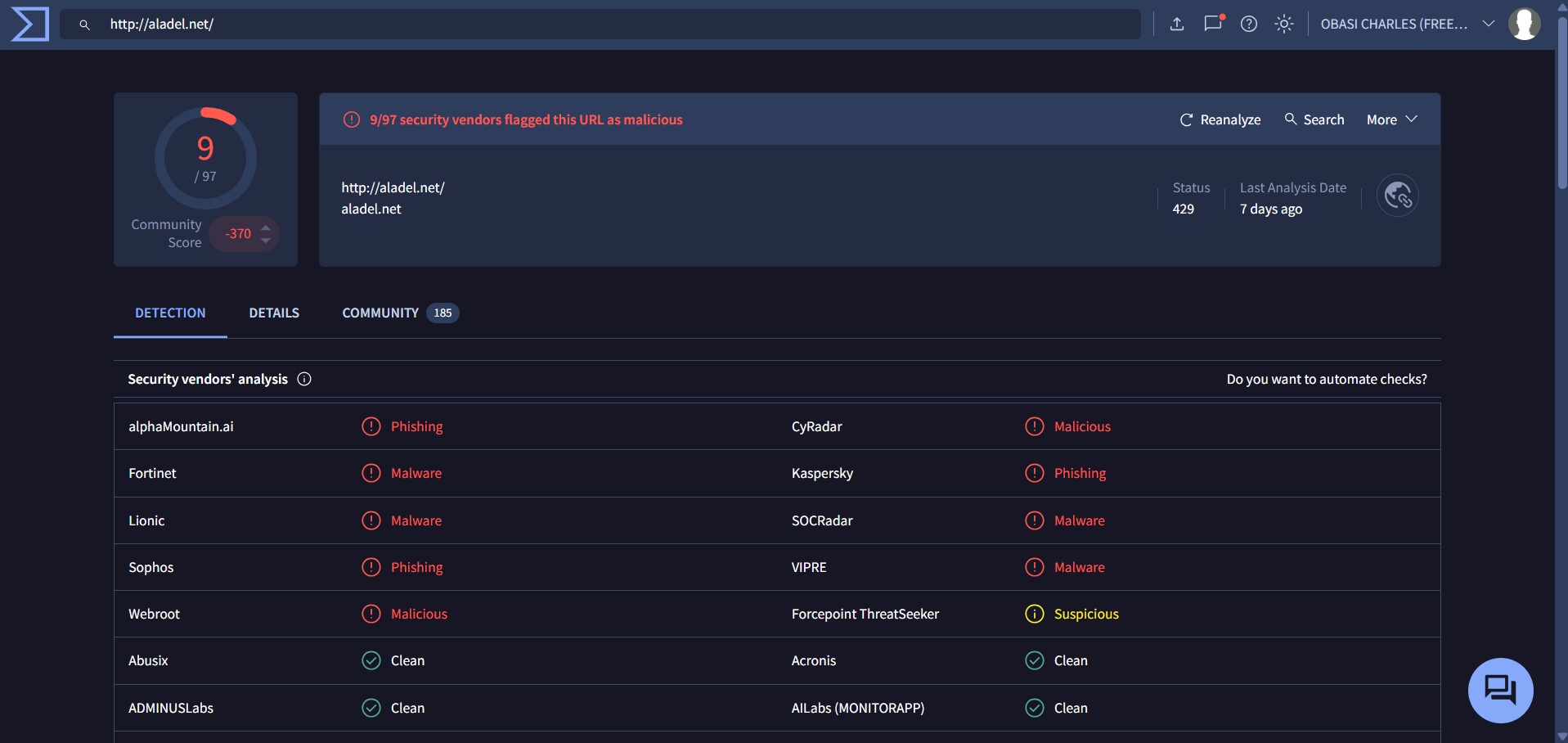
### **3.2 Execution Process**

* **File Execution in Sandbox:**Upon execution, the sandbox environment captured suspicios activities in the domain such as; malware and phishing.
* Each domain was scanned individually.
* The threat Intelligence platform analyzed domain relationships, including IP resolutions, subdomains, and historical data was collected.
* Sandboxing reviewed behavioral reports for dynamic execution analysis.

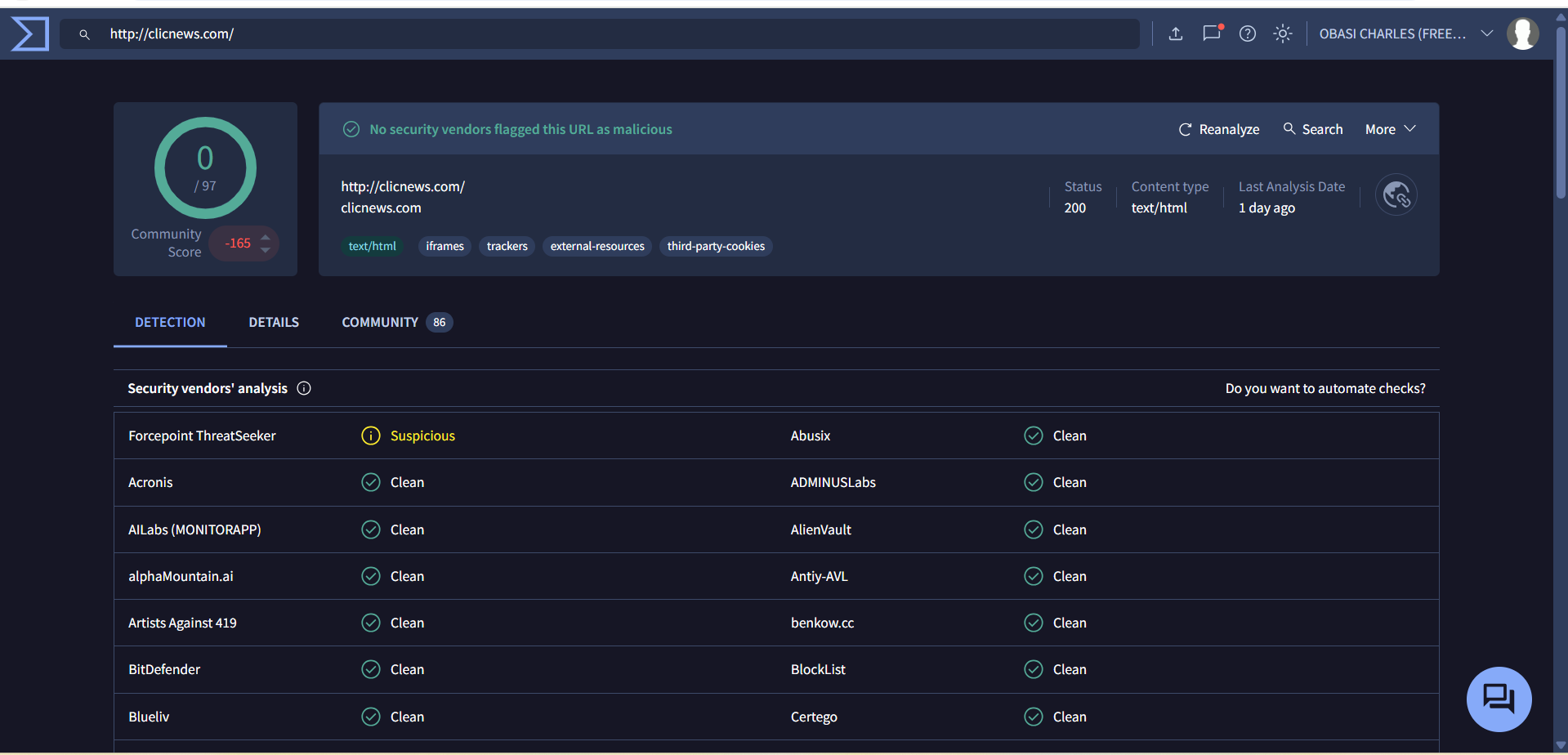
1. 17ebook.com



1. aladel.net



1. clicnews.com



### **3.3 Monitoring and Analysis:**

* **System Monitoring:**Threat intelligence analyzed reports for detected malware, suspicious scripts, and unauthorized system modifications.
* **Network Monitoring:**Tracked outbound connections, redirects, and communication with known malicious IPs.

## 

## 

## 

## 

## **4. Findings and Analysis**

### **4.1 Indicators of Compromise (IOCs):**

* **Detected IOCs:**

1. 17ebook.com

**Categories**

alphaMountain.ai Phishing (alphaMountain.ai)

BitDefender education

Dr.Web known infection source

Sophos phishing and fraud

Webroot Malware Sites

Forcepoint ThreatSeeker parked domain

**HTTP Response**

**Final URL**

https://ww3.17ebook.com/

**Serving IP Address**

[64.190.63.136](https://www.virustotal.com/gui/ip-address/64.190.63.136)

**Status code**

200

**Body length**

24.85 KB

**Body SHA-256**

829d8b216fdb88197cf2522d5cec02a51eabf294e69a389c23bc8cb290bda03a

**Community score = 11/97**

1. aladel.net

**Categories**

alphaMountain.ai Phishing (alphaMountain.ai)

Sophos phishing and fraud

Webroot Phishing and Other Frauds

Forcepoint ThreatSeeker compromised websites. parked domain

**HTTP Response**

**Final URL**

https://aladel.net/

**Serving IP Address**

[162.210.196.171](https://www.virustotal.com/gui/ip-address/162.210.196.171)

**Status code**

429

**Body length**

17 B

**Body SHA-256**

[802600d124464157037a2519acb3cff90b97670fd04809ea902fbb95497a12ca](https://www.virustotal.com/gui/file/802600d124464157037a2519acb3cff90b97670fd04809ea902fbb95497a12ca)

**Community score = 9/97**

1. clicnews.com

**Categories**

alphaMountain.ai News (alphaMountain.ai)

BitDefender news

Forcepoint ThreatSeeker compromised websites

**HTTP Response**

**Final URL**

https://clicnews.com/

**Serving IP Address**

[13.248.169.48](https://www.virustotal.com/gui/ip-address/13.248.169.48)

**Status code**

200

**Community score = 0/97**

### 

### **4.2 Behavioral Analysis:**

* **17ebook.com:** Security vendors flagged this URL as malicious. Domain content and HTTP data suggest it might be trying to hide malicious activity or deliver harmful files like phising.
* **aladel.net:** Security vendors flagged this URL as malicious. It appeared to be a compromised forum and had files that were actively communicating with other systems.
* **clicnews.com:** No security vendors flagged this URL as malicious. Domain had no malicious content, but its data suggests it might have been compromised.

### **4.3 Risk and Impact Assessment:**

* **Potential Impact:**
* **17ebook.com:** High risk due to active malicious behavior, including potential malware distribution, phishing, and unauthorized system access.​
* **aladel.net:** Moderate risk from suspicious phising activities that could lead to system compromise if exploited.​
* **clicnews.com:** Low risk but should be closely monitored due to its history of hosting malicious content and compromise

## **5. Recommendations**

### **5.1 Immediate Remediation Actions:**

* **17ebook.com:**
  + Restrict all network traffic to and from the malicious IP addresses.​
  + Update security systems to detect and prevent access to known malicious URLs associated with this domain.​
* **aladel.net:**
  + Monitor systems to detect unauthorized modifications to browser extensions and self-launching applications.​
  + Implement application whitelisting to prevent the execution of untrusted software.​
* **clicnews.com:**
  + Maintain vigilance by closely monitoring the network traffic for connections to the IP address​
  + Regularly review and update web filtering policies to block access to domains with a history of malicious activity.

### **5.2 Long-Term Mitigation:**

* **Security Measures:**Threat intelligence updates must run regularly to maintain knowledge about dangerous Internet host domains.
* Employees require awareness training to understand the dangers associated with unverified web page utilization and phishing.​
* **Monitoring and Detection Enhancements:**
* Organizations should adopt advanced threat detection systems that actively monitor and eliminate potential threats.

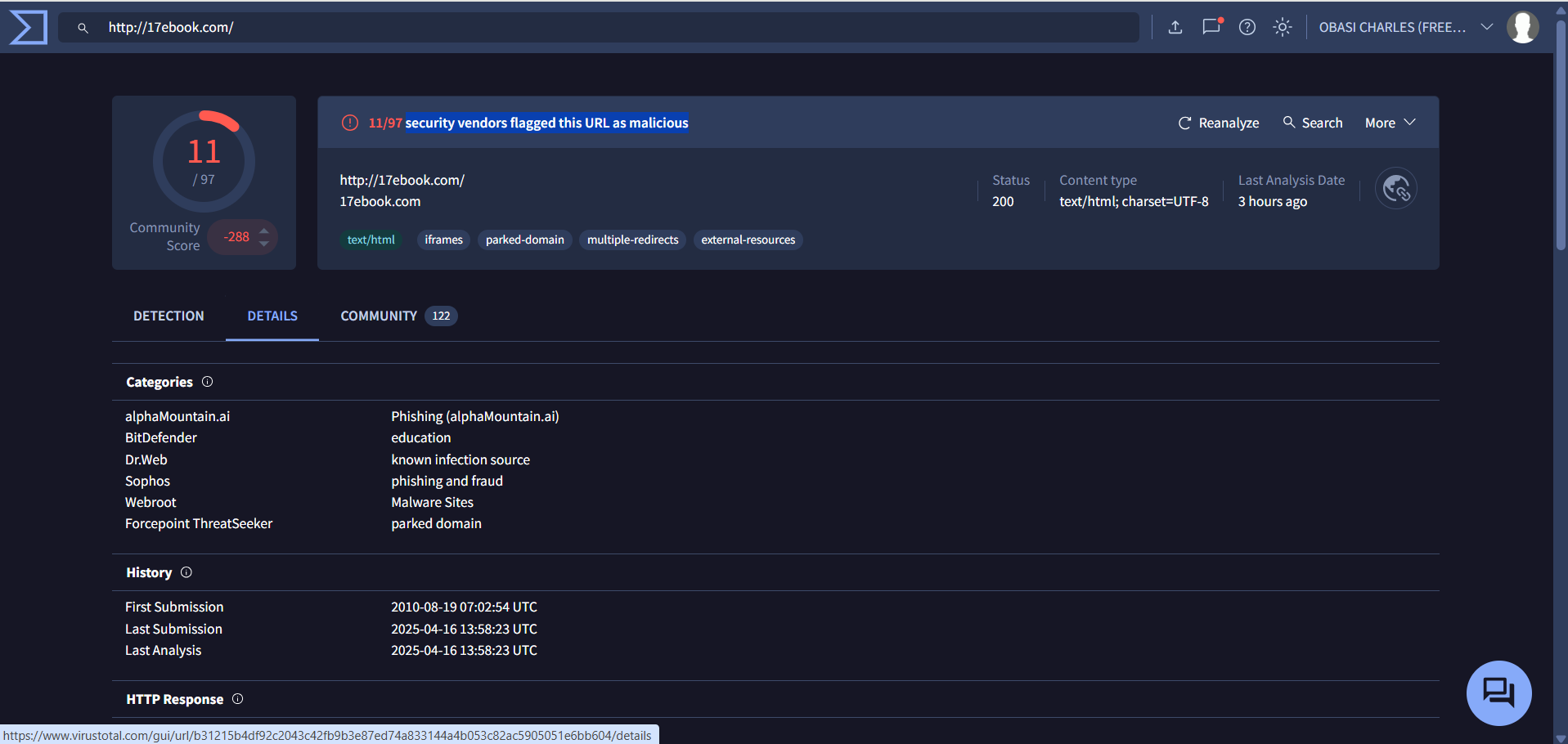
## **6. Conclusion**

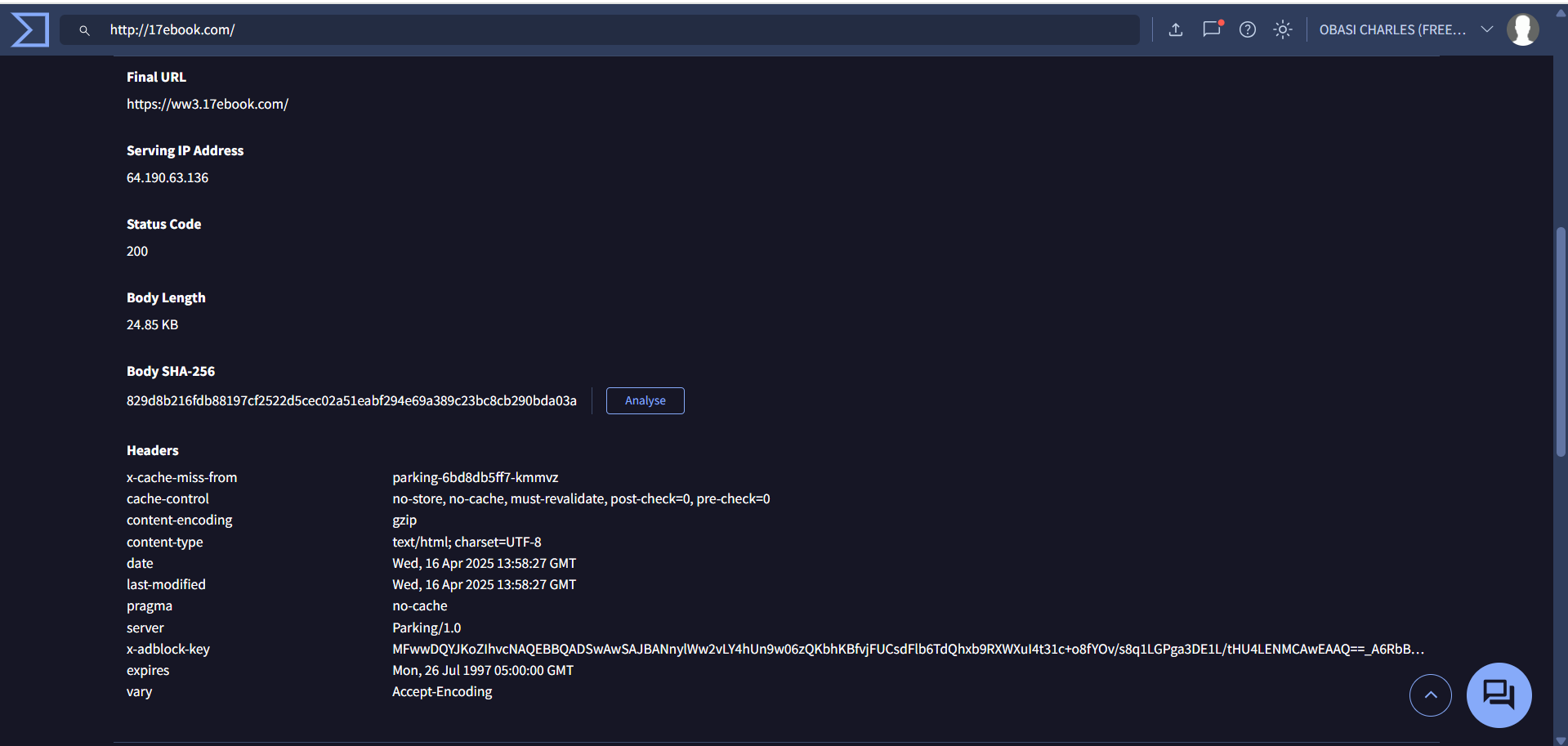
* **Summary of Findings:**The analysis with VirusTotal detected malicious activities like phishing and malware in 17ebook.com and aladel.net domains posing significantly high security risks. Immediate action is required to mitigate risks, and long-term strategies should focus on enhancing prompt malware detection capabilities. However, clicnews.com appears to be free from malicious indicators but associated with a malicious activity or compromise. These findings highlightd the importance of proactive domain research and ongoing threat intelligence monitoring in cybersecurity operations. Organizations may use systems like VirusTotal to not only detect current risks, but also predict and mitigate new ones.
* **Next Steps:**
* Quick steps for blocking and monitoring identified malicious domains should be prioritized.
* Enforcing security measures to reduce and mitigate risks and attacks.
* Organizing employee awareness programs along with repeatedly monitoring their systems to combat future threats. Immediate remediation should involve isolating infected systems, blocking malicious IPs, and removing persistence mechanisms.
* Long-term actions should focus on improving endpoint protection and prompt malware detection capabilities.

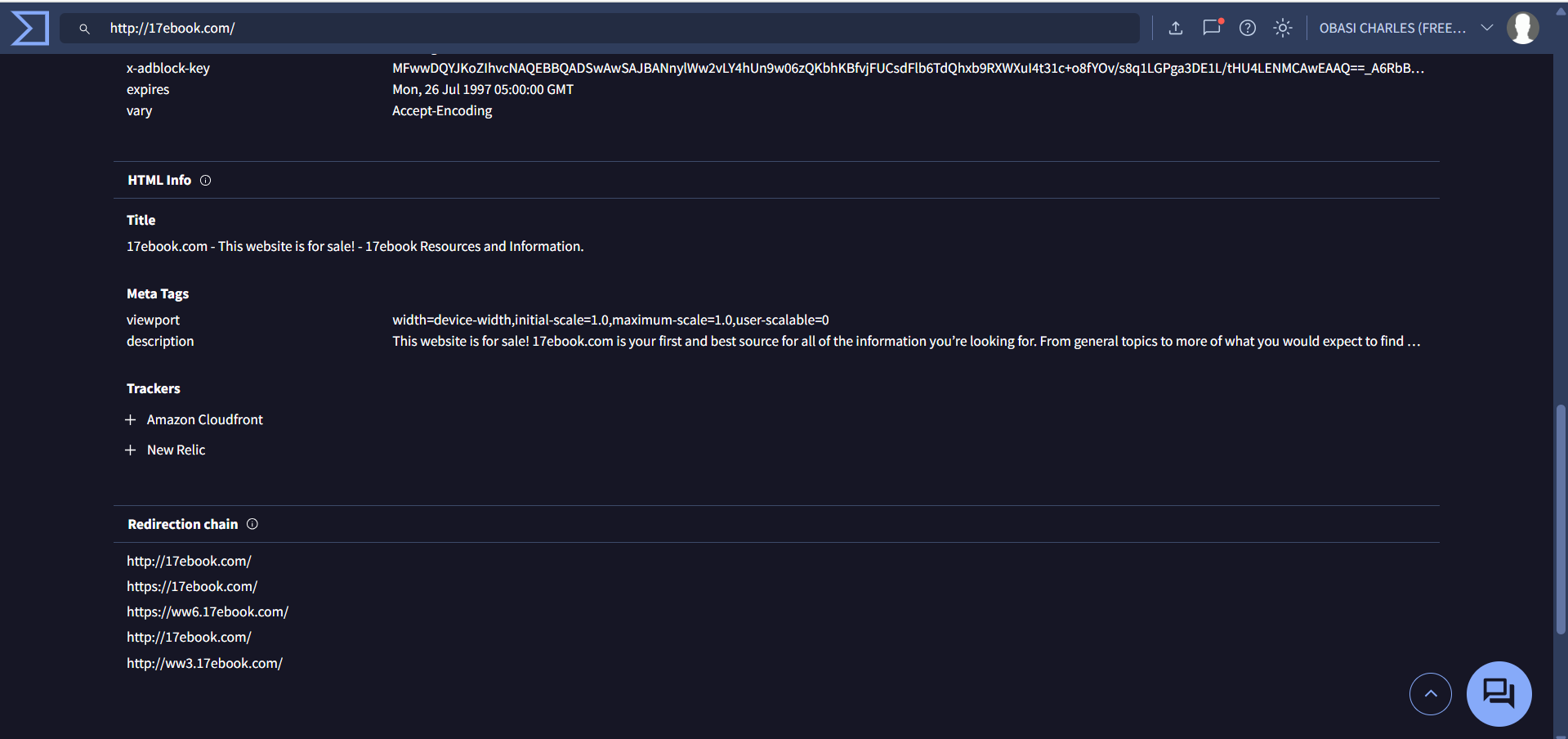
## **Appendix: Additional Data**

* **Raw Logs and Tool Outputs:**
* **Additional Visualizations and Screenshots:**

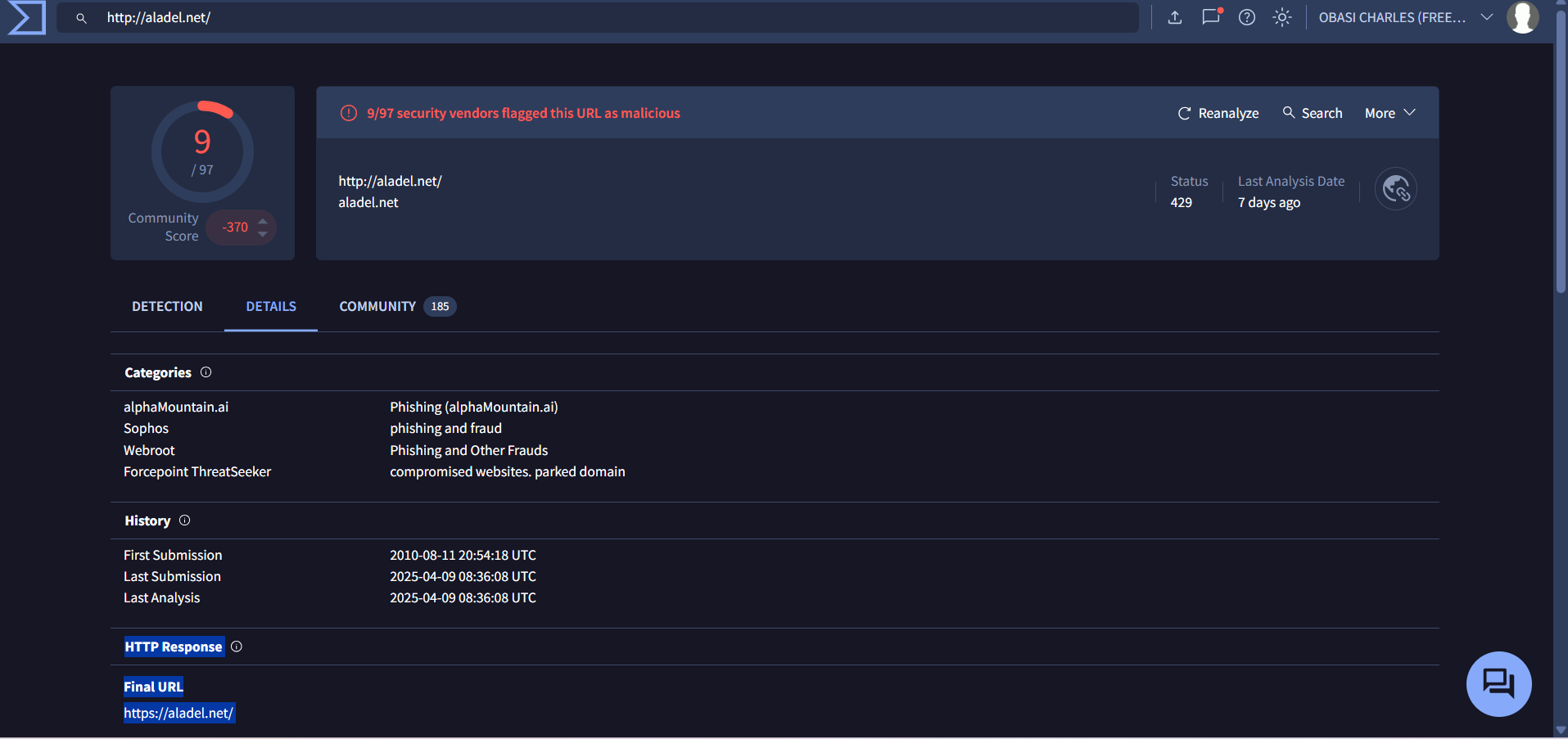
**17ebook.com**

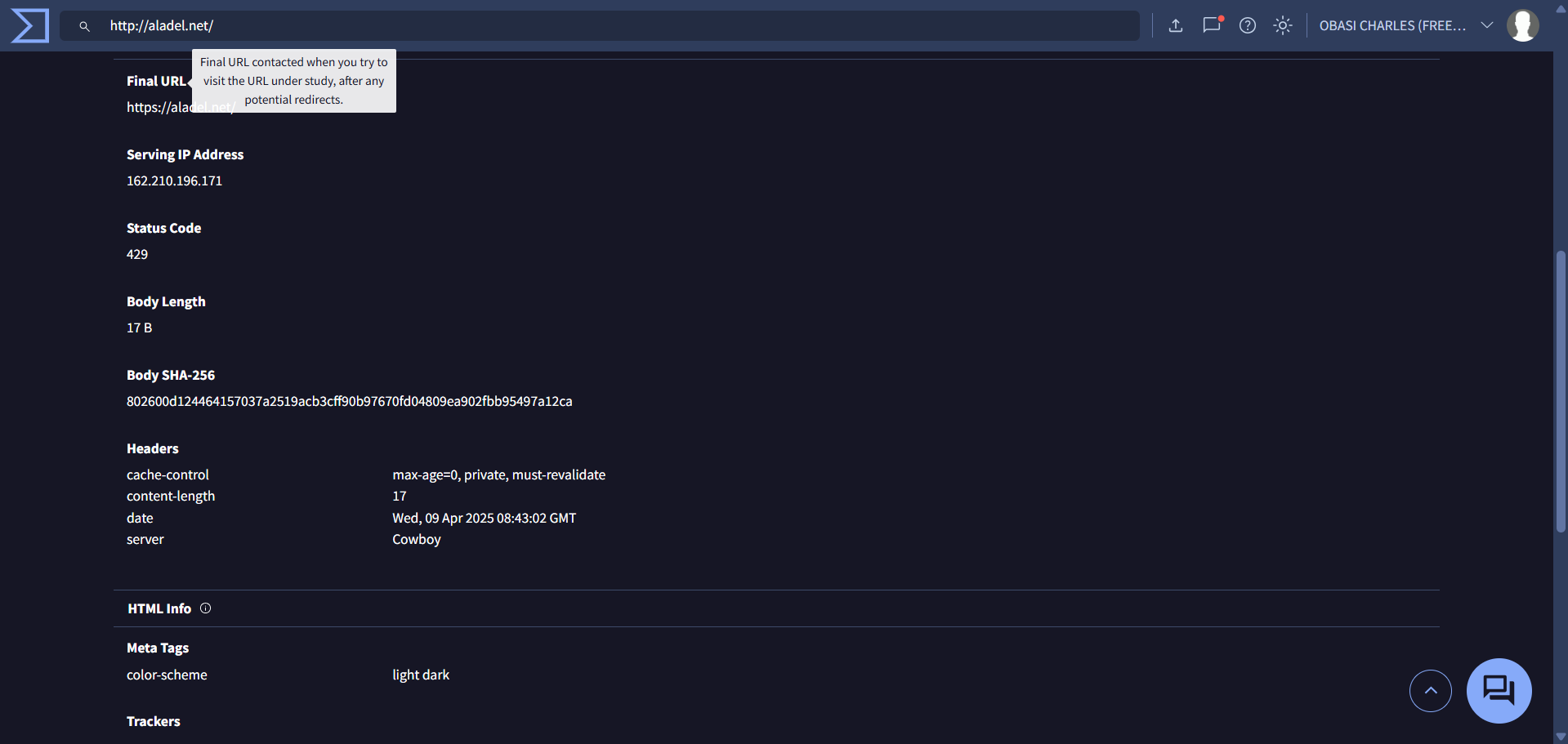






**aladel.net**

****

****

**clicnews.com**

