HON$EC
DEEPWEB GUARDIAN

ace hack3.0

DEEPWEB GUARDIAN

TEAM - HON$EC

HON$EC
DEEPWEB GUARDIAN

ABOUT TEAM:

- **PROJECT NAME** :- DEEPWEB GUARDIAN
- **TEAM NAME** :- HON$EC
- **TEAM LEADER** :- LOKESH KUMAR
- **TEAM MEMBER1** :- NIKHIL KUMAR GOYAL
- **TEAM MEMBER2** :- ABHIJITH SOMAN
- **TEAM MEMBER3** :- DAKSHA SONI

H N$EC
DEEPWEB GUARDIAN

INTRODUCTION

The Deep Web Guardian project aims to provide comprehensive monitoring and protection services for the dark web. The dark web, a part of the deep web accessible only through specialized software, presents a myriad of challenges due to its anonymity and the illicit activities often conducted within its confines. The project's significance lies in its mission to enhance cybersecurity by actively monitoring dark web activities, identifying potential threats, and implementing protective measures to safeguard individuals and organizations against cybercrime, data breaches, and other malicious activities.

H N$EC
DEEPWEB GUARDIAN

FUNCTIONALITY OVERVIEW

- **Single URL Scraping:** Deep Web Guardian's Single URL Scraping feature allows users to extract content from specific dark web URLs, including text, images, and media.

- **Onion Link Finder:** The Onion Link Finder module automatically searches the dark web for onion links, enabling users to discover hidden websites, forums, and marketplaces operating within the Tor network.

- **Vulnerability Scanning (XSS):** Deep Web Guardian's Vulnerability Scanning feature focuses on detecting cross-site scripting (XSS) vulnerabilities within dark web pages and applications.

H N$EC
DEEPWEB GUARDIAN

FUNCTIONALITY OVERVIEW

- **Email Extraction:** The Email Extraction functionality of Deep Web Guardian enables users to extract email addresses from dark web sources such as forums and marketplaces.

- **Link Analysis:** Deep Web Guardian's Link Analysis feature examines the relationships between URLs, domains, and web entities within the dark web.

- **Website Scanning:** The Website Scanning capability of Deep Web Guardian allows users to conduct comprehensive scans of dark web websites for security vulnerabilities and malware infections.

H N$EC
DEEPWEB GUARDIAN

OBJECTIVES & GOALS

- **Threat Intelligence Gathering**: To gather intelligence on potential cyber threats, including data breaches, malware distribution, hacking tools, and vulnerabilities being exploited.

- **Risk Management**: To assess and mitigate the risks associated with data breaches, leaks of sensitive information, and potential reputational damage to organizations.

- **Protecting Sensitive Information**: To monitor for any leaked credentials, intellectual property, or sensitive data belonging to an organization that may be traded or sold on the dark web.

IMPLEMENTATION DETAILS

Description of Technologies and Libraries Used:

- **Python Programming Language:** It provides a robust foundation for implementing various functionalities required for dark web monitoring.
- **Requests Library for HTTP Requests:** It allows easy retrieval of web content from dark web sources for analysis and monitoring purposes.
- **Beautiful Soup for Web Scraping:** Beautiful Soup is a Python library used for web scraping and parsing HTML and XML documents. It enables extraction of structured data from dark web pages, facilitating analysis of content for threats and illicit activities.

IMPLEMENTATION DETAILS

Description of Technologies and Libraries Used:

- **Concurrent Futures for Parallel Processing:** Concurrent Futures is a built-in Python library that provides a high-level interface for asynchronous execution of tasks. By utilizing parallel processing, it enhances the efficiency of dark web monitoring by enabling concurrent retrieval and analysis of multiple web pages.

- **Color Coding for Visual Appeal:** Color coding is implemented for visual appeal and ease of interpretation of monitoring results. Different colors may represent various categories of threats or levels of severity, providing users with intuitive insights into the monitored dark web activities.

H N$EC
DEEPWEB GUARDIAN

METHODOLOGY

Scrapping:

- All the internal, external and broken links attached within the online link.
  he takes it out and gives it.

onion link finder:

- Whoever submits the onion link, whatever links are attached to it, he extracts everything and gives it.

XSS Scanner:

- Finding vulnerabilities in .onion links, If xss vulnerability is found inside the website then it tells us.

H N$EC
DEEPWEB GUARDIAN

METHODOLOGY

Extract Emails:

- All the emails connected with Onion Link are extracted and given.

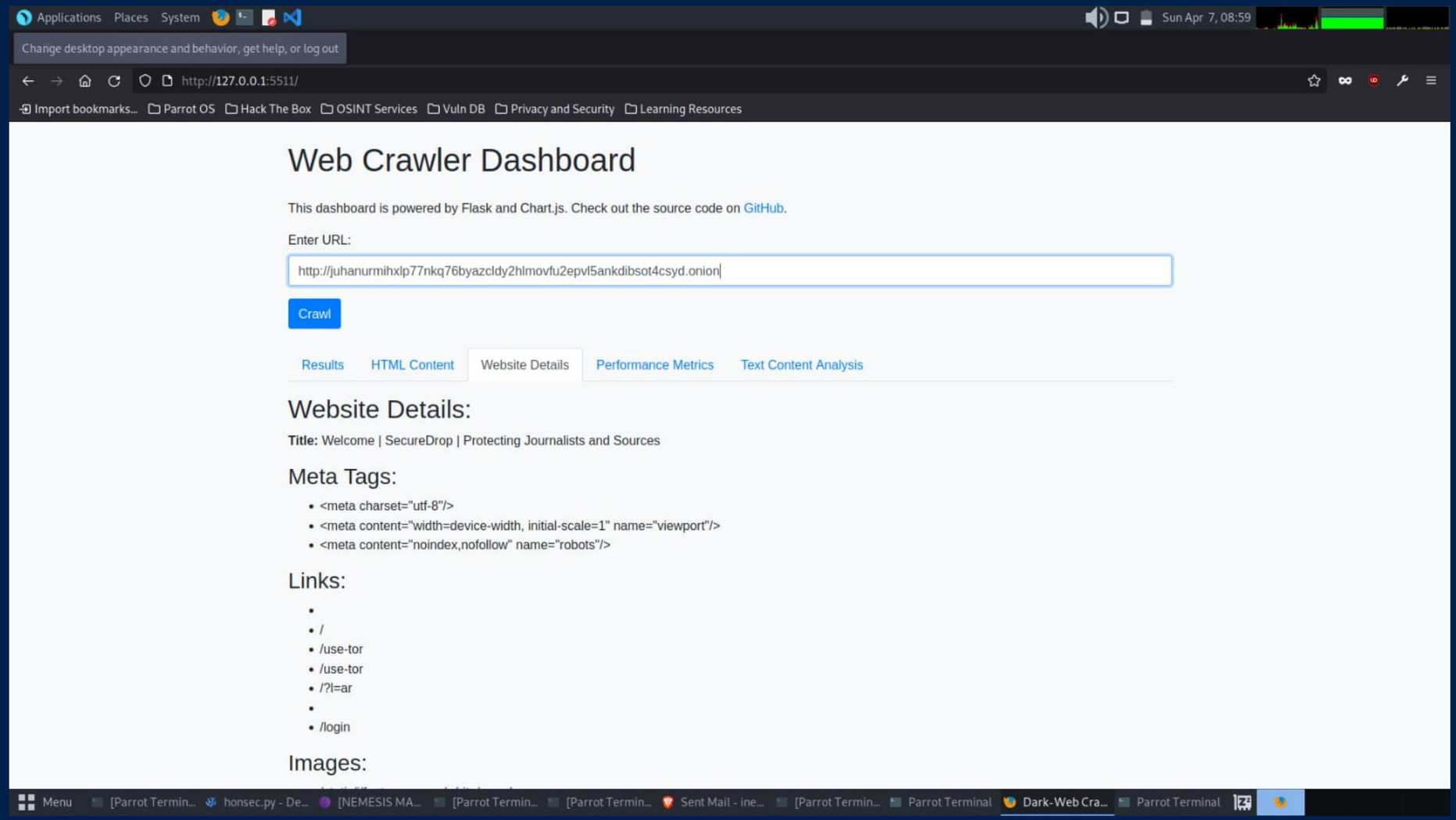
Link Analysis:

- In this part, if the content inside the online link is positive then polarity will be shown as zero.

Website Scanning:

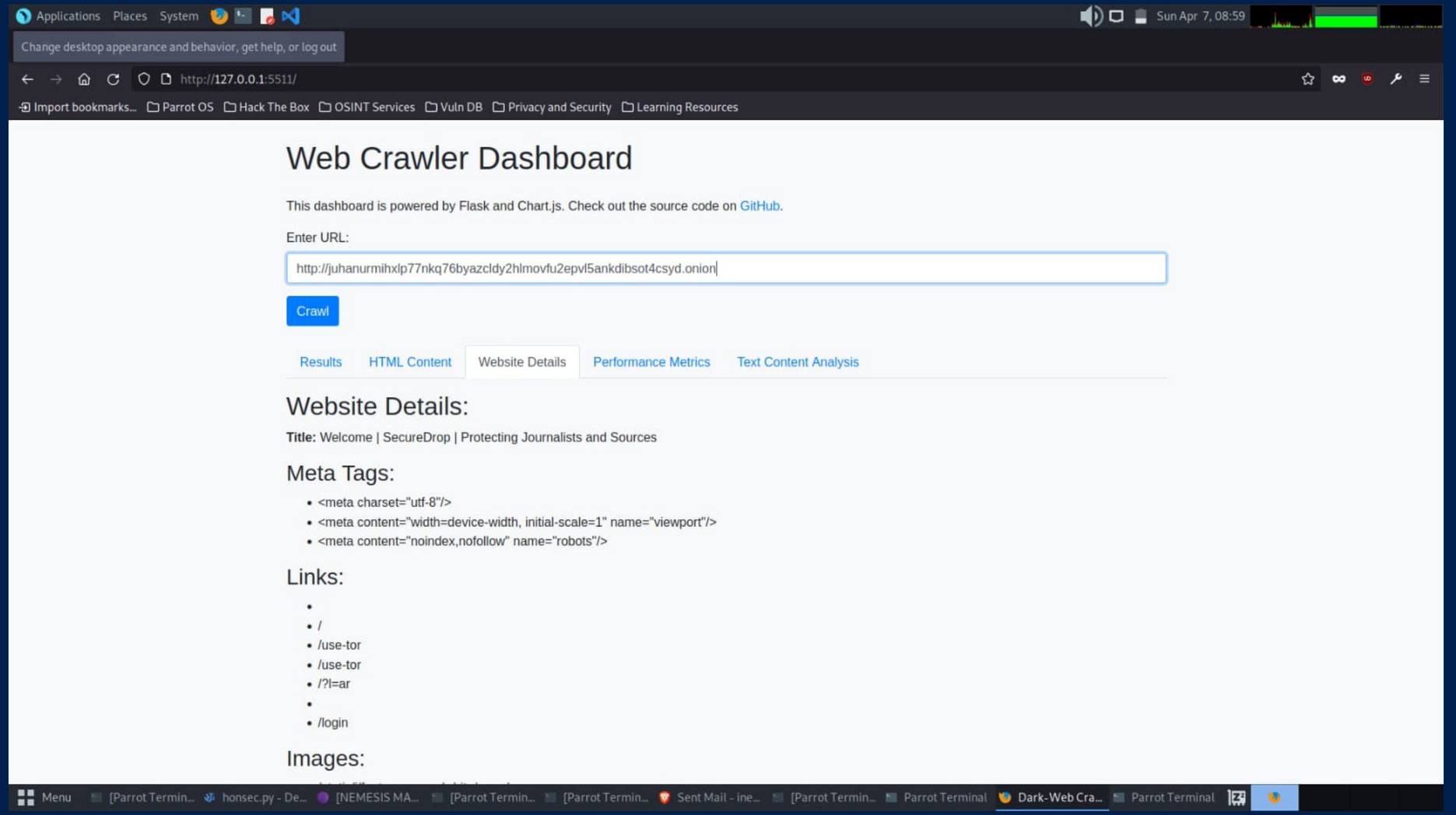
- In onion website scanning, if our keywords match, then it prints the keywords.

RESULTS & FINDINGS



H(C)N$EC
DEEPWEB GUARDIAN

RESULTS & FINDINGS



H N$EC
DEEPWEB GUARDIAN

RESULTS & FINDINGS

```
[+] Choose an Option:
[1] Scrape from Single URL
[2] Onion Link Finder
[3] Vulnerability Scanning (XSS)
[4] Extract Emails
[5] Link Analysis
[6] Website Scanning
[0] Exit
[+] Enter Option No. -> 1
[+] Enter the URL to scrape: http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion
[+] Link Analysis Results:
Internal Links:
External Links:
  - http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion
  - http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion/
  - http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion/use-tor
  - http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion/use-tor
```

H N$EC
DEEPWEB GUARDIAN

RESULTS & FINDINGS

```
o7buwllkigyd.onion/bitcoin-investment/index8.html
Http Bitcoin - What is it? - CryptoWiki
==================================================
https://ahmia.fi/search/redirect?search_term=http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion&redirect_url=http://invest2duvjcj6dhjvvbfahdqdis4kwsafgzau4xkwbe
is7p2ikdcxad.onion/lurk-bitcoin/index7.html
Http Bitcoin - What is it? - Dark Crypto
==================================================
https://ahmia.fi/search/redirect?search_term=http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion&redirect_url=http://invest5wj5bagh4cipukyssxvhxq5ma7qljeogeijwx2
habi7lefo3qd.onion/bitcoin-asics/index22.html
Http Bitcoin : What is it? : Wikipedia
==================================================
https://ahmia.fi/search/redirect?search_term=http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion&redirect_url=http://invest2lc7z65nxrwvszo5olitqas2epnqkpwoz6kfng
2yjzoc7kc5qd.onion/transactions-bitcoin/index14.html
Http Bitcoin : What is it? : TOR WiKi
==================================================
https://ahmia.fi/search/redirect?search_term=http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion&redirect_url=http://invest4togyppwg45e4ug2nou7jkbfutvr6dhwg7wahv
x7z4kjc4sgqd.onion/monero-pool/index.html
Http Bitcoin - What is it? - Dark Crypto
==================================================
https://ahmia.fi/search/redirect?search_term=http://jkta32w5gvk6pmqdfwj67psojot3l2iwoqbdvrvywi5bkudfeandq7id.onion&redirect_url=http://invest4togyppwg45e4ug2nou7jkbfutvr6dhwg7wahv
x7z4kjc4sgqd.onion/ethereum-developer/index6.html
Http Bitcoin : What is it? : Dark Crypto
```

FUTURE SCOPES

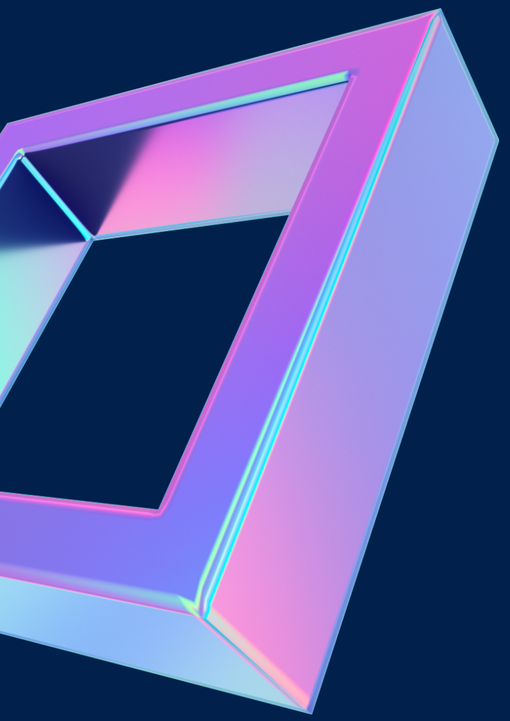
- **Enhanced User Interface:** Enhancing the user interface with intuitive design and interactive features will improve user experience and facilitate ease of navigation within the monitoring platform.

- **Integration with Additional Security Tools:** Integrating the monitoring system with additional security tools and platforms will expand its capabilities and effectiveness in threat detection and mitigation. Integration with threat intelligence platforms, SIEM (Security Information and Event Management) systems, and endpoint security solutions will enable seamless sharing of data and correlation of insights for comprehensive threat analysis.

- **Support for More Advanced Web Scanning Techniques:** Enhancing the monitoring system with support for more advanced web scanning techniques, such as dynamic analysis and behavior-based detection, will enable detection of sophisticated threats and malware payloads.

CONCLUSION

In conclusion, Dark Web monitoring emerges as an indispensable shield against cyber threats, offering organizations a proactive defense mechanism. By diligently tracking illicit activities within the hidden recesses of the internet, businesses can swiftly detect potential breaches and safeguard sensitive data. This proactive approach not only fortifies defenses but also bolsters resilience in the face of evolving cyber threats. Embracing Dark Web monitoring signifies a commitment to staying ahead of malicious actors, mitigating risks, and preserving trust with stakeholders. In today's digital landscape, where data breaches loom large, investing in such proactive measures becomes imperative for ensuring the security and integrity of organizational assets.



Thank You