**🛡️ Recon and Enumeration Toolkit**

# Table of Contents

1. Introduction  
2. Tools & Techniques Used  
3. Results & Observations  
4. Conclusion  
5. References

# 1. Introduction

This report presents a cybersecurity reconnaissance and vulnerability assessment performed on a demo website(**www.apple.com**). The focus is on mapping the attack surface and identifying potential security weaknesses using open-source intelligence (OSINT) tools. These tools aid in subdomain enumeration, directory brute-forcing, fuzzing, and detecting exploitable vulnerabilities. The assessment demonstrates common techniques employed in ethical hacking and penetration testing.

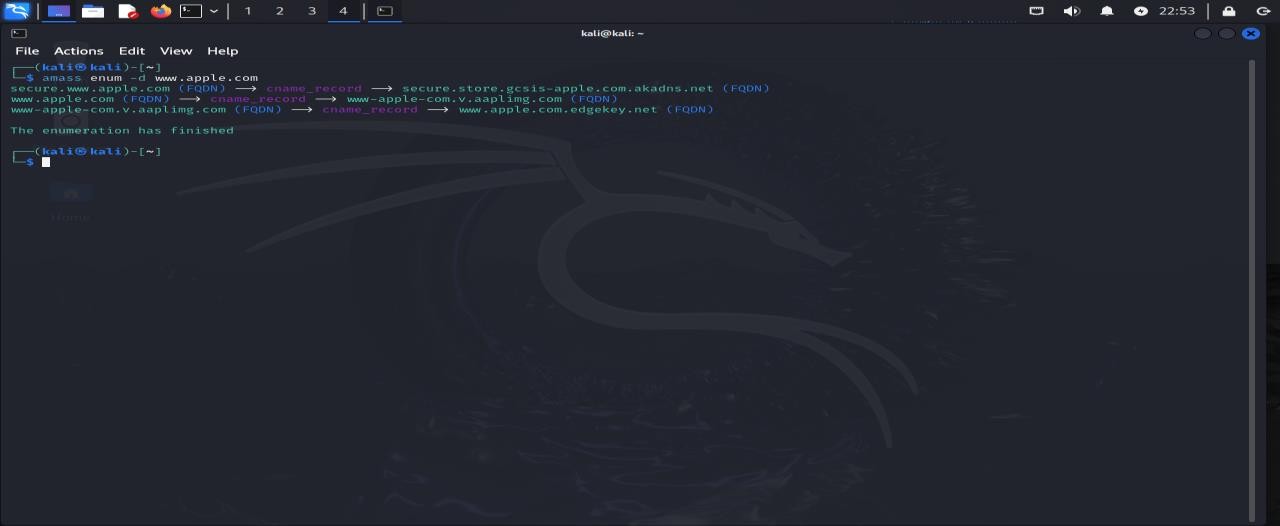
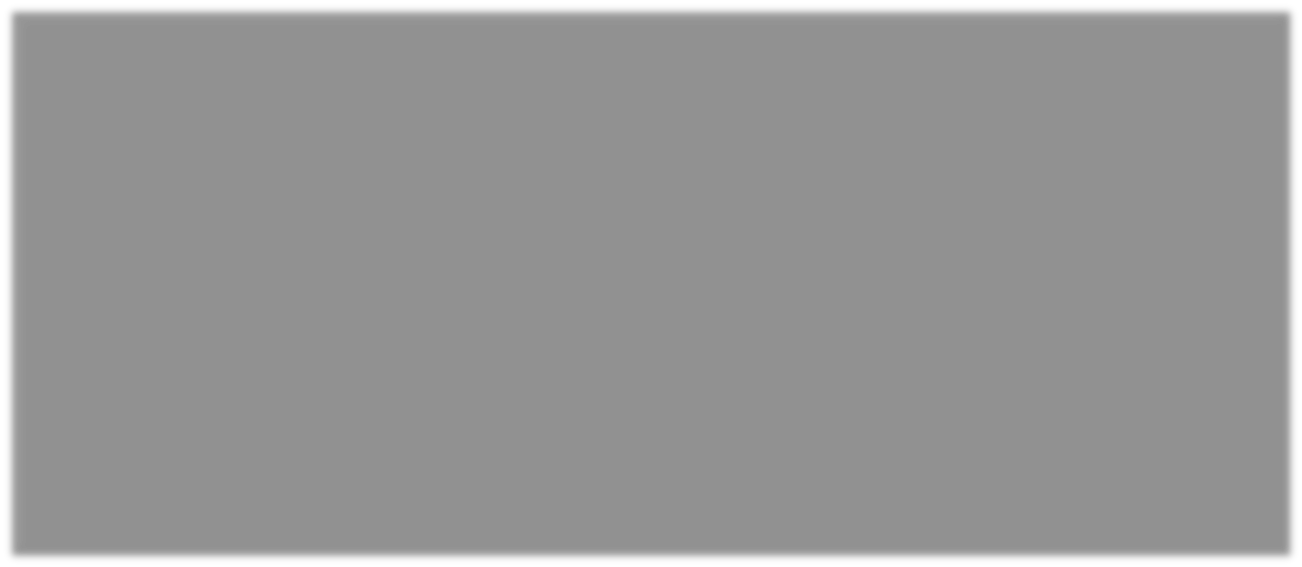
The purpose of this assignment is to showcase practical applications of these tools in discovering assets and vulnerabilities that can be used to strengthen an organization's security posture.

# 2. Tools & Techniques Used

## Amass

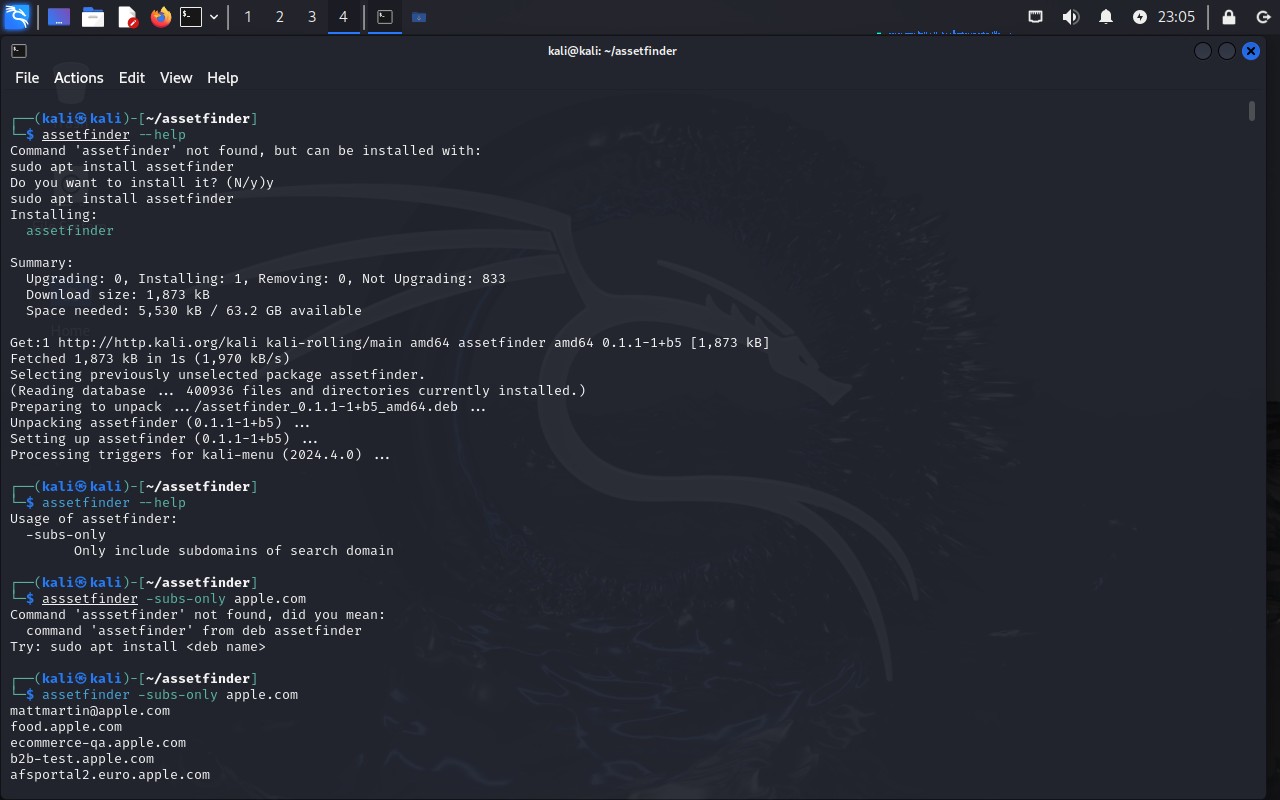
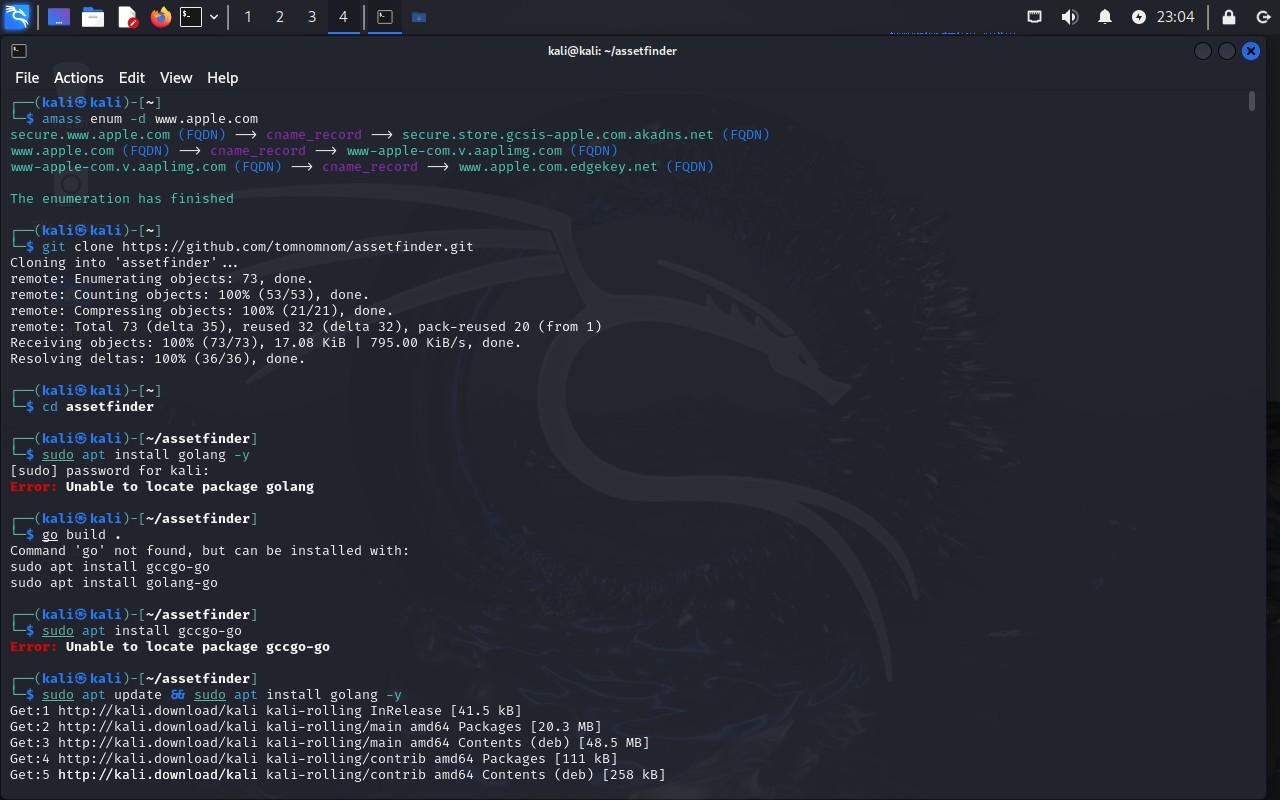
Description: Amass is an open-source tool used for domain enumeration and subdomain discovery, essential for OSINT and reconnaissance.

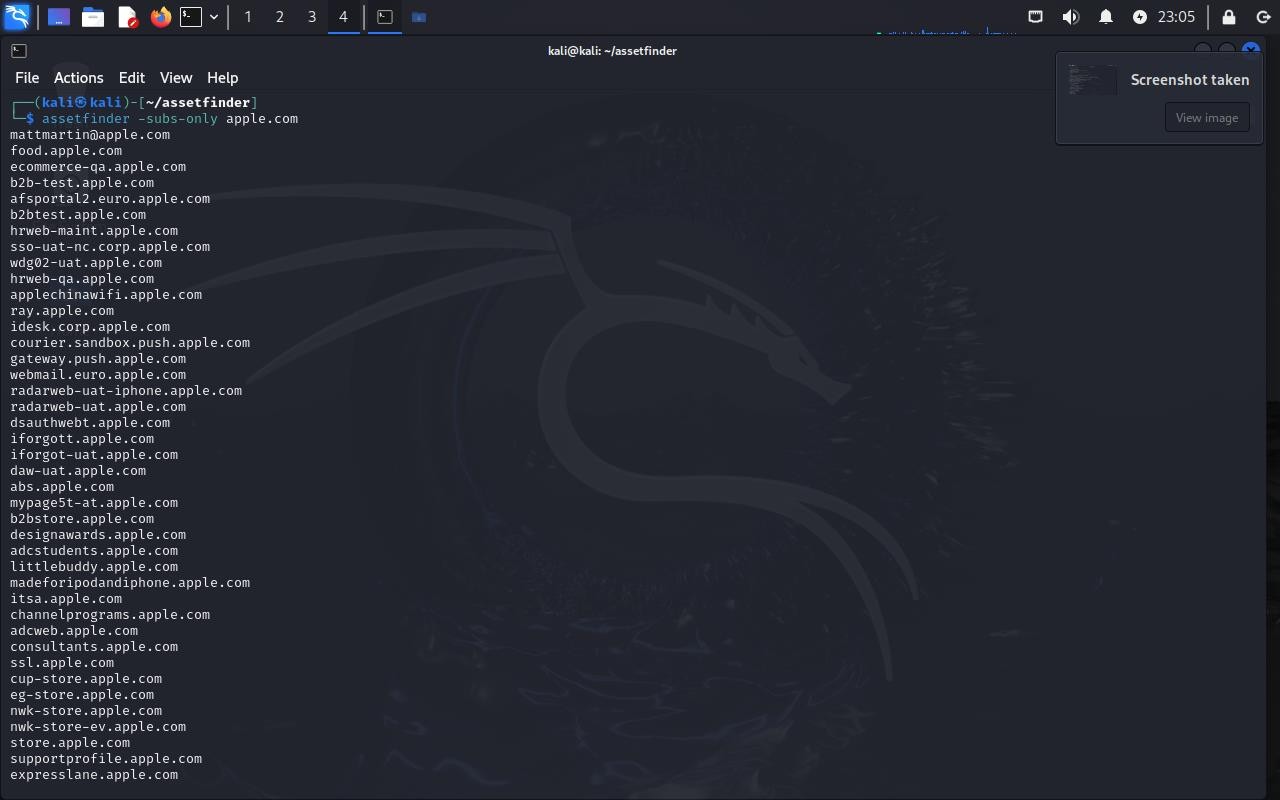
Usage Example: Command: amass enum -d apple.com



## Assetfinder

Description: Assetfinder finds subdomains and asset information to reduce the attack surface. Usage Example: Command: assetfinder --subs-only apple.com



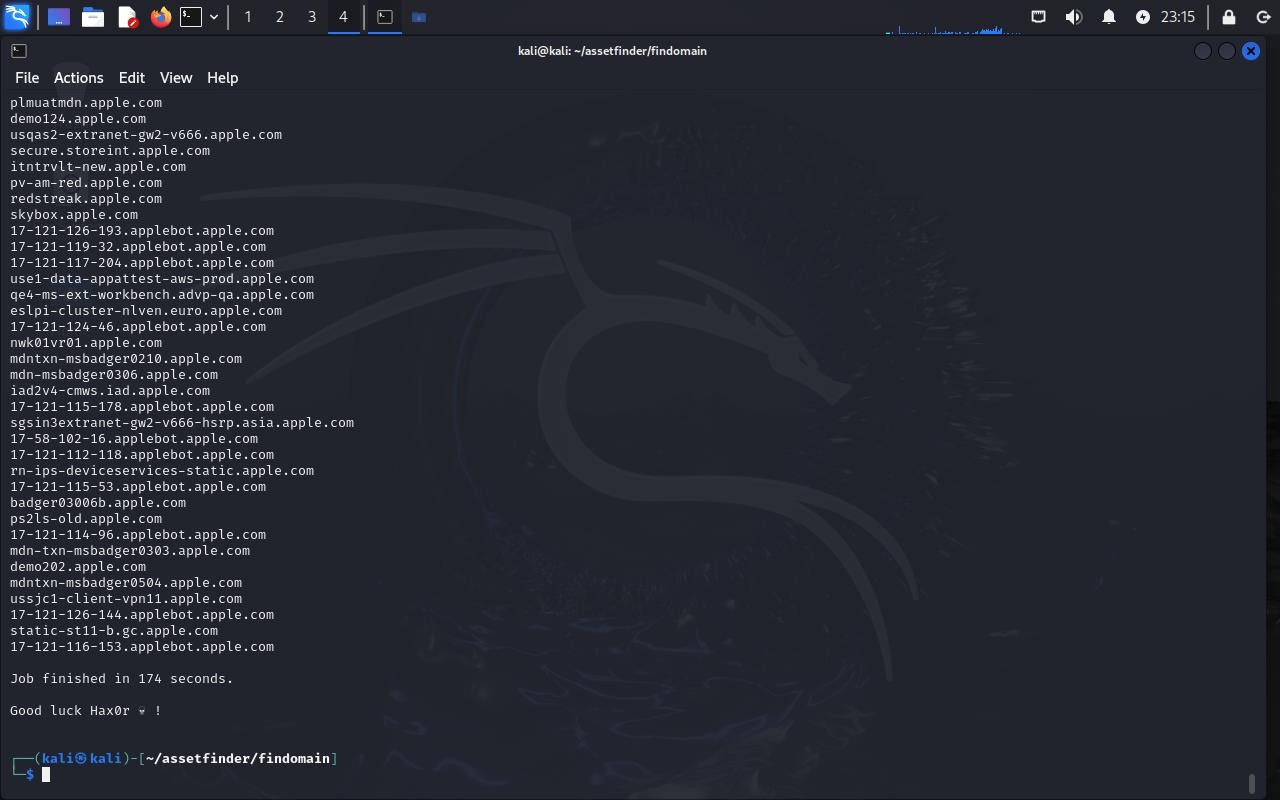


## Findomain

Description: Findomain is a fast subdomain enumeration tool that aids in identifying an organization's digital footprint.

Usage Example: Command: findomain -t apple.com

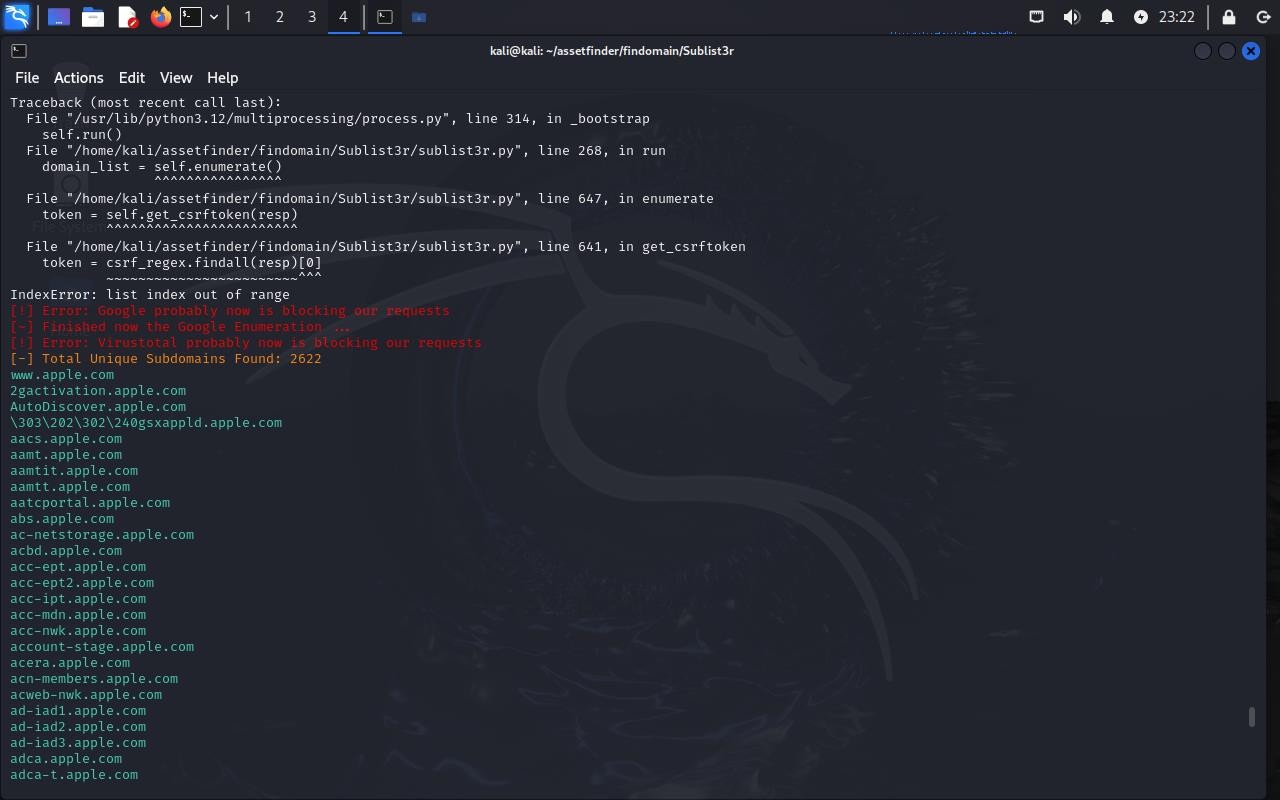
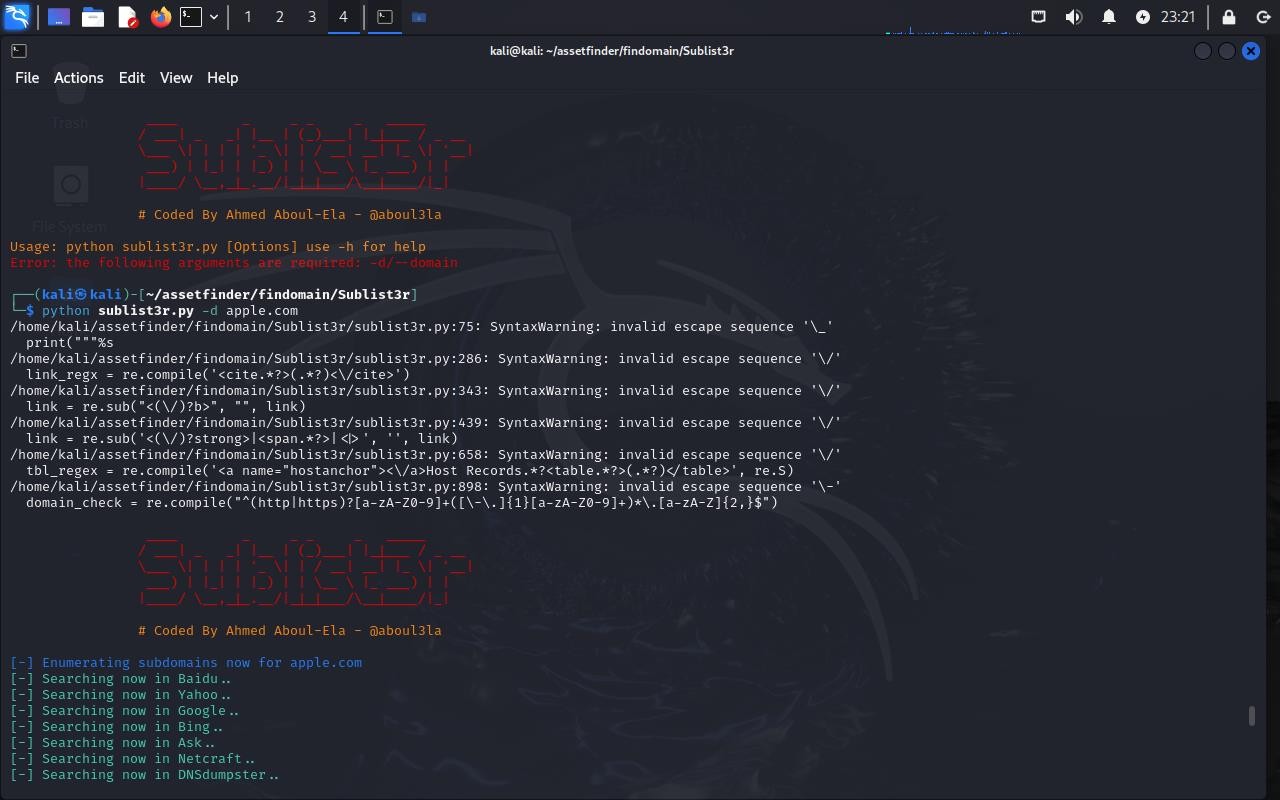




## Sublist3r

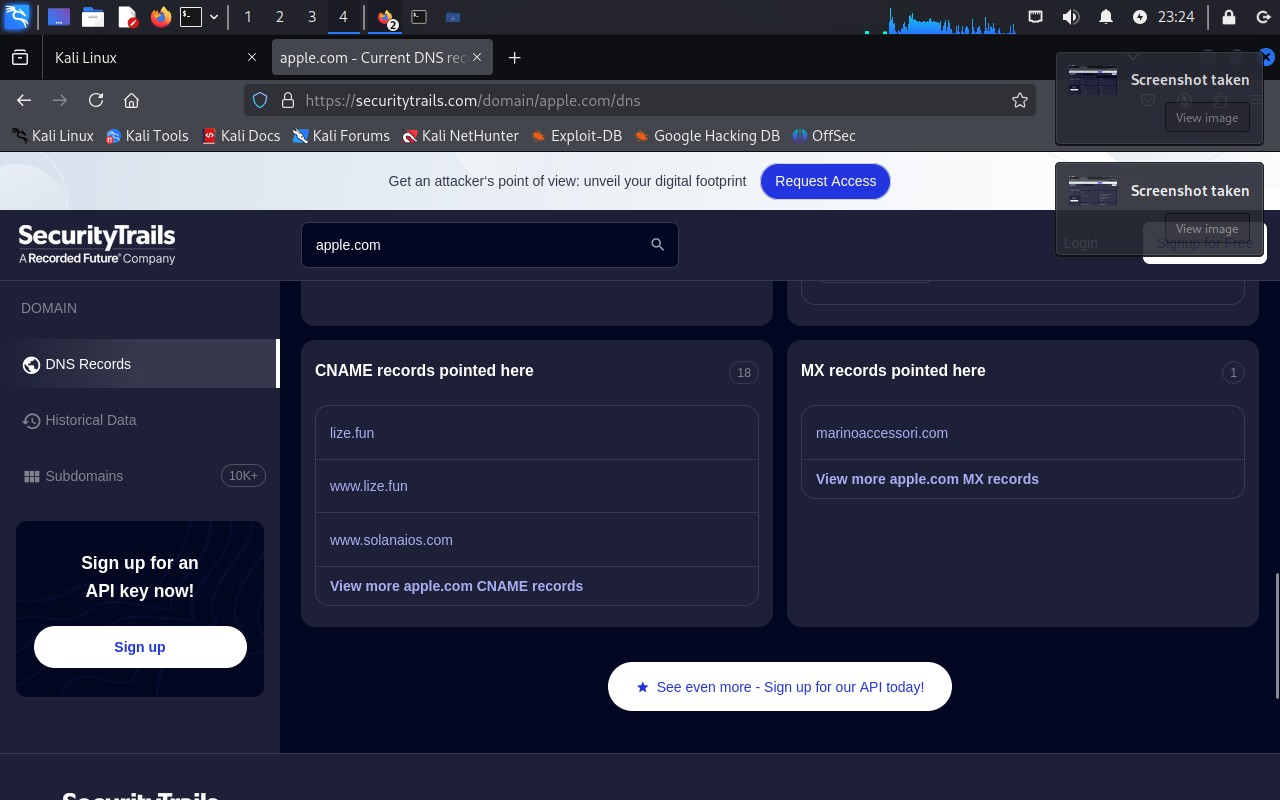
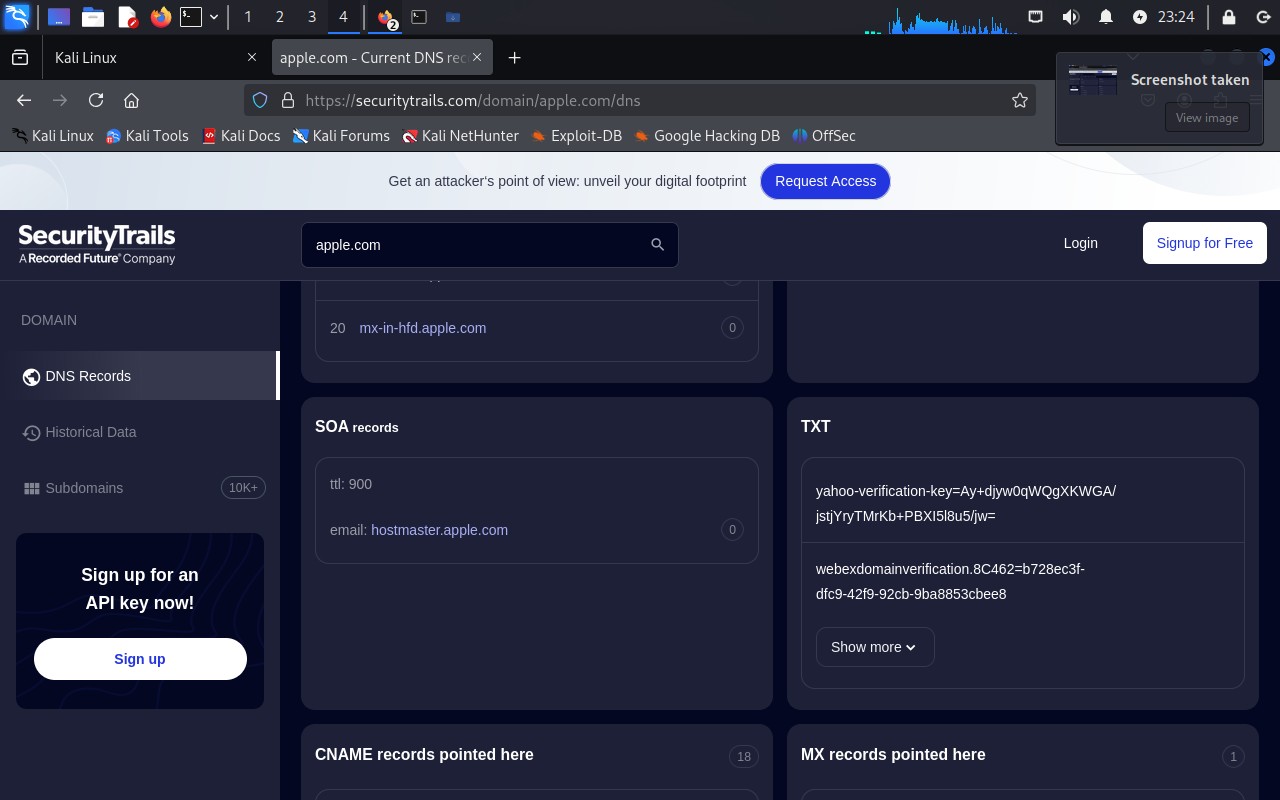
Description: Sublist3r leverages search engines and APIs to discover subdomains for security testing.

Usage Example: Command: python3 sublist3r.py -d apple.com



## SecurityTrails

Description: SecurityTrails provides comprehensive domain and DNS data for asset monitoring and threat intelligence.

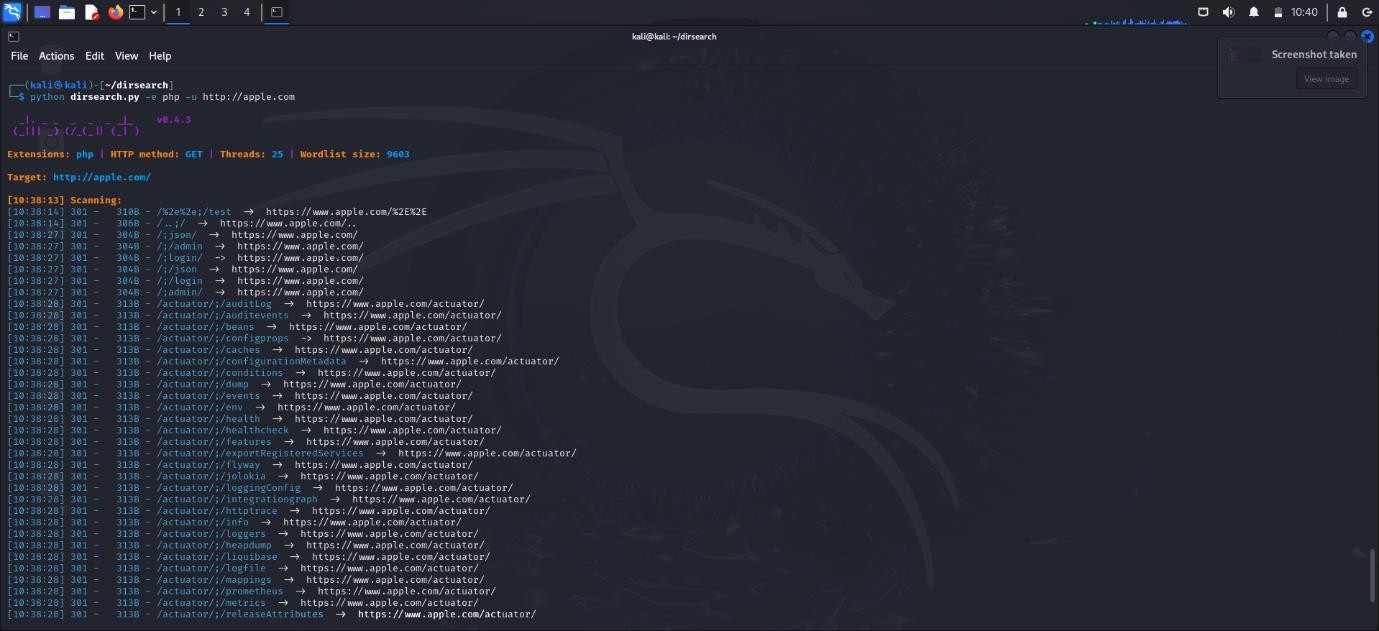
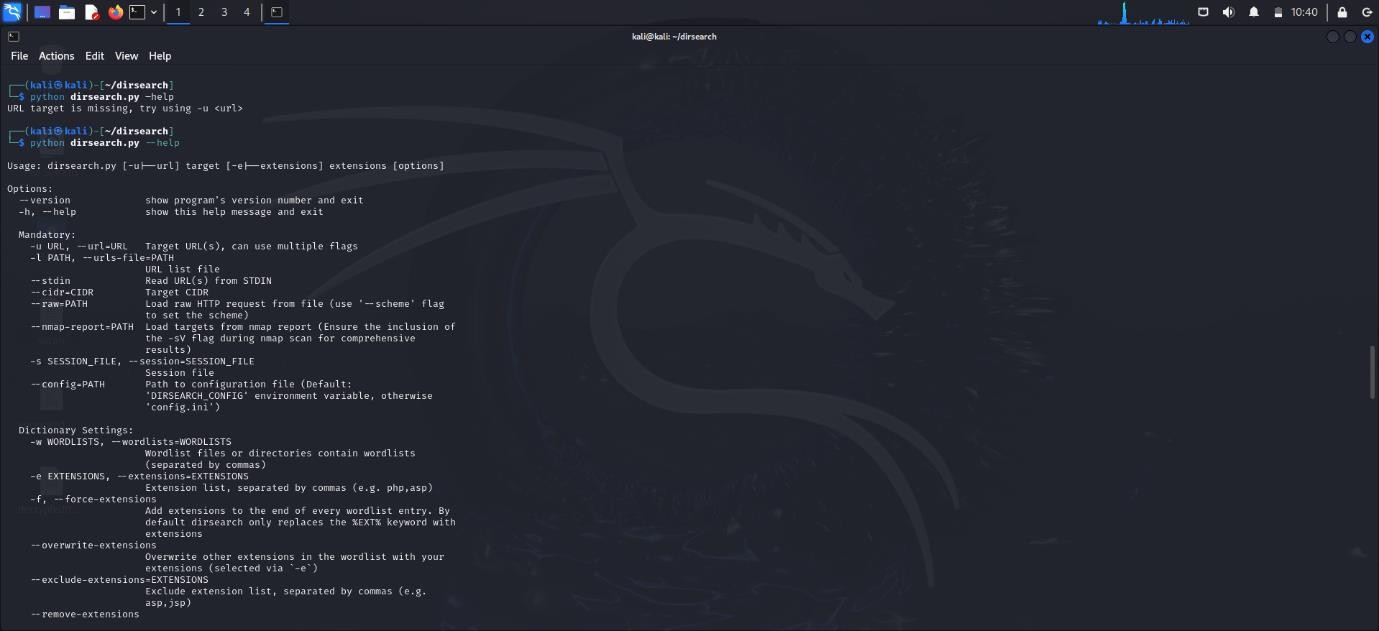
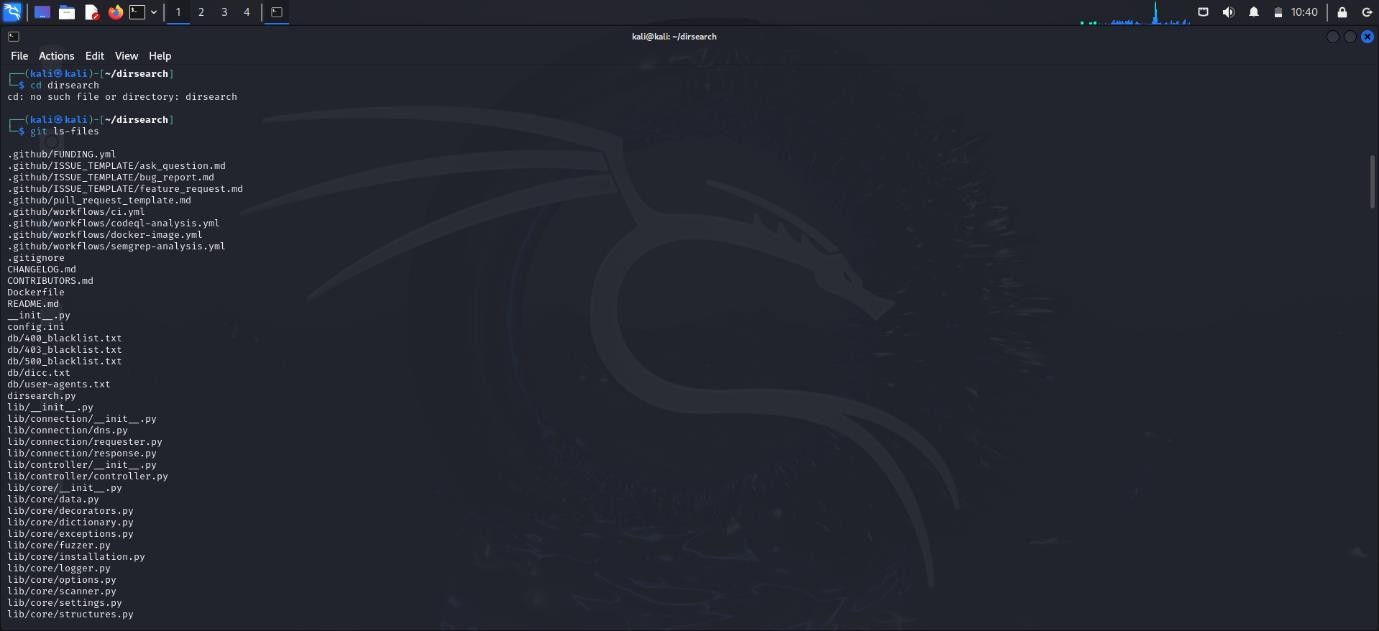
Usage Example: Requires API access at securitytrails.com

## Dirsearch

Description: Dirsearch brute-forces directories and files on web servers to uncover hidden resources and misconfigurations.

Usage Example: Command: python3 dirsearch.py -u https://example.com -e php,html,js

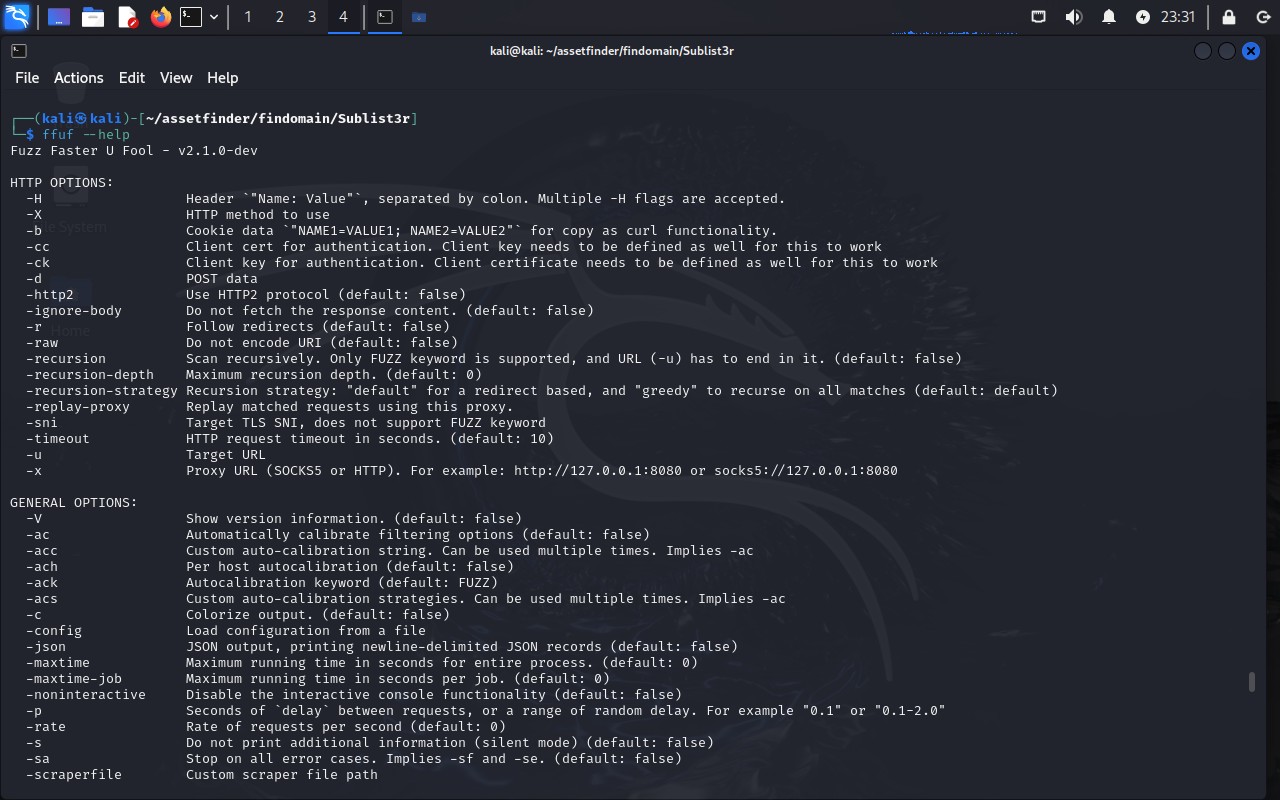


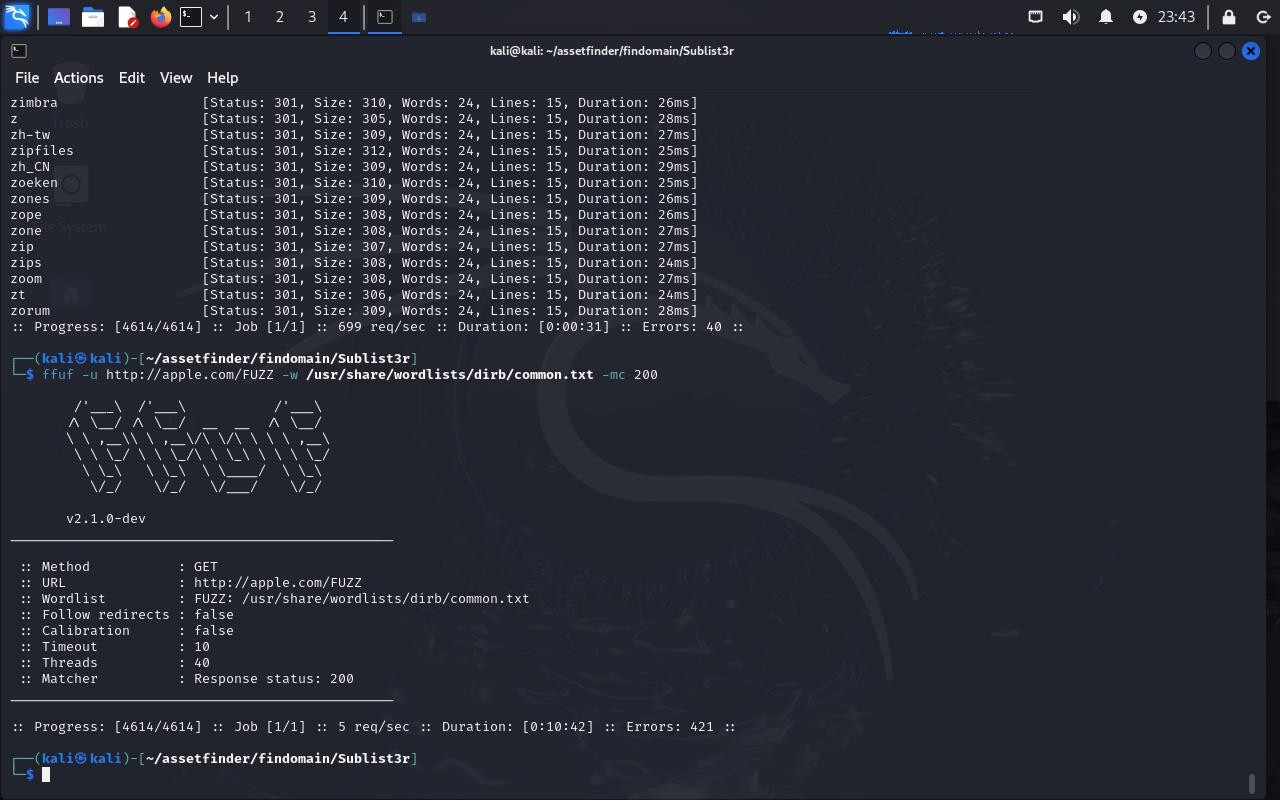
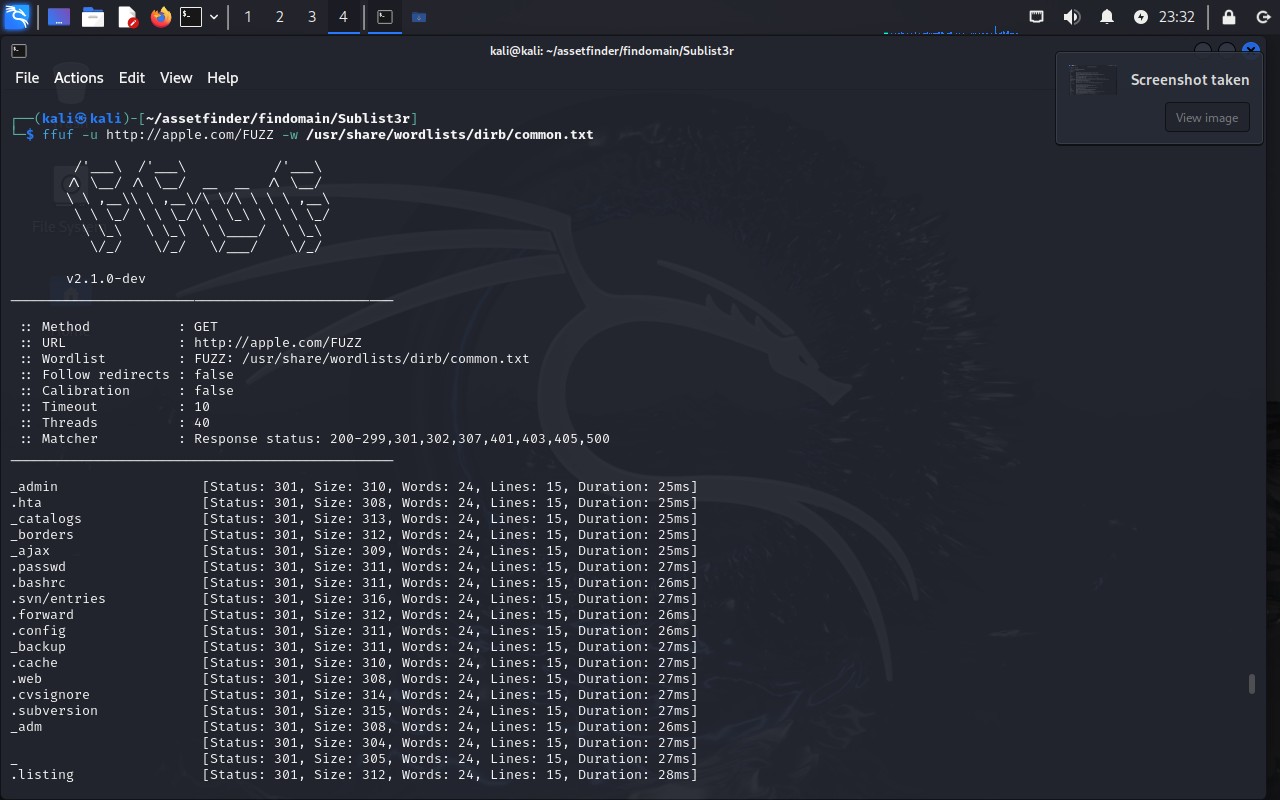


## FFUF (Fuzz Faster U Fool)

Description: FFUF is a fast web fuzzer for finding hidden files, directories, and parameters.

Usage Example: Command: ffuf -u [https://apple.com/FUZZ -w /path/to/wordlist.txt](https://apple.com/FUZZ%20-w%20/path/to/wordlist.txt)

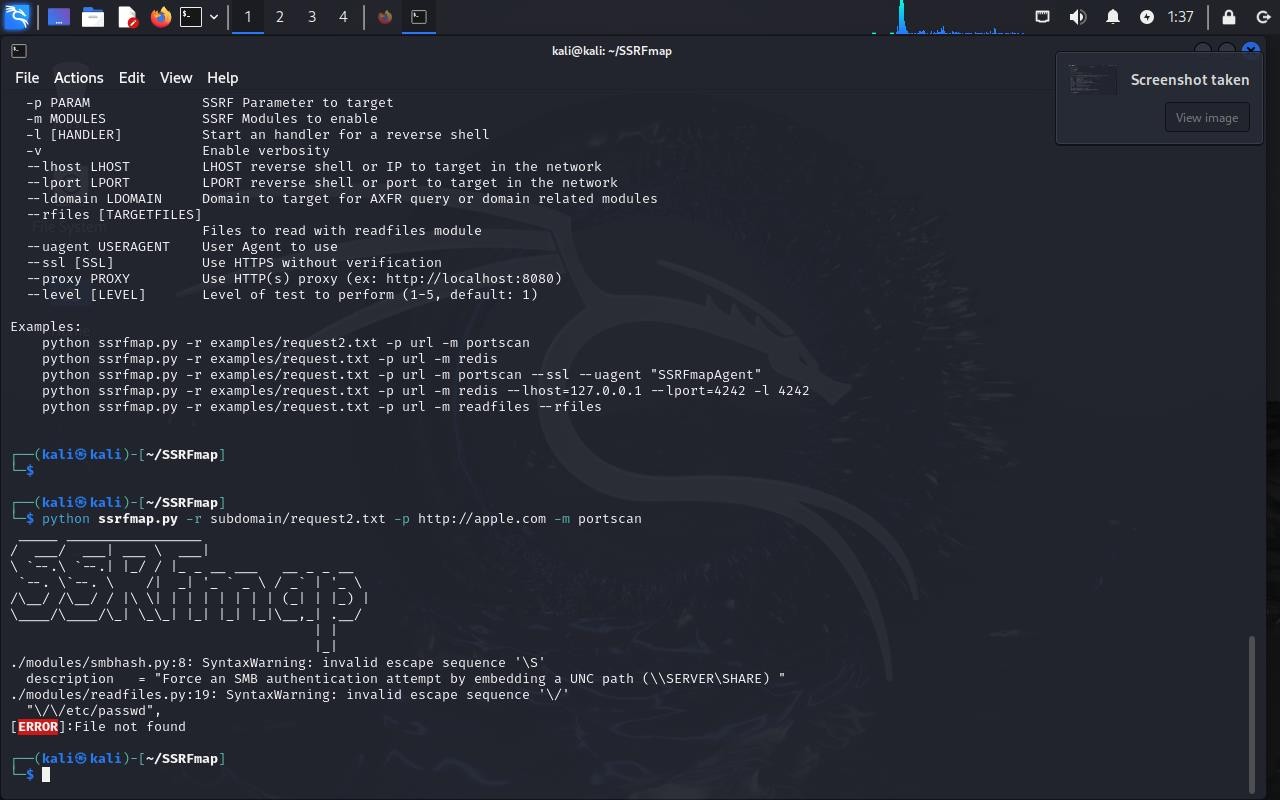


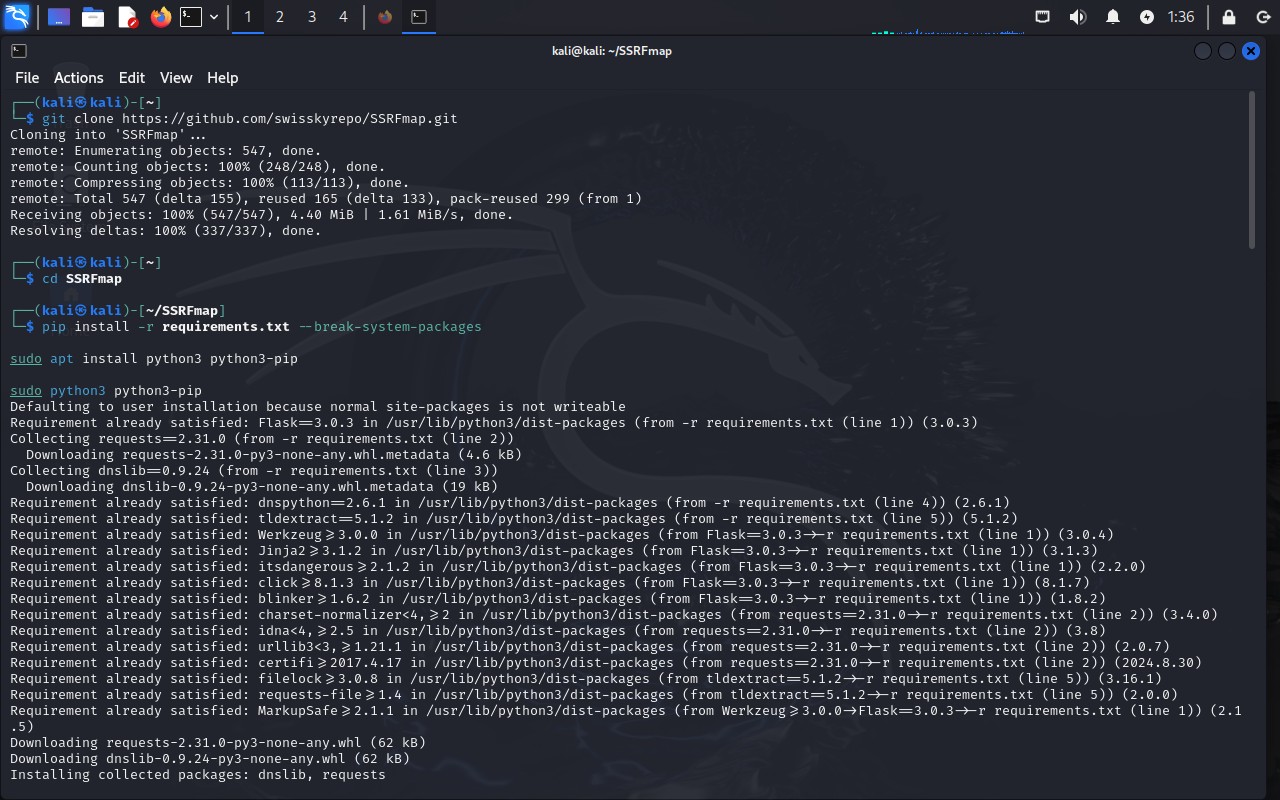


## SSRFmap

Description: SSRFmap automates Server-Side Request Forgery (SSRF) exploitation, facilitating internal resource access.

Usage Example: Command: python3 ssrfmap.py -l urls.txt -p awsKeys

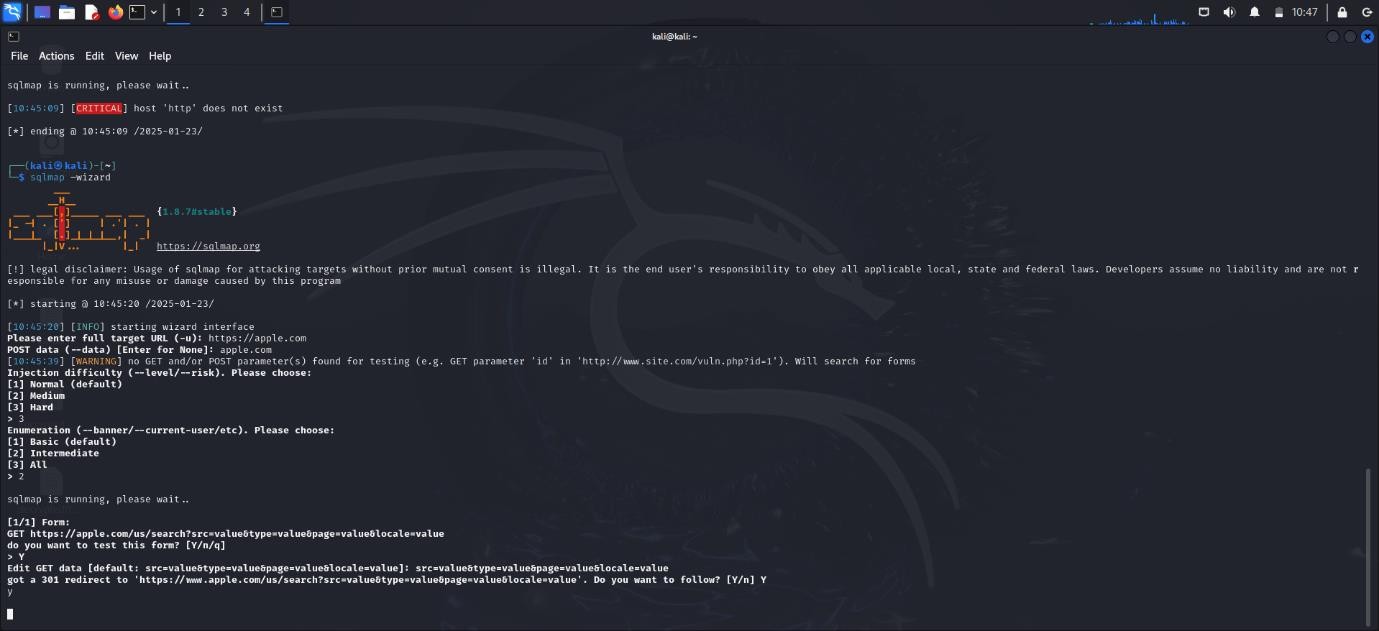
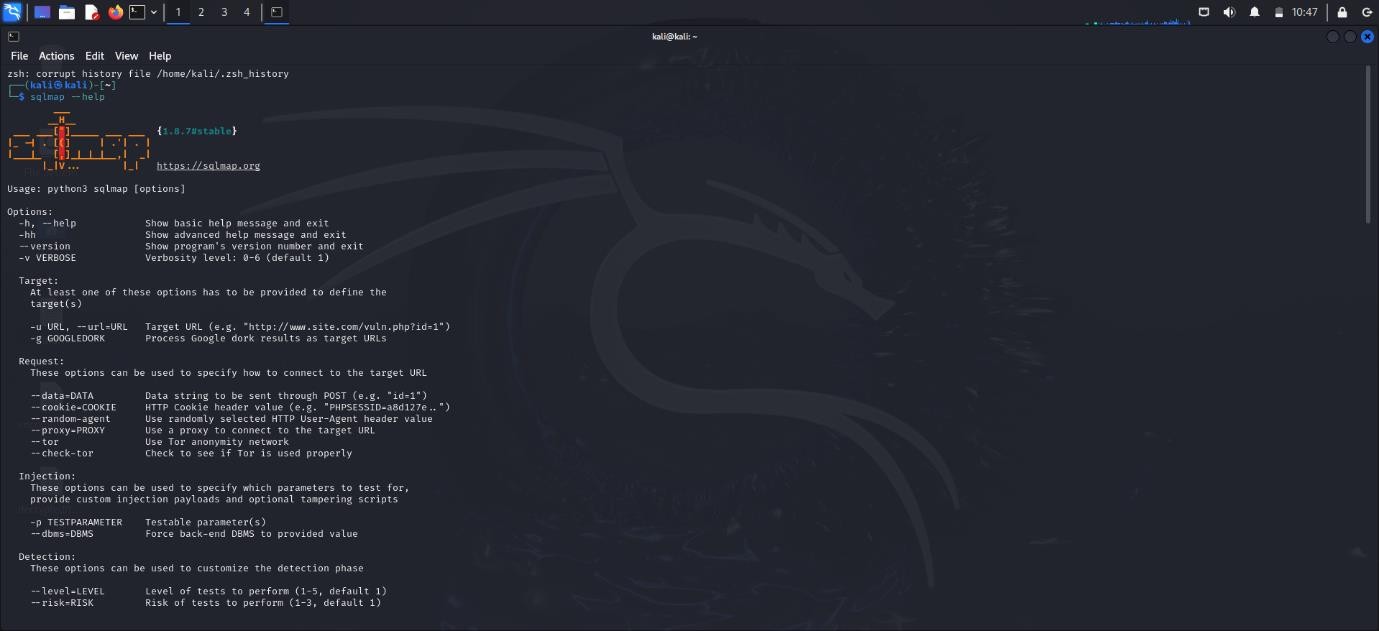




## SQLMap

Description: SQLMap automates SQL injection detection and exploitation in web applications.

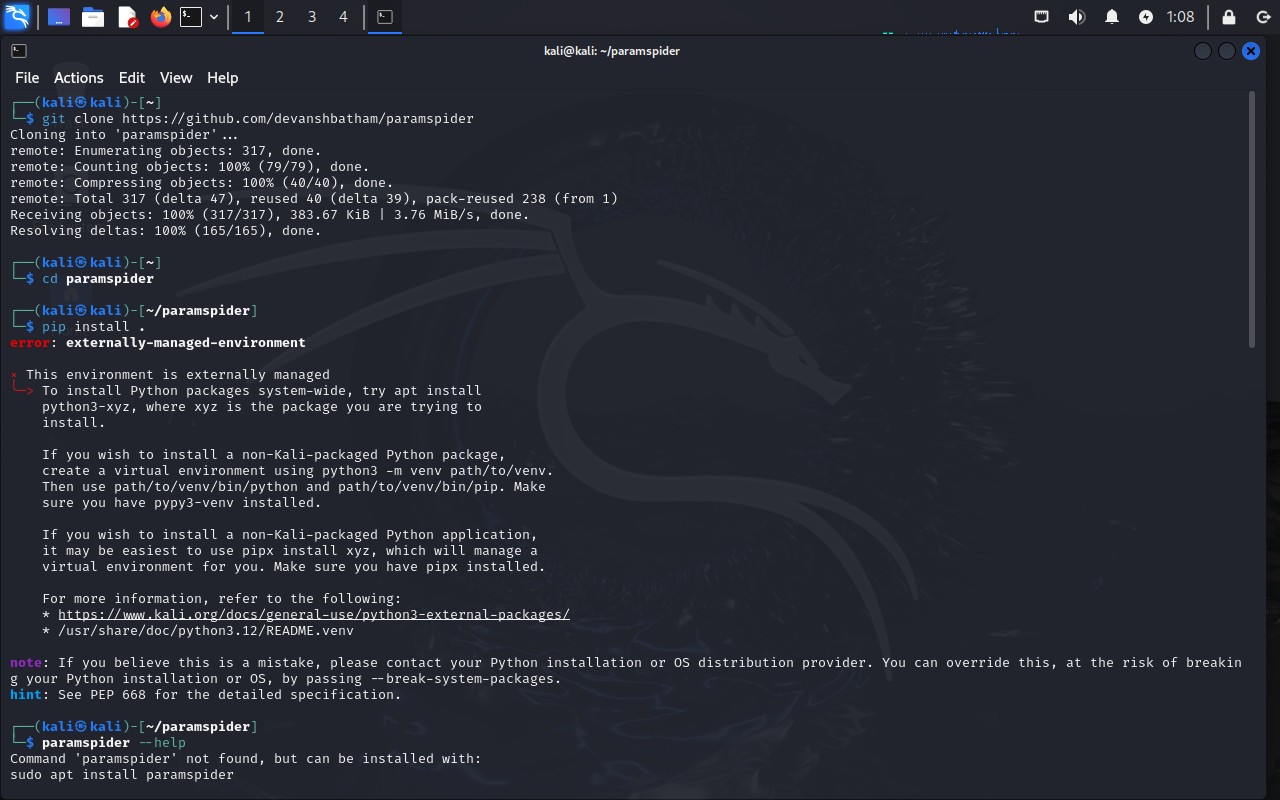
Usage Example: Command: python3 sqlmap.py -u "http://apple.com/index.php?id=1" –dbs

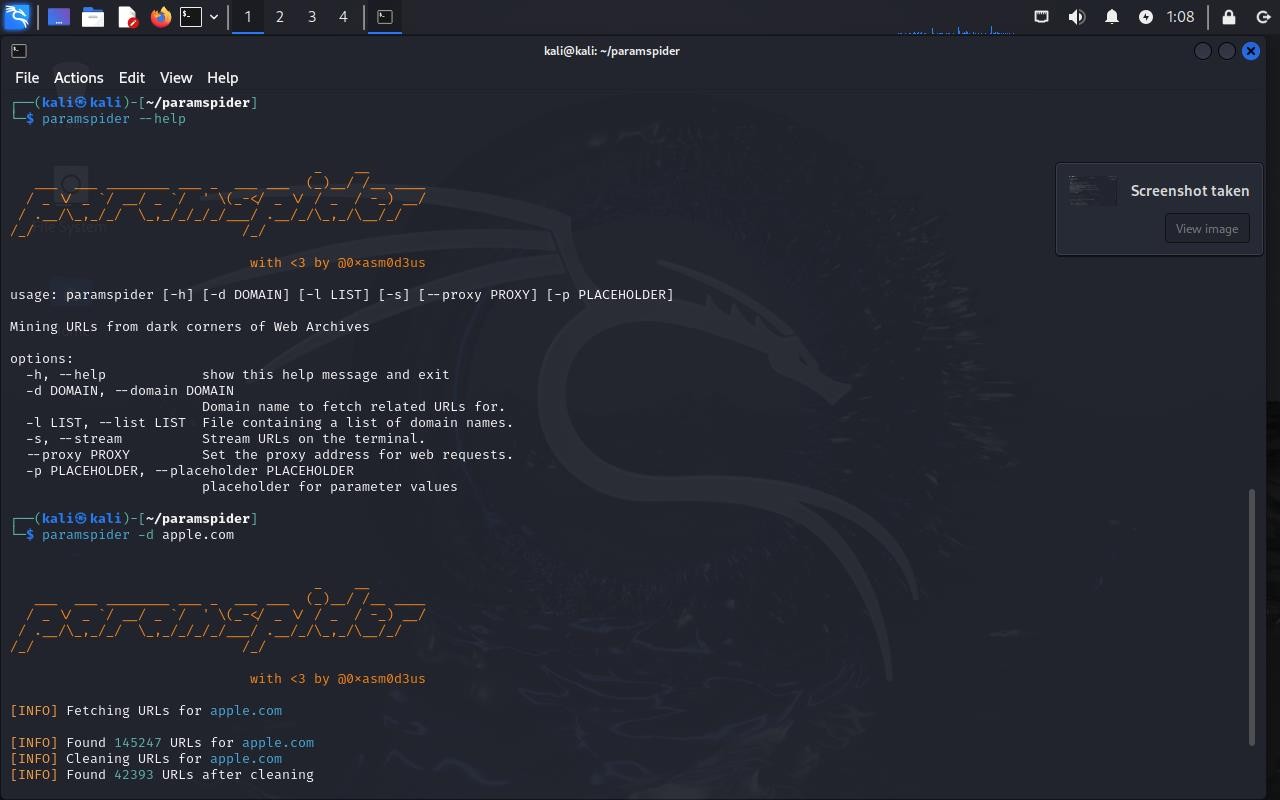
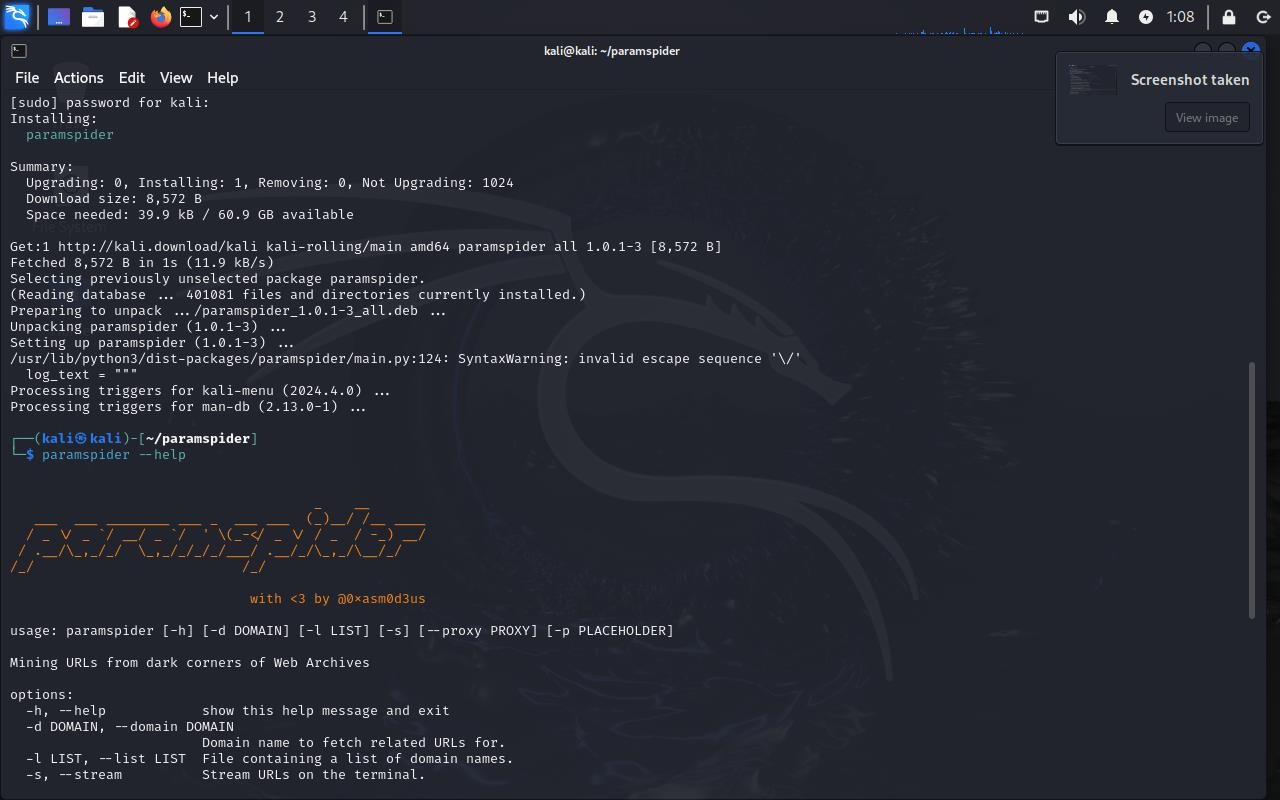


## ParamSpider

Description: ParamSpider discovers GET and POST parameters for vulnerability assessments like XSS or SQLi testing.

Usage Example: Command: python3 paramspider.py --domain apple.com

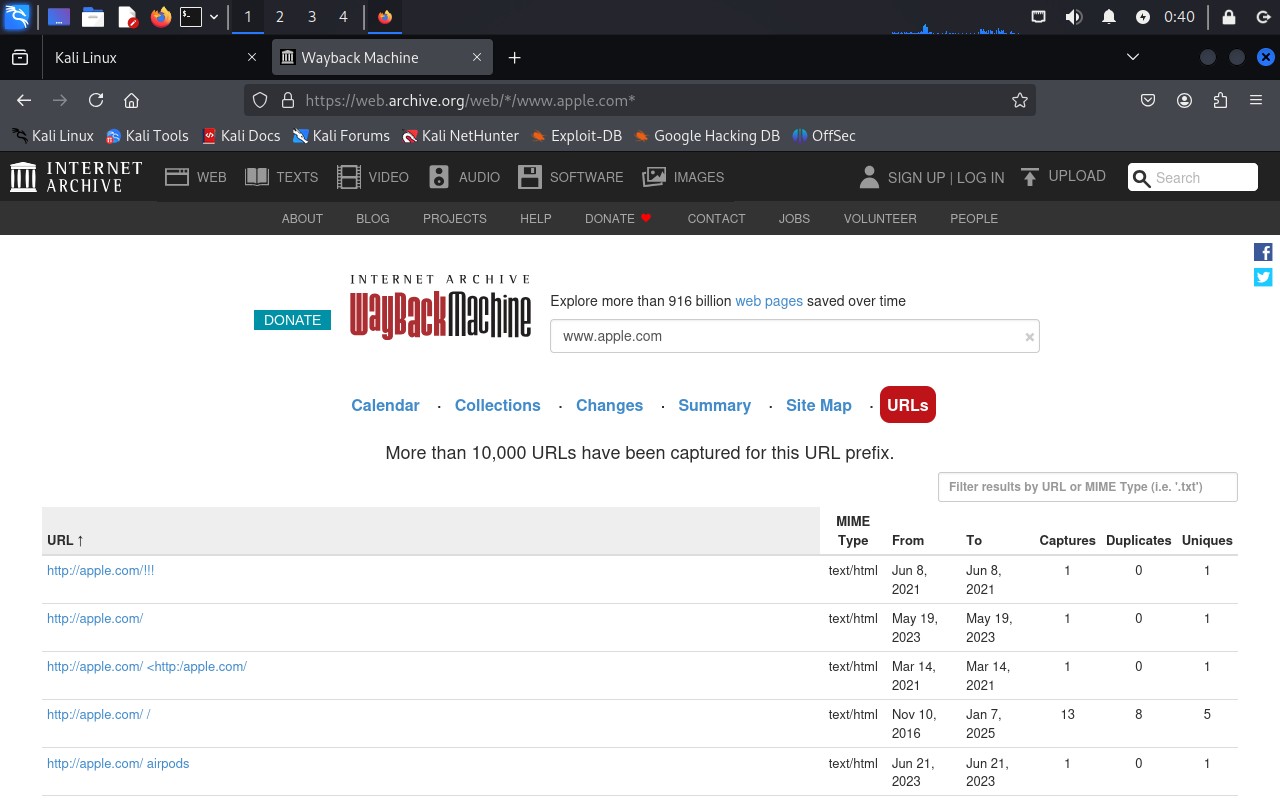




## WaybackURLs

Description: WaybackURLs collects archived URLs from the Wayback Machine to identify old or hidden endpoints.

Usage Example: Command: echo apple.com | Waybackurls



# 3. Results & Observations

The tools provided extensive reconnaissance data on the demo website. Subdomain enumeration revealed multiple active subdomains. Directory brute-forcing identified hidden resources, and parameter discovery highlighted potential areas for injection attacks. The results emphasize the importance of asset management and regular security audits.

# 4. Conclusion

This assignment demonstrates the effectiveness of OSINT and reconnaissance tools in identifying digital assets and vulnerabilities. Organizations should adopt proactive security measures to monitor and protect their external assets to minimize their attack surface.

# 5. References

OWASP Amass - https://owasp.org/www-project-amass/

Assetfinder - https://github.com/tomnomnom/assetfinder

Findomain - https://github.com/findomain/findomain

Sublist3r - https://github.com/aboul3la/Sublist3r

SecurityTrails - https://securitytrails.com

Dirsearch - https://github.com/maurosoria/dirsearch

FFUF - https://github.com/ffuf/ffuf

SSRFmap - https://github.com/swisskyrepo/SSRFmap

SQLMap - https://github.com/sqlmapproject/sqlmap

ParamSpider - https://github.com/devanshbatham/ParamSpider

WaybackURLs - https://github.com/tomnomnom/waybackurls