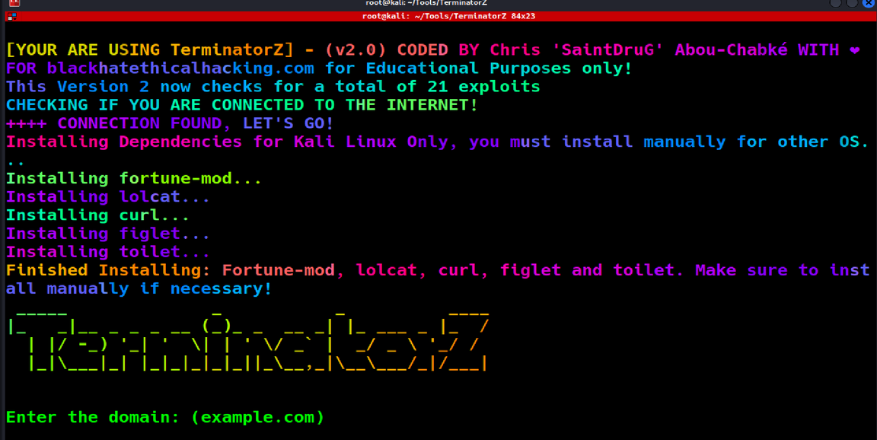
**Offensive Security Tool: TerminatorZ**



**Join our**[**Patreon**](https://www.patreon.com/blackhatethicalhacking)**Channel and Gain access to 70+ Exclusive Walkthrough Videos.**

[](https://www.patreon.com/posts/maltego-recon-2-102851956)

**Reading Time: 3 Minutes**

**TerminatorZ**

TerminatorZ is written by Chris “SaintDruG” Abou-Chabke from Black Hat Ethical Hacking and is designed for Offensive Security attacks.

TerminatorZ is a highly sophisticated and efficient web security tool that scans for potential vulnerabilities in your web applications. It uses a combination of advanced techniques, including using popular tools like waybackurls and curl, to scan your web applications and highlight any potential vulnerabilities but in a passive and quick way for a quick look. The results are displayed in an easy-to-read format in the terminal, and only vulnerable results are saved for further investigation. With its lightweight and fast nature, TerminatorZ is the perfect tool for any Red Teamer.

**See Also: So you want to be a hacker?**[**Offensive Security and Ethical Hacking Course**](https://www.blackhatethicalhacking.com/courses/offensive-security-and-ethical-hacking-course/)

**What Makes TerminatorZ Unique**

TerminatorZ is special because it’s a highly customized for quick and speed high priority known CVES. The script then reads each URL from urls.txt and checks for various vulnerabilities including RCE, CSRF, LFI, open redirect, Log4J, RFI, path traversal, and SQL injection. For each vulnerability, the script performs a test by sending a specific HTTP request and looking for a specific response.

If the vulnerability is detected, the script will write a message to the domain.txt file indicating that the URL is vulnerable. If the vulnerability is not detected, the script will write a message indicating that the URL is not vulnerable.

**Total POCs it will check so far after v2: 24**

**The Flow and Methodology**

The tool starts by asking the user to input the domain they wish to scan. It then creates a folder to store the results and starts the scan. The scan utilizes curl to make HTTP requests to the target domain and checks for various vulnerabilities by injecting known payloads. The tool then checks the responses for indicators of exploitation and validates the results to determine if the target is vulnerable.

The tool’s methodology is carefully designed to ensure that each type of vulnerability is checked specifically and thoroughly. The tool employs a highly analytical and methodical approach to the scanning process, which results in the identification of even the most elusive vulnerabilities. The tool’s logic is designed to be highly efficient and effective, making it the ultimate choice for red team security experts and web security professionals.

In conclusion, TerminatorZ is a game-changer in the world of web security. Its combination of technology, methodology, and expert logic makes it the ultimate tool for identifying and mitigating web application vulnerabilities. Speed is sometimes needed, if you want more tools that do not focus on speed, please make sure to check our other ones.

**See Also:**[**Exploit XSS Injections with a Powerful One-Line Technique**](https://www.blackhatethicalhacking.com/articles/exploit-xss-injections-with-a-powerful-one-line-technique/)

**See Also:**[**Offensive Security Tool: XSSRocket**](https://www.blackhatethicalhacking.com/tools/xssrocket/)

**Features**

Scans for various web application vulnerabilities, including:

* File Upload
* Command Injection
* Host Header Injection
* HTTP Parameter Pollution (HPP)
* Clickjacking
* CORS Misconfiguration
* Sensitive Data Exposure
* Session Fixation
* XSS (Cross-site scripting)
* SSRF (Server-side request forgery)
* XXE (XML external entity)
* Insecure deserialization
* Remote Code Execution via Shellshock (RCE)
* SQL Injection (SQLi)
* Cross-Site Scripting (XSS)
* Cross-Site Request Forgery (CSRF)
* Remote Code Execution (RCE)
* Log4J
* Directory Traversal (DT)
* File Inclusion (FI)
* Sensitive Data Exposure (SDE)
* Server Side Request Forgery (SSRF)
* Shell Injection (SI)
* Broken Access Control (BAC)
* Generates Random Sun Tzu Quote for Red Teamers, Checks if you are connected to the Internet too!
* Utilizes tools such as waybackurls, curl, and others for comprehensive vulnerability assessments
* Lightweight and fast, delivering results in real-time directly to the terminal
* Only reports vulnerabilities, making it easy to prioritize and remediate vulnerabilities in a timely manner

**Requirements**

* waybackurls: This tool can be installed by running **go install github.com/tomnomnom/waybackurls@latest**
* cURL: This tool is commonly pre-installed on Kali Linux and Ubuntu, but can be installed by running **apt-get install curl** on Ubuntu or **brew install curl** on MacOS
* httpx: is a fast and multi-purpose HTTP toolkit that allows running multiple probes using the retryable http library. To install it: **go install -v github.com/projectdiscovery/httpx/cmd/httpx@latest**
* lolcat: **pip install lolcat** for rainbow beauty
* You also need, toilet, fortune-mod but the new update will install them in the beginning.

**See Also:**[**Write up: A primer on OS Command Injection Attacks**](https://www.blackhatethicalhacking.com/articles/a-primer-on-os-command-injection-attacks/)

**Installation**

git clone https://github.com/blackhatethicalhacking/TerminatorZ.git

cd TerminatorZ

chmod +x TerminatorZ.sh

./TerminatorZ

**Compatibility**

This tool has been tested on Kali Linux, Ubuntu and MacOS.

**Disclaimer**

This tool is provided for educational and research purpose only. The author of this project is no way responsible for any misuse of this tool. We use it to test under NDA agreements with clients and their consents for pentesting purposes and we never encourage to misuse or take responsibility for any damage caused.