

Forum:[Hack Forums](#)

Thread: [HailMarry Recon/Pentesting Tool for Automated Multi-Tool Analysis \(Pentesting only\)](#)

MadScientist - September 9, 2026, 10:25 pm

Small Python script for pentesting that spins up 6 independent xterm windows (or which you chose in the interactive menu) — WPScan, SQLMap, Nikto, NMap, Nuclei, and Findomain — each running against a single target, tiled into an equal grid on your screen so you can watch them all at once instead of tabbing between terminals.

Designed for Kali and to be run through a proxy like Burp on port 8080 (a local http proxy is required - but you can edit code to change that). Has multi-monitor support to designate which one to run on. Required tools are attempted to be installed automatically. You can remove the proxy support in the code easily, I like it for pentesting as it pumps Burp with data to dig through.

WPScan requires you to edit your API code into the script.

Does SQLInjection, Wordpress analysis, DNS domain finder, Port scan, Vulnerability analysis, target analysis and spidering/network flaws.

Features:

Auto MultiPlatform SQLi Tampering

Auto-tiles into a grid on whichever monitor you're actually using (multi-monitor aware)

Pick specific tools to run (--terminals nmap,nuclei) or run all six

No-args interactive mode — just run it and it'll prompt you for the host, which tools, and which monitor

Auto-installs tools if it's missing

Each terminal keeps running independently and stays open after the command finishes

Usage:

```
python3 HailMarry.py https://target.com
```

```
python3 HailMarry.py --terminals wpscan,nmap,findomain target.com
```

```
python3 HailMarry.py --list-terminals
```

```
python3 HailMarry.py --list-monitors
```

```
python3 HailMarry.py
```

Requires: xterm, xdotool, xrandr, plus the individual tools (wpscan, sqlmap, nikto, nmap, nuclei — findomain auto-installs if not found.

For authorized testing/recon on targets you have permission to scan.

VERY NOISY if you're running all modules at the same time so there's support for one by one or multi usage. You'll get IP blocked very fast if you run the full 6 modules at once. Adding multi proxy support would be easy so each terminals running a different IP but using for local testing on my computer lab personally

<https://pastebin.com/CiJdzQ1s>

Vagueness - September 11, 2026, 12:59 am

This is handy af and save a lot of time

Dotexe - September 11, 2026, 1:09 am

Good stuff, but given how many AI agents are doing the same even with better output (hexstrike/cyberstrike), I don't see the reason of using this. Although I'd congrats you if you did it manually without the help of AI

MadScientist - September 11, 2026, 2:18 pm

(Sep 11, 2026 01:09 AM)Dotexe Wrote: [\[CITE\]](#) Good stuff, but given how many AI agents are doing the same even with better output (hexstrike/cyberstrike), I don't see the reason of using this.

Although I'd congrats you if you did it manually without the help of AI

Interesting I'll have to look more into it, what do you use for automation without responses on Linux (or Win)

vampirehq - September 11, 2026, 3:00 pm

thanks i will try it rn hoping some results

Dotexe - September 11, 2026, 3:36 pm

(Sep 11, 2026 02:18 PM)MadScientist Wrote: [\[CITE\]](#) Interesting I'll have to look more into it, what do you use for automation without responses on Linux (or Win)

I usually use local model Qwen 3.8 and chain with some of the main tools I use for web assessments like nmap, subfinder, nuclei, dnsenum, the harvester and slowly onboard new apps on the go. It really depends on the project I am working on. I tried jailbreaking some models but it gets patched quite often and I don't have the time to repeat the process. Luckily I don't aim to get the projects done fast so I couldn't care less for choosing Anthropic/OpenAI models over the local one. Ideally if you can build an AI MCP agent yourself, that would be the best approach.