

# AI-Powered Cybersecurity Scanner

This AI-powered cybersecurity scanner automates security assessments using Nmap, Gobuster, and FFUF. It scans for open ports, hidden directories, and vulnerable endpoints, helping security researchers identify potential risks. Optimized with custom wordlists, auto-calibration, and filtering for better accuracy.

## Key Features:

- Uses Nmap for port scanning with optimized parameters.
- Gobuster for directory enumeration with custom wordlists.
- FFUF for fuzzing hidden endpoints efficiently.
- Filters out common false positives for better accuracy.
- Supports auto-calibration to adapt to different targets.

## Installation & Usage:

1. Install required tools: Nmap, Gobuster, FFUF.
2. Ensure the script has execution permissions.
3. Run the script: `python3 scanner.py <target_domain>`
4. Analyze the output for potential vulnerabilities.

## Optimization Tips:

- Use a tailored wordlist for better Gobuster results.
- Adjust the number of threads (-t) based on server response time.
- Save outputs using '> results.txt' for better analysis.
- Check virtual hosts using Nmap's --script http-vhosts option.