FireFart/WordpressPingbackPortScanner

FireFart/WordpressPingbackPortScanner - Author not stated, GitHub.

- Published: date not stated
- Original: <https://web.archive.org/web/20170903113359/https://github.com/FireFart/WordpressPingbackPortScanner>
- Current location: <https://web.archive.org/web/20180611030944/https://github.com/FireFart/WordpressPingbackPortScanner>
- Preserved from: https://web.archive.org/web/20180611030944/https://github.com/FireFart/WordpressPingbackPortScanner (live) on 2026-08-09
- Capture timestamp: 20170903113359
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

WordpressPingbackPortScanner

- 53 commits
- 1 branch
- 0 releases
- 2 contributors
- Ruby 100.0%

Ruby

[image: image] Fetching latest commit…

Cannot retrieve the latest commit at this time.

Permalink

README.md

WordpressPingbackPortScanner

Wordpress exposes a so called Pingback API to link to other blogposts. Using this feature you can scan other hosts on the intra- or internet via this server. You can also use this feature for some kind of distributed port scanning: You can scan a single host using multiple Wordpress Blogs exposing this API. This issue was fixed in Wordpress 3.5.1. Older versions are vulnerable, if the XML-RPC Interface is active.

http://www.acunetix.com/blog/web-security-zone/wordpress-pingback-vulnerability/

Examples

Before you start you need to install all dependencies with

```
gem install bundler
bundle install
```

Quick-scan a target via a blog:

```
ruby wppps.rb -t http://www.target.com http://www.myblog.com/
```

Use multiple blogs to scan a single target:

```
ruby wppps.rb -t http://www.target.com http://www.myblog1.com/ http://www.myblog2.com/ http://www.myblog3.com/
```

Scan a free wordpress.com blog (all ports) from the internal network:

```
ruby wppps.rb -a -t http://localhost http://myblog.wordpress.com/
```