

teler - Protect Your WebApp!

Tell me, what kind of **threat** are you?

@dwiswant0

Insert Picture of
Adorable Character



About

- Dwi Siswanto
- *Not-really* Bug Bounty Hunter
- Top #1 Nuclei templates contributors
- Security Engineer @ Kitabisa
- noobSecurity Team



Background

TL;DR



Detection
≠
Prevention

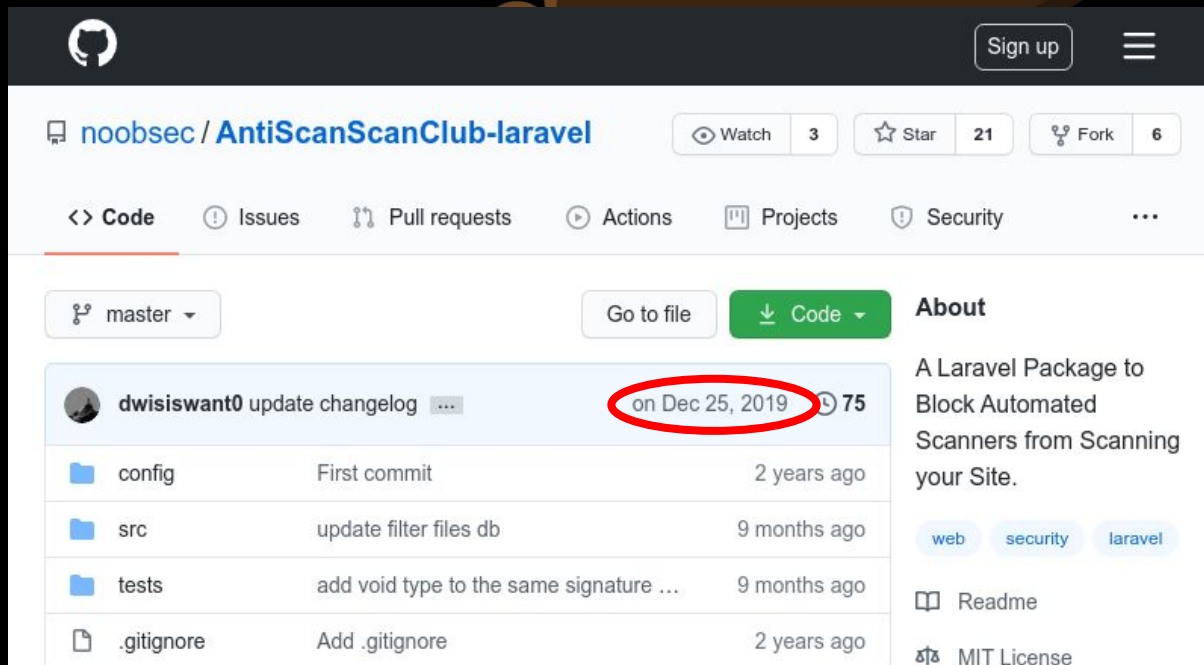
Background

TL;DR



Background

TL;DR



The screenshot shows the GitHub repository page for `noobsec / AntiScanScanClub-laravel`. The repository has 3 watchers, 21 stars, and 6 forks. The `Code` tab is selected, showing a file tree with folders `config`, `src`, and `tests`, and a file `.gitignore`. The commit history shows a commit by `dwiswant0` titled "update changelog" on Dec 25, 2019, with 75 commits. The `About` section describes it as a Laravel Package to Block Automated Scanners from Scanning your Site, with tags for `web`, `security`, and `laravel`. It also includes links to the `Readme` and `MIT License`.

File/Folder	Description	Time
config	First commit	2 years ago
src	update filter files db	9 months ago
tests	add void type to the same signature ...	9 months ago
.gitignore	Add .gitignore	2 years ago

Background

TL;DR

A screenshot of a GitHub repository page for 'noobsec / AntiScanScanClub-laravel'. The repository has 3 watchers, 21 stars, and 6 forks. The 'Code' tab is selected. The commit history shows a commit by 'dwiswant0' on Dec 25, 2019, which is circled in red. Below the commit history, there is a table of files and folders.

File/Folder	Commit Message	Time
config	First commit	2 years a
src	update filter files db	9 months a
tests	add void type to the same signature ...	9 months a
.gitignore	Add .gitignore	2 years a



Features

Features

- Real-time!

Features

- Real-time!
- Alerting

Features

- Real-time!
- Alerting
 - Slack

Features

- Real-time!
- Alerting
 - Slack
 - Discord

Features

- Real-time!
- Alerting
 - Slack
 - Discord
 - Telegram

Features

- Real-time!
- Alerting
 - Slack
 - Discord
 - Telegram
- Monitoring

Features

- Real-time!
- Alerting
 - Slack
 - Discord
 - Telegram
- Monitoring
 - Prometheus

Features

- Real-time!
- Alerting
 - Slack
 - Discord
 - Telegram
- Monitoring
 - Prometheus



What can teler detect?

What can teler detect?

- Request URI

What can teler detect?

- Request URI
 - URL → Directory Bruteforce

What can teler detect?

- Request URI
 - URL → Directory Bruteforce
 - Parameters → Common Web Attack

What can teler detect?

- Request URI
 - URL → Directory Bruteforce
 - Parameters → Common Web Attack
- Request Headers

What can telnet detect?

- Request URI
 - URL → Directory Bruteforce
 - Parameters → Common Web Attack
- Request Headers
 - User-Agent → Bad Crawler? Bot?

What can teler detect?

- Request URI
 - URL → Directory Bruteforce
 - Parameters → Common Web Attack
- Request Headers
 - User-Agent → Bad Crawler? Bot?
 - Referrer → Bad Referrer? Bot?

What can teler detect?

- Request URI
 - URL → Directory Bruteforce
 - Parameters → Common Web Attack
- Request Headers
 - User-Agent → Bad Crawler? Bot?
 - Referrer → Bad Referrer? Bot?
- IP Address

What can teler detect?

- Request URI
 - URL → Directory Bruteforce
 - Parameters → Common Web Attack
- Request Headers
 - User-Agent → Bad Crawler? Bot?
 - Referrer → Bad Referrer? Bot?
- IP Address → Bad IP Address? Bot?

What can teler detect?

- Request URI
 - URL → Directory Bruteforce
 - Parameters → Common Web Attack
- Request Headers
 - User-Agent → Bad Crawler? Bot?
 - Referrer → Bad Referrer? Bot?
- IP Address → Bad IP Address? Bot?-net?

Config

Config

- Log?

Config

- Log? *Flexible!*

Config

- Log? *Flexible!*

```
:::1 - - [09/Sep/2020:05:56:48 +0700] "GET / HTTP/1.1" 200 5 "-" "curl/7.47.0"
```

=

```
$remote_addr $remote_user - [$time_local] "$request_method $request_uri  
$request_protocol" $status $body_bytes_sent "$http_referer" "$http_user_agent"
```

Config

- Log? *Flexible!*

```
:::1 - - [09/Sep/2020:05:56:48 +0700] "GET / HTTP/1.1" 200 5 "-" "curl/7.47.0"
```

=

```
$remote_addr $remote_user - [$time_local] "$request_method $request_uri  
$request_protocol" $status $body_bytes_sent "$http_referer" "$http_user_agent"
```

Config

- Whitelist?

Config

- Whitelist? *Yes!*

Config

- Whitelist? *Yes!*
 - Written in *regExp* patterns

Config

- Whitelist? Yes!
 - Written in *regExp* patterns



Config

- Cache resources

Config

- Cache resources
- Exclude threats

Config

- Cache resources
- Exclude threats
- Notification alerts

Config

- Cache resources
- Exclude threats
- Notification alerts
- Prometheus metrics

EFFICIENCY



It can go too far.

20 line-buffer/concurrently
(can be configured)

EFFICIENCY



It can go too far.

20 line-buffer/concurrently
(can be configured)

and
It has incremental log analyzer
ability as well!

Resources



Resources

- PHPIDS

Resources

- PHPIDS
- Nginx Ultimate Bad Bot Blocker

Resources

- PHPIDS
- Nginx Ultimate Bad Bot Blocker
- Crawler Detect

Resources

- PHPIDS
- Nginx Ultimate Bad Bot Blocker
- Crawler Detect
- dirsearch

Resources

- PHPIDS
- Nginx Ultimate Bad Bot Blocker
- Crawler Detect
- dirsearch
- nuclei-templates

Resources

The screenshot shows the GitHub interface for the repository 'kitabisa / teler-resources'. At the top, there are statistics for Watch (5), Star (1), and Fork (0). Below this is a navigation bar with links for Code, Issues, Pull requests, Actions, Projects, Security, and a menu icon. The main content area features a file browser for the 'master' branch, showing a commit history table and a list of files. The commit history table includes entries for 'dwwiswant0' and 'db'. The file list includes 'db', '.gitignore', 'LICENSE', and 'README.md'. The 'About' section on the right lists 'teler Resource Collections', 'Readme', and 'MIT License'. The 'Releases' section indicates 'No releases published', and the 'Packages' section indicates 'No packages published'. The 'README.md' content is partially visible at the bottom, showing the repository title 'teler Resource Collections'.

kitabisa / **teler-resources** Watch 5 Star 1 Fork 0

<> Code Issues Pull requests Actions Projects Security ...

master Go to file Code

Avatar	Commit Message	Time
	Update resources [Tue Sep 8 00:...	yesterday 36
	Update resources [Mon Sep 7 00:...	2 days ago
	Add gitignores	last month
	Initial commit	last month
	Add badge	21 days ago

db .gitignore LICENSE README.md

About
teler Resource Collections
Readme
MIT License

Releases
No releases published

Packages
No packages published

README.md

teler Resource Collections

Resources



kitabisa / **teler-resources** Watch 5 Star 1 Fork 0

[Code](#) [Issues](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [...](#)

master Go to file Code **About**

teler Resource Collections

[Readme](#)

[MIT License](#)

Releases

No releases published

Packages

No packages published

Commit History

File	Commit Message	Time
db	Update resources [Mon Sep 7 00:...	2 days ago
.gitignore	Add gitignores	last month
LICENSE	Initial commit	last month
README.md	Add badge	21 days ago

README.md

[teler Resource Collections](#)

DEMO



Thank you!

Go get it at



[kitabisa/teler](https://github.com/k Kitabisa/teler)



[kitabisa/teler:latest](https://github.com/k Kitabisa/teler:latest)

Reach me out



[dwisiswant0](https://twitter.com/dwisiswant0)



me@dw1.io

