teler - Protect Your WebApp!

Tell me, what kind of threat are you?

@dwisiswant0

Kitabisa.com

About

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

dwisiswant0

Background

TL;DR

Detection

≠

Prevention

Background

TL;DR

Background

TL;DR

Sign up

noobsec / **AntiScanScanClub-laravel**

Watch 3 | Star 21 | Fork 6

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

master | Go to file | Code

dwisiswant0 update changelog ... on Dec 25, 2019 75

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

About

A Laravel Package to Block Automated Scanners from Scanning your Site.

web | security | laravel

Readme

MIT License

Background

TL;DR

Sign up

noobsec / AntiScanScanClub-laravel

Watch 3 Star 21 Fork 6

Code Issues Pull requests Actions Projects Security ...

master Go to file Code

dwisiswant0 update changelog ... on Dec 25, 2019

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 teler 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 reg*E*xp patterns

Config

- Whitelist? *Yes!*
  - Written in reg*E*xp 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

20 line-buffer/concurrently
(can be configured)

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

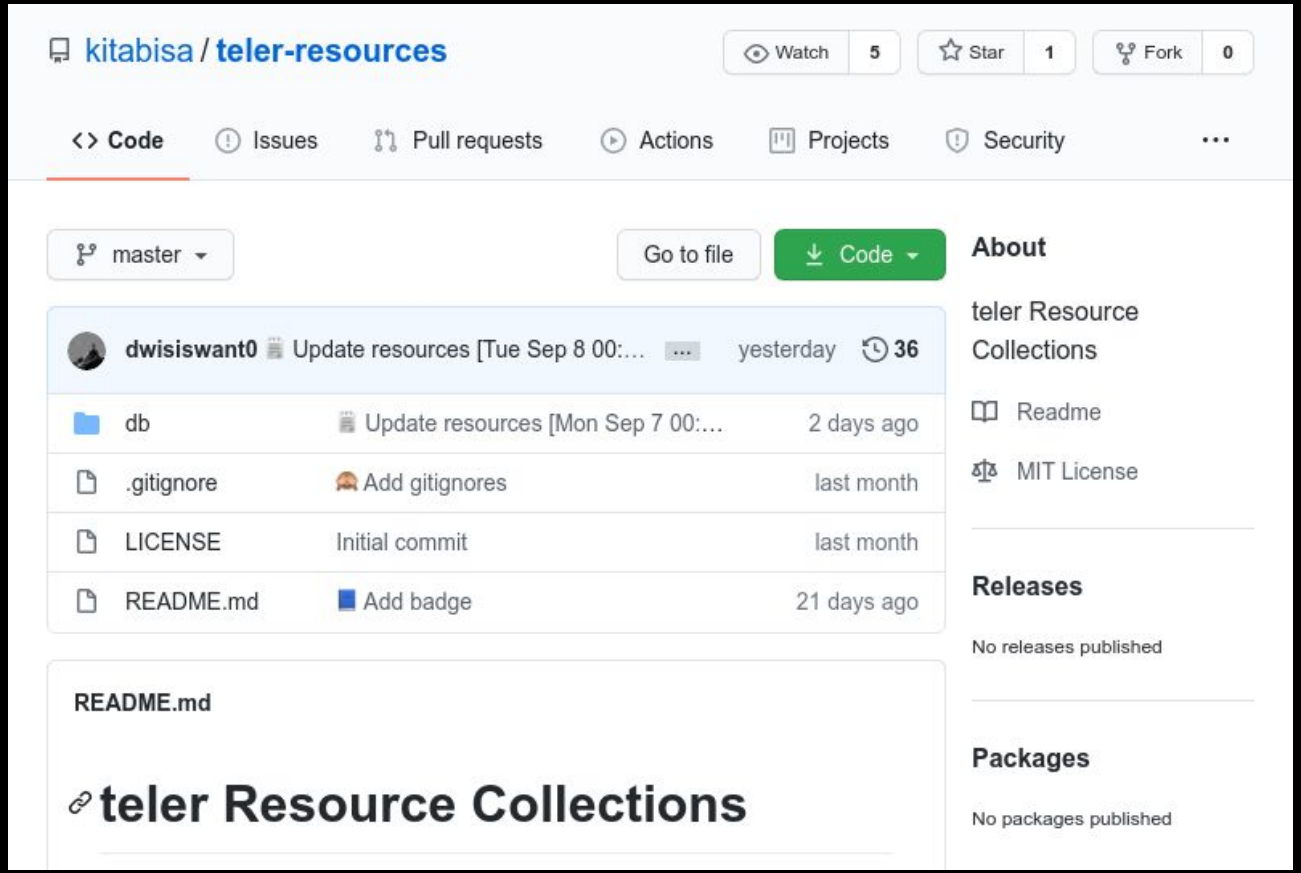
Resources

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

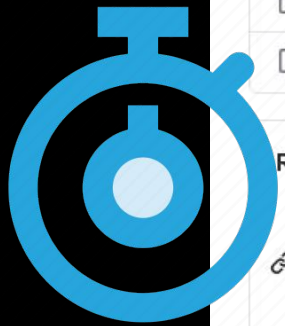
Resources

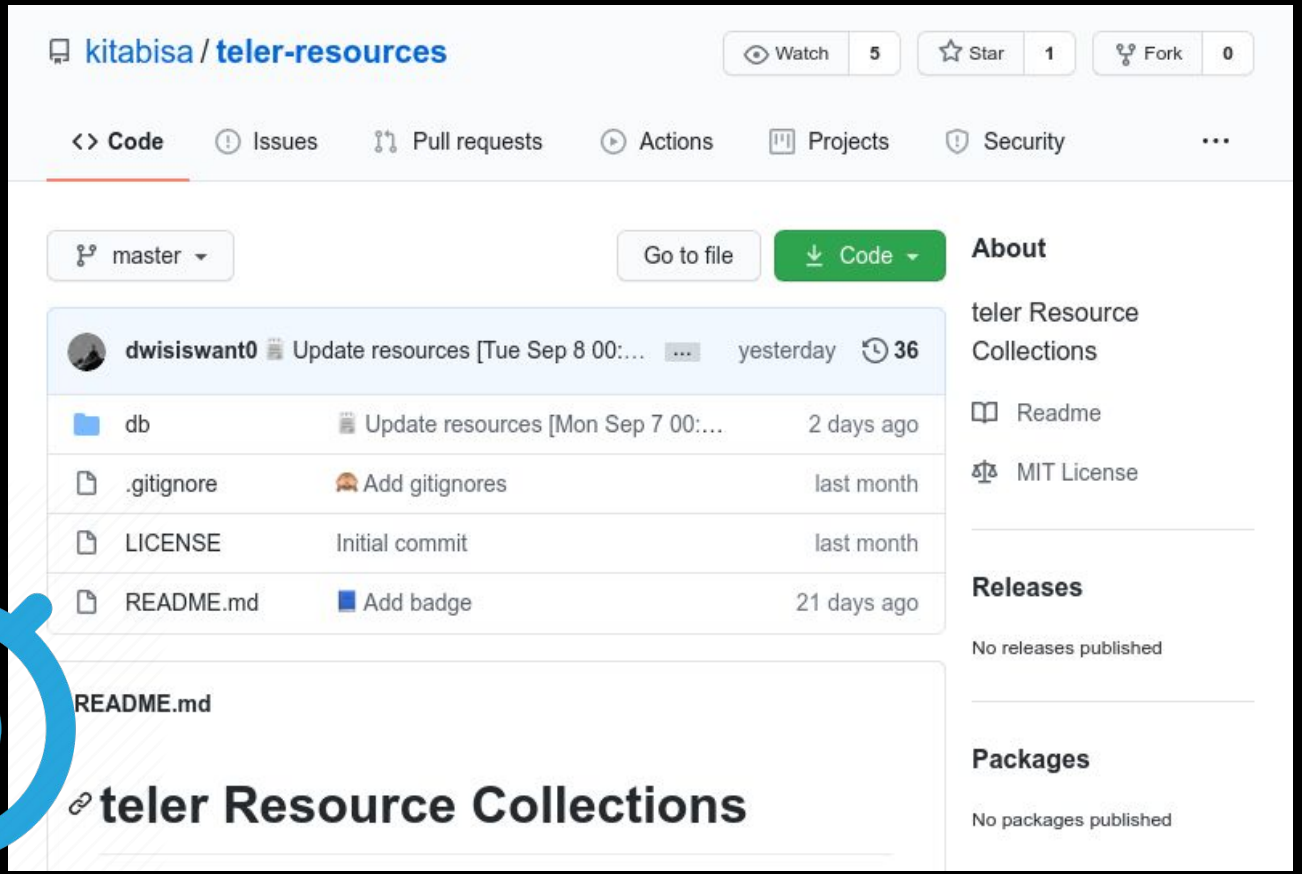
- PHPIDS
- Nginx Ultimate Bad Bot Blocker
- Crawler Detect
- dirsearch
- nuclei-templates

Resources


kitabisa / teler-resources
Watch 5
Star 1
Fork 0
Code
Issues
Pull requests
Actions
Projects
Security
master
Go to file
Code
dwisiswant0 Update resources [Tue Sep 8 00:...
yesterday
36
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
About
teler Resource Collections
Readme
MIT License
Releases
No releases published
Packages
No packages published

Resources




kitabisa / teler-resources
Watch 5
Star 1
Fork 0
Code
Issues
Pull requests
Actions
Projects
Security
master
Go to file
Code
dwisiswant0 Update resources [Tue Sep 8 00:...
yesterday
36
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
About
teler Resource Collections
Readme
MIT License
Releases
No releases published
Packages
No packages published

DEMO

Thank you!

Go get it at

kitabisa/teler

kitabisa/teler:latest

Reach me out

dwisiswant0

me@dw1.io

Kitabisa.com