# Web 문제 풀이

# 문제 컨셉

Apache UserDir + Laravel = RCE !

# Apache Userdir

http://site/~user/hi.txt

/home/user/public_html/hi.txt 로 접근이 가능!

# Laravel?

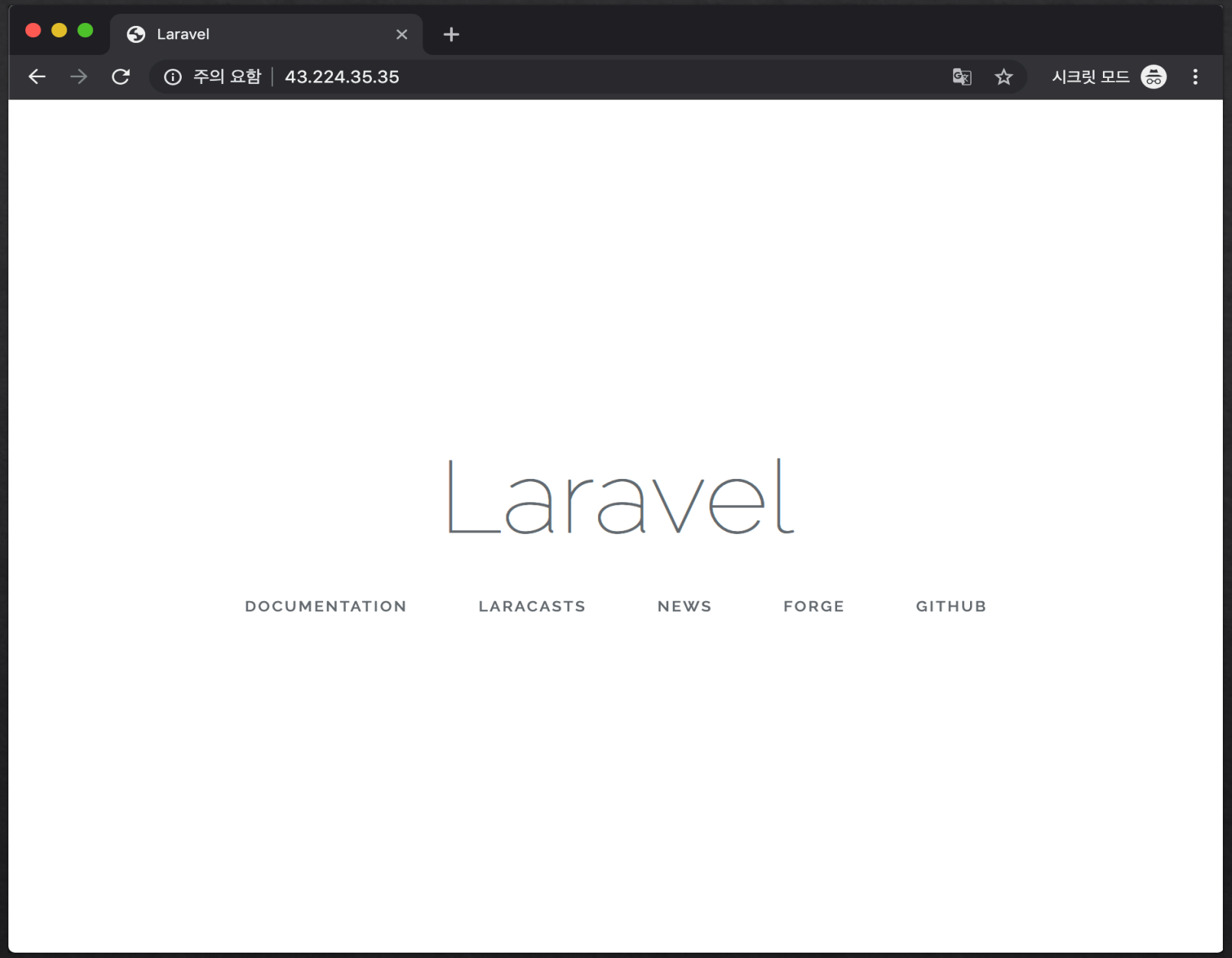
Web Framework! 좋음 추천

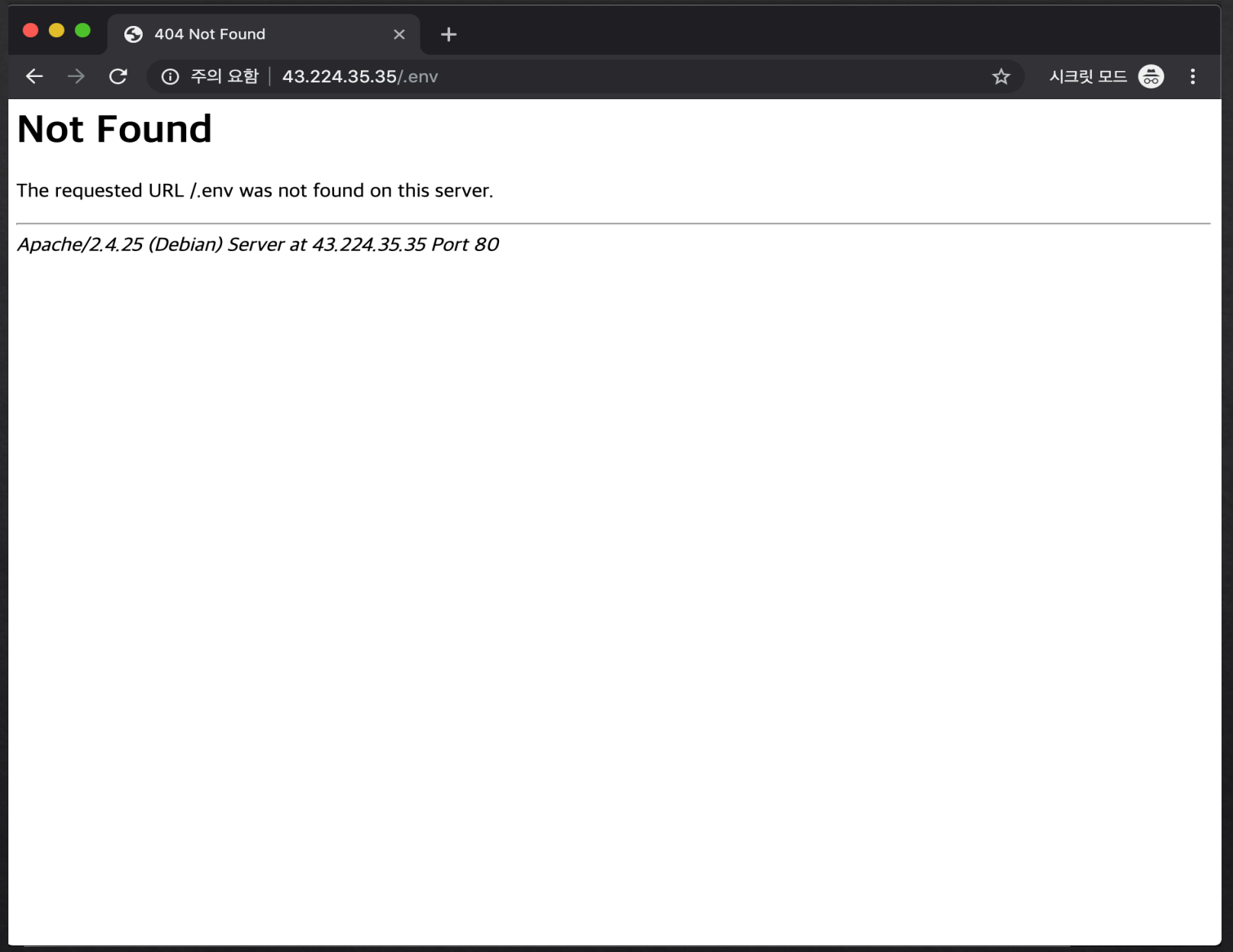
# Docker file!

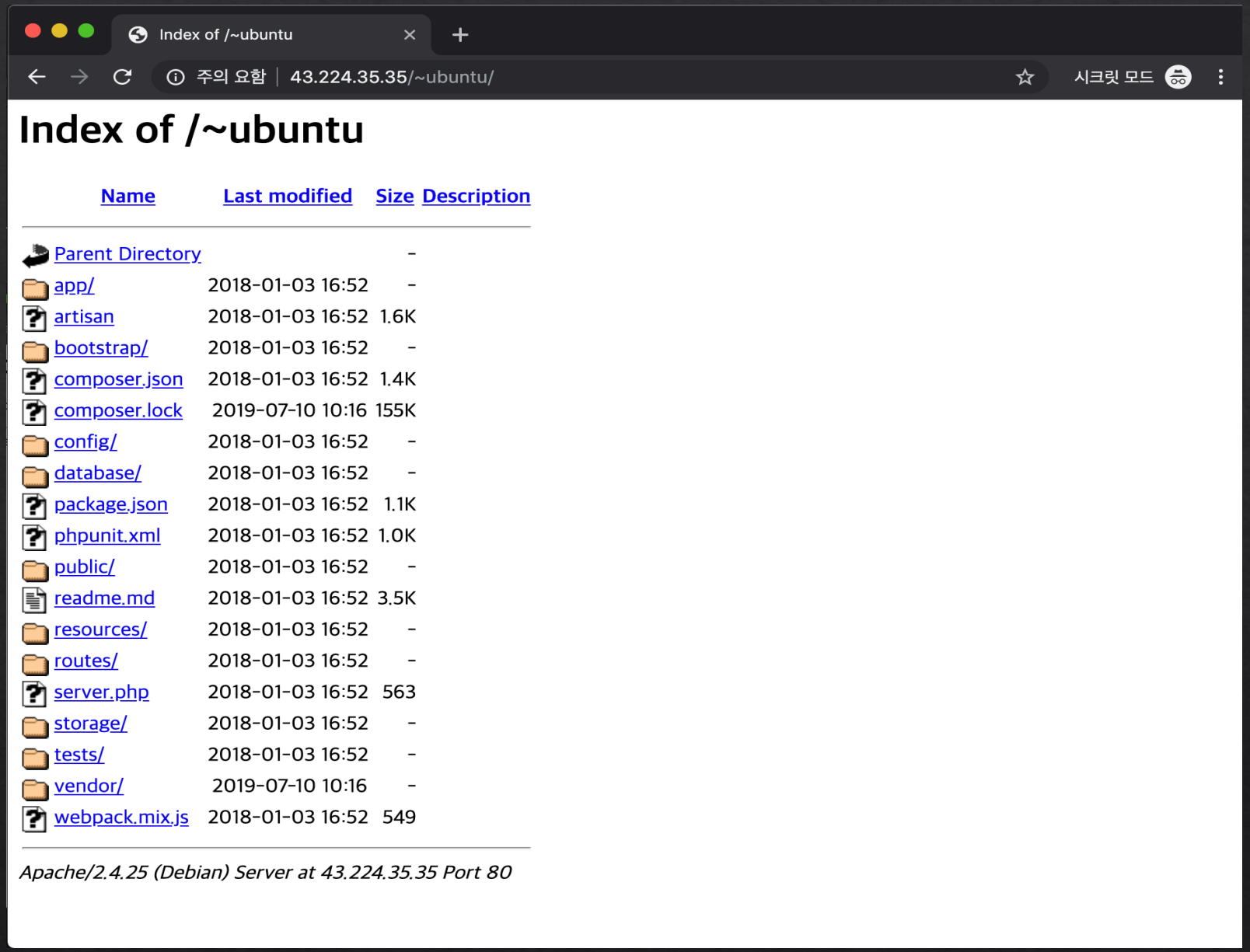
RUN apt-get update …&& a2enmod userdir

…

WORKDIR /home/ubuntu/public_html


Laravel
주의 요함 | 43.224.35.35
시크릿 모드
Laravel
DOCUMENTATION
LARACASTS
NEWS
FORGE
GITHUB

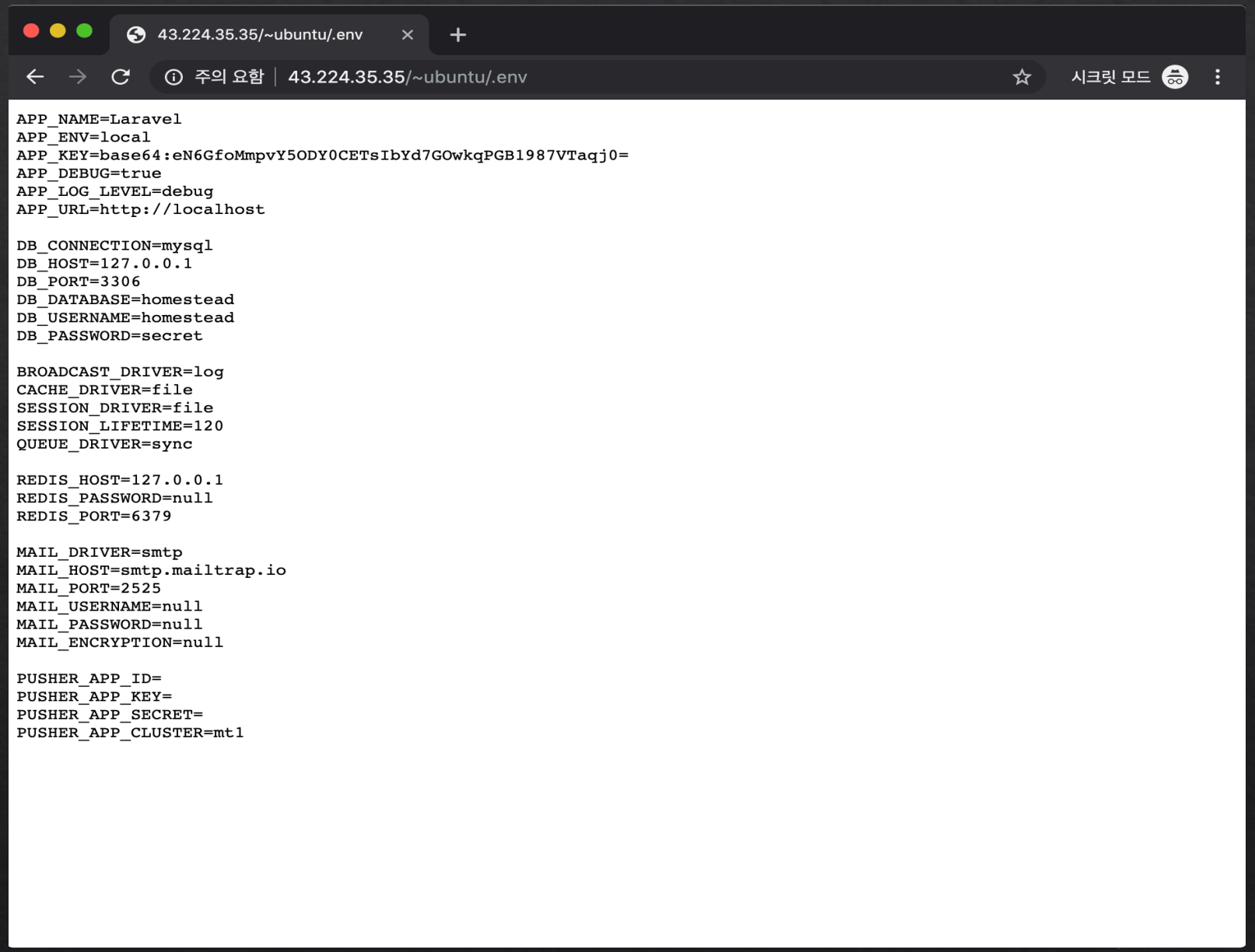

404 Not Found
주의 요함 | 43.224.35.35/.env
시크릿 모드
Not Found
The requested URL /.env was not found on this server.
Apache/2.4.25 (Debian) Server at 43.224.35.35 Port 80




# Index of /~ubuntu

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| app/ | 2018-01-03 16:52 | - | |
| artisan | 2018-01-03 16:52 | 1.6K | |
| bootstrap/ | 2018-01-03 16:52 | - | |
| composer.json | 2018-01-03 16:52 | 1.4K | |
| composer.lock | 2019-07-10 10:16 | 155K | |
| config/ | 2018-01-03 16:52 | - | |
| database/ | 2018-01-03 16:52 | - | |
| package.json | 2018-01-03 16:52 | 1.1K | |
| phpunit.xml | 2018-01-03 16:52 | 1.0K | |
| public/ | 2018-01-03 16:52 | - | |
| readme.md | 2018-01-03 16:52 | 3.5K | |
| resources/ | 2018-01-03 16:52 | - | |
| routes/ | 2018-01-03 16:52 | - | |
| server.php | 2018-01-03 16:52 | 563 | |
| storage/ | 2018-01-03 16:52 | - | |
| tests/ | 2018-01-03 16:52 | - | |
| vendor/ | 2019-07-10 10:16 | - | |
| webpack.mix.js | 2018-01-03 16:52 | 549 | |

*Apache/2.4.25 (Debian) Server at 43.224.35.35 Port 80*


43.224.35.35/~ubuntu/.env
주의 요함 | 43.224.35.35/~ubuntu/.env
시크릿 모드
APP_NAME=Laravel
APP_ENV=local
APP_KEY=base64:eN6GfoMmpvY5ODY0CETsIbYd7GOwkqPGB1987VTaqj0=
APP_DEBUG=true
APP_LOG_LEVEL=debug
APP_URL=http://localhost
DB_CONNECTION=mysql
DB_HOST=127.0.0.1
DB_PORT=3306
DB_DATABASE=homestead
DB_USERNAME=homestead
DB_PASSWORD=secret
BROADCAST_DRIVER=log
CACHE_DRIVER=file
SESSION_DRIVER=file
SESSION_LIFETIME=120
QUEUE_DRIVER=sync
REDIS_HOST=127.0.0.1
REDIS_PASSWORD=null
REDIS_PORT=6379
MAIL_DRIVER=smtp
MAIL_HOST=smtp.mailtrap.io
MAIL_PORT=2525
MAIL_USERNAME=null
MAIL_PASSWORD=null
MAIL_ENCRYPTION=null
PUSHER_APP_ID=
PUSHER_APP_KEY=
PUSHER_APP_SECRET=
PUSHER_APP_CLUSTER=mt1

# Laravel Unserialize!

https://github.com/ambionics/phpggc

Done

# Q n A

https://fb.com/adm1nkyj
adm1nkyj@gmail.com