Nginx ??

?? nginx ????

```
http {
    ##
    # Basic Settings
    ##
    server_tokens off;
...
```

???????

vi /etc/nginx/conf.d/whiteListIP.conf

```
allow 192.168.1.1;
allow 192.168.1.2;
allow 192.168.2.0/24;
deny all;
```

PHP ??

CentOS 7?/etc/php.ini
Ubuntu 16.04?/etc/php/7.0/fpm/php.ini

```
; Disallow dangerous functions
disable_functions = phpinfo, system, mail, exec

; Maximum execution time of each script, in seconds
max_execution_time = 30

; Maximum amount of time each script may spend parsing request data
max_input_time = 60

; Maximum amount of memory a script may consume (8MB)
memory_limit = 8M

; Maximum size of POST data that PHP will accept.
post_max_size = 8M

; Whether to allow HTTP file uploads.
file_uploads = Off

; Maximum allowed size for uploaded files.
upload_max_filesize = 2M

; Do not expose PHP error messages to external users
display_errors = Off
```

```
; Restrict PHP information leakage
expose_php = Off

; Log all errors
log_errors = On

; Ensure PHP redirects appropriately
cgi.force_redirect = 0

; Enable SQL safe mode
sql.safe_mode = On

; Avoid Opening remote files
allow_url_fopen = Off
```

Using fail2ban

- https://easyengine.io/tutorials/nginx/fail2ban/
- https://hostpresto.com/community/tut...n-on-centos-7/

????

- https://www.cyberciti.biz/tips/linux...-security.html
- https://www.digitalocean.com/communi...n-ubuntu-14-04
- Limiting Access to Proxied HTTP Resources
- Nginx Block And Deny IP Address OR Network Subnets
- Top 25 Nginx Web Server Best Security Practices