



Homework 4

Homework 4

❑ Secure your web server

- No Apache version
- No email showing when error occurred
 - 40x, 50x
- No PHP version

```
$ lynx -head -mime_header http://www.ubuntu.com
HTTP/1.0 200 OK
Date: Fri, 20 Nov 2009 09:25:46 GMT
Server: Apache/2.2.8 (Ubuntu) mod_python/3.3.1 Python/2.5.2 PHP/5.2.4-2ubuntu5.7 with Suhosin-Patch mod_ssl/2.2.8
X-Powered-By: PHP/5.2.4-2ubuntu5.7
Content-Type: text/html; charset=utf-8
Age: 13
Content-Length: 0
X-Cache: HIT from avocado.canonical.com
X-Cache-Lookup: HIT from avocado.canonical.com:80
Via: 1.0 avocado.canonical.com:80 (squid/2.6.STABLE18)
Connection: close
```

Homework 4 - DNS



- web2.nasa IN A <Your Server IP>
- slave.nasa IN A <Your Slave IP 1>
- slave.nasa IN A <Your Slave IP 2>
- slave.nasa IN A <Your Slave IP 3>


Remind

- Don't change any setting about homework 1
- NAP2016-WEB1.nasa
- NAP2016-DNS1.nasa
- NAP2016-DNS2.nasa

Homework 4 - Web

- ❑ http://Web2.nasa.name.idv.tw/for_ta_info.php
 - Print out phpinfo();

/for_ta_info.php  web 202 

PHP Version 7.1.1


System	FreeBSD jal.tw 10.3-RELEASE-p11 FreeBSD 10.3-RELEASE-p11 #0: Mon Oct 24 18:47:18 UTC 2016 root@amd64-builder.daemonology.net:/usr/obj/usr/src/sys/GENERIC i386
Build Date	Jan 31 2017 13:04:06
Configure Command	'./configure' '--with-layout=GNU' '--localstatedir=/var' '--with-config-file-scan-dir=/usr/local/etc/php' '--disable-all' '--enable-libxml' '--enable-mysqld' '--with-libxml-dir=/usr/local' '--with-pcre-regex=/usr/local' '--program-prefix=' '--disable-cli' '--disable-cgi' '--with-apxs2=/usr/local/sbin/apxs' '--enable-dtrace' '--prefix=/usr/local' '--mandir=/usr/local/man' '--infodir=/usr/local/info' '--build=i386-portbld-freebsd10.3' 'build_alias=i386-portbld-freebsd10.3' 'CFLAGS=-O2 -pipe -fstack-protector -fno-strict-aliasing' 'CPPFLAGS=' 'CPP=cpp'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/usr/local/etc
Loaded Configuration File	/usr/local/etc/php.ini
Scan this dir for additional .ini files	/usr/local/etc/php
Additional .ini files parsed	/usr/local/etc/php/ext-18-session.ini, /usr/local/etc/php/ext-20-json.ini, /usr/local/etc/php/ext-20-mbstring.ini, /usr/local/etc/php/ext-20-openssl.ini, /usr/local/etc/php/ext-20-simplexml.ini, /usr/local/etc/php/ext-20-xml.ini, /usr/local/etc/php/ext-20-zlib.ini
PHP API	20160303
PHP Extension	20160303
Zend Extension	320160303
Zend Extension Build	API320160303,NTS
PHP Extension Build	API20160303,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring

Show client ip

- ❑ <http://Web2.nasa.name.idv.tw/myip.php>
- ❑ No additional info and content only showing ip
 - Careful about X-Forwarded-For Confusion
 - Considering below blog, and decide which variable is correct.
 - <http://devco.re/blog/2014/06/19/client-ip-detection/>
 - Ex: <http://web2.nasa.nasa.idv.tw/myip.php>
 - Detect script will using X-Forwarded-For to confused you.

Site Protect

- ❑ `http://<Your Server IP>/`
- ❑ `http://Web2.nasa.name.idv.tw/`
 - Must be a empty page
 - Content-Length must be 0
 - Ex: <http://web2.nasa.nasa.idv.tw>
 - Ex: <http://140.131.188.41>