

NAMA SEKOLAH : SMK NEGERI 2 BANDUNG

Rabu, 15 Mei 2024

Ketua Tim :

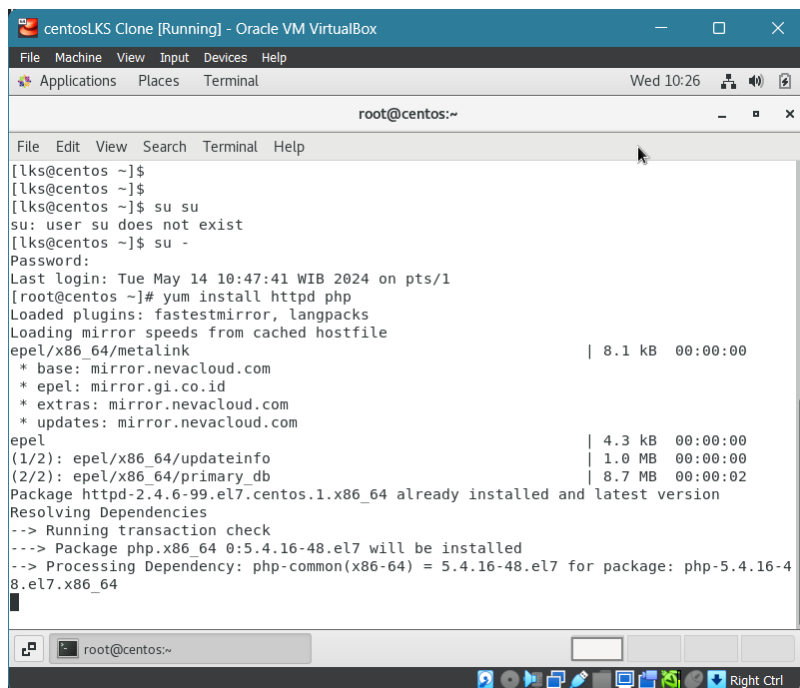
Muhammad Akhtar Khawarizmi

Anggota Tim :

Harvi Muhammad Zakhir

Analisis dan Patching Security Header Web

1. Instalasi HTTPD dan PHP



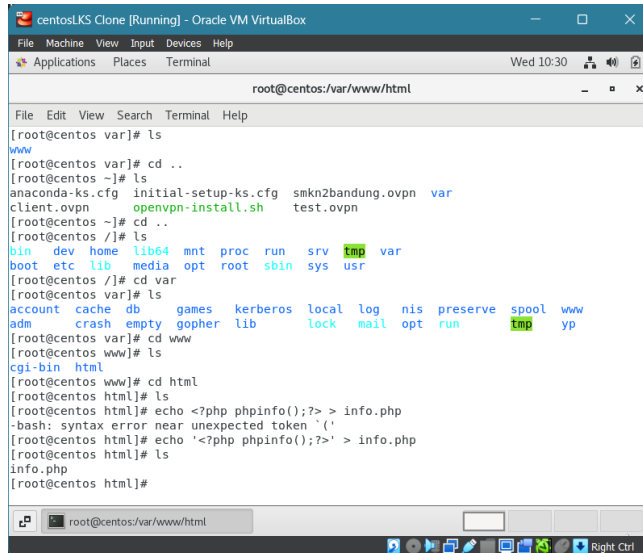
```
centosLKS Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal Wed 10:26
root@centos:~
File Edit View Search Terminal Help
[lks@centos ~]$
[lks@centos ~]$
[lks@centos ~]$ su su
su: user su does not exist
[lks@centos ~]$ su -
Password:
Last login: Tue May 14 10:47:41 WIB 2024 on pts/1
[root@centos ~]# yum install httpd php
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
epel/x86_64/metalink | 8.1 kB 00:00:00
* base: mirror.nevacloud.com
* epel: mirror.gi.co.id
* extras: mirror.nevacloud.com
* updates: mirror.nevacloud.com
epel | 4.3 kB 00:00:00
(1/2): epel/x86_64/updateinfo | 1.0 MB 00:00:00
(2/2): epel/x86_64/primary_db | 8.7 MB 00:00:02
Package httpd-2.4.6-99.el7.centos.1.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
--> Package php.x86_64 0:5.4.16-48.el7 will be installed
--> Processing Dependency: php-common(x86-64) = 5.4.16-48.el7 for package: php-5.4.16-48.el7.x86_64
```

HTTPD adalah singkatan dari "Hypertext Transfer Protocol Daemon" dan merupakan software web server yang digunakan untuk melayani konten web melalui protokol HTTP.

Sedangkan PHP merupakan bahasa pemrograman yang digunakan untuk pengembangan web, kode php berjalan di sisi server sebelum hasilnya diberikan kepada pengguna.

Pertama-tama mari kita install HTTPD dan PHP terlebih dahulu pada CentOS

2. Membuat File yang berisi phpinfo() bernama info.php



```
centosKS Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Terminal
root@centos:/var/www/html

File Edit View Search Terminal Help
[root@centos var]# ls
www
[root@centos var]# cd ..
[root@centos ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg  smkn2bandung.ovpn  var
client.ovpn      openvpn-install.sh    test.ovpn
[root@centos ~]# cd ..
[root@centos /]# ls
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib  media  opt  root  sbin  sys  usr
[root@centos /]# cd var
[root@centos var]# ls
account  cache  db  games  kerberos  local  log  nis  preserve  spool  www
adm      crash  empty  gopher  lib      lock  mail  opt  run      tmp      yp
[root@centos var]# cd www
[root@centos www]# ls
cgi-bin  html
[root@centos www]# cd html
[root@centos html]# ls
[root@centos html]# echo <?php phpinfo();?> > info.php
-bash: syntax error near unexpected token `('
[root@centos html]# echo '<?php phpinfo();?>' > info.php
[root@centos html]# ls
info.php
[root@centos html]#
```

Selanjutnya kita akan membuat file yang berisi phpinfo() di dalam folder `/var/www/html/`
phpinfo() digunakan untuk menampilkan informasi secara rinci mengenai konfigurasi php pada server.

3. Kita coba restart terlebih dahulu httpdnya setelah diinstal

```
[root@centos html]# sudo systemctl restart httpd
```

4. Selanjutnya kita coba cek Security Header pada info.php menggunakan curl -I

```
[root@centos html]# curl -I http://192.168.10.181/info.php
HTTP/1.1 200 OK
Date: Wed, 15 May 2024 03:33:08 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
X-Powered-By: PHP/5.4.16
Content-Type: text/html; charset=UTF-8
```

```
[root@centos html]#
```

curl digunakan untuk mentransfer data, kita memakai flag `-I` yang dimana akan mengirimkan request HEAD, permintaan ini hanya mengambil header respons dari server, tanpa menampilkan isi asli dari halaman website

Setelah kita mengeceknya, dapat dilihat bahwa belum ada konfigurasi Keamanan header website

5. Kita coba buka file info.php di browser



PHP Version 5.4.16	
System	Linux centos.lks 3.10.0-1160.118.1.el7.x86_64 #1 SMP Wed Apr 24 16:01:50 UTC 2024 x86_64
Build Date	Apr 1 2020 04:08:16
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/phar.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525.NTS
PHP Extension Build	API20100525.NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower,

Website sudah berhasil dideploy dan dapat diakses di web browser

6. Selanjutnya kita akan melakukan berbagai Patching pada header website, pertama-tama mari kita mulai dari header HSTS

```
[root@centos html]# sudo echo "Header always set Strict-Transport-Security \"max-age=31536000; includeSubDomains\" >> /etc/httpd/conf/httpd.conf
[root@centos html]# curl -I http://92.168.10.181/info.php
^C
```

HSTS Merupakan singkatan dari “HTTP Strict Transport Security” yang dirancang untuk melindungi pengguna dari serangan seperti Man-In-The-Middle Attack. Dengan menggunakan header ini kita dapat memaksa peramban untuk selalu menggunakan HTTPS untuk mengakses web tersebut, walaupun pengguna memasukkan url dengan skema HTTP

7. Selanjutnya kita mempatch X-Frame-Options

```
[root@centos html]# sudo echo "Header always set X-Frame-Options \"SAMEORIGIN\" >> /etc/httpd/conf/httpd.conf
[root@centos html]#
```

X-Frame-Options adalah header yang memberi tahu peramban web apakah halaman web dimuat dalam frame atau iframe. Header ini dapat berfungsi untuk melindungi situs web dari serangan clickjacking, dimana attacker menipu pengguna dengan menampilkan halaman web target di dalam frame yang disamarkan.

Nilai yang kami gunakan adalah “SAMEORIGIN”, yang berarti halaman web hanya diizinkan memuat dalam frame jika asalnya sama dengan halaman yang memuatnya/domain yang sama.

8. Lalu kita lanjut ke X-Content-Type-Options

```
[root@centos html]# sudo echo "Header always set X-Content-Type-Options \"nosniff\" >> /etc/httpd/conf/httpd.conf
[root@centos html]#
```

X-Content-Type-Options adalah header keamanan HTTP yang memberi tahu peramban web bagaimana harus menangani jenis konten (Content-Type) dari respons yang diterima dari server.

Kami menggunakan nilai “nosniff”, yang menginstruksikan peramban untuk tidak melakukan sniffing (pemeriksaan secara otomatis) terhadap jenis konten dan langsung menggunakan jenis konten yang diberikan oleh server.

9. Setelah itu kita lanjut mempatch Referrer-Policy

```
[root@centos html]# sudo echo "Header always set Referrer-Policy \"same-origin\" >> /etc/httpd/conf/httpd.conf
[root@centos html]#
```

Referrer-Policy adalah header keamanan HTTP yang mengontrol informasi yang disertakan dalam header HTTP Referer ketika pengguna mengarahkan ke tautan eksternal atau navigasi dari satu halaman web ke halaman web lainnya.

Nilai yang kami gunakan yaitu “same-origin” untuk membatasi informasi Referer hanya pada navigasi dari sumber yang sama, sehingga hanya halaman dari sumber yang sama yang dapat melihat informasi tersebut.

10. Selanjutnya kita akan mempatch Permission Policy

```
[root@centos html]# sudo echo "Header always set Permissions-Policy \"accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()\" >> /etc/httpd/conf/httpd.conf
[root@centos html]#
```

Permission-Policy memberikan kontrol terhadap izin akses ke fitur API browser yang sensitif. Header ini digunakan untuk menentukan kebijakan izin yang diberikan oleh peramban kepada situs web untuk mengakses sensor perangkat (seperti accelerometer, kamera, geolokasi), perangkat keras (seperti mikrofon, USB), dan fitur lainnya.

11. Yang Terakhir kita akan mempatch Content-Security-Policy (CSP)

```
[root@centos html]# sudo echo "Header always set Content-Security-Policy \"default-src 'self'; script-src 'self' https://cdn.example.com; style-src 'self' https://fonts.googleapis.com; img-src 'self' https://example.com\" >> /etc/httpd/conf/httpd.conf
[root@centos html]#
```

Content-Security-Policy digunakan untuk mengontrol sumber mana yang diizinkan untuk dimuat dalam halaman web. Ini membantu melindungi situs web dari serangan XSS (Cross-Site Scripting) dengan cara membatasi sumber-sumber yang diizinkan untuk skrip, gambar, CSS, dan objek lainnya yang dimuat dalam halaman.

Pada command diatas kami menggunakan nilai “self” pada “default-src”, “script-src”, “style-src”, “img-src” sehingga hanya mengizinkan penggunaan file dari situs itu sendiri atau domain.

12. Setelah selesai mempatching header website, mari kita restart terlebih dahulu httpdnya

```
[root@centos html]# sudo systemctl restart httpd
```

Restart seringkali diperlukan agar perubahan yang dibuat dapat mulai diterapkan.

13. Untuk Mengecek hasil dari patching yang telah kita lakukan, mari kita cek lagi

menggunakan curl -I http://<ip>/info.php

```
[root@centos html]# curl -I http://192.168.10.181/info.php
HTTP/1.1 200 OK
Date: Wed, 15 May 2024 03:42:51 GMT
Server: Apache/2.4.6 (CentOS) PHP/5.4.16
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Permissions-Policy: accelerometer=(), camera=(), geolocation=(), gyroscope=(), magnetometer=(), microphone=(), payment=(), usb=()
Content-Security-Policy: default-src 'self'; script-src 'self' https://cdn.example.com; style-src 'self' https://fonts.googleapis.com; img-src 'self' https://example.com
X-Powered-By: PHP/5.4.16
Content-Type: text/html; charset=UTF-8
```

Dan hasilnya kita berhasil menambahkan HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy, dan Content-Seeurity-Policy pada header website.