A brief introduction to PHP and HTTPS in Apache

A practical approach in arch linux

Prof. Rossano Pablo Pinto
2017 - v0.9.2
Agenda

- Introduction
- Installation
- HTTP 1.1 protocol inspection
- Apache configuration – Arch Linux
  - PHP
  - HTTPS
- Tests
Introduction

- **WEB servers**
  - Usually listens on port 80 (HTTP well-known-port)
  - Uses HTTP protocol
  - CLIENT/SERVER model
Installation

- pacman -S apache
- systemctl start httpd
- systemctl status httpd
  - Observe that it shows **disabled**. So enable it for this target:
- systemctl enable httpd.service
HTTP protocol Inspection

• Access some web server:

telnet hypnos 80

Trying 192.168.200.52...

Connected to hypnos.fatec.br.

Escape character is '^[].'

GET / HTTP/1.1

Host: hypnos

2 Enters

Resposta no próximo slide...
HTTP protocol Inspection

HTTP/1.1 200 OK

Date: Tue, 20 Nov 2012 17:28:06 GMT

Server: Apache/2.2.3 (CentOS)

Last-Modified: Wed, 15 Aug 2012 00:19:52 GMT

ETag: "1ed17b-547-e2b31a00"

Accept-Ranges: bytes

Content-Length: 1351

Content-Type: text/html; charset=ISO-8859-1

<HTML>

<HEAD>

</HEAD>
HTTP protocol Inspection

• “Emulate” a web server:
  • Run http-dump program:

    scp aluno@MAQUINA-DO-PROFESSOR:http-dump .

    Example: scp aluno@192.168.80.45:/tmp/http-dump .

    ./http-dump 9999

• Open firefox and type the following URL:

    http://localhost:9999/
HTTP protocol Inspection

- Observe the http-dump output:

Message received:

GET / HTTP/1.1
Host: localhost:9999
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:15.0) Gecko/20100101 Firefox/15.0.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: org.cups.sid=04e22f9a096c8e9570427c2feb7a56f
Directories and files

- `/srv/http/` → document root
- `/etc/httpd/` → config directory
- `/etc/httpd/conf/httpd.conf` → main configuration file
- `/usr/lib/systemd/system/httpd.service` → httpd systemd unit
Initial test

- echo '<html>Hi</html>' > /srv/http/index.html

- links http://localhost
Apache configuration
A brief overview of file httpd.conf

- **ServerRoot "/usr"** -> install base dir (modules) - used when path names don't start with "/". (See path examples with LoadModule)
- **PidFile run/httpd.pid** -> /var/run/httpd.pid (file that keeps the apache pid)
- **Timeout 300** -> timeout in seconds for idle connections to be terminated
- **KeepAlive On** -> allow HTTP/1.1 to use it's ability to make several requests using a single connection
- **MaxKeepAliveRequests 100** -> maximum number of requests using a single connection
- **KeepAliveTimeout 15** -> timeout in seconds for idle connections to be terminated
- **Listen 80** -> server port to listen to connections
Apache configuration
A brief overview of file httpd.conf

- Include file -> include other configuration files
- LoadModule -> load a module
- User apache -> User owner of the apache process
- Group apache -> Group owner of the apache process
- DocumentRoot "/srv/http" -> directory to host resources (htmls, image files, etc..) to be returned to requesters
- DirectoryIndex index.html index.html.var -> default file to be returned when asked for a resource using only a dir name
- AccessFileName .htaccess -> per directory configuration - useful for authentication (but not so secure nowadays)
Apache useful commands

- `httpd -t` - verify configuration files syntax
- `httpd -S` - test VirtualHost configuration
- `apachectl stop`
- `apachectl start`
- `apachectl restart`
- `httpd -l` - list available modules at server
- `httpd -M` - list loaded modules
- `httpd -L` - list directives and affected modules
PHP - Installing

- `pacman -S php-apache`
PHP - Enabling

- `nano /etc/httpd/conf/httpd.conf`

  ```
  #LoadModule mpm_event_module modules/mod_mpm_event.so
  LoadModule mpm_prefork_module modules/mod_mpm_prefork.so
  LoadModule php7_module modules/libphp7.so
  ...
  DirectoryIndex index.html index.php
  ...
  Include conf/extra/php7_module.conf
  ```

- `systemctl restart httpd.service`


- Test: links http://localhost/info.php
HTTPS

- URL starting with “https://” uses SSL (Secure Sockets Layer) to secure communication between CLIENT and SERVER
- SSL runs in a separate layer under HTTP
- SSL is now known as TLS (Transport Layer Security) - BUT IT'S STILL POPULAR KNOWN AS SSL
  - SSL 1.0 → SSL 2.0 → SSL 3.0 → TLS 1.0 → TLS 1.1 → TLS 1.2 → TLS 1.3 (draft)
HTTPS

• Steps to use SSL + HTTP:

1. Site owner generates PUBLIC and PRIVATE keys
2. Site owner generates a Certificate Signing Request (CSR) - Contains PUBLIC KEY + COMPANY NAME
3. Site owner sends the CSR to a Certificate Authority (CA) in order to be SIGNED
4. CA returns a SIGNED CERTIFICATE which contains:
   • site PUBLIC KEY
   • site COMPANY NAME
   • CA “signature”
HTTPS

- Steps to use SSL + HTTP:
  - Real example at wiki.locaweb.com.br/pt-br/SSL
HTTPS

1) Generate private key using RSA parameters:

```
openssl genrsa -out ca.key 2048
```

2) Generate CSR (Certificate Signing Request)

```
openssl req -new -key ca.key -out ca.csr
```

3) Generate x509 Self Signed Certificate (valid for 365 days)

```
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
```

This step emulates a Certificate Authority (CA)
HTTPS

4) Copy files to locations described in extra/httpd-ssl.conf (next slide):

    cp ca.crt /etc/httpd/conf/server.crt
    cp ca.key /etc/httpd/conf/server.key

5) nano /etc/httpd/conf/httpd.conf: find and load the following modules:

    ssl_module # SSL MODULE. Modules are used by SSL:
    log_config_module # Flexible logging of clients
    setenvif_module # Set internal environment variable
    socache_shmcb_module # Shared object cache provider

(According to “Required modules:” in extra/httpd-ssl.conf)
HTTPS

6) Edit httpd.conf: uncomment line:
Include conf/extra/httpd-ssl.conf

7) Restart apache
systemctl restart httpd.service

8) Test: open a browser and type the url:
links https://localhost

More details:
www.openssl.org/docs/apps/x509.html, httpd.apache.org/docs/current/mod/{mod_log_config.html, mod_socache_shmcb.html, mod_setenvif_module, mod_ssl.html}
HTTPS

- Viewing certificates at Firefox version 44.0.2
  - Type at the URL field: `about:preferences#advanced`
    - View Certificates (Tab Servers or Authorities)
      - Authorities
        - Select some certificate and click “View”
        - Select some certificate and click “Export” (use this file at the examples below - replace server.crt with the file you saved at this step)

- Viewing keys with openssl
  - `openssl rsa -in server.key -noout -text`

- Viewing certificates with openssl
  - `openssl x509 -in server.crt -noout -text`
HTTPS

• Calculating public key associated with a private key
  • openssl rsa -in server.key -pubout

• Saving public key associated with a private key
  • openssl rsa -in server.key -pubout -out server.pub.key
HTTPS only

- Previous configuration still allows http (port 80) connection
- To disable non-ssl connection comment line "Listen 80" on file httpd.conf