

Curso Apache Security

Descripción General

Objetivo

Duración

20 horas

Requisitos

Conocimientos básicos de Linux

www.cursoslinux.com.mx

ventas@plct.com.mx

PLCT S.A. de C.V.

Tel.: 55 4522 7839/55 1800 7696/7224447684

1. SSL/TLS Strong Encryption: An Introduction

1.1 Cryptographic Techniques

1.2 Certificates

1.3 Secure Sockets Layer (SSL)

1.4 Establishing a Session

1.5 Key Exchange Method

1.6 Cipher for Data Transfer

1.7 Digest Function

1.8 Handshake Sequence Protocol

1.9 Data Transfer

1.10 Securing HTTP Communication

2. SSL/TLS Strong Encryption: Compatibility

2.1 Configuration Directives

2.2 Environment Variables

2.3 Custom Log Functions

3. SSL/TLSStrongEncryption:How-To

3.1 Cipher Suites and Enforcing Strong Security

3.2 Client Authentication and Access Control

4. SSL/TLSStrongEncryption:FAQ

4.1 About The Module

4.2 Installation

4.3 Configuration

4.4 Certificates

4.5 The SSL Protocol

4.6 mod_ssl Support

5. Authentication, Authorization and Access Control

5.1 Related Modules and Directives

5.2 Introduction

5.3 The Prerequisites

5.4 Getting it working

5.5 Letting more than one person in

5.6 Possible problems

5.7 Alternate password storage

5.8 More information

6. Apache Tutorial: Dynamic Content with CGI

6.1 Introduction

www.cursoslinux.com.mx

ventas@plct.com.mx

PLCT S.A. de C.V.

Tel.: 55 4522 7839/55 1800 7696/7224447684

6.2 Configuring Apache to permit CGI

6.3 Writing a CGI program

6.4 But it's still not working!

6.5 What's going on behind the scenes?

6.6 CGI modules/libraries

7. Apache Tutorial: Introduction to Server Side Includes

7.1 Introduction

7.2 What are SSI?

7.3 Configuring your server to permit SSI

7.4 Basic SSI directives

7.5 Additional examples

7.6 What else can I config?

7.7 Executing commands

7.8 Advanced SSI techniques

7.9 Conclusion

8. Apache Tutorial: .htaccess files

8.1 .htaccess files

8.2 What they are/How to use them

8.3 When (not) to use .htaccess files

8.4 How directives are applied

8.5 Authentication example

8.6 Server Side Includes example

8.7 CGI example

8.8 Troubleshooting

9. Per-user web directories

9.1 Per-user web directories

9.2 Setting the file path with UserDir

9.3 Redirecting to external URLs

9.4 Restricting what users are permitted to use this feature

9.5 Enabling a cgi directory for each user

9.6 Allowing users to alter configuration

10. AccessControl

10.1 Related Modules and Directives

10.2 Access control by host

10.3 Access control by environment variable

10.4 Access control with mod_rewrite

10.5 More information

11. Server and Supporting Programs

11.1 httpd - Apache Hypertext Transfer Protocol Server

11.2 ab - Apache HTTP server benchmarking tool

www.cursoslinux.com.mx

ventas@plct.com.mx

PLCT S.A. de C.V.

Tel.: 55 4522 7839/55 1800 7696/7224447684

11.3 apachectl - Apache HTTP Server Control Interface
11.4 apxs - APache eXtenSion tool
11.3 apachectl - Apache HTTP Server Control Interface
11.4 apxs - APache eXtenSion tool
11.5 configure - Configure the source tree
11.6 dbmmanage - Manage user authentication files in DBM format
11.7 htcacheclean - Clean up the disk cache
11.8 htdbm - Manipulate DBM password databases
11.9 htdigest - manage user files for digest authentication
11.10 htpasswd - Manage user files for basic authentication
11.11 httxt2dbm - Generate dbm files for use with RewriteMap
11.12 logresolve - Resolve IP-addresses to hostnames in Apache log files

11.13 rotatelog - Piped logging program to rotate Apache logs
11.14 suexec - Switch user before executing external programs
11.15 log_server_status
11.16 split-logfile
12. RelevantStandards
12.1 HTTP Recommendations
12.2 HTML Recommendations
12.3 Authentication
12.4 Language/Country Codes
13. PasswordFormats
13.1 Basic Authentication
13.2 Digest Authentication