METASPLOITABLE

CAJA NEGRA

CRITICAS No INTER4ESANTES:

# La vulnerabilidades criticas detectadas en modo ejecutivo, ninguna afecta a la maquina ya que, éstas se refieren a puertas traseras y ejecucon de código malicioso en versiones PHP < 5.4.43, asi como al servicio Ftp anonimo y al programa IRCdemoin y phpMyAdmin.

# La Maquina de estudio presenta instalada la versión 5-4.5 PHP, por lo que no se vería afectada por esta vulnerabilidad, únicamente encontrando una dependencia etiquetada como low por exitir relación con el servicio “Get request” que puede ser usado para ejecutar esta vulnerabilidad.

# HIGH NO INTERESANTES

# 1.- Drupal Database Abstraction API SQLi

# No tiene instalada la maquina la aplicación Drupal que es la afectada por ella

# 2.-

**HIGH 9.3\* - 67260 PHP 5.4.x < 5.4.17 Buffer Overflow**

**HIGH 7.5\* 6.7 71427 PHP 5.4.x < 5.4.23 OpenSSL openssl\_x509\_parse() Memory Corruption**

**HIGH 7.2\* 6.7 73862 PHP 5.4.x < 5.4.28 FPM Unix Socket Insecure Permission Escalation**

**HIGH 7.5\* 5.9 76281 PHP 5.4.x < 5.4.30 Multiple Vulnerabilities**

**HIGH 7.5\* 6.7 78545 PHP 5.4.x < 5.4.34 Multiple Vulnerabilities**

# HIGH 7.5\* 6.6 80330 PHP 5.4.x < 5.4.36 'process\_nested\_data' RCE

# )HIGH 7.3 5.9 66585 PHP 5.4.x < 5.4.13 Information Disclosure

# HIGH 7.3 5.9 69401 PHP 5.4.x < 5.4.19 Multiple Vulnerabilities

# HIGH 7.3 6.7 81080 PHP 5.4.x < 5.4.37 Multiple Vulnerabilities

# HIGH 7.3 3.6 85298 PHP 5.4.x < 5.4.44 Multiple Vulnerabilities

# HIGH 7.3 6.7 85885 PHP 5.4.x < 5.4.45 Multiple Vulnerabilities

# Todas estas no les afecta a la maquina ya que como hemos dicho tiene la versión 5.4.5 de pHP

# 3.- SSL Medium Strength Cipher Suites Supported (SWEET32):

# Esta vuelnabilidad afecta a cualquier cifrado que utilice longitudes de claves de al menos 64 bits y menos de 112 bits, o bien que utilice la suite de cifrado 3DES.

# La maquina analizada uno de los cifrados que soporta es el “3des-cbc”, pero analizados las medidas e los cifrados que utiliza sus servicios no tiene ninguno entre 64 a 112bits , además tiene puerto 443 cerrado.

# HIGH INTERESANTES: