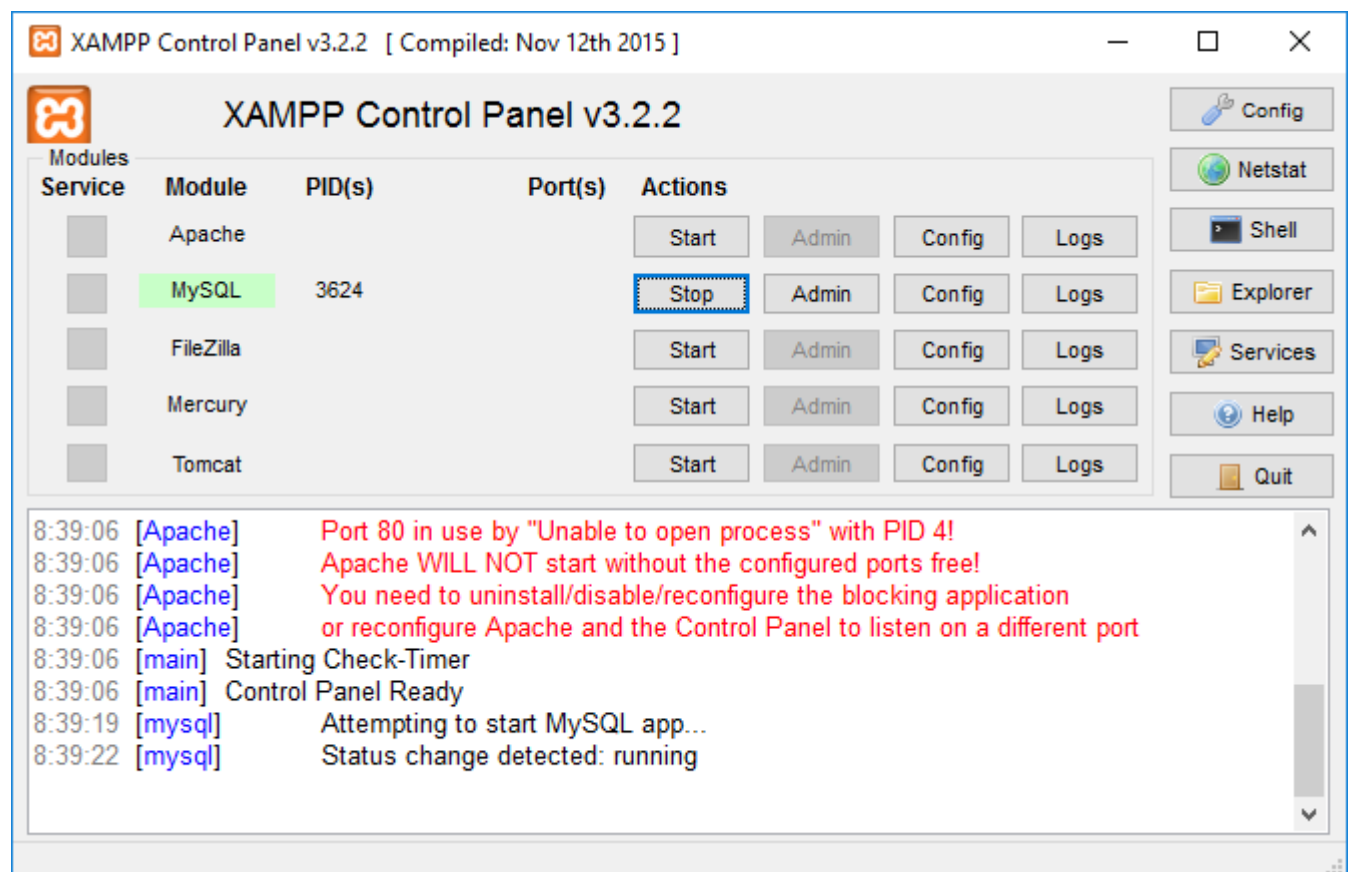


Crear un fichero HTML con el contenido de la tabla posts de WordPress con PowerShell

Antes de ejecutar el código en PowerShell es necesario arrancar MySQL



Comprobar la base de datos a la que nos vamos a conectar

Unnamed\jesusninoc\ - HeidiSQL Portable 9.4.0.5125

Archivo Editar Buscar Herramientas Ira Ayuda

Donar al proyecto HeidiSQL

Filtro de bases de datos Filtro de tablas

Host: 127.0.0.1 Base de datos: jesusninoc Consulta

Nombre	Filas	Tamaño	Creado	Actualizado	Motor	Comentario
wp_404_to_301	0	1,0 KiB	2017-09-05 08:42:57	2017-09-05 08:42:57	MyISAM	
wp_alm	1	2,4 KiB	2017-09-05 08:42:57	2017-09-05 08:42:57	MyISAM	
wp_blc_filters	0	1,0 KiB	2017-09-05 08:42:57	2017-09-05 08:42:57	MyISAM	
wp_blc_instances	2.840	690,6 KiB	2017-09-05 08:42:58	2017-09-05 08:42:58	MyISAM	
wp_blc_links	1.750	2,7 MiB	2017-09-05 08:42:58	2017-09-05 08:42:59	MyISAM	
wp_blc_synch	1.901	80,1 KiB	2017-09-05 08:42:59	2017-09-05 08:42:59	MyISAM	
wp_commentmeta	0	48,0 KiB	2017-09-05 08:42:59		InnoDB	
wp_comments	0	96,0 KiB	2017-09-05 08:43:00		InnoDB	
wp_links	0	32,0 KiB	2017-09-05 08:43:01		InnoDB	
wp_options	2.492	1,8 MiB	2017-09-05 08:43:01		InnoDB	
wp_postmeta	15.279	4,5 MiB	2017-09-05 08:43:04		InnoDB	
wp_posts	2.738	5,2 MiB	2017-09-05 08:43:08		InnoDB	
wp_termmeta	0	4,0 KiB	2017-09-05 08:43:20	2017-09-05 08:43:20	MyISAM	
wp_terms	1.852	304,0 KiB	2017-09-05 08:43:21		InnoDB	
wp_term_relationships	71.708	7,0 MiB	2017-09-05 08:43:12		InnoDB	

```

6 /* Juego de caracteres: utf8mb4 */
7 SHOW STATUS;
8 SHOW VARIABLES;
9 SHOW DATABASES;
10 USE `jesusninoc`;
11 /* Entrando a la sesión "Unnamed" */
12 SELECT `DEFAULT_COLLATION_NAME` FROM `information_schema`.`SCHEMATA` WHERE `SCHEMA_NAME`='jesusninoc';
13 SHOW TABLE STATUS FROM `jesusninoc`;
14 SHOW FUNCTION STATUS WHERE `Db`='jesusninoc';
15 SHOW PROCEDURE STATUS WHERE `Db`='jesusninoc';
16 SHOW TRIGGERS FROM `jesusninoc`;
17 SELECT `DEFAULT_COLLATION_NAME` FROM `information_schema`.`SCHEMATA` WHERE `SCHEMA_NAME`='information_schema';
18 SHOW TABLE STATUS FROM `information_schema`;
19 SHOW FUNCTION STATUS WHERE `Db`='information_schema';
20 SHOW PROCEDURE STATUS WHERE `Db`='information_schema';
21 SHOW TRIGGERS FROM `information_schema`;
22 SHOW EVENTS FROM `information_schema`;
23 SELECT *, EVENT_SCHEMA AS `Db`, EVENT_NAME AS `Name` FROM information_schema.`EVENTS` WHERE `EVENT_SCHEMA`='jesusninoc';

```

jesusninoc: 20 tables

Conectado: 00:00 h MariaDB 10.1.19 Activo durante: 00:01 h UTC: 2017-09-07 6:41 Preparado.

Ejecutar el código para crear el HTML con los datos de la base de datos

[crayon-6a9d868d51f9d401916637/]



Acceso al cmd.exe medio: X

file:///C:/Users/juan/output.html

Acceso al cmd.exe mediante vulnerabilidad LFI

Se intenta en diferentes subcarpetas:

```

/scripts/.../winnt/system32/cmd.exe
/msadc/.../winnt/system32/cmd.exe
/_vti_bin/.../winnt/system32/cmd.exe

```

Detectado en la consulta:

```

SELECT [cs-uri-stem], COUNT(*) AS EXPRI
FROM tabla
where [cs-uri-stem] like '%?%'
GROUP BY [cs-uri-stem]
ORDER BY 2 desc

```

Bloquear el ataque utilizando la IP de origen o la cadena de entrada '..??.'