Online CTF idsecconf Walkthrough

Ahmad Maulana <hmadrwx@gmail.com>

CTF?

CTF IDSECCONF atau *Capture The Flag* adalah salah satu permainan simulasi hacking yang diadakan tiap tahun berbarengan dengan diadakannya kegiatan IDSECCONF.

CTF ini dilakukan secara online, siapapun bisa menjadi pesertanya dengan cukup melakukan registrasi via web.

Untuk CTF online tahun 2012 beralamat di http://ctf.2012.idsecconf.org dikuti oleh lebih kurang 250 peserta yang valid (divalidasi via email) dan dilaksanakan selama 11 Hari (26 April 2012 - 6 Mei 2012) dengan jumlah level (*challenge*) sebanyak 8 buah (meliputi *4 level application reverse engineering, 2 level network analysis and hacking, 2 level web hacking*).

ctf.2012.idsecconf.org [redacted]

LEVEL

1 - Reverse Engineering #1

2 - Reverse Engineering #2

3 - Reverse Engineering #3

4 - Reverse Engineering #4

5 - Packet Network Analysis #1

6 - Web Application Hacking #1

7 - Packet Network Analysis #2

8 - Web Application Hacking #2

IDSECCONF Indonesian Security Conference 2012

Level 1 – Simple Reverse Engineering

Level 1 : Simple Reverse Engineering

Enter the Key :

Your Filename : level1_442740844946736

Submit

Find the key Here

Level 1 – Simple Reverse Engineering

```
@ctf2%
@ctf2%ls -la level1_866532021194308
ls -la level1_866532021194308
-r-xr-x--- 1 level1 level1 6693 May  7 17:03 level1_866532021194308
@ctf2%
@ctf2%strings level1_866532021194308
strings level1_866532021194308
/lib/ld-linux.so.2
__gmon_start__
libc.so.6
_IO_stdin_used
printf
scanf
__libc_start_main
GLIBC_2.0
PTRhP
[^_]
1112996984
level1_866532021194308
Enter Password :
Your Key is : vitDep2K9t
Permission Denied
@ctf2%
```

Level 2 – Simple Reverse Engineering

Level 2 : Simple Reverse Engineering

Enter the Key :

Your Filename : level2_908625534903849

Submit

Find the key Here

Level 2 – Simple Reverse Engineering

```
@ctf2%
@ctf2%strings level2_908625534903849
strings level2_908625534903849
/lib/ld-linux.so.2
__gmon_start__
libc.so.6
_IO_stdin_used
printf
scanf
__libc_start_main
__xstat
GLIBC_2.0
PTRh
QVh`
[^_]
Your Key is : %i
Access Denied
985156509
level2_908625534903849
Enter Password :
/tmp/949715574066345
Permission Denied
@ctf2%
```

Level 2 – Simple Reverse Engineering

```
@ctf2%
@ctf2%echo "" > /tmp/949715574066345
echo "" > /tmp/949715574066345
@ctf2%
@ctf2%./level2_908625534903849
./level2_908625534903849
Enter Password :985156509
985156509

Your Key is : 616 @ctf2%
@ctf2%
```

Level 3 – Medium Reverse Engineering

Level 3 : Medium Reverse Engineering

Enter the Key :

Your Filename : level3_1101829990745967

Submit

Find the key Here

Level 3 – Medium Reverse Engineering

```
@ctf2%strings level3_1101829990745967
strings level3_1101829990745967
/lib/ld-linux.so.2
__gmon_start__
libc.so.6
_IO_stdin_used
printf
scanf
__libc_start_main
__xstat
GLIBC_2.0
PTRh
QVh`
[^_]
Your Key is : %i
Access Denied
Enter Password :
/tmp/50350562019559
Permission Denied
@ctf2%
@ctf2%
```

Level 3 – Medium Reverse Engineering

```
1  Dump of assembler code for function main:
2  0x08048460 <main+0>: lea 0x4(%esp),%ecx
3  0x08048464 <main+4>: and $0xfffffff0,%esp
4  0x08048467 <main+7>: pushl -0x4(%ecx)
5  0x0804846a <main+10>: push %ebp
6  0x0804846b <main+11>: mov %esp,%ebp
7  0x0804846d <main+13>: push %ecx
8  0x0804846e <main+14>: sub $0x24,%esp
9  0x08048471 <main+17>: movl $0x79017dd,-0x8(%ebp)
10 0x08048478 <main+24>: movl $0x80485f2,(%esp)        > "Enter Password :"
11 0x0804847f <main+31>: call 0x8048340 <printf@plt>
12 0x08048484 <main+36>: lea -0xc(%ebp),%eax
13 0x08048487 <main+39>: mov %eax,0x4(%esp)
14 0x0804848b <main+43>: movl $0x8048603,(%esp)        > "%d"
15 0x08048492 <main+50>: call 0x8048330 <scanf@plt>
16 0x08048497 <main+55>: mov -0xc(%ebp),%eax
17 0x0804849a <main+58>: cmp -0x8(%ebp),%eax
18 0x0804849d <main+61>: jne 0x80484ad <main+77>
19 0x0804849f <main+63>: movl $0x8048606,(%esp)        > "/tmp/503505620195559"
20 0x080484a6 <main+70>: call 0x8048404 <file_exists>
21 0x080484ab <main+75>: jmp 0x80484b9 <main+89>
22 0x080484ad <main+77>: movl $0x804861b,(%esp)        > "Permission Denied"
23 0x080484b4 <main+84>: call 0x8048340 <printf@plt>
24 0x080484b9 <main+89>: mov $0x0,%eax
25 0x080484be <main+94>: add $0x24,%esp
26 0x080484c1 <main+97>: pop %ecx
27 0x080484c2 <main+98>: pop %ebp
28 0x080484c3 <main+99>: lea -0x4(%ecx),%esp
29 0x080484c6 <main+102>: ret
30 End of assembler dump.
```

Level 3 – Medium Reverse Engineering

```
1  Dump of assembler code for function file_exists:
2  0x08048404 <file_exists+0>: push %ebp
3  0x08048405 <file_exists+1>: mov %esp,%ebp
4  0x08048407 <file_exists+3>: sub $0x78,%esp
5  0x0804840a <file_exists+6>: lea -0x60(%ebp),%eax
6  0x0804840d <file_exists+9>: mov %eax,0x4(%esp)
7  0x08048411 <file_exists+13>: mov 0x8(%ebp),%eax
8  0x08048414 <file_exists+16>: mov %eax,(%esp)
9  0x08048417 <file_exists+19>: call 0x8048540 <stat>
10 0x0804841c <file_exists+24>: mov %eax,-0x8(%ebp)
11 0x0804841f <file_exists+27>: cmpl $0x0,-0x8(%ebp)          > compare file exist/not
12 0x08048423 <file_exists+31>: jne 0x8048448 <file_exists+68>
13 0x08048425 <file_exists+33>: movl $0x3fb,-0x4(%ebp)
14 0x0804842c <file_exists+40>: mov -0x4(%ebp),%eax
15 0x0804842f <file_exists+43>: mov %eax,0x4(%esp)
16 0x08048433 <file_exists+47>: movl $0x80485d0,(%esp)         > "Your Key is : %i "
17 0x0804843a <file_exists+54>: call 0x8048340 <printf@plt>
18 0x0804843f <file_exists+59>: movl $0x0,-0x64(%ebp)
19 0x08048446 <file_exists+66>: jmp 0x804845b <file_exists+87>
20 0x08048448 <file_exists+68>: movl $0x80485e2,(%esp)         > "Access Denied  "
21 0x0804844f <file_exists+75>: call 0x8048340 <printf@plt>
22 0x08048454 <file_exists+80>: movl $0x0,-0x64(%ebp)
23 0x0804845b <file_exists+87>: mov -0x64(%ebp),%eax
24 0x0804845e <file_exists+90>: leave
25 0x0804845f <file_exists+91>: ret
26 End of assembler dump.
```

Level 3 – Medium Reverse Engineering

```
(gdb) b main
b main
Breakpoint 1 at 0x804846e
(gdb)
Note: breakpoint 1 also set at pc 0x804846e.
Breakpoint 2 at 0x804846e
(gdb) r
r
Starting program: /home/level1/level3/level3_1101829990745967

Breakpoint 1, 0x0804846e in main ()
(gdb)
(gdb) b *0x0804841c
b *0x0804841c
Breakpoint 3 at 0x804841c
(gdb)
Note: breakpoint 3 also set at pc 0x804841c.
Breakpoint 4 at 0x804841c
(gdb) jump *0x0804841c
jump *0x0804841c
Continuing at 0x804841c.

Breakpoint 3, 0x0804841c in file_exists ()
(gdb)
```

Level 3 – Medium Reverse Engineering

```
Breakpoint 3, 0x0804841c in file_exists ()
(gdb) p $eax
p $eax
$1 = -13628
(gdb)
$2 = -13628
(gdb) set var $eax=0
set var $eax=0
(gdb)
(gdb) n
n
Single stepping until exit from function file_exists,
which has no line number information.
Cannot access memory at address 0x3ff
(gdb)
Single stepping until exit from function __libc_start_main,
which has no line number information.
Your Key is : 1019
Program exited normally.
(gdb)
```

Level 4 – Medium Reverse Engineering

Level 4 : Medium Reverse Engineering

Enter the Key :

Your Filename : level4_765506219060163

Submit

Find the key Here

IDSECCONF Indonesian Security Conference 2012

Level 4 – Medium Reverse Engineering

```
@ctf4%ls -la level4_765506219060163
ls -la level4_765506219060163
-rwxr-xr-x 1 level4 level4 6676 May  8 07:38 level4_765506219060163
@ctf4%
@ctf4%strings level4_765506219060163
strings level4_765506219060163
/lib/ld-linux.so.2
__gmon_start__
libc.so.6
_IO_stdin_used
printf
__libc_start_main
GLIBC_2.0
PTRh
[^_]
@ctf4%
@ctf4%./level4_765506219060163
./level4_765506219060163
Find your key From here@ctf4%
@ctf4%
```

Level 4 – Medium Reverse Engineering

```
Dump of assembler code for function main:
0x080483a4 <main+0>: lea 0x4(%esp),%ecx
0x080483a8 <main+4>: and $0xfffffff0,%esp
0x080483ab <main+7>: pushl -0x4(%ecx)
0x080483ae <main+10>: push %ebp
0x080483af <main+11>: mov %esp,%ebp
0x080483b1 <main+13>: push %ecx
0x080483b2 <main+14>: sub $0x44,%esp
0x080483b5 <main+17>: movb $0x1c,-0x16(%ebp)
0x080483b9 <main+21>: movb $0x36,-0x15(%ebp)
0x080483bd <main+25>: movb $0x3b,-0x14(%ebp)
0x080483c1 <main+29>: movb $0x36,-0x13(%ebp)
0x080483c5 <main+33>: movb $0x34,-0x12(%ebp)
0x080483c9 <main+37>: movb $0x0,-0x11(%ebp)
0x080483cd <main+41>: movb $0x2d,-0x2e(%ebp)
0x080483d1 <main+45>: movb $0x50,-0x2d(%ebp)
0x080483d5 <main+49>: movb $0x55,-0x2c(%ebp)
0x080483d9 <main+53>: movb $0x4b,-0x2b(%ebp)
0x080483dd <main+57>: movb $0x7,-0x2a(%ebp)
0x080483e1 <main+61>: movb $0x60,-0x29(%ebp)
0x080483e5 <main+65>: movb $0x56,-0x28(%ebp)
0x080483e9 <main+69>: movb $0x5c,-0x27(%ebp)
0x080483ed <main+73>: movb $0x59,-0x26(%ebp)
0x080483f1 <main+77>: movb $0x7,-0x25(%ebp)
0x080483f5 <main+81>: movb $0x52,-0x24(%ebp)
0x080483f9 <main+85>: movb $0x4c,-0x23(%ebp)
0x080483fd <main+89>: movb $0x60,-0x22(%ebp)
0x08048401 <main+93>: movb $0x7,-0x21(%ebp)
0x08048405 <main+97>: movb $0x2d,-0x20(%ebp)
0x08048409 <main+101>: movb $0x59,-0x1f(%ebp)
0x0804840d <main+105>: movb $0x56,-0x1e(%ebp)
0x08048411 <main+109>: movb $0x54,-0x1d(%ebp)
0x08048415 <main+113>: movb $0x7,-0x1c(%ebp)
0x08048419 <main+117>: movb $0x4f,-0x1b(%ebp)
0x0804841d <main+121>: movb $0x4c,-0x1a(%ebp)
0x08048421 <main+125>: movb $0x59,-0x19(%ebp)
0x08048425 <main+129>: movb $0x4c,-0x18(%ebp)
0x08048429 <main+133>: movb $0x0,-0x17(%ebp)
0x0804842d <main+137>: lea -0x2e(%ebp),%eax
0x08048430 <main+140>: mov %eax,-0x10(%ebp)
0x08048433 <main+143>: jmp 0x8048444 <main+160>
0x08048435 <main+145>: mov -0x10(%ebp),%edx
0x08048438 <main+148>: movzbl (%edx),%eax
0x0804843b <main+151>: add $0x19,%eax
0x0804843e <main+154>: mov %al,(%edx)
0x08048440 <main+156>: addl $0x1,-0x10(%ebp)
0x08048444 <main+160>: mov -0x10(%ebp),%eax
0x08048447 <main+163>: movzbl (%eax),%eax
0x0804844a <main+166>: test %al,%al
0x0804844c <main+168>: jne 0x8048435 <main+145>
0x0804844e <main+170>: lea -0x2e(%ebp),%eax
0x08048451 <main+173>: mov %eax,0x4(%esp)
0x08048455 <main+177>: movl $0x8048580,(%esp)            > "%s"
0x0804845c <main+184>: call 0x80482d8 <printf@plt>
```

Level 4 – Medium Reverse Engineering

```
bash:~$ for i in $(sed -n '/movb/p' level4-main.txt | awk -F" " {'print $4'} | cut -d"," -f1 | cut -d"$" -f2); do echo $(($i));done
28
54
59
54
52
0
45
80
85
75
7
96
86
92
89
7
82
76
96
7
45
89
86
84
7
79
76
89
76
0
bash
```

```
bash:~$ for j in $(for i in $(sed -n '/movb/p' level4-main.txt | awk -F" " {'print $4'} | cut -d"," -f1 | cut -d"$" -f2); do echo $(($i)); done);
> do expr $j + 25; done
53
79
84
79
77
25
70
105
110
100
32
121
111
117
114
32
107
101
121
32
70
114
111
109
32
104
101
114
101
25
bash:~$
```

Level 4 – Medium Reverse Engineering

```
bash:~$ for x in $(for j in $(for i in $(sed -n '/movb/p' level4-main.txt | awk -F" " {'print $4'} | cut -d"," -f1 | cut -d"$" -f2);
> do echo $(($i)); done);
> do expr $j + 25; done);
> do printf \\$(printf '%03o' $x); done
5OTOMFind your key From here
bash:~$
```

Level 5 – Packet Network Analysis #1

Level 5 : Packet Network Analysis #1

Enter the Key :

Your Filename : 54ebf5047e755ecced033c90810d5a3b

Submit

your file here

Level 5 – Packet Network Analysis #1

```
@ctf5%export PATH=/usr/sbin:$PATH
export PATH=/usr/sbin:$PATH
@ctf5%
@ctf5%tshark -r 54ebf5047e755ecced033c90810d5a3b
tshark -r 54ebf5047e755ecced033c90810d5a3b
  1    0.000000 172.16.204.135 -> 172.16.204.138 ICMP Echo (ping) request
  2    0.000630 172.16.204.138 -> 172.16.204.135 ICMP Echo (ping) reply
  3    4.999864 00:0c:29:2d:f5:8c -> 00:0c:29:5f:02:23 ARP Who has 172.16.204.135?  Tell 172.16.204.138
  4    4.999877 00:0c:29:5f:02:23 -> 00:0c:29:2d:f5:8c ARP 172.16.204.135 is at 00:0c:29:5f:02:23
  5    5.455687 172.16.204.135 -> 172.16.204.138 TCP 55794 > https [SYN] Seq=0 Win=14600 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 TS
3219736 TSER=0 WS=4
  6    5.456040 172.16.204.138 -> 172.16.204.135 TCP https > 55794 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 TSV=92414710 TSE
3219736 WS=6
  7    5.456056 172.16.204.135 -> 172.16.204.138 TCP 55794 > https [ACK] Seq=1 Ack=1 Win=14608 [TCP CHECKSUM INCORRECT] Len=0 TSV=2
9737 TSER=92414710
  8    5.459239 172.16.204.135 -> 172.16.204.138 SSL Client Hello
  9    5.460691 172.16.204.138 -> 172.16.204.135 TCP https > 55794 [ACK] Seq=1 Ack=85 Win=14528 Len=0 TSV=92414713 TSER=23219737
 10    5.460706 172.16.204.138 -> 172.16.204.135 SSLv3 Server Hello, Certificate, Server Hello Done
 11    5.460711 172.16.204.135 -> 172.16.204.138 TCP 55794 > https [ACK] Seq=85 Ack=895 Win=16400 [TCP CHECKSUM INCORRECT] Len=0 TS
3219738 TSER=92414714
 12    5.462051 172.16.204.135 -> 172.16.204.138 SSLv3 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
 13    5.463387 172.16.204.138 -> 172.16.204.135 SSLv3 Change Cipher Spec, Encrypted Handshake Message
 14    5.469558 172.16.204.135 -> 172.16.204.138 SSLv3 Application Data
 15    5.473119 172.16.204.138 -> 172.16.204.135 SSLv3 Application Data, Application Data
 16    5.473143 172.16.204.138 -> 172.16.204.135 SSLv3 Encrypted Alert
 17    5.473146 172.16.204.138 -> 172.16.204.135 TCP https > 55794 [FIN, ACK] Seq=1243 Ack=616 Win=16640 Len=0 TSV=92414724 TSER=23
740
 18    5.473387 172.16.204.135 -> 172.16.204.138 SSLv3 Encrypted Alert
 19    5.473514 172.16.204.135 -> 172.16.204.138 TCP 55794 > https [RST, ACK] Seq=639 Ack=1244 Win=18176 [TCP CHECKSUM INCORRECT] L
0 TSV=23219741 TSER=92414724
 20    9.281096 172.16.204.1 -> 172.16.204.255 NBNS Name query NB <01><02>__MSBROWSE__<02><01>
 21    9.281121 172.16.204.1 -> 172.16.204.255 NBNS Name query NB WORKGROUP<1d>
 22   13.119922 00:50:56:c0:00:08 -> ff:ff:ff:ff:ff:ff ARP Who has 172.16.204.135?  Tell 172.16.204.1
```

Level 5 – Packet Network Analysis #1

```
 28  13.129597 172.16.204.1 -> 172.16.204.135 TCP 49246 > krb524 [PSH, ACK] Seq
3

0000  00 0c 29 5f 02 23 00 50 56 c0 00 08 08 00 45 00   ..)_.#.PV.....E.
0010  03 c8 1b 53 40 00 40 06 2b 33 ac 10 cc 01 ac 10   ...S@.@.+3......
0020  cc 87 c0 5e 11 5c f8 0d bc d6 73 ee f0 4a 80 18   ...^.\....s..J..
0030  ff ff d1 32 00 00 01 01 08 0a 1d 6e 80 9d 01 62   ...2.......n...b
0040  55 95 2d 2d 2d 2d 2d 42 45 47 49 4e 20 50 52 49   U.-----BEGIN PRI
0050  56 41 54 45 20 4b 45 59 2d 2d 2d 2d 2d 0a 4d 49   VATE KEY-----.MI
0060  49 43 64 77 49 42 41 44 41 4e 42 67 6b 71 68 6b   ICdwIBADANBgkqhk
0070  69 47 39 77 30 42 41 51 45 46 41 41 53 43 41 6d   iG9w0BAQEFAASCAm
0080  45 77 67 67 4a 64 41 67 45 41 41 6f 47 42 41 4b   EwggJdAgEAAoGBAK
0090  6a 6f 65 6a 39 62 7a 66 58 45 44 55 6e 33 0a 72   joej9bzfXEDUn3.r
00a0  6d 75 66 65 57 79 72 77 66 4e 5a 78 78 67 4e 45   mufeWyrwfNZxxgNE
00b0  6c 46 55 4b 59 45 59 30 34 61 77 76 33 54 54 4d   lFUKYEY04awv3TTM
00c0  5a 4e 55 57 4f 65 30 35 68 55 68 72 75 68 5a 68   ZNUWOe05hUhruhZh
00d0  54 39 39 50 43 6a 48 4c 30 4e 6e 76 2b 57 44 0a   T99PCjHL0Nnv+WD.
00e0  72 5a 36 4b 50 54 55 36 57 2f 54 48 46 48 68 46   rZ6KPTU6W/THFHhF
00f0  45 4b 6d 48 73 55 50 69 2f 2f 33 67 71 6f 42 46   EKmHsUPi//3gqoBF
0100  37 63 37 51 73 4e 30 4e 77 73 41 61 6d 37 6d 65   7c7QsN0NwsAam7me
0110  4b 61 4f 68 39 61 5a 47 4e 68 39 68 61 79 45 43   KaOh9aZGNh9hayEC
0120  0a 4f 34 6b 55 7a 42 65 42 5a 72 77 38 4d 6b 4c   .O4kUzBeBZrw8MkL
0130  35 78 72 62 2b 65 59 64 70 63 35 55 72 41 67 4d   5xrb+eYdpc5UrAgM
0140  42 41 41 45 43 67 59 42 63 6b 45 4a 6d 4e 46 35   BAAECgYBckEJmNF5
0150  54 58 2b 52 55 63 38 70 2f 4b 6a 37 31 77 63 36   TX+RUc8p/Kj71wc6
0160  68 0a 47 4d 4d 56 75 42 77 67 75 37 6d 66 43 4d   h.GMMVuBwgu7mfCM
0170  62 71 32 6a 4f 68 78 78 63 31 41 52 56 54 72 58   bq2jOhxxc1ARVTrX
0180  77 6c 65 6e 63 4b 31 2f 78 41 78 64 58 52 46 77   wlencK1/xAxdXRFw
0190  38 63 70 6c 2b 77 58 4a 41 71 41 4f 48 33 52 48   8cpl+wXJAqAOH3RH
01a0  33 49 0a 61 48 42 58 66 4c 67 48 73 6c 37 53 30   3I.aHBXfLgHsl7S0
01b0  65 35 70 54 55 4b 63 30 73 4c 57 6b 75 33 72 58   e5pTUKc0sLWku3rX
01c0  44 49 4a 61 42 69 6b 31 41 42 59 37 43 42 39 6a   DIJaBik1ABY7CB9j
```

Level 5 – Packet Network Analysis #1

```
@ctf5%openssl pkcs8 -nocrypt -in a -out b
openssl pkcs8 -nocrypt -in a -out b
@ctf5%
@ctf5%cat b
cat b
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCo6Ho/W831xA1J965rn3lsq8HzWccYDRJRVCmBGNOGsL900zGT
VFjntOYVIa7oWYU/fTwoxy9DZ7/lg62eij01Olv0xxR4RRCph7FD4v/94KqARe3O
0LDdDcLAGpu5nimjofWmRjYfYWshAjuJFMwXgWa8PDJC+ca2/nmHaXOVKwIDAQAB
AoGAXJBCZjReU1/kVHPKfyo+9cHOoRjDFbgcILu5nwjG6tozoccXNQEVU618JXp3
Ctf8QMXV0RcPHKZfsFyQKgDh90R9yGhwV3y4B7Je0tHuaU1CnNLC1pLt61wyCWgY
pNQAWOwgfYzlZpYsRN6Crzyx0C5ZXDMvAQTdw34Jm0XbdFECQQDXToaeGHRsk8rx
IJUGHT/bC+37vxsSBeZP3TCXfdfWa2dV7zKfi8H+aDbEAqFzi7zob3NUZIpU2bDH
ITsDpH3DAkEAyNT8IC7m5DseTyAPa2+NlwXcoaxWOlWGubIOkutEWRLNTe67dlh0
RT8CqGc8+/m3hfkn0E72saL0jfhXAgUMeQJAM0olj2vL8EGUyrQ0S+yT1Z6V5q6z
yCtXnhbXCH+V9yJGz5XXvWIRqIUy5qapx1i2e7hxBN2ehnAFSKqF4GxC+QJBAKLw
yq6B3ysFHA4ugNQ16bbCNsOlQ0CI64n2AQUKhKWQL6ovK0FVeuBDwzBGsp/tdwzn
nXnQ1y5AfBJDjrRAzGECQQCRW113Dj85NNHVqUbOcODbdeEjshi3670rgdvdMhhZ
hd1Wwh3H91h7+Z5q1Pdx8CCx8SBd9OWIJxEiSmPFcZis
-----END RSA PRIVATE KEY-----
@ctf5%
```

```
@ctf5%
@ctf5%sed -r
VATE KEY----
<RIVATE KEY-
@ctf5%
@ctf5%cat a
cat a
-----BEGIN R
MIICdwIBADAN
rmufeWyrwfNZ
rZ6KPTU6W/TH
O4kUzBeBZrw8
GMMVuBwgu7mf
aHBXfLgHsl7S
My8BBN3Dfgmk
Z1XvMp+Lwf5c
b42XBdyhrFY6
BQx5AkAzSiWP
pqnHWLZ7uHEE
ifYBBQqEpZAv
Pzk00dWpRs5w
5YgnESJKY8Vx
-----END PRI
@ctf5%
```

Level 5 – Packet Network Analysis #1

```
@ctf5%tshark -r 54ebf5047e755ecced033c90810d5a3b -o "ssl.keys_list:172.16.204.138,443,http,b" -R "(http)"
<ssl.keys_list:172.16.204.138,443,http,b" -R "(http)"
 14   5.469568 172.16.204.135 -> 172.16.204.138 HTTP GET /bendera6.php HTTP/1.1
 15   5.473119 172.16.204.138 -> 172.16.204.135 HTTP HTTP/1.1 200 OK  (text/html)
@ctf5%
@ctf5%ts                                                                    tp)" -V
<ssl.key
Frame 14
    Arri
    [Tim
    [Tim
    [Tim
    Fram
    Fram
    Capt
    [Fra
    [Pro
Ethernet II
    Destina
        Add
        ...
        ...
    Source:
        Add
        ...
        ...
    Type: I
Internet Pr
```

```
bash:~$ echo "MW1zbDMzcHdoM24xbWRpMw==" | base64 -d
1ms133pwh3n1mdi3
bash:~$
```

```
        Response Code: 200
    Date: Sat, 28 Apr 2012 14:02:43 GMT\r\n
    Server: Apache/2.2.15 (CentOS)\r\n
    X-Powered-By: PHP/5.3.3\r\n
    Content-Length: 24\r\n
        [Content length: 24]
    Connection: close\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    \r\n
Line-based text data: text/html
    MW1zbDMzcHdoM24xbWRpMw==

@ctf5%
```

IDSECCONF Indonesian Security Conference 2012

Level 6 – Web Application Hacking #1

Level 6 : Web Application Hacking #1

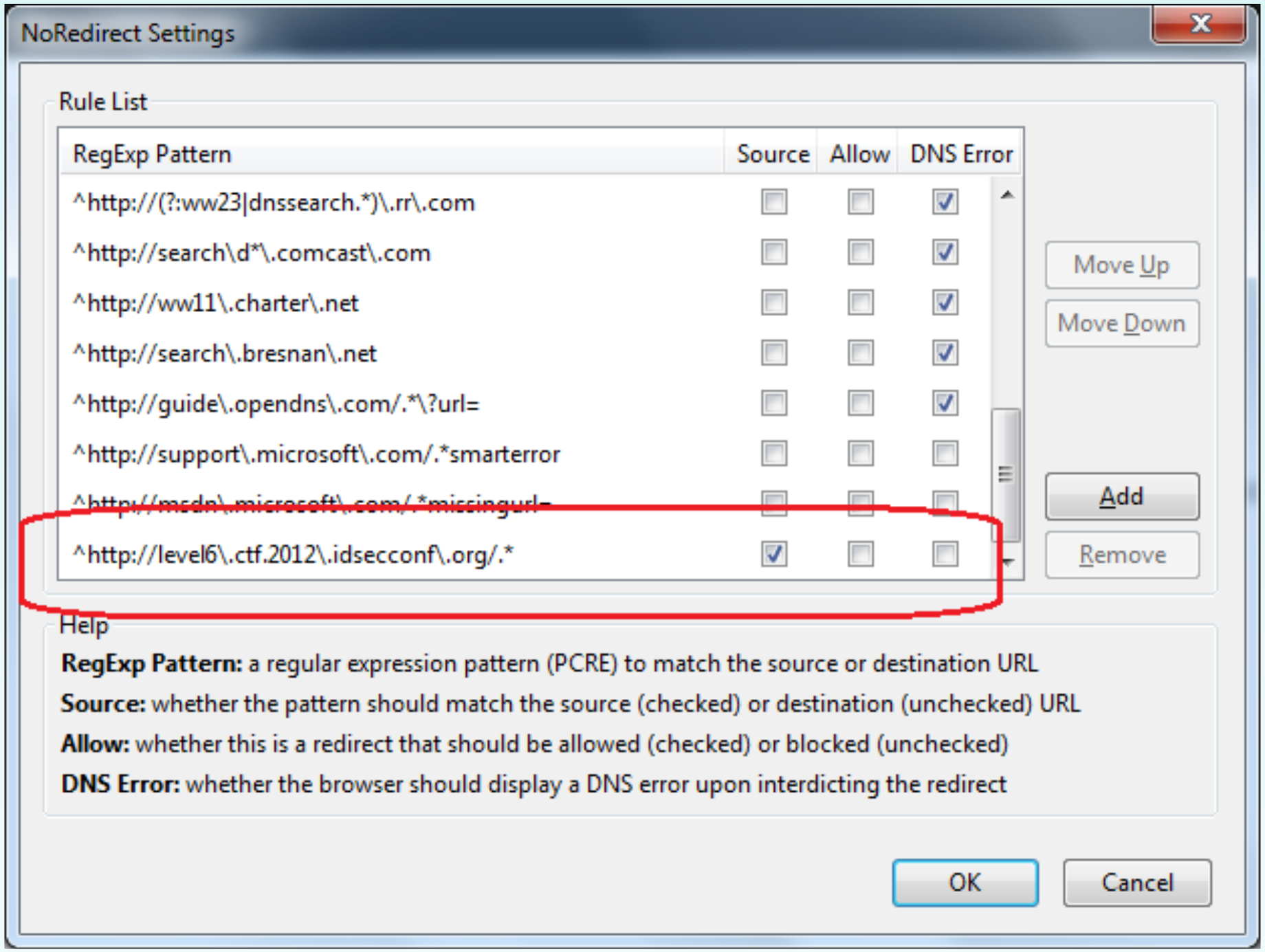
Enter the Key :

Your linkname : R03UF6H1WGIAJ4PPFOIMCEL6Q7O7DO1EFIZ07ULW0S5I213G8T

Submit

Find your key from this url

Level 6 – Web Application Hacking #1



IDSECCONF Indonesian Security Conference 2012

Level 6 – Web Application Hacking #1

Firefox | http://level6.ctf....IZ07ULW0S5I213G8T/ | ctf.2012.idsecconf.org : Level 5 : ZM3...

level6.ctf.2012.idsecconf.org/R03UF6H1WGIAJ4PPFOIMCEL6Q7O7DO1EFIZ07ULW0S5I213G8T/

Disable | Cookies | CSS | Forms | Images | Information | Miscellaneous | Outline | Resize

HTTP/302: http://level6.ctf.2012.idsecconf.org/R03UF6H1WGIAJ4PPFOIMCEL6Q7O7DO1EFIZ07ULW0S5I213G8T.html

Firefox | http://level6.ctf....ULW0S5I213G8T.html | ctf.2012.idsecconf.org : Level 5 : ZM3...

level6.ctf.2012.idsecconf.org/R03UF6H1WGIAJ4PPFOIMCEL6Q7O7DO1EFIZ07ULW0S5I213G8T.html

Disable | Cookies | CSS | For

HTTP/302: http://ctf.2012.idsecconf.org/

Your Key : ODM1MjgyMzMwMDIz

```
bash:~$ echo "ODM1MjgyMzMwMDIzOTUx" | base64 -d
835282330023951
bash:~$
```

Level 7 – Packet Network Analysis #2

Level 7 : Packet Network Analysis #2

Enter the Key :

Your Filename : cd5395c645996447f4af7f2c474b6dd2

Submit

your file here

Submit The Key#1 from your file and get Key Level7 to 125.5.115.34:8000

Level 7 – Packet Network Analysis #2

```
@ctf5%
@ctf5%tshark -r cd5395c645996647f4af7f2c474b6dd2 -R "(tcp.port==8000)" -V | grep "Data:"
<96447f4af7f2c474b6dd2 -R "(tcp.port==8000)" -V | grep "Data:"
     Data: 3078363120307836652030783634203078373 20D0A
     Data: 160301005A010000560303 4F9FAD176C3D0171AB5A3B99AD...
     D
     D$ echo 3078363720307837352030783665203078373 3 | xxd -r -p
     D
     D 0x67 0x75 0x6e 0x73$
     D
     D
@ctf5
```

Level 7 – Packet Network Analysis #2

```
$ cat level7.py
from twisted.internet import ssl, reactor
from twisted.internet.protocol import ClientFactory, Protocol

class EchoClient(Protocol):
    def connectionMade(self):
        self.transport.write("0x61 0x6e 0x64 0x72")

    def dataReceived(self, data):
        print "Server said:", data
        self.transport.loseConnection()

class EchoClientFactory(ClientFactory):
    protocol = EchoClient

    def clientConnectionFailed(self, connector, reason):
        print "Connection failed - goodbye!"
        reactor.stop()

    def clientConnectionLost(self, connector, reason):
        print "Connection lost - goodbye!"
        reactor.stop()

if __name__ == '__main__':
    factory = EchoClientFactory()
    reactor.connectSSL('125.5.115.34', 8000, factory, ssl.ClientContextFactory())
    reactor.run()
$ python level7.py
Server said: w3lc0m3t0th3jungl3
Connection lost - goodbye!
```

Level 8 – Web Application Hacking #2

Level 8 : Web Application Hacking #2

Enter the Key :

Your Filename :

Submit

Go to 125.5.115.34:8888 and find the key

Level 8 – Web Application Hacking #2

Firefox ctf.2012.ids

125.5.115.34:8888

Disable Cookies CS

web.Server Traceback :

not supported method

Usage :

[ctf,{user:(fileid)}]

[ctf,{key:(certid)}]

Source of: http://ctf.2012.idsecconf.org/level8/ - Mozilla Firefox

File Edit View Help

```
1
2  <!--
3  /*
4   *    ------------------------------------------------------------------
5   *    IDSECCONF CTF Online 2012
6   *    ------------------------------------------------------------------ fileid
7   *    Copyright (C) 2012
8   *        Dedi Dwianto (dedi.dwianto[at]idsecconf[dot]org) IptSC6Gvi0I5HOhhNyDF
9   *    ------------------------------------------------------------------
10  */
11 -->
12
13 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
14     "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
15 <html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en">
16
17 <head>
18     <link rel="stylesheet" href="/static/css/global.css" />
19     <link href="/static/css/bootstrap.css" rel="stylesheet">
20     <link href="/static/css/bootstrap-responsive.css" rel="stylesheet">
21
22
23     <title>ctf.2012.idsecconf.org : Last Level 8</title>
24     <script type="text/javascript" src="/static/js/bootstrap-collapse.js"></script>
```

IDSECCONF Indonesian Security Conference 2012

Level 8 – Web Application Hacking #2

en.wikipedia.org/wiki/JSON-RPC

sable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options

Version 1.0

A simple request and response:

```
--> { "method": "echo", "params": ["Hello JSON-RPC"], "id": 1}
<-- { "result": "Hello JSON-RPC", "error": null, "id": 1}
```

This example shows parts of a communication from an example chat application. The chat service sends notifications for each chat

```
--> {"method": "postMessage", "params": ["I have a question:"], "id": 101}
<-- {"method": "userLeft", "params": ["user3"], "id": null}
<-- {"result": 1, "error": null, "id": 101}
...
```

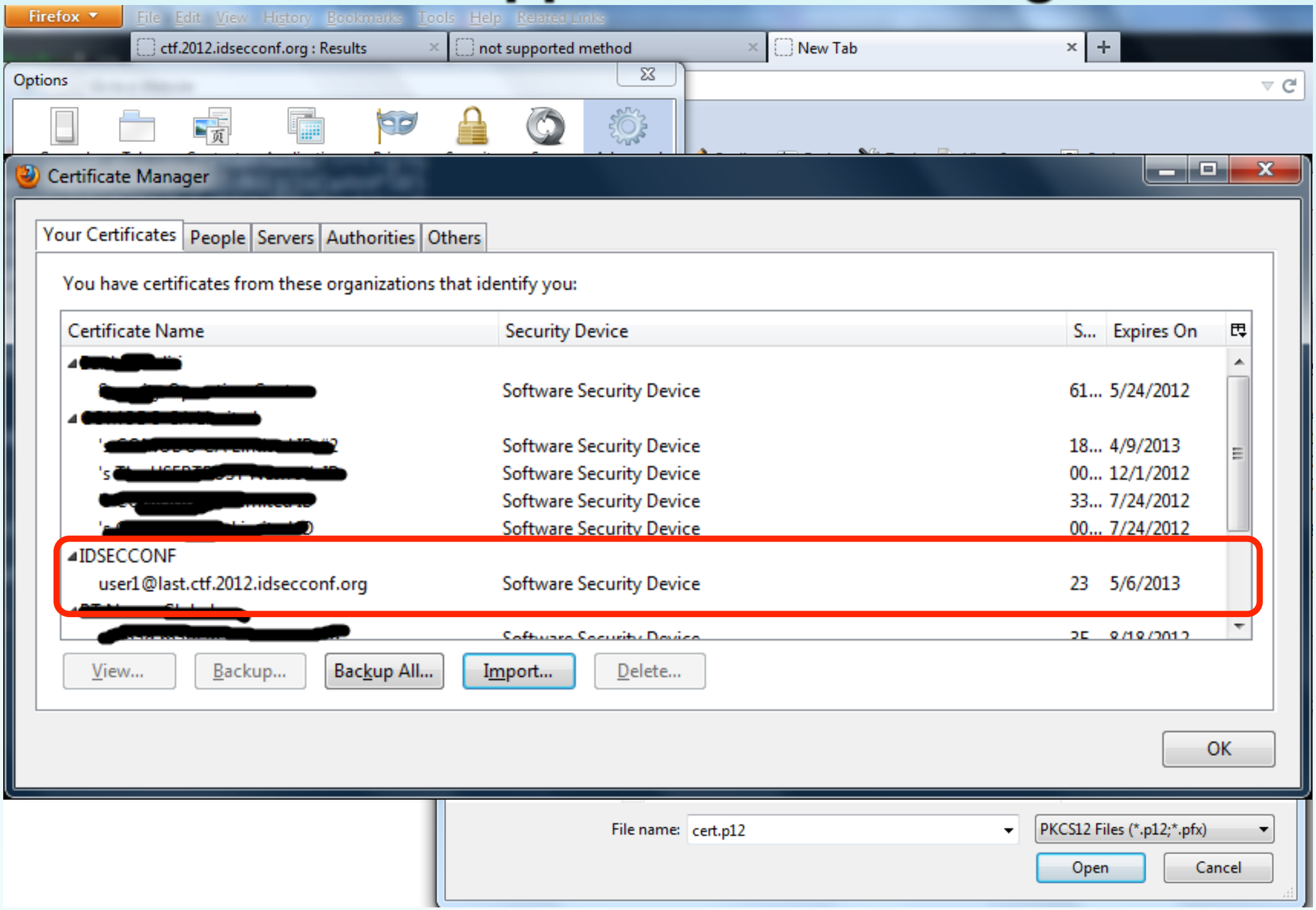
```
bash:~$ curl -X POST --data '{"method" : "ctf.user", "params": ["IptSC6GviOI5HOhhNyDF"]}' http://125.5.115.34:8888/
["File name : 023dc06eadf025af4a8fdf73e3cf4f85, Download from : http://ctf.2012.idsecconf.org/static/file8/023dc06eadf025af4a8fdf73e3cf4f85"]
bash:~$

bash:~$

bash:~$ curl -X POST --data '{"method" : "ctf.key", "params": ["023dc06eadf025af4a8fdf73e3cf4f85"]}' http://125.5.115.34:8888/
["File Password : OsXQ38JcSZsh"]
bash:~$
```

IDSECCONF Indonesian Security Conference 2012

Level 8 – Web Application Hacking #2

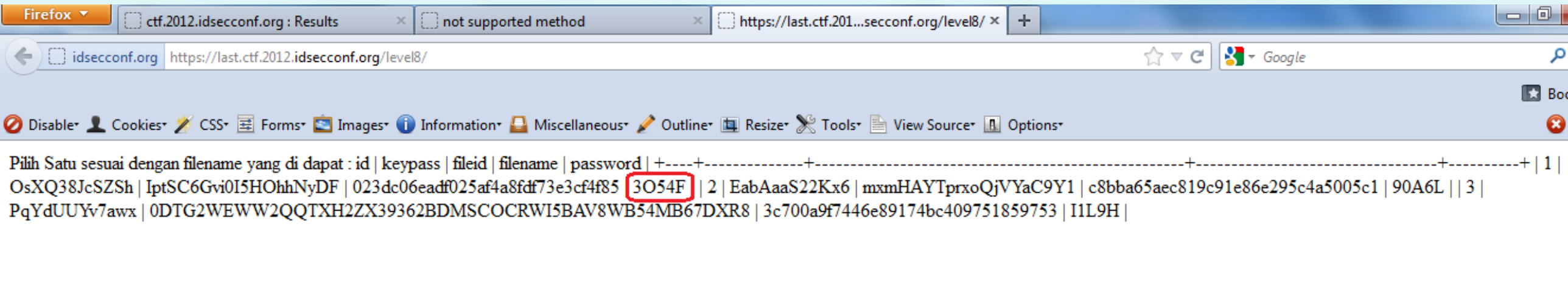
```
bash:~$ cat 023dc06eadf025af4a8fdf73e3cf4f85
Next go to : https://last.ctf.2012.idsecconf.org/level8/
---------

Bag Attributes
    localKeyID: 03 32 48 AE B0 E5 7E E6 99 1D 27 5E 74 60 A9 C7 46 29 0C A3
subject=/C=ID/ST=DKI Jakarta/L=Jakarta/O=ECHO/OU=CTF/CN=user1@last.ctf.2012.idsecconf.org/emailAddress=ctf@idsecconf.org
issuer=/C=ID/ST=DKI Jakarta/L=Jakarta/O=IDSECCONF/OU=CTF/CN=CTF IDSECCONF CA/emailAddress=ctf@idsecconf.org
-----BEGIN CERTIFICATE-----
MIICpTCCAg4CASMwDQYJKoZIhvcNAQEFBQAwgZQxCzAJBgNVBAYTAklEMRQwEgYD
VQQIEwtES0kgSmFrYXJ0YTEQMA4GA1UEBxMHSmFrYXJ0YTESMBAGA1UEChMJSURT
RUNDT05GMQwwCgYDVQQLEwNDVEYxGTAXBgNVBAMTEENURiBJRFNFQ0NPTkYgQ0Ex
IDAeBgkqhkiG9w0BCQEWEWN0ZkBpZHNlY2NvbmYub3JnMB4XDTEyMDUwNjAzMDAy
NFoXDTEzMDUwNjAzMDAyNFowgaAxCzAJBgNVBAYTAklEMRQwEgYDVQQIEwtES0kg
SmFrYXJ0YTEQMA4GA1UEBxMHSmFrYXJ0YTENMAsGA1UEChMERUNITzEMMAoGA1UE
CxMDQ1RGMSowKAYDVQQDFCF1c2VyMUBsYXN0LmN0Zi4yMDEyLmlkc2VjY29uZi5v
cmcxIDAeBgkqhkiG9w0BCQEWEWN0ZkBpZHNlY2NvbmYub3JnMIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQDIn7HWDqSERYP88yGFtzTS1XfaF8nm5mmggwKOUX1L
FmI0hggwTg+dfE3GoBJ4VWm8qGifO4jh8HpLIpn97D+tHG9l5cl1EWyFliy+rLwF
YmXXFDU7IB5DTHlWfhcuHxB8eN8j2//luBIAHJR4s7e0DIy26Y+qnOTttMG8RDEq
hQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAGMU9h0BhcupyyF+zbHH4AF4MyMOKoxJ
DdXF7UzuBZHlt5Iri2lhUzAPw13D950RVMKe7Sc21mHCzLwg41TKZYda309JuJkp
qsjmdQw2VKmhg/AQgoJMMvM2hiK2XzYEA0A7XY6XxKhbMoRzKgXFv9H+Apjsvmri
hbc2aL++7BMU
-----END CERTIFICATE-----
Bag Attributes: <No Attributes>
subject=/C=ID/ST=DKI Jakarta/L=Jakarta/O=IDSECCONF/OU=CTF/CN=CTF IDSECCONF CA/emailAddress=ctf@idsecconf.org
issuer=/C=ID/ST=DKI Jakarta/L=Jakarta/O=IDSECCONF/OU=CTF/CN=CTF IDSECCONF CA/emailAddress=ctf@idsecconf.org
-----BEGIN CERTIFICATE-----
MIIDpTCCAw6gAwIBAgIJAJoSiQvN6H0kMA0GCSqGSIb3DQEBBQUAMIGUMQswCQYD
VQQGEwJJRDEUMBIGA1UECBMLREtJIEpha2FydGExEDAOBgNVBAcTB0pha2FydGEx
EjAQBgNVBAoTCUlEU0VDQ09ORjEMMAoGA1UECxMDQ1RGMRkwFwYDVQQDExBDVEYg
SURTRUNDT05GIENBMSAwHgYJKoZIhvcNAQkBFhFjdGZAaWRzZWNjb25mLm9yZzAe
Fw0xMjA1MDYwMjE2MTRaFw0xMzA1MDYwMjE2MTRaMIGUMQswCQYDVQQGEwJJRDEU
MBIGA1UECBMLREtJIEpha2FydGExEDAOBgNVBAcTB0pha2FydGExEjAQBgNVBAoT
CUlEU0VDQ09ORjEMMAoGA1UECxMDQ1RGMRkwFwYDVQQDExBDVEYgSURTRUNDT05G
IENBMSAwHgYJKoZIhvcNAQkBFhFjdGZAaWRzZWNjb25mLm9yZzCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAv7hlLH+BMhcSQoLWsUC9gOB7vkasn3Auf/epzP8b
jgqLf1YbRPJsYgkTObWZZcNzCYMjJJiZfNwv1Csa+xQIKQN/veIognLzK2VmADMF
7eniLJKLS8QBUX9D1+Cgjxp/V0bCvSVK7xffisDUaEmr1aNfbFMCG3XCSCQKbea7
DqECAwEAAaOB/DCB+TAdBgNVHQ4EFgQUaYCgKLyEf4MEwJBFUBTYGX0aucowgckG
A1UdIwSBwTCBvoAUaYCgKLyEf4MEwJBFUBTYGX0aucqhgZqkgZcwgZQxCzAJBgNV
BAYTAklEMRQwEgYDVQQIEwtES0kgSmFrYXJ0YTEQMA4GA1UEBxMHSmFrYXJ0YTES
MBAGA1UEChMJSURTRUNDT05GMQwwCgYDVQQLEwNDVEYxGTAXBgNVBAMTEENURiBJ
RFNFQ0NPTkYgQ0ExIDAeBgkqhkiG9w0BCQEWEWN0ZkBpZHNlY2NvbmYub3JnggkA
mhKJC83ofSQwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOBgQCxBDxN2Aok
```

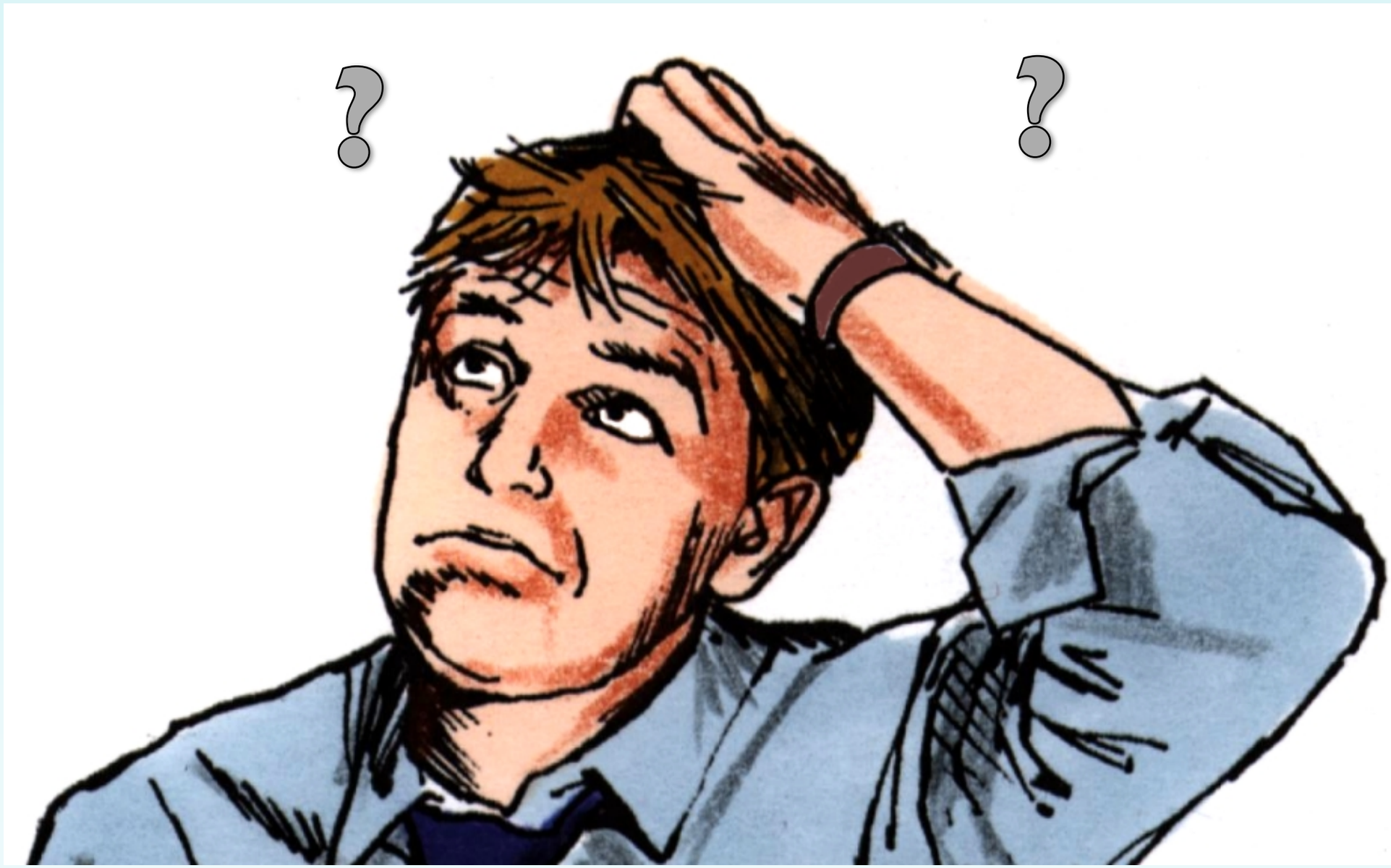
Level 8 – Web Application Hacking #2



IDSECCONF Indonesian Security Conference 2012

Level 8 – Web Application Hacking #2





IDSECCONF Indonesian Security Conference 2012