



# LOST IN TRANSLATION HACK IN THE BOX MALASYA 2013

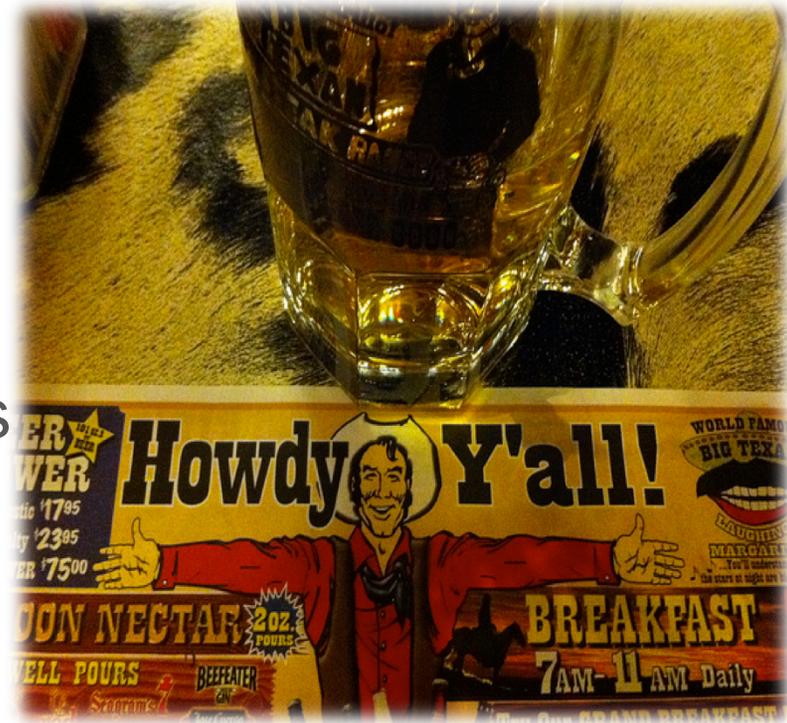
JOAQUIM ESPINHARA, SECURITY CONSULTANT SPIDERLABS @jespinhara

LUIZ EDUARDO, DIRECTOR SPIDERLABS @efffn



# Agenda

- Introduction
- Goals of this preso
- Motivations
- What's the issue here?
- A few different scenarios
- Takeaways



# whois luiz-eduardo

- Head of SpiderLabs LAC
- Knows a thing or two about WiFi
- NOC @ DEF CON
- Conference Organizer
- Amateur Photographer
- le /at/ trustwave /dot/ com
- @effffn





## whois Joaquim Espinhara

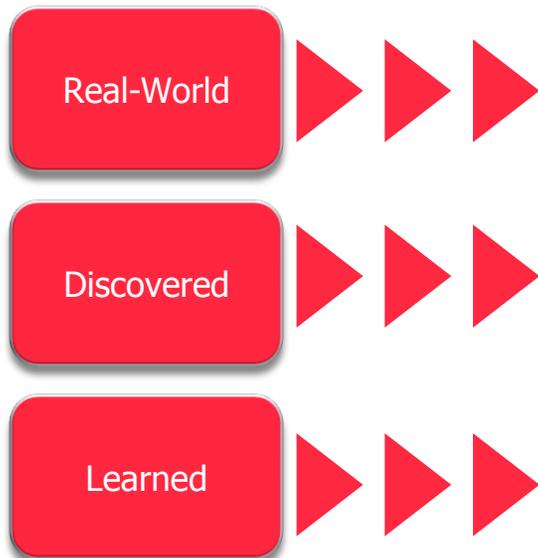
- Security Consultant Spiderlabs (LAC)
- Network Penetration Tester
- [jespinhara/at/trustwave/dot/com](mailto:jespinhara@trustwave.com)
- [@jespinhara](https://twitter.com/jespinhara)

®

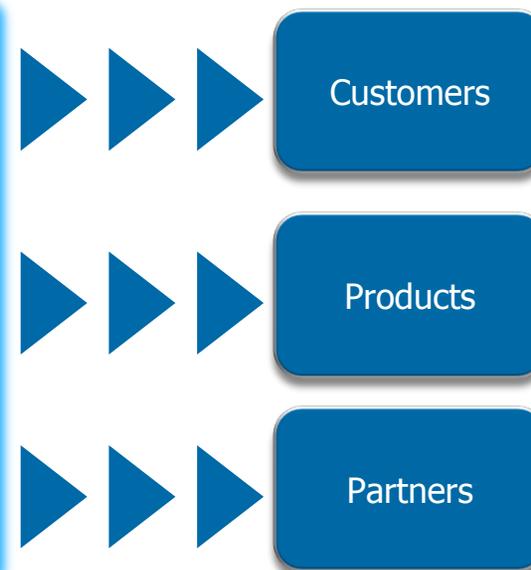
# Trustwave SpiderLabs

Trustwave SpiderLabs uses real-world and innovative security research to improve Trustwave products, and provides unmatched expertise and intelligence to customers.

## THREATS



## PROTECTIONS



Research and Development (R&D)  
Analysis and Testing (A&T)  
Response and Investigation (R&I)

# Goals of this presentation



# The English Language

88



[http://en.wikipedia.org/wiki/List\\_of\\_countries\\_where\\_English\\_is\\_an\\_official\\_language](http://en.wikipedia.org/wiki/List_of_countries_where_English_is_an_official_language)

# Why people buy security solutions?

I need this security solution because

---





# Security Assessment Tools (or services) why?

- To test their environment?
- To attack someone else if you're an attacker?
- Or you hire a pentest?
  - ... is it really a pentest?

# THE Fundamental Problem



# So... how things should work?



# Wrong... wrong? What do you mean?

```
select @@version_wrong
```

Msg 137, Level 15, State 2, Line 1

Must declare the scalar variable "@@version\_wrong".

```
Set Language 'Portuguese'
```

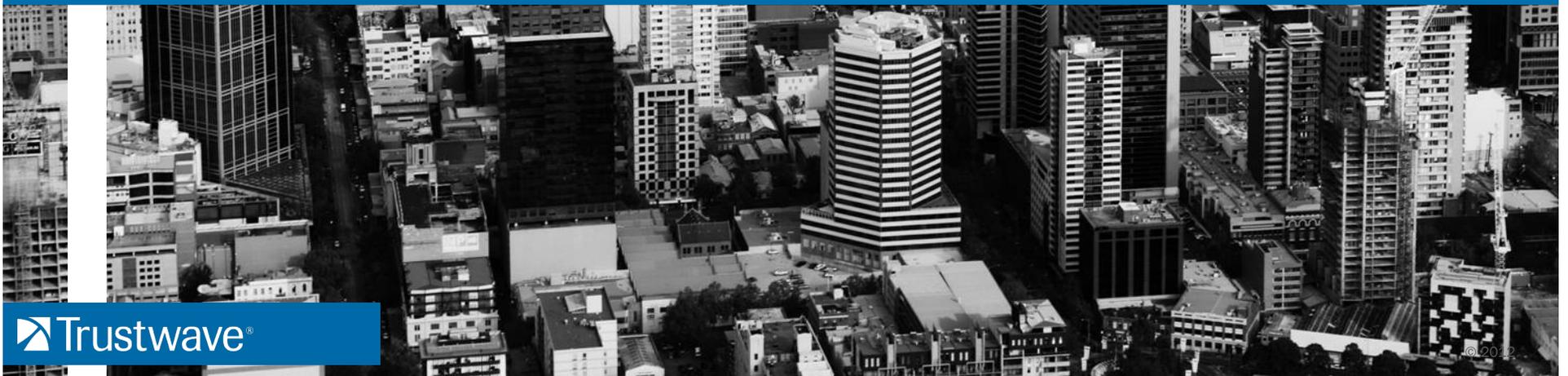
```
select @@version_wrong
```

Msg 137, Level 15, State 2, Line 1

É necessário declarar a variável escalar "@@version\_wrong".



# SOME RESULTS/ TEST CASES





# The Basic Scenario

- Broken WebApp
- MySQL backend DB
- Scanners

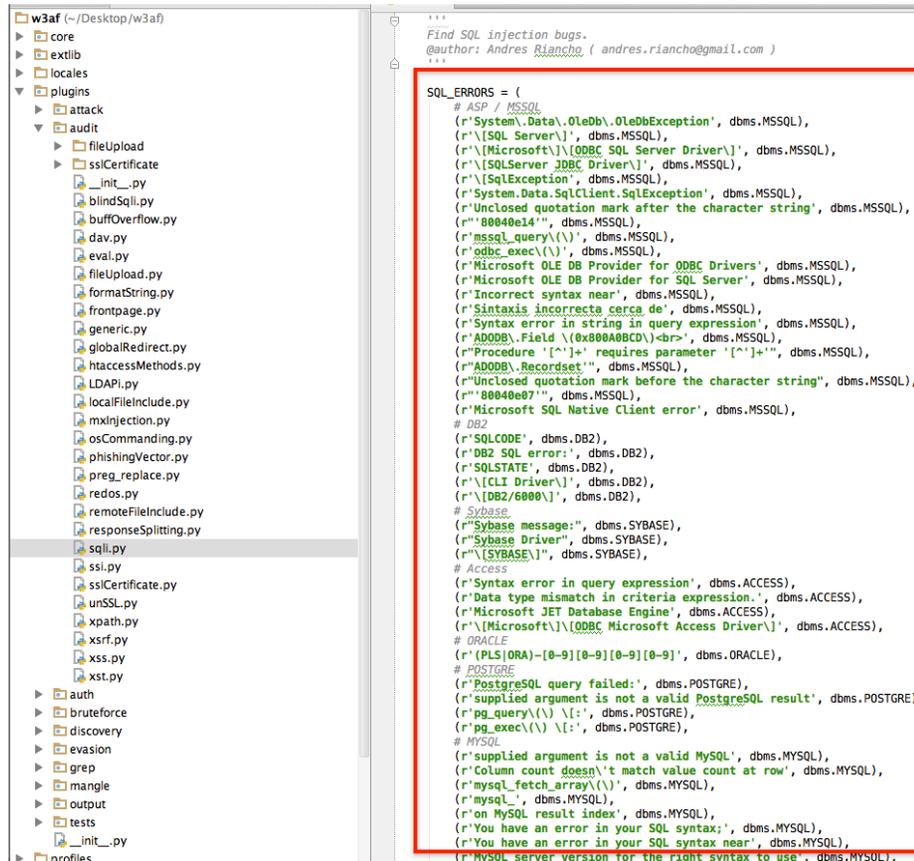
# A simple web app scan...

## Error SQL Injection

- w3af Scanner
  - EN: [+] Found
  - RU: [-] Not Found
  - PT: [-] Not Found
- Paid Scanner
  - EN: [+] Found
  - RU: [-] Not Found
  - PT: [-] Not Found

# A simple web app scan... w3af case

- “filters” or “matches”
- Only english



The image shows a file explorer on the left displaying the directory structure of the w3af project. The 'plugins' directory is expanded, showing sub-directories like 'attack' and 'audit', and various Python files such as 'fileUpload.py', 'sslCertificate.py', 'blindSql.py', 'dov.py', 'eval.py', 'formatString.py', 'generic.py', 'globalRedirect.py', 'LDAP.py', 'localFileInclude.py', 'mXInjection.py', 'osCommanding.py', 'phishingVector.py', 'preg\_replace.py', 'redos.py', 'remoteFileInclude.py', 'responseSplitting.py', 'sql.py', 'ssl.py', 'unSSL.py', 'xpath.py', 'xsrf.py', 'xss.py', and 'xst.py'. The 'audit' sub-directory is also visible, containing files like 'fileUpload', 'sslCertificate', 'blindSql.py', 'dov.py', 'eval.py', 'formatString.py', 'generic.py', 'globalRedirect.py', 'LDAP.py', 'localFileInclude.py', 'mXInjection.py', 'osCommanding.py', 'phishingVector.py', 'preg\_replace.py', 'redos.py', 'remoteFileInclude.py', 'responseSplitting.py', 'sql.py', 'ssl.py', 'unSSL.py', 'xpath.py', 'xsrf.py', 'xss.py', and 'xst.py'.

On the right, a code editor displays the 'SQL\_ERRORS' list, which is a tuple of tuples. Each tuple contains a regular expression pattern and a database engine name. The patterns are designed to detect various SQL injection errors across different database engines. The list includes errors for Microsoft SQL Server (MSSQL), Oracle, PostgreSQL, and MySQL. The patterns are enclosed in a red box in the original image.

```
Find SQL injection bugs.
@author: Andres Riancho ( andres.riancho@gmail.com )

SQL_ERRORS = (
    # ASP / MSSQL
    (r'System\.Data\.OleDb\.OleDbException', dbms.MSSQL),
    (r'[SQL Server]', dbms.MSSQL),
    (r'[Microsoft]\.[ODBC SQL Server Driver]', dbms.MSSQL),
    (r'[SQLServer JDBC Driver]', dbms.MSSQL),
    (r'[SqlException]', dbms.MSSQL),
    (r'System.Data.SqlClient.SqlException', dbms.MSSQL),
    (r'Unclosed quotation mark after the character string', dbms.MSSQL),
    (r''00040e14'', dbms.MSSQL),
    (r'mssql_query\(\)', dbms.MSSQL),
    (r'odbc_exec\(\)', dbms.MSSQL),
    (r'Microsoft OLE DB Provider for ODBC Drivers', dbms.MSSQL),
    (r'Microsoft OLE DB Provider for SQL Server', dbms.MSSQL),
    (r'Incorrect syntax near', dbms.MSSQL),
    (r'Syntax error in string in query expression', dbms.MSSQL),
    (r'Syntax error in string in query expression', dbms.MSSQL),
    (r'ADODB.Field \(0x000ABCD\)-'', dbms.MSSQL),
    (r'Procedure '[^']*' requires parameter '[^']*+', dbms.MSSQL),
    (r'ADODB.Recordset!', dbms.MSSQL),
    (r'Unclosed quotation mark before the character string", dbms.MSSQL),
    (r''00040e07'', dbms.MSSQL),
    (r'Microsoft SQL Native Client error', dbms.MSSQL),
    # DB2
    (r'SQLCODE', dbms.DB2),
    (r'DB2 SQL error:', dbms.DB2),
    (r'SQLSTATE', dbms.DB2),
    (r'\[CLI Driver\]', dbms.DB2),
    (r'\[DB2/6000\]', dbms.DB2),
    # Sybase
    (r'Sybase message:', dbms.SYBASE),
    (r'Sybase Driver', dbms.SYBASE),
    (r'\[SYBASE\]', dbms.SYBASE),
    # Access
    (r'Syntax error in query expression', dbms.ACCESS),
    (r'Data type mismatch in criteria expression.', dbms.ACCESS),
    (r'Microsoft JET Database Engine', dbms.ACCESS),
    (r'[Microsoft]\.[ODBC Microsoft Access Driver]', dbms.ACCESS),
    # ORACLE
    (r'(PLS|ORA)-[0-9][0-9][0-9]', dbms.ORACLE),
    # PostgreSQL
    (r'PostgreSQL query failed:', dbms.POSTGRE),
    (r'supplied argument is not a valid PostgreSQL result', dbms.POSTGRE),
    (r'pg_query\(\) \:', dbms.POSTGRE),
    (r'pg_exec\(\) \:', dbms.POSTGRE),
    # MySQL
    (r'supplied argument is not a valid MySQL', dbms.MYSQL),
    (r'Column count doesn't match value count at row', dbms.MYSQL),
    (r'mysql_fetch_array\(\)', dbms.MYSQL),
    (r'mysql_', dbms.MYSQL),
    (r'on MySQL result index', dbms.MYSQL),
    (r'You have an error in your SQL syntax;', dbms.MYSQL),
    (r'You have an error in your SQL syntax near', dbms.MYSQL),
    (r'MYSQL server version for the right syntax to use', dbms.MYSQL).
```

# A simple web app scan... w3af case

how to solve this?

- Add specific matches strings for each language
- File: plugins/audit/sqli.py
- Manual Penetration Test! 😊



## Another web app scan... Scanner 2

- 2 Broken Web Apps
- 3 Different Languages
- and...
- 3 Different Results

# Another web app scan... Scanner 2

- Web App I

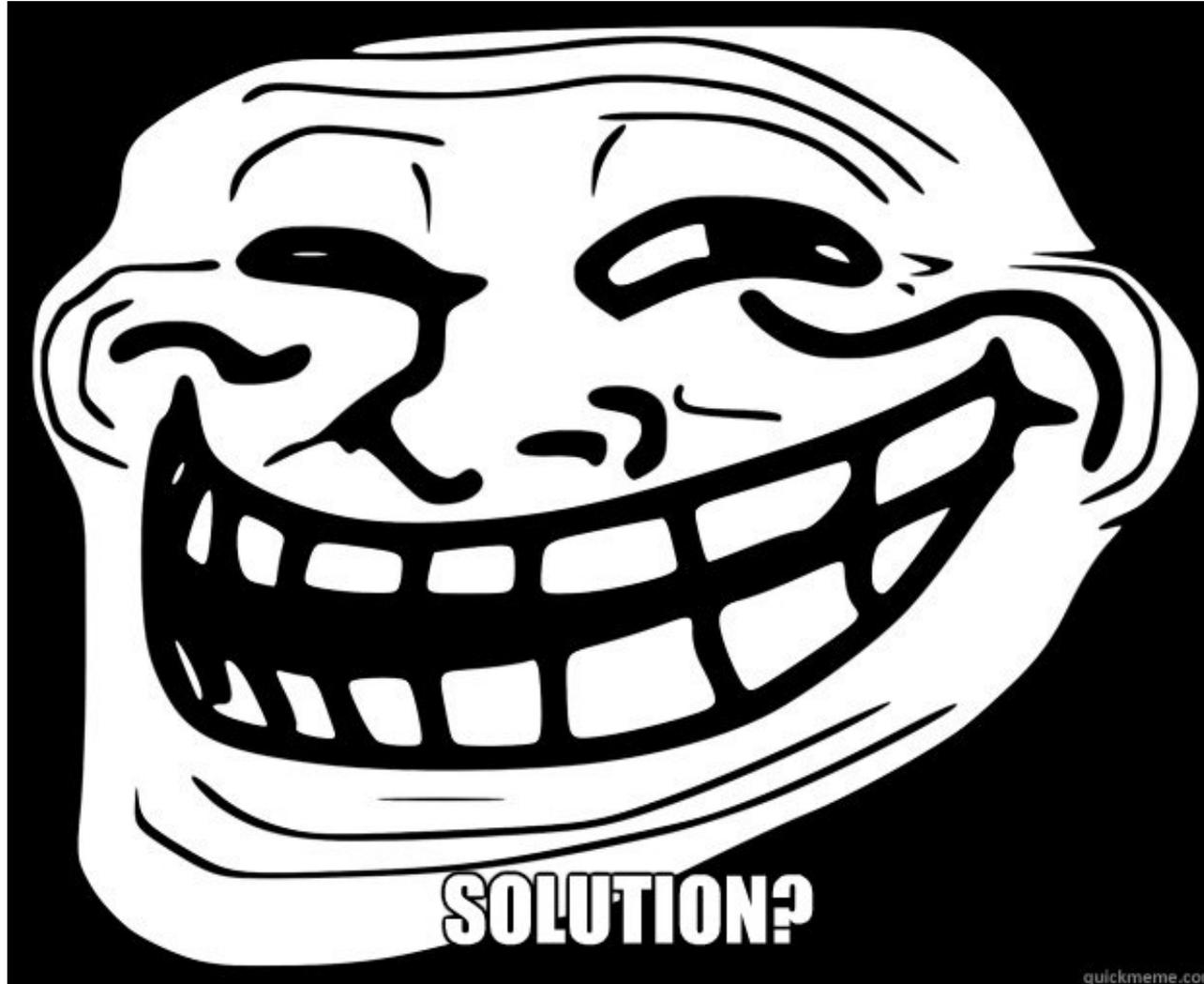
	EN	RU	PT
Critical	21	9	7
Total	36	15	12

- Web App II

	EN	RU	PT
Critical	86	78	82
Total	3130	3121	3118

- Error SQL Injection – Only in EN

## Another web app scan... Scanner 2

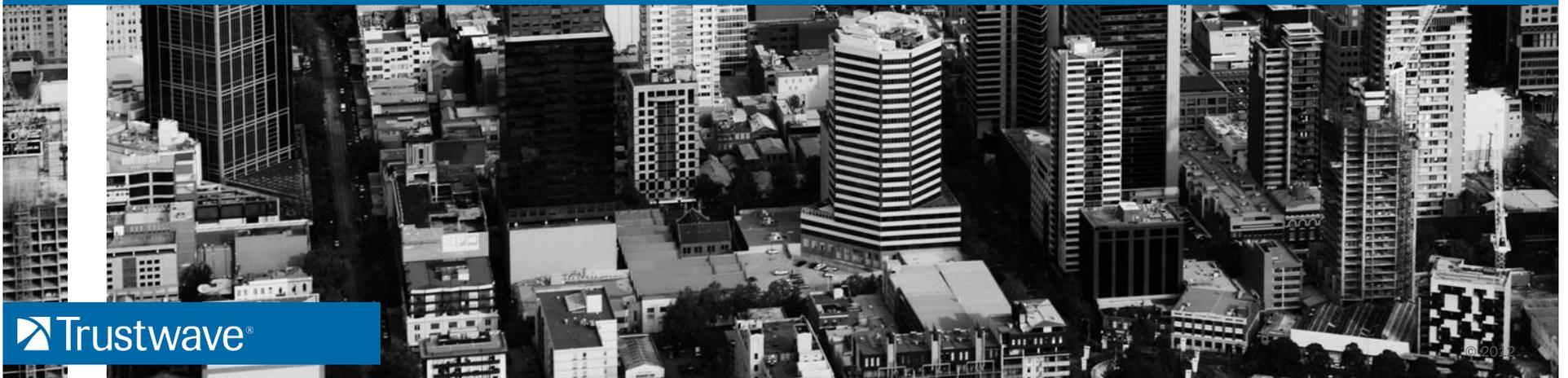


# What are the possibilities/ consequences?

- Evil attacker !
  - Error SQL Injection previously known
  - Set Error Message Language
    - `mysqld -language=portuguese`
    - `mysqld -language=/usr/local/share/portuguese`
- Results
  - Scan automatized show less results
  - Kids won't find the bug
- how about an “evil admin”?



# DEMOS



# Demo 1 – The usual suspect

## My Awesome Photoblog

[Home](#) | [test](#) | [ruxcon](#) | [2010](#) | [All pictures](#) | [Admin](#)

last picture:

---

No Copyright

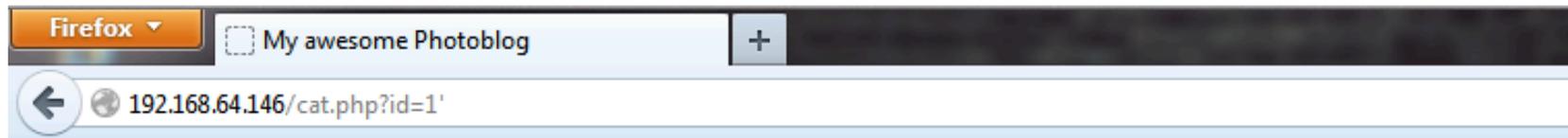
# Doesn't the DB send error codes?

```
mysql> select * from categories+;  
ERROR 1064 (42000): Voc+ tem um erro de sintaxe no seu SQL pr+ximo a '+' na linh  
a 1  
mysql> _
```

```
mysql> select * from categories+;  
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that  
corresponds to your MySQL server version for the right syntax to use near '+' at  
line 1  
mysql> _
```

## and the error codes...

- `mysql_errno()`

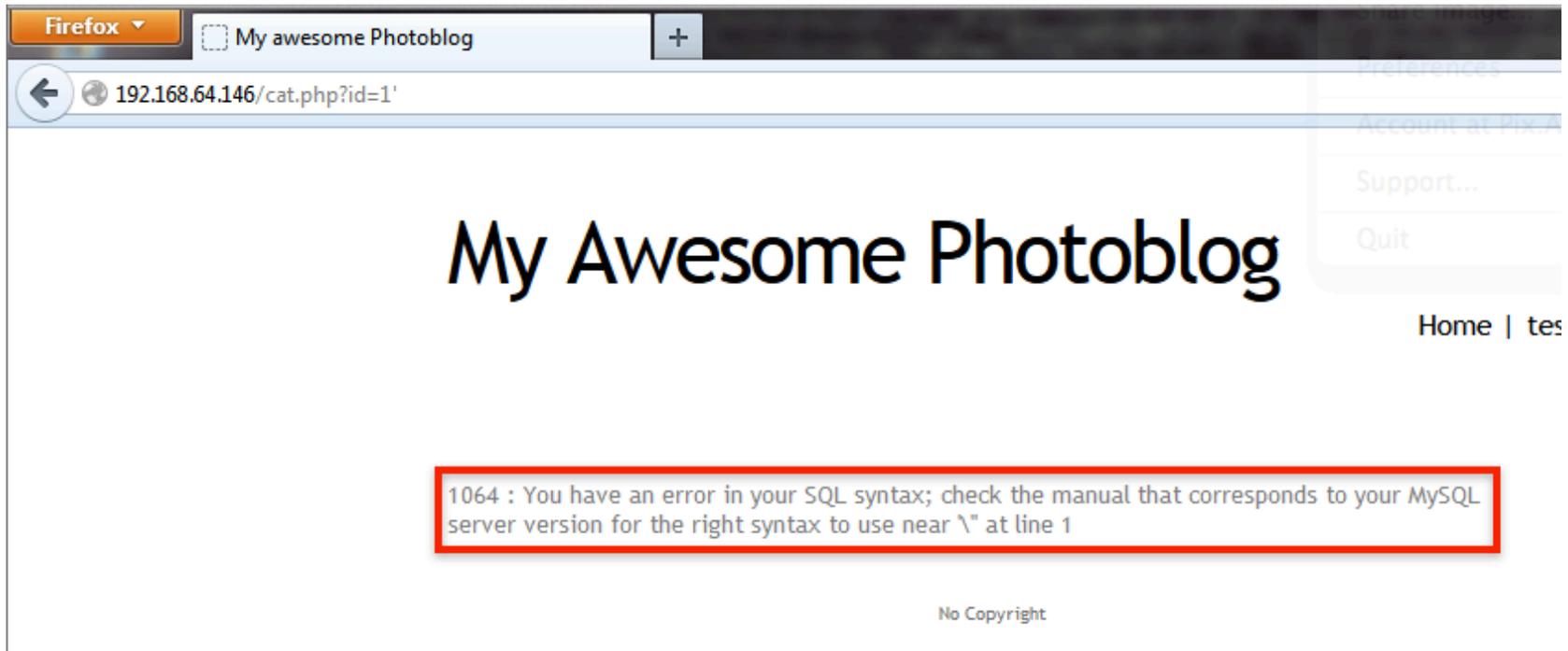


# My Awesome Photoblog

1064 : Você tem um erro de sintaxe no seu SQL próximo a \" na linha 1

No Copyright

# Wrong... wrong? What do you mean?



The screenshot shows a Firefox browser window with the title bar 'My awesome Photoblog'. The address bar contains the URL '192.168.64.146/cat.php?id=1'. The main content area displays the title 'My Awesome Photoblog' and a navigation menu with links for 'Preferences', 'Account at Pix.A', 'Support...', and 'Quit'. Below the title, there is a red-bordered box containing the following error message: '1064 : You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near `\" at line 1'. At the bottom of the page, the text 'No Copyright' is visible.

# The Attack Tool Problem

- File: lib/rex/post/meterpreter/ui/console/command\_dispatcher/mimikatz.rb

```
def system_check
  unless (client.sys.config.getuid == "NT AUTHORITY\\SYSTEM")
    print_warning("Not currently running as SYSTEM")
    return false
  end
end
```

## Takeaways...

- We demonstrated \*just a couple\* of cases where this could be a problem. What else could be in your environment taking advantage of this?
- How to fix this? Some behavior based solution that does not rely on signatures AT ALL?
- How about all the other solutions?
- At this point... you should be asking yourself...
  - Am I (really) secure? Or...
  - Do I want to be secure? 😊



# THANKS!

Joaquim Espinhara @jespinhara

Luiz Eduardo @efffn

[blog.spiderlabs.com](http://blog.spiderlabs.com)

@spiderlabs



 Trustwave®

© 2012