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

**THREATS**

- Real-World
- Discovered
- Learned

**PROTECTIONS**

- Customers
- Products
- Partners

Response and Investigation (R&I)
Analysis and Testing (A&T)
Research and Development (R&D)
Goals of this presentation
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
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

<table>
<thead>
<tr>
<th></th>
<th>EN</th>
<th>RU</th>
<th>PT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>21</td>
<td>9</td>
<td>7</td>
</tr>
<tr>
<td>Total</td>
<td>36</td>
<td>15</td>
<td>12</td>
</tr>
</tbody>
</table>

- Web App II

<table>
<thead>
<tr>
<th></th>
<th>EN</th>
<th>RU</th>
<th>PT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>86</td>
<td>78</td>
<td>82</td>
</tr>
<tr>
<td>Total</td>
<td>3130</td>
<td>3121</td>
<td>3118</td>
</tr>
</tbody>
</table>

- 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”?
Doesn’t the DB send error codes?

```
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()`
Wrong... wrong? What do you mean?

My Awesome Photoblog

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
The Attack Tool Problem

- File: lib/rex/post/meterpreter/ui/console/command_dispatcher/mimikatz.rb

```ruby
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 @effffn

blog.spiderlabs.com
@spiderlabs