

Breaking from MySQL to Linux system (SQL Injection).

quotes!

I tried using the method in question a) but replacing the union for:

```
Select <?phpinfo.php>? into outfile  
'/http/arquivos/phpinfo.php'
```

I tried encoding both the php code as the filename with hex. I also tried replace the quote (') in the name by (%). But nothing worked.

The OWASP testing guide say that if my server have magic_quotes on which is my case, it's not possible.

http://www.owasp.org/index.php/Testing_for_MySQL

However, NGSsoftware disagree:

<http://www.ngssoftware.com/papers/HackproofingMySQL.pdf>

I also tried to use char() encoding and the GBK 0xbf27 (never had tried it before, but appear not work in this case).

Any idea how to complain this attack?

c) Cause I'm using a bunch of NULL to validade the union statment, I can't do (at last i don't know how to do) complex select, which require use the comma (,), else it will break my union statment. How to deal when my injected query have MORE comma's than the comma's used in NULL to validade the select?

d) Any idea how to break from mysql to the linux system?

Cheers

Flickr agora em português. Você cria, todo mundo vê.
<http://www.flickr.com.br/>

This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real" vulnerabilities fast.
Click to try it, buy it or download a solution FREE today!

Breaking from MySQL to Linux system (SQL Injection).

<http://www.cenzic.com/downloads>
