

RE: Password Tesing using SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2003-03/0091.html>

From: Balwant Rathore (balwant@mahindrabt.com)

Date: 03/17/03

Date: Mon, 17 Mar 2003 20:46:47 +0530
From: "Balwant Rathore" <balwant@mahindrabt.com>
To: "Indian Tiger" <indiantiger@mailandnews.com>
Date: Mon, 17 Mar 2003 20:43:01 +0530

Hi,

Comments in-line

> *I am facing problem to compare two files one on the client &
> another one on the server so for that I want some way to transfer
> file from the clinet site to the server site.*

You can try as follows:

1. Display master..sysxlogins.passowrd data in browser using SQL Injections.
2. Compare encrypted password using pwdcompare function. As you have mentioned.

```
pwdcompare(rtrim>Password-List.word),master..sysxlogins.password) = 1;
```

I tried this but it doesn't display encrypted passwords in browser. And I was not in position to give sufficient time on this.

Sincerely,

Balwant Rathore, CISSP
Security Practices Group,
Mahindra-British Telecom Ltd.
Oberoi Estate Gardens, Chandivali,
Mumbai - 400 072, India.
Tel : +91 22 56922000 Extn - 8010
Fax : +91 22 28528959
Mobile: +91 98208 03333

Disclaimer

This message (including any attachments) contains confidential information intended for a specific individual and purpose, and is protected by law. If you are not the intended recipient, you should delete this message and are hereby notified that

RE: Password Tesing using SQL Injection

SecurityFocus Penetration: RE: Password Tesing using SQL Injection

any disclosure, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited.

Visit us at <http://www.mahindrabt.com>

Did you know that you have VNC running on your network?
Your hacker does. Plug your security holes now!
Download a free 15-day trial of VAM:
http://www2.stillsecure.com/download/sf_vuln_list.html