Exposure of Sensitive Information Lead To Admin Account Take Over in notrinos/notrinoserp 1

Valid Reported on Aug 18th 2022

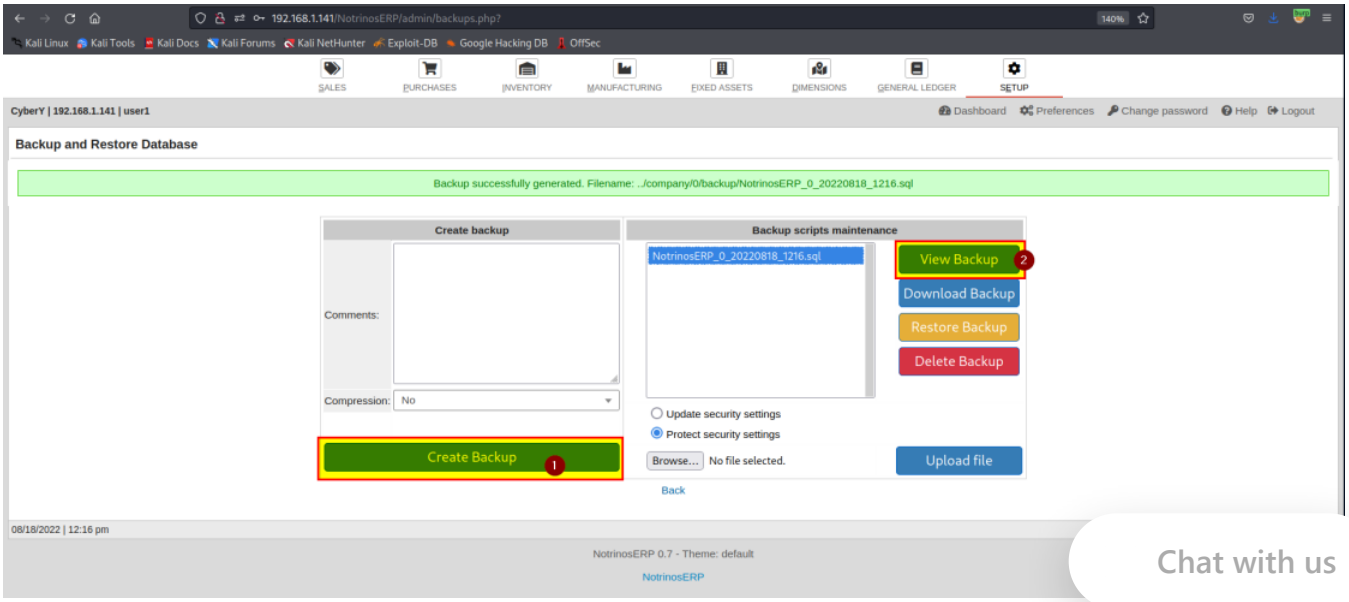
Description

The AP officers account is authorized to Backup and Restore the Database, Due to this he/she can download the backup and see the password hash of the System Administrator account, The weak hash (MD5) of the password can be easily cracked and get the admin password.

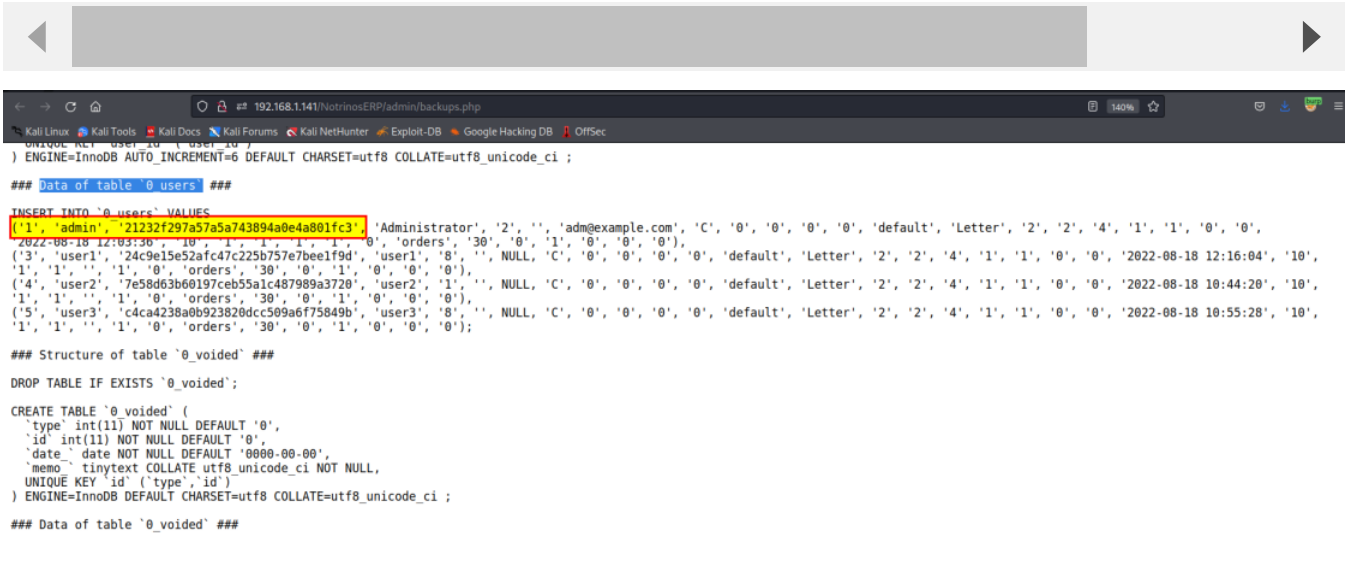
Proof of Concept

Steps to reproduce

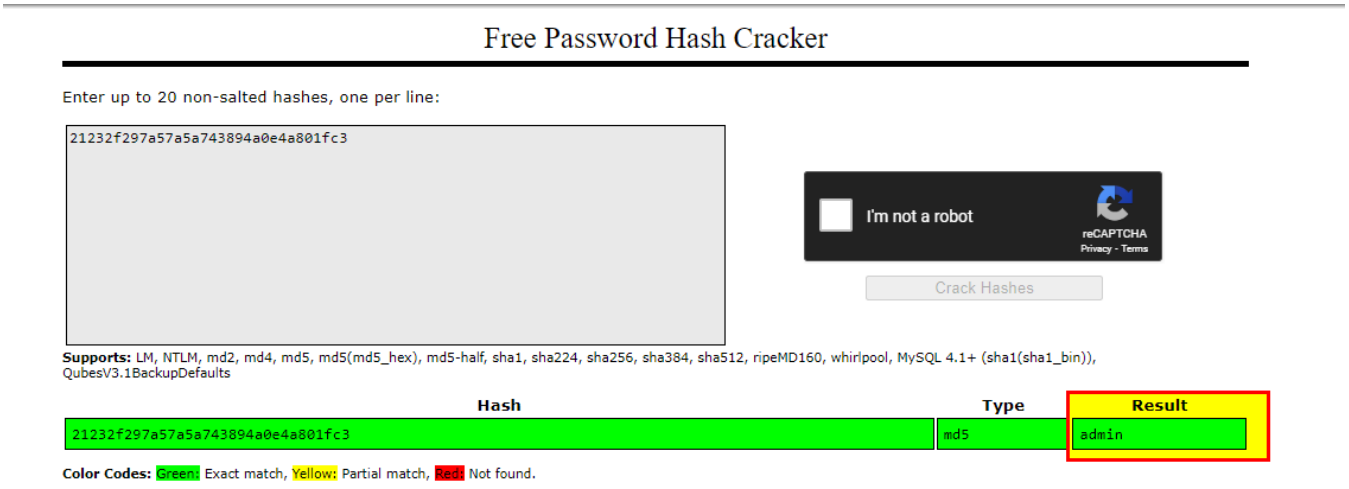
```
1- Login as  AP officers account.
2- Click on Create Backup.
3- After the Backup is created click on View Backup, this will open a new t
```



4- Scroll down to `Data of table 0_users`, and you see the MD5 hash of the



5- Crack the MD5 hash using hashcat or any tool.



Impact

This will lead to privilege escalation from AP officers account to the System Administrator account. and gain more functionality such as Create/Update Companies. Install/Update Languages. Install/Activate Extensions. Install/Activate Themes. Install/Activate Chart of Accounts. Software Upgrade.

References

- CWE

CVE
CVE-2022-2921

(Published)

Vulnerability Type
CWE-359: Exposure of Private Personal Information to an Unauthorized Actor

Severity
High (8.8)

Registry
Other

Affected Version
<=0.7

Visibility
Public

Status
Fixed

Found by

Abdullah Baghuth
@0xcybery
amateur

Fixed by

Phương
@notrinos
unranked

This report was seen 694 times.

We are processing your report and will contact the **notrinos/notrinoserp** team within 24 hours.
3 months ago

We have contacted a member of the **notrinos/notrinoserp** team and are waiting to hear back
3 months ago

Phương assigned a CVE to this report 3 months ago

Phương validated this vulnerability 3 months ago

Abdullah Baghuth has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Phương marked this as fixed in **0.7** with commit **1b9903** 3 months ago

Phương has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Phương gave praise 3 months ago

Thanks Abdullah Baghuth for detecting this, the weak hash md5 now be changed to bcrypt: https://github.com/notrinos/notrinoserp/commit/1b9903f4deea3289872793e60d730c63ecbf7b45

The researcher's credibility has slightly increased as a result of the maintainer's thanks: +1

Sign in to join this conversation

terms

privacy policy

Chat with us