

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

1



Valid

Reported on Aug 18th 2022

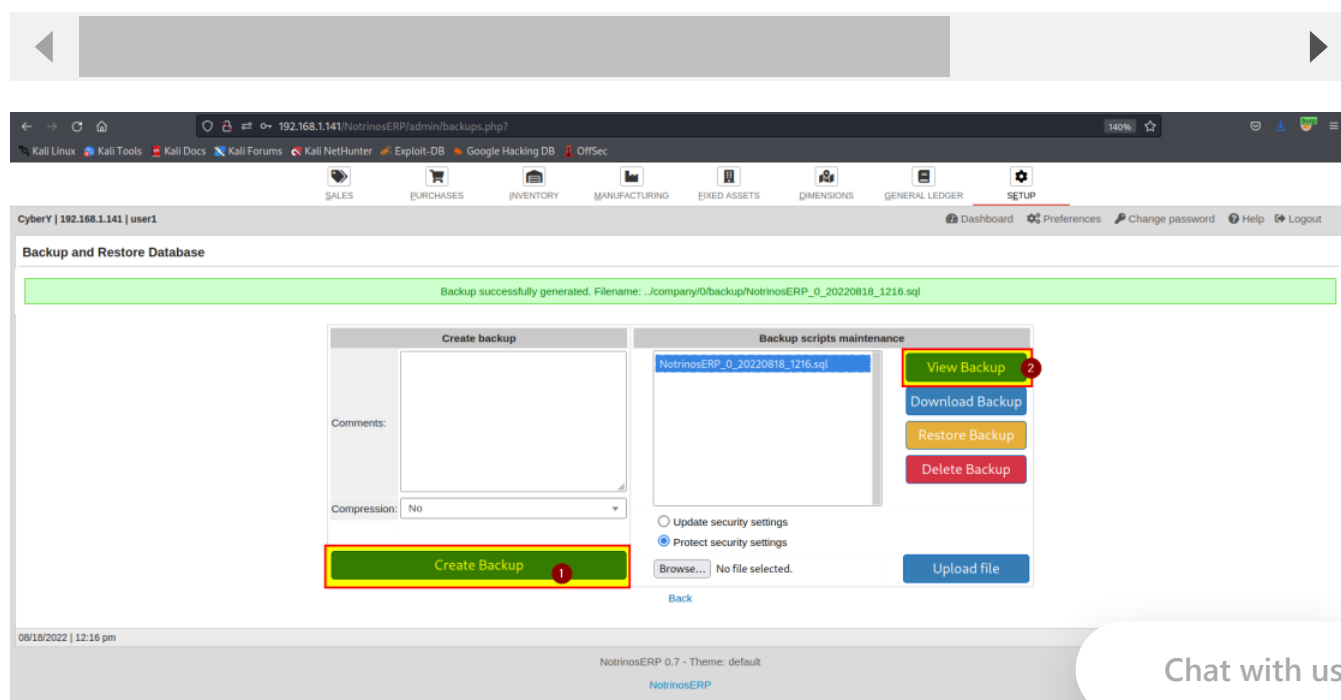
## Description

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



Chat with us

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

```

< >
192.168.1.141/NotrinosERP/admin/backups.php
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
) ENGINE=InnoDB AUTO_INCREMENT=6 DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci ;

### Data of table `0_users` ###
INSERT INTO `0_users` VALUES
('1', 'admin', '21232f297a57a5a743894a0e4a801fc3', 'Administrator', '2', '', 'adm@example.com', 'C', '0', '0', '0', '0', 'default', 'Letter', '2', '2', '4', '1', '1', '0', '0',
'2022-08-18 12:03:36', '0', '1', '1', '1', '1', '0', 'orders', '30', '0', '1', '0', '0', '0'),
('3', 'user1', '24c9e15e52afc47c225b757e7bee1f9d', 'user1', '8', '', NULL, 'C', '0', '0', '0', '0', 'default', 'Letter', '2', '2', '4', '1', '1', '0', '0', '2022-08-18 12:16:04', '10',
'1', '1', '1', '0', 'orders', '30', '0', '1', '0', '0', '0'),
('4', 'user2', '7e58d63b60197ceb55a1c487989a3720', 'user2', '1', '', NULL, 'C', '0', '0', '0', '0', 'default', 'Letter', '2', '2', '4', '1', '1', '0', '0', '2022-08-18 10:44:20', '10',
'1', '1', '1', '0', 'orders', '30', '0', '1', '0', '0', '0'),
('5', 'user3', 'c4ca4238a0b923820dc509a6f75849b', 'user3', '8', '', NULL, 'C', '0', '0', '0', '0', 'default', 'Letter', '2', '2', '4', '1', '1', '0', '0', '2022-08-18 10:55:28', '10',
'1', '1', '1', '0', 'orders', '30', '0', '1', '0', '0', '0');

### Structure of table `0_voided` ###
DROP TABLE IF EXISTS `0_voided`;
CREATE TABLE `0_voided` (
  `type` int(11) NOT NULL DEFAULT '0',
  `id` int(11) NOT NULL DEFAULT '0',
  `date` date NOT NULL DEFAULT '0000-00-00',
  `memo` tinytext COLLATE utf8_unicode_ci NOT NULL,
  UNIQUE KEY `id` (`type`,`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8 COLLATE=utf8_unicode_ci ;

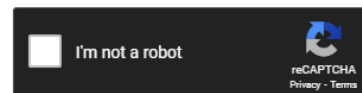
### Data of table `0_voided` ###
```

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

## Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

21232f297a57a5a743894a0e4a801fc3



Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
21232f297a57a5a743894a0e4a801fc3	md5	admin

**Color Codes:**   Exact match,   Partial match,   Not found.

## 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

(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 ✓

Chat with us

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

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

Phường has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

♥ Phường 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

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

part of 418sec

company

about

team

Chat with us

[terms](#)

[privacy policy](#)

[Chat with us](#)