

## Incorrect Privilege Assignment in phpipam/phpipam

0



Valid

Reported on Feb 4th 2022

### Description

The phpIPAM 1.4.5 incorrectly assigns a privilege to a particular actor, creating an unintended sphere of control for that actor in the Import/Export feature. A normal user with the role of **User** could download XLS file of IP addresses, hostfile dump and export system database that contains sensitive information via generate-xls.php, generate-hosts.php and generate-mysql.php endpoints respectively. It is supposedly accessible by the Administrator only for such administrative operations.

### Proof of Concept

Tested version: phpIPAM 1.4.5

-

Affected endpoints:

- 1 GET http://{HOST}/app/admin/import-export/generate-xls.php
- 2 GET http://{HOST}/app/admin/import-export/generate-mysql.php
- 3 GET http://{HOST}/app/admin/import-export/generate-hosts.php

-

Steps to reproduce:

- 1 Go to affected endpoints mentioned above.
- 2 Login as a user with the role of **User**.
- 3 We can export XLS files of IP addresses, MySQL database dump and the hostfile dump.

### Impact

This vulnerability is capable of fully compromising the system database, revealing sensitive information of relevant parties.

### Occurrences



generate-xls.php L13-L22



generate-hosts.php L15-L24

[Chat with us](#)



generate-mysql.php L14-L18

## References

- [CWE-266: Incorrect Privilege Assignment](#)

CVE

CVE-2022-1225

(Published)

Vulnerability Type

CWE-266: Incorrect Privilege Assignment

Severity

Medium (6.5)

Visibility

Public

Status

Fixed

Found by



Faisal Fs



@faisalfs10x

unranked



Fixed by



garyallan

@garyallan

maintainer

This report was seen 789 times.

We are processing your report and will contact the **phpipam** team within 24 hours.

10 months ago

We have contacted a member of the **phpipam** team and are waiting to hear back.

Chat with us

We have sent a follow up to the **phpipam** team. We will try again in 7 days. 10 months ago

We have sent a second follow up to the **phpipam** team. We will try again in 10 days.  
9 months ago

We have sent a third and final follow up to the **phpipam** team. This report is now considered stale. 9 months ago

A **phpipam/phpipam** maintainer has acknowledged this report 8 months ago

**garyallan** modified the report 8 months ago

**garyallan** validated this vulnerability 8 months ago

Faisal Fs  has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

**garyallan** marked this as fixed in 1.4.6 with commit **f6a49f** 8 months ago

**garyallan** has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

**generate-mysql.php#L14-L18** has been validated ✓

**generate-xls.php#L13-L22** has been validated ✓

**generate-hosts.php#L15-L24** has been validated ✓

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us