



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# PHP Volunteer Management System 1.0.2 - Multiple Vulnerabilities

**EDB-ID:**

18941

**CVE:**

**EDB Verified:** 

**Author:**

[ASHOO](#)

**Type:**

[WEBAPPS](#)

**Exploit:**  

**Platform:**

[PHP](#)

**Date:**

2012-05-28

**Vulnerable App:** 





```
# Exploit Title: PHP Volunteer Management System v 1.0.2 Multiple
Vulnerabilities
# Date: 05/28/12
# Author: Ashoo
# Mail: ashoo.online@gmail.com
# Software Site: https://sourceforge.net/projects/phpvolunteer/
# Version: 1.0.2
# Tested on: IIS6.0-Windows 2003
```

```
##### ToC #####
```

```
1.0 Introduction
2.0 Unrestricted File Upload
3.0 Persistent XSS
```

```
##### 1.0 Introduction #####
```

This is a PHP Volunteer Management software. Keep track of Volunteer hours worked and location assignments. This system is built on PHP/MySQL.

```
##### 2.0 Unrestricted File Upload #####
```

Bug:

Upload document (personal or Shared) functionality of application allow unrestricted file upload.

This can be abused by the attacker to upload backdoor to webserver.

PoC:

```
http://192.168.6.12/?p=upload_shared_document - Shared document upload
```

```
http://192.168.6.12/?p=upload_personal_document - personal document
upload
```

Upload php backdoor (r57, c99, etc) to the server.backdoor shell will be uploaded to

mods/documents/uploads/ directory of shell.Will provide complete control over webserver.

```
##### 3.0 Persistent XSS #####
```

Bug:

The persistent cross site scripting vulnerability exists in "add news information section"

A remote attacker with privileges can exploit this vulnerability.

PoC:

```
http://localhost/?p=add_news_information
```

In "Information to Display" text box Insert the following test strings  
<script> alert("xss me"); </script>  
fill other entries and submit!

EXPLOIT DATABASE

EXPLOITS

GHDB

PAPERS

SHELLCODES

SEARCH EDB

SEARCHSPLOIT MANUAL

SUBMISSIONS

ONLINE TRAINING

switch to the dashboard or login page, it is getting executed :-)

```
#####
#Ash00!!#
#####
```

Tags:

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.