

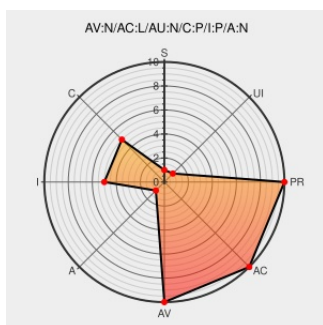


CVE-2006-5905

Published on: 11/15/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:03 PM UTC

CVE-2006-5905

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Web Directory Pro](#) from [Web Directory Pro](#) contain the following vulnerability:

Web Directory Pro allows remote attackers to (1) backup the database and obtain the backup via a direct request to admin/backup_db.php or (2) modify configuration via a direct request to admin/options.php.

CVE-2006-5905 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Web Directory PRO "admin/backup_db.php" Database Disclosure Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com

[web.archive.org](#)
[text/html](#)

[X](#) [SECUNIA 35327](#)

Web Directory Pro bypass Vulnerabilities - CXSecurity WLB

[securityreason.com](#)
[text/html](#)

[CX](#) [SREASON 1859](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF](#) [webdirectorypro-url-security-bypass\(30009\)](#)

Web Directory PRO - Remote Database Backup - PHP webapps Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 8878](#)

SecurityFocus

[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20061104](#)
[Web Directory Pro bypass Vulnerabilities](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Web Directory Pro	Web Directory Pro	All	All	All	All
Application	Web Directory Pro	Web Directory Pro	All	All	All	All
cpe:2.3:a:web_directory_pro:web_directory_pro:*:*:*:*:*:						
cpe:2.3:a:web_directory_pro:web_directory_pro:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)