



# CVE-2013-5000

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-5000                                                                                                                                         |
| <b>State</b>           | PUBLIC                                                                                                                                                |
| <b>Assigner</b>        | cve@mitre.org                                                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                                          |
| <b>Published</b>       | 2013-07-31 13:20:00 UTC                                                                                                                               |
| <b>Updated</b>         | 2013-07-31 13:20:00 UTC                                                                                                                               |
| <b>Description</b>     | phpMyAdmin 3.5.x before 3.5.8.2 allows remote attackers to obtain sensitive information via an invalid request, which reveals the database structure. |

## Risk And Classification

### Problem Types: CWE-200

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product    | Version | Update | Edition | Language |
|-------------|------------|------------|---------|--------|---------|----------|
| Application | Phpmyadmin | Phpmyadmin | 3.5.0.0 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.1.0 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.2.0 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.2.1 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.2.2 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.3.0 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.4   | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.5   | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.6   | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.7   | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.7   | rc1    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.8   | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.8   | rc1    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.8.1 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.0.0 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.1.0 | All    | All     | All      |
| Application | Phpmyadmin | Phpmyadmin | 3.5.2.0 | All    | All     | All      |

|             |                            |                            |         |     |     |     |
|-------------|----------------------------|----------------------------|---------|-----|-----|-----|
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.2.1 | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.2.2 | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.3.0 | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.4   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.5   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.6   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.7   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.7   | rc1 | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.8   | All | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.8   | rc1 | All | All |
| Application | <a href="#">Phpmyadmin</a> | <a href="#">Phpmyadmin</a> | 3.5.8.1 | All | All | All |

| References                            |         |                                                            |                     |
|---------------------------------------|---------|------------------------------------------------------------|---------------------|
| Reference                             | Source  | Link                                                       | Tags                |
| phpMyAdmin - Security - PMASA-2013-12 | CONFIRM | <a href="http://www.phpmyadmin.net">www.phpmyadmin.net</a> | Vendor Advisory     |
| CVE Program record                    | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>               | canonical           |
| NVD vulnerability detail              | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>             | canonical, analysis |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.