



# CVE-2008-1711

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

## Summary

|                        |                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2008-1711                                                                                                       |
| <b>State</b>           | PUBLIC                                                                                                              |
| <b>Assigner</b>        | cve@mitre.org                                                                                                       |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                        |
| <b>Published</b>       | 2008-04-09 19:05:00 UTC                                                                                             |
| <b>Updated</b>         | 2017-09-29 01:30:00 UTC                                                                                             |
| <b>Description</b>     | Terong PHP Photo Gallery (aka Advanced Web Photo Gallery) 1.0 stores passwords in cleartext in a MySQL database, wh |

## Risk And Classification

### Problem Types: CWE-310

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                                    | Version | Update | Edition | Language |
|-------------|------------------------|--------------------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Terong</a> | <a href="#">Advanced Web Photo Gallery</a> | 1.0     | All    | All     | All      |
| Application | <a href="#">Terong</a> | <a href="#">Advanced Web Photo Gallery</a> | 1.0     | All    | All     | All      |

## References

| Reference                                                                                                  | Source     | Link                            |
|------------------------------------------------------------------------------------------------------------|------------|---------------------------------|
| PHP Photo Gallery 1.0 (photo_id) SQL Injection Vulnerability                                               | EXPLOIT-DB | <a href="#">www.exploit-db.</a> |
| PHP Photo Gallery "photo_id" SQL Injection - Secunia Advisories - Vulnerability Intelligence - Secunia.com | SECUNIA    | <a href="#">secunia.com</a>     |
| IBM X-Force Exchange                                                                                       | XF         | <a href="#">exchange.xforce</a> |
| CVE Program record                                                                                         | CVE.ORG    | <a href="#">www.cve.org</a>     |
| NVD vulnerability detail                                                                                   | NVD        | <a href="#">nvd.nist.gov</a>    |

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)