



# CVE-2011-4265

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

## Summary

|                        |                                                                                                                                 |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2011-4265                                                                                                                   |
| <b>State</b>           | PUBLIC                                                                                                                          |
| <b>Assigner</b>        | vultures@jpcert.or.jp                                                                                                           |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                    |
| <b>Published</b>       | 2011-12-08 11:55:00 UTC                                                                                                         |
| <b>Updated</b>         | 2012-03-05 05:00:00 UTC                                                                                                         |
| <b>Description</b>     | Cross-site scripting (XSS) vulnerability in phpWebSite before 1.0.0 allows remote attackers to inject arbitrary web script or h |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor     | Product    | Version | Update | Edition | Language |
|-------------|------------|------------|---------|--------|---------|----------|
| Application | Phpwebsite | Phpwebsite | 0.10    | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.10.0  | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.10.1  | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.10.2  | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.7.3   | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.8.2   | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.8.3   | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.0   | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.1   | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.2   | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.2.1 | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.3   | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.3.1 | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.3.2 | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.9.3.3 | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | All     | All    | All     | All      |
| Application | Phpwebsite | Phpwebsite | 0.10    | All    | All     | All      |

|             |                            |                            |         |     |     |     |
|-------------|----------------------------|----------------------------|---------|-----|-----|-----|
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.10.0  | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.10.1  | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.10.2  | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.7.3   | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.8.2   | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.8.3   | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.0   | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.1   | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.2   | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.2.1 | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.3   | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.3.1 | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.3.2 | All | All | All |
| Application | <a href="#">Phpwebsite</a> | <a href="#">Phpwebsite</a> | 0.9.3.3 | All | All | All |

| References                                                  |         |                              |                     |
|-------------------------------------------------------------|---------|------------------------------|---------------------|
| Reference                                                   | Source  | Link                         | Tags                |
| JVN#70502960: phpWebSite vulnerable to cross-site scripting | JVN     | <a href="#">jvn.jp</a>       |                     |
| JVNDB-2011-000103                                           | JVNDB   | <a href="#">jvndb.jvn.jp</a> |                     |
| CVE Program record                                          | CVE.ORG | <a href="#">www.cve.org</a>  | canonical           |
| NVD vulnerability detail                                    | NVD     | <a href="#">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.