



# CVE-2006-0407

Published on: 01/24/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

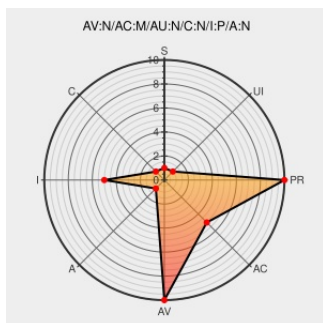
## CVE-2006-0407

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Az Bulletin Board](#) from [Azbb](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in post.php in AZ Bulletin Board (AZbb) 1.1.00 and earlier allows remote attackers to inject arbitrary web script or HTML via the (1) nickname parameter and (2) an iframe tag in the topic parameter. NOTE: the original disclosure specified the name parameter, but a correction was later provided. NOTE: followup posts have both disputed and confirmed the original claim.

CVE-2006-0407 has been assigned by [M](#) [cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**MEDIUM**

Authentication

**NONE**

Confidentiality  
Impact

**NONE**

Integrity  
Impact

**PARTIAL**

Availability  
Impact

**NONE**

## CVE References

Description

Tags

Link

SecurityFocus

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

[BUGTRAQ 20060308 Re: \[CORRECTIONS AND ADDITIONS\]Azbb v1.1.00 Cross-Site Scripting](#)

SecurityFocus

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

[BUGTRAQ 20060123 Azbb v1.1.00 Cross-Site Scripting](#)

IBM X-Force Exchange

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

[XF azbulletinboard-post-xss\(24274\)](#)

SecurityFocus

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

[BUGTRAQ 20060128 \[CORRECTIONS AND ADDITIONS\]Azbb v1.1.00 Cross-Site Scripting](#)

AZ Bulletin Board Post.PHP HTML Injection  
Vulnerabilities

[Exploit](#)  
[cve.report \(archive\)](#)

[BUG BID 16351](#)

[text/html](#)

Webmail : Solution de messagerie  
professionnelle - OVHcloud- OVH

[www.vupen.com](#)[text/html](#) [VUPEN ADV-2006-0298](#)

SecurityFocus

[www.securityfocus.com](#)[text/html](#) [BUGTRAQ 20060309 Re: Re: \[CORRECTIONS AND ADDITIONS\]Azbb v1.1.00 Cross-Site Scripting](#)

Secunia - Advisories - AZ Bulletin Board Cross-  
Site Scripting Vulnerabilities

[Vendor Advisory](#)[web.archive.org](#)[text/html](#) [SECUNIA 18565](#)

KAPDA :: Azbb v1.1.00 Cross\_Site\_Scripting

[Exploit](#)[Vendor Advisory](#)[kapda.ir](#)[text/html](#) [MISC kapda.ir/advisory-236.html](#)

SecurityFocus

[www.securityfocus.com](#)[text/html](#) [BUGTRAQ 20060308 Re: \[CORRECTIONS AND ADDITIONS\]Azbb v1.1.00 Cross-Site Scripting](#)

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](mailto: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 | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.0    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.0rc1 | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.0rc2 | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.1    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.10   | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.11   | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.12   | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.2    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.3    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.4    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.5    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.6    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.7    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.8    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.9    | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.1.00   | All    | All     | All      |
| Application | <a href="#">Azbb</a> | <a href="#">Az Bulletin Board</a> | 1.0.0    | All    | All     | All      |

|                                                     |      |                   |          |     |     |     |
|-----------------------------------------------------|------|-------------------|----------|-----|-----|-----|
| Application                                         | Azbb | Az Bulletin Board | 1.0.0rc1 | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.0rc2 | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.1    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.10   | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.11   | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.12   | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.2    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.3    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.4    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.5    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.6    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.7    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.8    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.0.9    | All | All | All |
| Application                                         | Azbb | Az Bulletin Board | 1.1.00   | All | All | All |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.0:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.0rc1:****:*:*: |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.0rc2:****:*:*: |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.1:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.10:****:*:*:   |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.11:****:*:*:   |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.12:****:*:*:   |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.2:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.3:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.4:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.5:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.6:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.7:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.8:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.9:****:*:*:    |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.1.00:****:*:*:   |      |                   |          |     |     |     |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.0:****:*:*:    |      |                   |          |     |     |     |

|                                                  |
|--------------------------------------------------|
|                                                  |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.0rc1:*****: |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.0rc2:*****: |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.1:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.10:*****:   |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.11:*****:   |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.12:*****:   |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.2:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.3:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.4:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.5:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.6:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.7:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.8:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.0.9:*****:    |
| cpe:2.3:a:azbb:az_bulletin_board:1.1.00:*****:   |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)