

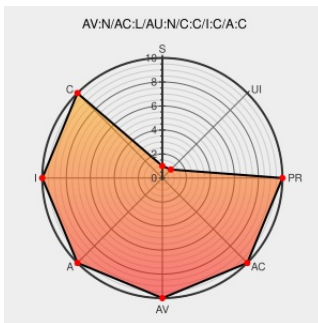


CVE-2007-2985

Published on: 06/01/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:42 PM UTC

CVE-2007-2985

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

Certain versions of [Pheap](#) from [Pheap](#) contain the following vulnerability:

Pheap 2.0 allows remote attackers to bypass authentication by setting a pheap_login cookie value to the administrator's username, which can be used to (1) obtain sensitive information, including the administrator password, via settings.php or (2) upload and execute arbitrary PHP code via an update_doc action in edit.php.

CVE-2007-2985 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **10 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

COMPLETE

COMPLETE

COMPLETE

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF pheap-edit-code-execution\(34592\)](#)

Pheap 2.0 - Authentication Bypass / Remote Code Execution - PHP webapps Exploit

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

[EXPLOIT-DB 4006](#)

Pheap PHP Code Execution and Information Disclosure - Advisories - Secunia

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

[SECUNIA 25460](#)

No Description Provided

[osvdb.org](#)

[OSVDB 36737](#)

[Inactive Link](#) [Not Archived](#)

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	Pheap	Pheap	2.0	All	All	All
Application	Pheap	Pheap	2.0	All	All	All
cpe:2.3:a:pheap:pheap:2.0:*:*:*:*:*:						
cpe:2.3:a:pheap:pheap:2.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)