Sense of Security	Authorisation. Jason Edelstein
	Release date. 31 July 2009.

Sense of Security – Security Advisory – SOS-09-005.

XOOPS Multiple Cross-Site Scripting Vulnerabilities.

31 July 2009.

XOOPS Multiple Cross-Site Scripting Vulnerabilities - Security Advisory - SOS-09-005

Release Date.	31-Jul-2009
Last Update.	-
Vendor Notification Date.	15-Jun-2009
Product.	XOOPS
Platform.	Independent
Affected versions.	2.3.3 (verified), possibly others
Severity Rating.	Medium
Impact.	Cookie/credential theft, impersonation, loss of confidentiality
Attack Vector.	Remote
Solution Status.	Vendor patch
CVE reference.	Not yet assigned

Details.

XOOPS is a content management system written in PHP. During an application penetration test Sense of Security identified that Input passed to the “op” parameter of viewpmsg.php, and in the query string of user.php are vulnerable to Cross-Site Scripting vulnerabilities. This occurred as a result of the application not properly filtering HTML tags which allowed malicious JavaScript to be embedded. When input is incorrectly validated and not properly sanitised and then displayed in a web page, attackers can trick users into viewing the web page and causing malicious code to be executed.

Proof of Concept.

http://IP/xoops-2.3.3/htdocs/modules/pm/viewpmsg.php?op="><script>alert('vulnerable')</script><link id='

http://lP/xoops-2.3.3/htdocs/modules/profile/user.php?"><script>alert('vulnerable')</script>

Solution.

Vendor patch

Discovered by.

SOS Labs.

About us.

Sense of Security is a leading provider of IT security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application security consultancy and trusted IT security advisor to many of the countries largest organisations.

Sense of Security Pty Ltd

Level 3, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: http://www.senseofsecurity.com.au
E: info@senseofsecurity.com.au

The latest version of this advisory can be found at:
http://www.senseofsecurity.com.au/advisories/SOS-09-005.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php