

# Multiple Vulnerabilities in Phorum 3.4.5

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-01/0038.html>

---

**From:** Calum Power (*enune\_at\_fribble.net*)

**Date:** 01/05/04

Date: Tue, 6 Jan 2004 09:03:37 +1100 (EST)

To: bugtraq@securityfocus.com

Phorum 3.4.5 Vulnerabilities

---

Credit:

Author: : Calum Power

Version(s) : <= 3.4.5

Vendor : Phorum

Vendor URL : <http://phorum.org>

Vendor Contacted: Yes

Vendor Fix: Phorum has released Phorum v3.4.6 as a response to this advisory. Please patch your vulnerable software ASAP.

Vulnerability:

Type: Cross-Site Scripting, SQL Injection

Severity: Moderately Critical

Summary:

Phorum versions prior to 3.4.6 are vulnerable to cross-site scripting and SQL injection bugs that could allow for the remote compromise of any server running the affected software.

Details:

VULN #1:

An XSS vulnerability exists in the script 'common.php' that allows arbitrary code

execution on the client-side browser.

Ironically, this vulnerability is in the 'phorum\_check\_xss()' function.

The vulnerable code is below:

```
if(!is_array($value) && $key!="body" && $key!="subject" && $key!="hide" && strpos($value, "<script")){
    echo "script detected in $key";
```

By sending a HTTP/POST variable to any Phorum script, an attacker could craft the key of the variable into

an XSS attack, providing the value of the variable contains the string "<script".

## SecurityFocus Bugtraq: Multiple Vulnerabilities in Phorum 3.4.5

\*\*\* This vulnerability has been fixed in Phorum 5.0.2alpha. \*\*\*

Severity: Medium – This vulnerability may be exploited to obtain user login details, spam, or perform social–engineering upon the user.

### VULN #2:

Another XSS vulnerability exists in the script 'profile.php'. This vulnerability exists via insufficient sanitization of the variable 'EditError'. If a user is logged on, an attacker could use this vulnerability to include arbitrary code on the user's browser.

NOTE: Phorum (common.php) does checks for '<script>' tags, however XSS attacks are NOT limited to just the <script> tags! An attacker could use many forms of XSS (such as <iframe>) to launch attacks upon users.

\*\*\* This vulnerability has been fixed in Phorum 5.0.2alpha. \*\*\*

Severity: Medium/Low – This can only be exploited when the user is logged on, but as such could be used to reset passwords, or change any other user info without the user knowing.

### VULN #3:

Once again, there is an XSS vulnerability in the script 'login.php' that may allow attackers to execute arbitrary code in the users' browser (Woah, deja moo...)

This exploit is due to (again) the 'Error' variable not being sanitized correctly.

I have created Proof–of–Concept code (using an <iframe>) that allows for the stealing of user passwords as they are submitted into the form.

\*\*\* This vulnerability has been fixed in Phorum 5.0.2alpha. \*\*\*

Severity: High/Critical – Due to the nature of the page, sensitive form values could be harvested by an attacker.

### VULN #4:

A SQL Injection vulnerability exists in the script 'register.php' in the field 'hide\_email'.

This vulnerability could lead to the execution of SQL commands inside the script.

\*\*\* This code appears to not exist in Phorum 5.0.2alpha, so is therefore fixed. \*\*\*

Severity: High – Due to the location in which the SQL injection variable is placed, it is increasingly hard to exploit this vulnerability to obtain any sort of privilege escalation.

--

Information Security is like decent coffee – When you have it it's blissful, but it disappears just as you get a taste for it.

- text/plain attachment: [advisory.txt](#)