

# [UNIX] Manti's Bug Listings of Private Projects Can be Viewed Through Cookie Manipulation

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0076.html>

---

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

*Date:* 08/21/02

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

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

Date: Wed, 21 Aug 2002 14:43:51 +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.

-----

Manti's Bug Listings of Private Projects Can be Viewed Through Cookie Manipulation

---

## SUMMARY

<<http://mantisbt.sourceforge.net/>> Mantis is an Open Source web-based bug tracking system, written in PHP, which uses the MySQL database server. It is being actively developed by a small group of developers, and is considered to be in the beta stage. A vulnerability in the product allows attackers to view private projects by manipulating their cookies.

## DETAILS

Vulnerable systems:

- \* Mantis version 0.17.3

Immune systems:

- \* Mantis version 0.17.4a
- \* Mantis version 0.17.4

In Mantis, a user can select a project from a drop-down menu. After selection, all bug listings will be limited to that project.

## Securiteam: [UNIX] Manti's Bug Listings of Private Projects Can be Viewed Through Cookie Manipulation

The 'View Bugs' page, which is responsible for displaying a list of bugs in a project, did not check whether the user actually had access to the project defined in the cookie. It trusted the fact that only projects accessible to the user were listed in the drop-down menu.

This provides a malicious user with an opportunity to display the 'View Bugs' page with a private project selected.

It should be noted that this bug does not allow a user to get any more information than is listed in the View Bugs page. The page with more information about the bug is not accessible. In addition, private bugs are still not visible in the list.

Workaround / Solution:

Mantis 0.17.4 adds the appropriate permission checks to the 'View Bugs' page. All users are recommended to upgrade to this version as soon as possible.

If an upgrade is not an option, `view_all_bug_page.php` can be patched to add the appropriate checks. To do so, add the following function to `core_user_API.php`:

```
# Check to see if the current user has access on the specified
project
function check_access_to_project( $p_project_id ) {
    $t_project_view_state = get_project_field( $p_project_id,
'view_state' );

    # Administrators ALWAYS pass.
    if ( get_current_user_field( 'access_level' ) >= ADMINISTRATOR ) {
        return;
    }

    # public project accept all users
    if ( PUBLIC == $t_project_view_state ) {
        return;
    } else {
        # private projects require users to be assigned
        $t_project_access_level = get_project_access_level( $p_project_id
);
        # -1 means not assigned, kick them out to the project selection
screen
        if ( -1 == $t_project_access_level ) {
            print_header_redirect( 'login_select_proj_page.php' );
        } else { # passed
            return;
        }
    }
}
```

## Securiteam: [UNIX] Manti's Bug Listings of Private Projects Can be Viewed Through Cookie Manipulation

And in view\_all\_bug\_page.php, replace the following lines:

```
$t_where_clause .= ');  
}  
} else {  
  $t_where_clause = " WHERE project_id='$g_project_cookie_val';  
}  
# end project selection
```

with the following lines:

```
$t_where_clause .= ');  
}  
} else {  
  check_access_to_project($g_project_cookie_val);  
  $t_where_clause = " WHERE project_id='$g_project_cookie_val';  
}  
# end project selection
```

Detailed explanation:

To take advantage of this vulnerability, the attacker would need to know the project\_id of the private project he wishes to attack. This is not terribly difficult to accomplish, as the project\_id starts at 1 and increases by one for every project created. The attacker can just try each integer starting at 1, until (s)he finds the one (s)he's looking for.

The next step is to log in to Mantis at least once, so that the MANTIS\_PROJECT\_COOKIE, or however the cookie is called in that particular set-up, is set. The user can then manually change the cookie locally, and fill in the desired project\_id. Now all the user has to do is visit /view\_all\_bug\_page.php, and the list of public bugs in that project should be displayed.

An alternative method is by forging the HTTP headers, to send the desired cookie value with a request for /view\_all\_bug\_page.php. The results are the same.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:jlatour@calaquendi.net>>  
Jeroen Latour.

=====

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](mailto: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)

=====  
=====

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): "[NT] WebEasyMail Multiple Security Vulnerabilities (User disclosure, DoS)"
- **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)