The Embedded Code can break it!

Author: Punit Ganshani
Email Address: punit@ganshani.com
Downloaded from http://www.ganshani.com
Online Source:
http://www.neworder.box.sk/forum.php?did=edge10864&thread=173545

Where at one end is security and popularity, there at other end hackers are always on their toes to accept the challenge of breaking into systems that claim to be secure. The ever-growing email services like Hotmail, Yahoo, Indiatimes may face many security threats. There are many ways hackers have discovered how passwords can be stolen, how personal information can be obtained, or how a person can track the business deals you are up to.

Myarticle describes a serious security problem with majority of email service providers. Nowadays, the number of email service providers has increased to a large number but quantity should not sacrifice the quality! Email Service Providers give large amount of space but forget about the security of data that the users transfer through their email account. Yes! Many of the famous email service providers allow malicious users to easily steal the passwords of their users.

It seems quite astonishing and amazing but its true! It's a simple exploit that a person with some knowledge of Javascript (or VBScript) can implement. It involves sending e-mail message that contains Javascript (or VBScript) code as part of the message.

When a victim views this message (having embedded Javascript (or VBScript) code), the embedded Javascript (or VBScript) code forces the user to re-login to his email account. And when the victim fills in the textboxes of username and password, he doesn't know that he is actually passing the most important information to the email sender (hacker). Do you know how hard is he hitting the axe on his foot? In doing so, the victim's username, password, and IP address is sent to the malicious user (sender) by e-mail.

Once a malicious user (hacker or email sender) knows the password to the victim's account, he can assume full control of the account, including the ability to:

- Delete
- Send
- Read the victim's e-mail
- Check mail on other mail servers that the victim has configured for mail-checking
  access the victim's address book
- Discover other passwords sent as confirmation of registration in old e-mails
  change the password of the his account

And for tycoon companies such exploits can be a threat to their business! The security problem is easy to take advantage of.

A hacker needs only to embed the Javascript (or VBScript) code into the body of an e-mail message using a standard e-mail program such as Netscape Mail (free).

This exploit is a serious security concern for the following reasons: The malicious code runs as soon as e-mail message is viewed

- The resources required to launch the attack are minimal and freely available.
- The malicious e-mail can be sent from virtually anywhere, including libraries, internet cafes, or classroom terminals
- The exploit will work with any Javascript (or VBScript)-enabled browser, including the Microsoft Internet Explorer and Netscape Communicator.

HOW THE EXPLOIT WORKS!

Why does the exploit work? The security problem lies in service itself.

Many of the Email Provider make no attempt to filter Javascript (or VBScript) code from email messages thus allowing malicious users to embed arbitrary Javascript (or VBScript) programs into their e-mail messages.

These Javascript (or VBScript) programs do not normally constitute a security problem when used in personal web pages. But it can have a great effect on the user-interface properties of the victim's account. In the case of the exploits, the Javascript (or VBScript) alters the properties of every link in the interface that the user could click on.

The links are altered so that when the user clicks on them, (bogus) message is displayed, informing the user that they have timed-out of their session and must log in again to continue.

The (bogus) time-out page also gives the user some text-entry fields where they can type in their username and password to re-login.

However, when the user types in their username and password, the information is sent back to the malicious user.

In the exploits, the part of the program that does the actual "dirty-work" of mailing the password and username is provided by Geocities as a (free) service to all their members. This should not be viewed as an oversight or problem with Geocities, since there are thousands of equivalent server-side mailing programs that we could have used in its place.

The exploit is just one of many potentially damaging Javascript (or VBScript) programs that could be embedded into mail messages!

HOW TO PROTECT YOURSELF FROM THIS EXPLOIT!

Until email service providers fix the security problem, I suggest that users turn off Javascript (or VBScript) in their browsers.

Netscape users can turn Javascript (or VBScript) off in their preferences (edit /

preferences / advanced / disable Javascript).

Microsoft Internet Explorer users can turn Jscript off in their preferences (view / internet options /
security / custom settings / scripting / disable active scripting).

Again, to say there's no specific way to protect yourself from this exploit if you are surfing from a cyber cafe. However if you are a good observer and are good at memory, you can definitely save your email account from being hacked.

Whenever you face with a page as shown before saying **TIMED OUT** or something like the same, before entering your username and password just open the source code and see what is written in the following line

<form name="passwordform" action="**SEE THIS**"
method="post" target="_top"
AUTOCOMPLETE="OFF" >

If this contains any text that hyperlinks to a webpage or script that doesn't belong to your email service provider, then the sender is trying to hack your account.

Second way is that you try to put a wrong password. If it doesn't show you the warning of wrong password then it may be an attempt to hack your account.

This security loop hole is not found in email services like Hotmail, Yahoo or Indiatimes because when show **Timed Out**, always have the username typed in the text box. Secondly timed out is not printed unless and until you are disconnected from internet or you are sitting idle for a very long time.