Software Engineering Institute
Carnegie Mellon University

Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites

CERT Division

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

http://www.sei.cmu.edu

REV-03.18.2016.0

Copyright 2017 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0052

Table of Contents

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

1 Introduction

A problem has recently been identified that can be found on a wide variety of web sites: what you receive from a web site may not be what that site meant to send. If you click on a specially designed link, the site may unknowingly send you bad data, unwanted pictures, and programs (malicious scripts) to compromise your data.

The problem is not with web browsers themselves but with how web pages are constructed and how data entering and leaving web sites is validated. "Validate" means ensuring no "unintended" characters are sent back to the client.

This document includes:

- Frequently Asked Questions
- Steps for Changing Your Options in Web Browsers

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

2 Frequently Asked Questions

How do malicious web scripts get to my web browser?

A malicious web developer may attach a script to something you send to a web site, such as a URL, an element in a form, or a database inquiry. When the web site responds to you, the malicious script comes along, so that it is now on your browser.

Among the ways you can potentially expose your web browser to malicious scripts are these:

- following untrusted links in web pages, email messages, or newsgroup postings
- using interactive forms on an untrustworthy site
- viewing dynamically generated pages that contain content developed by anyone but yourself

You might link to what you consider a safe site, complete a form on a site that is not trustworthy, or search a database there.

What might happen if my web browser is exposed to a malicious script?

Among the possibilities are capturing your password and other information you believe is protected. You should also be concerned because malicious scripts can be used to expose restricted parts of your organization's local network (such as their intranet) to attackers who are on the Internet.

Attackers may also be able to use malicious scripts to infect cookies with copies of themselves. If the infected cookie is sent back to a vulnerable web site and passed back to your browser, the malicious script may start running again. Note: This is not a vulnerability in web cookies; rather, a malicious script takes advantage of the functionality of cookies.

How can I avoid the problem?

The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Follow the steps below to turn off options in your web browser that allow malicious scripts to run. If you're not using a current version of Netscape or Internet Explorer, (version 4 and 5, respectively), you might need to modify the steps.

Note that even with scripting disabled, attackers may still be able to influence the appearance of content provided by a legitimate site by embedding other HTML tags. In particular, malicious use of the< FORM> tag is not prevented by disabling scripting languages.

How will turning off the options affect my use of the web?

Turning off the options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some web sites. You may notice a difference in functionality when you visit legitimate sites that use scripts running within the browser to add useful features.

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Should I disable Java applets?

The risk associated with Java applets is significantly different from some of the other technologies. Java has a robust security mechanism designed to deal with situations like these that prevents sensitive information from being disclosed or client information from being damaged.

However, Java applets written by an attacker can still be loaded while your are viewing a legitimate web page. The problems that can arise are similar to those involving the <FORM> and other HTML tags. For example, an attacker could develop a "Trojan Horse" program that presented misleading information and prompted you for a password. If you failed to recognize the malicious applet for what it was, you could accidentally disclose sensitive information.

You must make your own determination about disabling Java applets, based on your tolerance for these risks. If you choose to disable Java, please see the detailed instructions below.

Isn't there a better way to fix the problem?

The CERT/CC is working with technology vendors and other security experts on a long-term, comprehensive solution to the problem of malicious scripts running on browsers.

Is there any more information available about this problem?

The CERT/CC has published an advisory containing more details about the problem, its impact, and ways to deal with it. CA-2000-02 is available from http://www.cert.org/advisories/CA-2000-02.html

You can also find information at the vendor URLs listed in the advisory.

The CERT/CC has also published a "tech tip" for web page developers and web site administrators, which you might want to pass along to the appropriate people in your organization. This document, "Malicious Content Mitigation for Web Developers," is available from http://www.cert.org/tech_tips/malicious_code_mitigation.html

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

3 Steps for Changing Your Options in Web Browsers - Netscape and Internet Explorer

Using Netscape 3.0 or higher

Note: If you are not using Netscape version 3.0 or higher, these instructions may not be correct. To determine your software version, from the **Help** menu, select **About Communicator...** . A web page appears with information about your browser including the version number.

1. Start Netscape Communicator as you would when browsing the Internet.
2. From the **Edit** menu, select **Preferences**. The Preferences dialog box appears.
3. From the **Category** list, click on **Advanced**. (Do NOT click on the plus (+) sign.) The Advanced Preferences panel appears.
4. If you decide to disable java, uncheck **Enable Java**.
5. Uncheck **Enable JavaScript**.
6. Click **OK** to accept the changes.
7. Click the **Padlock Icon** in the lower left hand corner of your browser. The Security Info dialog box appears.
8. Click the **Navigator** link from the list on the left. The Navigator Security Settings panel appears.
9. In the **Show a warning before:** section, make sure the options **Viewing a page with encrypted/unencrypted mix** and **Leaving an encrypted site** are checked.
10. Click **OK** to accept the changes and close the dialog box.

Using Internet Explorer 5

Note: If you are not using Internet Explorer version 5, these instructions may not work correctly. To determine your software version, from the **Help** menu, select **About Internet Explorer... .** A dialog box appears with information about your browser including the version number.

1. Start Internet Explorer as you would when browsing the Internet.
2. From the **Tools** menu select **Internet Options...** . The Internet Options dialog box appears.
3. Select the **Security** tab. The Security Options panel appears.
4. Click on the **Internet** zone to select it.
5. Click the **Custom Level** button. The Security Settings panel appears.
6. Select the **High** option from the pull-down list.
7. Click the **Reset** button. A dialog box appears asking if you are sure you want to change the security settings for this zone.
8. Click **Yes**. You now need to scroll through the settings list and make the changes listed in the following steps.
9. For the setting **Scripting ActiveX controls marked safe for Scripting**, check the radio button for **Disable** or **Prompt** depending on your level of trust.
10. If you decide to disable Java, for the setting **Java permissions**, check the radio button for **Disable Java**. Note: If you have Microsoft Virtual Machine installed, this setting will be under the **Microsoft VM** section. If you do not have a **Java permissions** setting, Java is already disabled.
11. For the setting **Active scripting** under the **Scripting** section, check the radio button for **Disable**.

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

12. Click **OK** to accept these changes. A dialog box appears asking if you are sure you want to make these changes.
13. Click **Yes**.
14. In the Internet Options dialog box, click the **Advanced** tab. The Advanced Options panel appears.
15. Make sure the setting **Warn if changing between secure and insecure** under the **Security** setting is checked.
16. Click **Apply** to save your changes.
17. Click **OK** to close the Internet Options dialog box.

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.