Advanced Information Security

Corporation

Advanced Information Security Corporation
Security Advisory Report

Mediafire Open URL Redirection

Report Date	30/04/2014
Final Report	Nicholas Lemonias
Stakeholders	Mediafire LLC
Service	www.Mediafire.com

Threat Level: Medium

Severity: Medium
CVSS Severity score: 5.0
Impact: Integrity, Confidentiality, Availability.

Mediafire Reference: #2014030910000639

Vulnerability:

(1) **Open URL Redirect Vulnerability**

Vendor Overview

Mediafire is a file hosting, file synchronization, and cloud storage service based in Shenandoah, Texas. Founded in June 2006 by Derek Labian and Tom Langridge, the company provides client software for Microsoft Windows, Mac OS X, Linux, Android, iOS and web browsers. Mediafire has 37 million registered users and attracted 1.3 billion unique visitors to its domain in 2012. MediaFire was ranked 10th in the "The Fastest Growing Cloud Apps of 2014" by SkyHigh Network [1] [2].

Description

The application is vulnerable to an unvalidated open redirect. The application permits unvalidated user-controlled input, which could force the web application into redirecting visitors to a heterogeneous third-party website. It is pertinent to note that the attack surface can be escalated visitors may be subject to phishing attacks, session hijacking, malware prograpagation, denial of service, or even remote code execution [3] [4]. The attack vector affected authenticated and unauthenticated users of the Mediafire website.
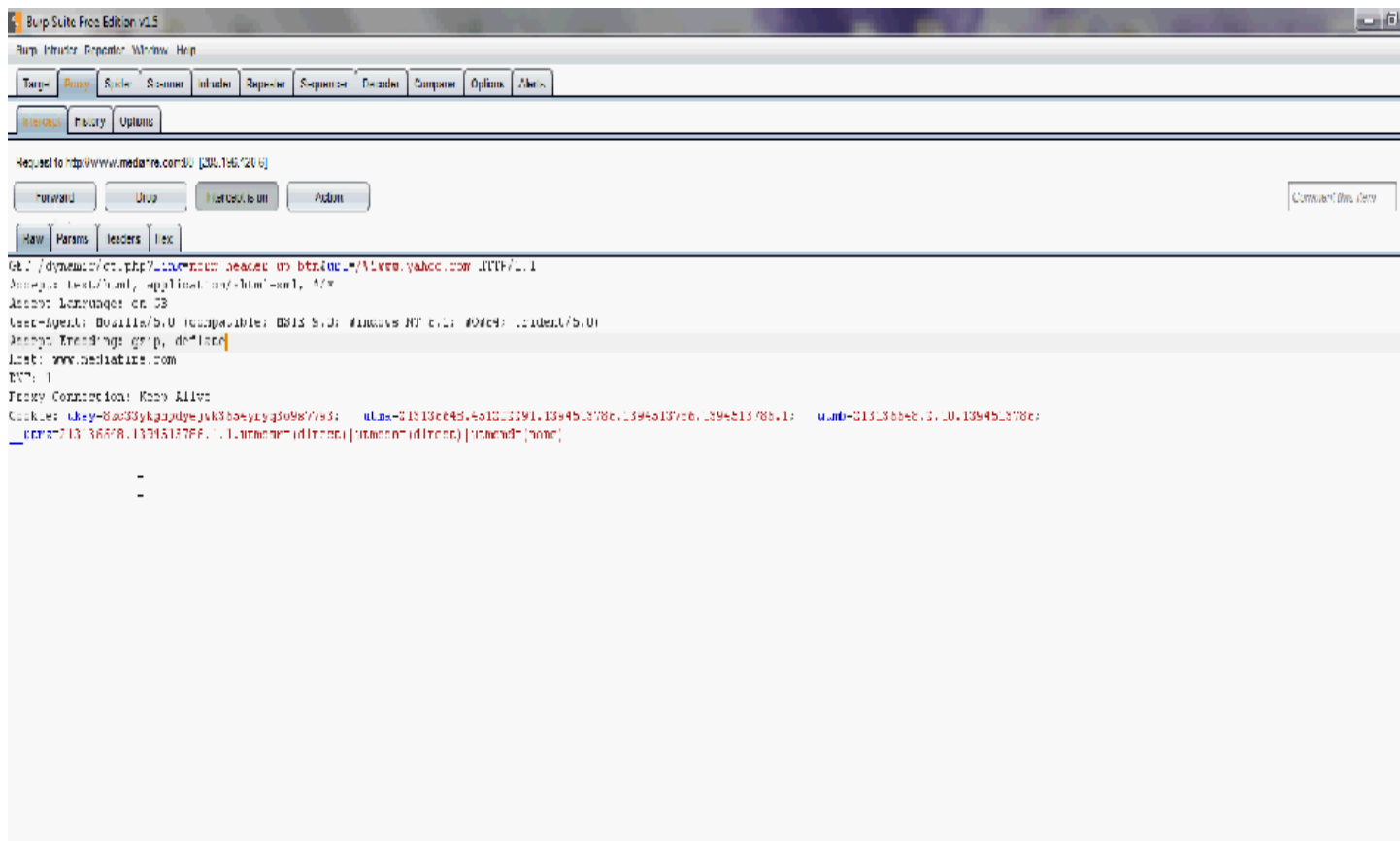
Appendices

Proof of Concept Image 1 – Mediafire LLC website
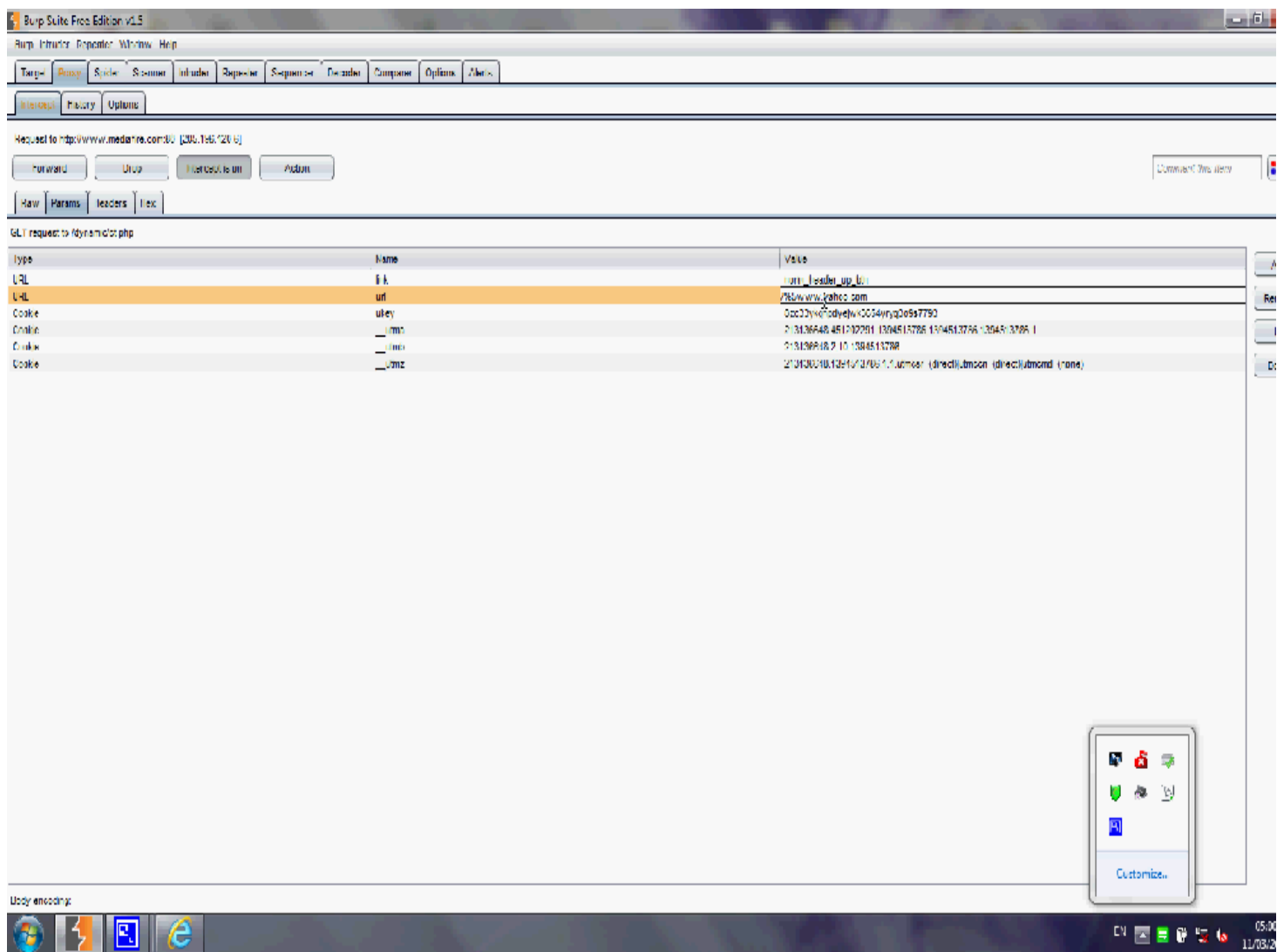
Proof of Concept 1:

http://www.mediafire.com/dynamic/ct.php?link=norm_header_up_btn&url=%2F%25%77%77%77%2E%79%61%68%6F%6F%2E%63%6F%6D%20%20

Proof of Concept Image 2 – Mediafire LLC website

Description

Parameter &url lacks adequate security validation controls. As a result, a malicious user can force the web application to send an http redirection code to the client, redirecting to a third-party website.

Proof of Concept Image 3 – Mediafire LLC website
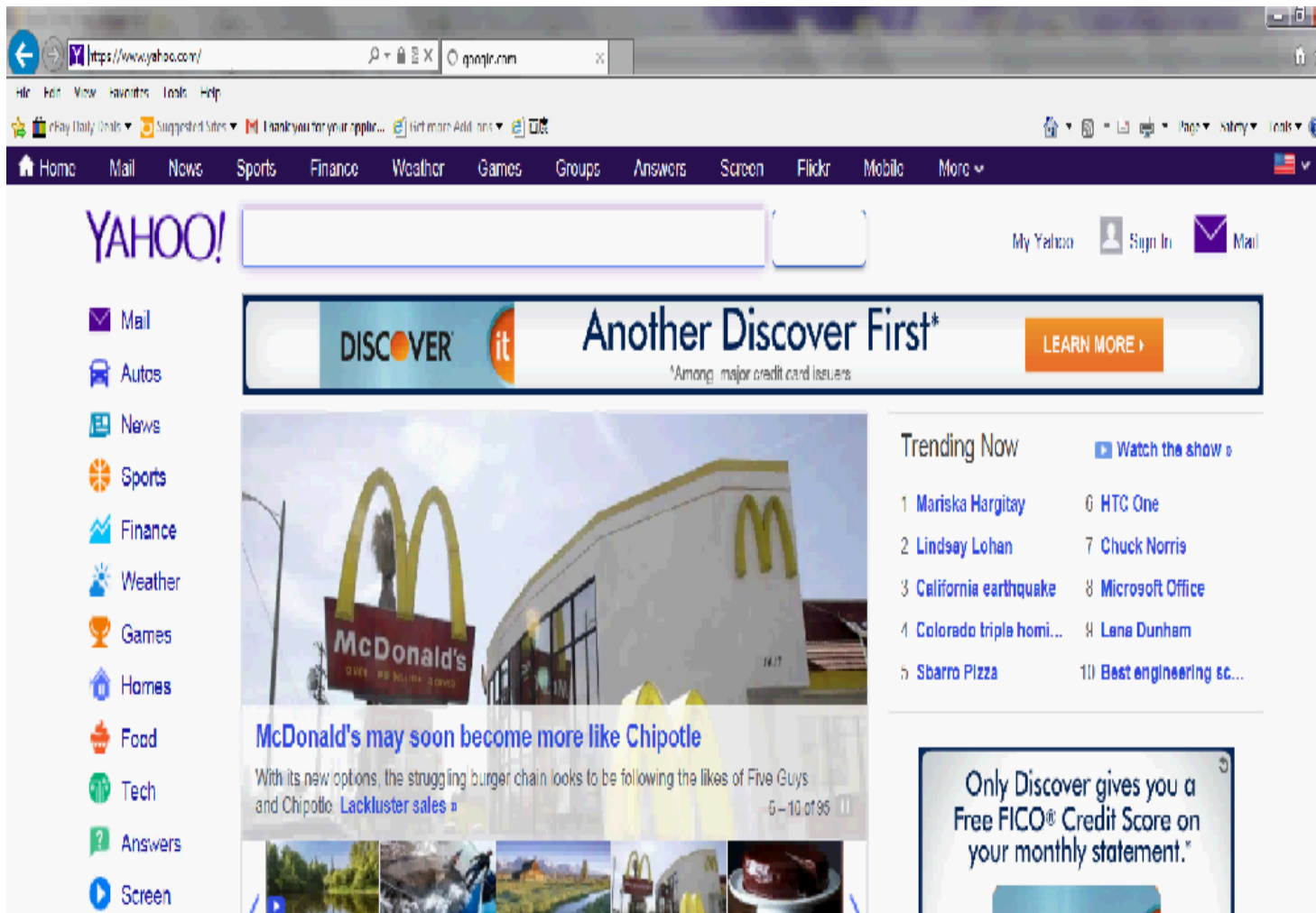
Description

Demonstration of an unsafe redirect to a heterogeneous third-party website ("www.yahoo.com").

References

[1] Mediafire Acknowledgement (2014). | *Mediafire.com Acknowledgement* [Online] Available at:
http://www.mediafire.com/view/mm71zzhufcdid45   [Last Accessed 11 March. 2014]

[2] Wikipedia (2014). *Mediafire | Wikipedia Mediafire.com.* [Online] Available at:
http://en.wikipedia.org/wiki/MediaFire   [Last Accessed 11 March. 2014]

[3] Microsoft Internet Explorer Vulnerability (2014). *Microsoft | Microsoft Security Advisory* [Online] Available at:
https://technet.microsoft.com/en-us/library/security/2963983.aspx [Last Accessed 26 April. 2014]

[4] OWASP (2014). *OWASP | Open Redirect – OWASP* [Online] Available at:
https://www.owasp.org/index.php/Open_redirect [Last Accessed 11 March. 2014]