Advanced Information Security

Corporation

06/01/2015

Advanced Information Security Corporation

Security Advisory Report

Microsoft Network (MSN) Multiple Vulnerabilities

Web Application Security Notification

Services Affected: www.Msn.com
Type: Web Application Vulnerabilities
MSRC Reference: [21027cl]

Threat Level: High
Severity: High
CVSS Severity Score: 7.8

Impact Type: Complete confidentiality, integrity and availability violation.

Vulnerability:
Filtration Bypass.
Authenticated/Unauthenticated Cross-Site Scripting.
Resource access via Uniform Resource Identifier (URI) scheme abuse. [2]
Command and parameter injections on local software.

Vendor Overview

Microsoft Corporation is an American multinational corporation headquartered in Redmond, Washington, that develops, manufactures, licenses, supports and sells computer software, consumer electronics and personal computers and services. Its best known software products are the Microsoft Windows line of operating systems, Microsoft Office suite, and Internet explorer web-browser.

Microsoft is the number one vendor and world's largest vendor by revenue. Microsoft was founded by Bill Gates and Paul Allen in 1975.

Service Overview

MSN (Originally the Microsoft Network) is a collection of Internet websites and services provided by Microsoft Corporation. The new re-launched service as of 2014, features 12 sections consisting of weather, news, sports, money, health & fitness, food and drink, travel, autos, video, entertainment and lifestyle. The top of the homepage provides access to popular sites like Outlook.com, Facebook, Twitter, OneNote , OneDrive and Skype. It is pertinent to note that, www.MSN.com has more than 415 million visitors worldwide, every month. [4]

Description

A malicious user could get unsuspecting visitors into divulging their credentials, to force a redirection to a heterogeneous third-party website, or to execute malicious code, on behalf of the attacker. An attacker can also fold malicious content into the content being delivered to visitors on the site.

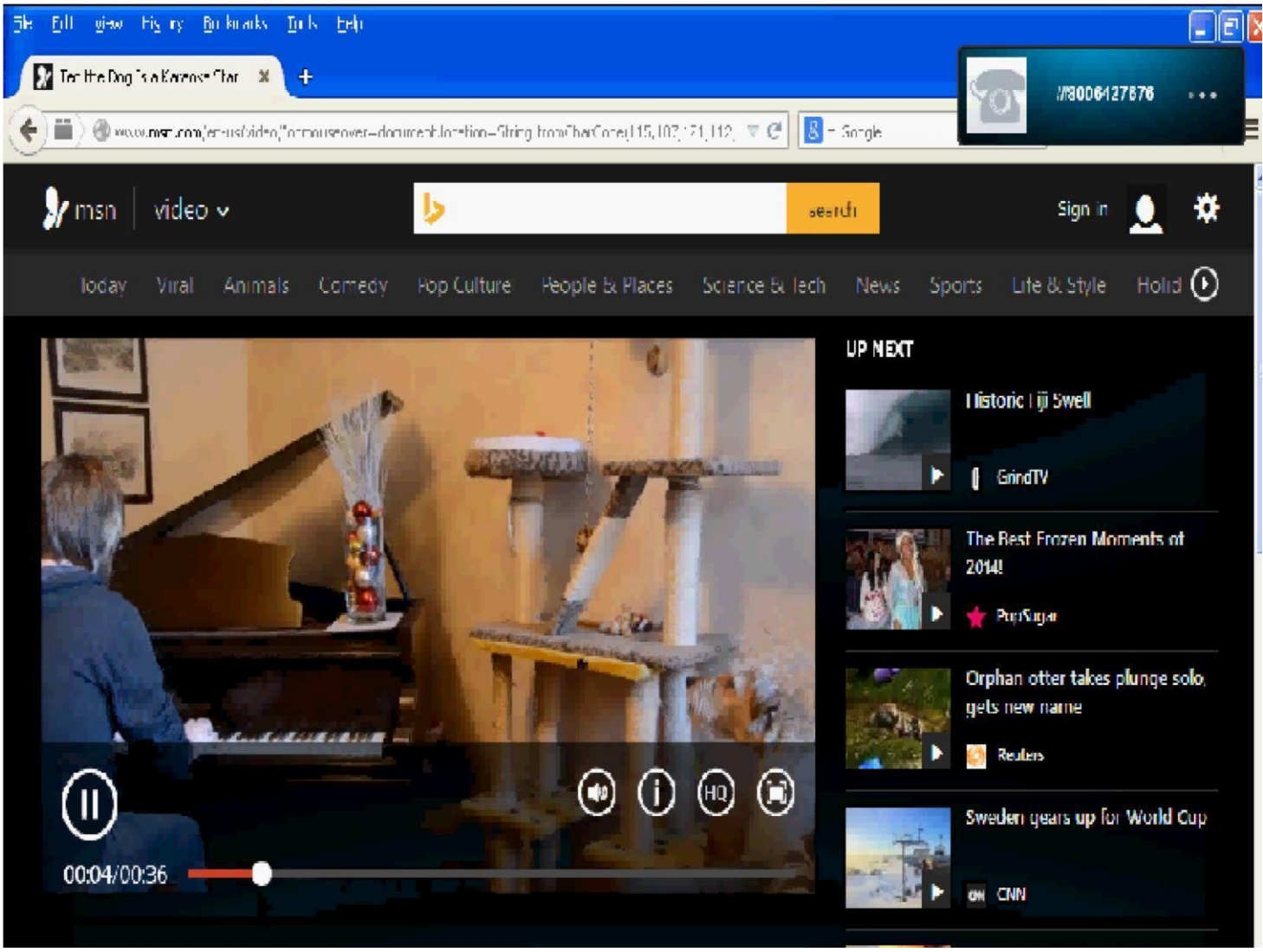
A malicious user can launch software installed locally on the visitor's Operating System, by injecting commands and software parameters via Uniform Resource Identifier schemes. A malicious user could inject local commands to the application called, with the privileges of the user visiting the website [2].

An already registered ("malicious") application, with a custom URI scheme in registry, can also be executed remotely.

In this attack "**Visitor** -> **Vendor**" trust-levels are directly impacted, since the vendor's website, and associated services have high levels of trust.

Appendices

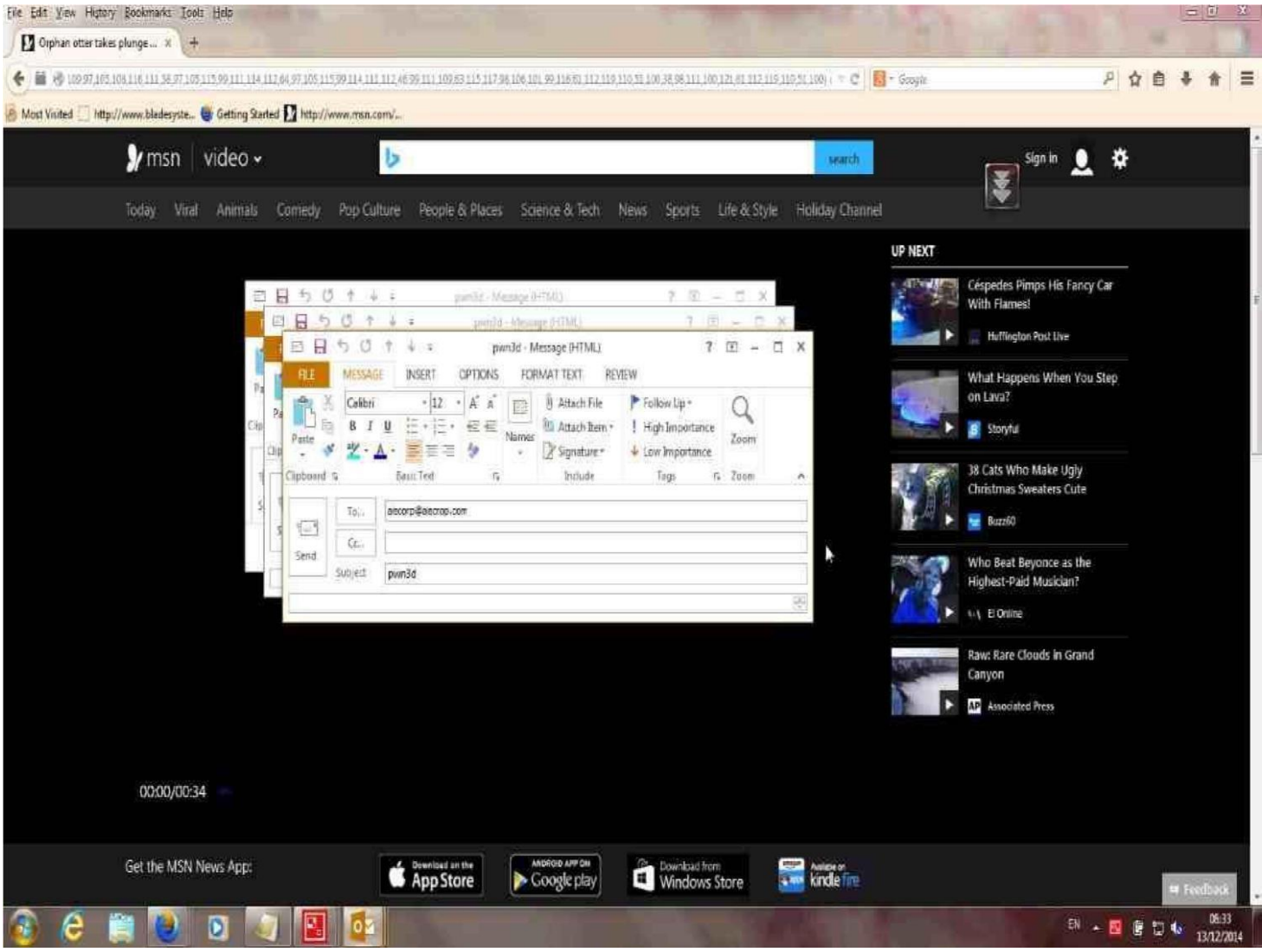
Proof of Concept Image 1



Description

Attack surface launches Skype, and initiates a Skype call to a third-party number, or username, just by visiting the affected page, and moving the mouse pointer onto a page element.

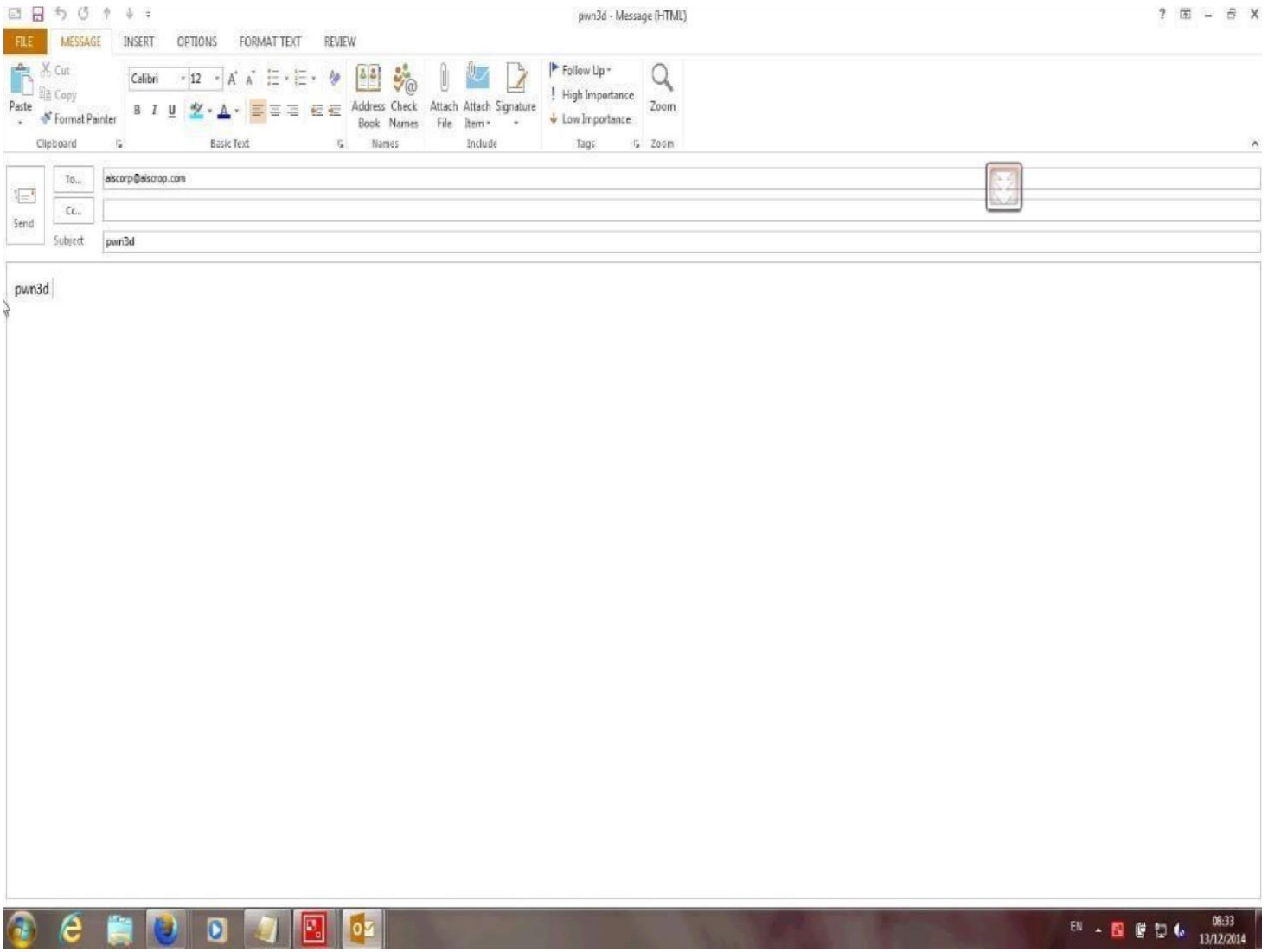
Proof of Concept Image 2



Description

Outlook software launch. Mail command injection proof of concept.

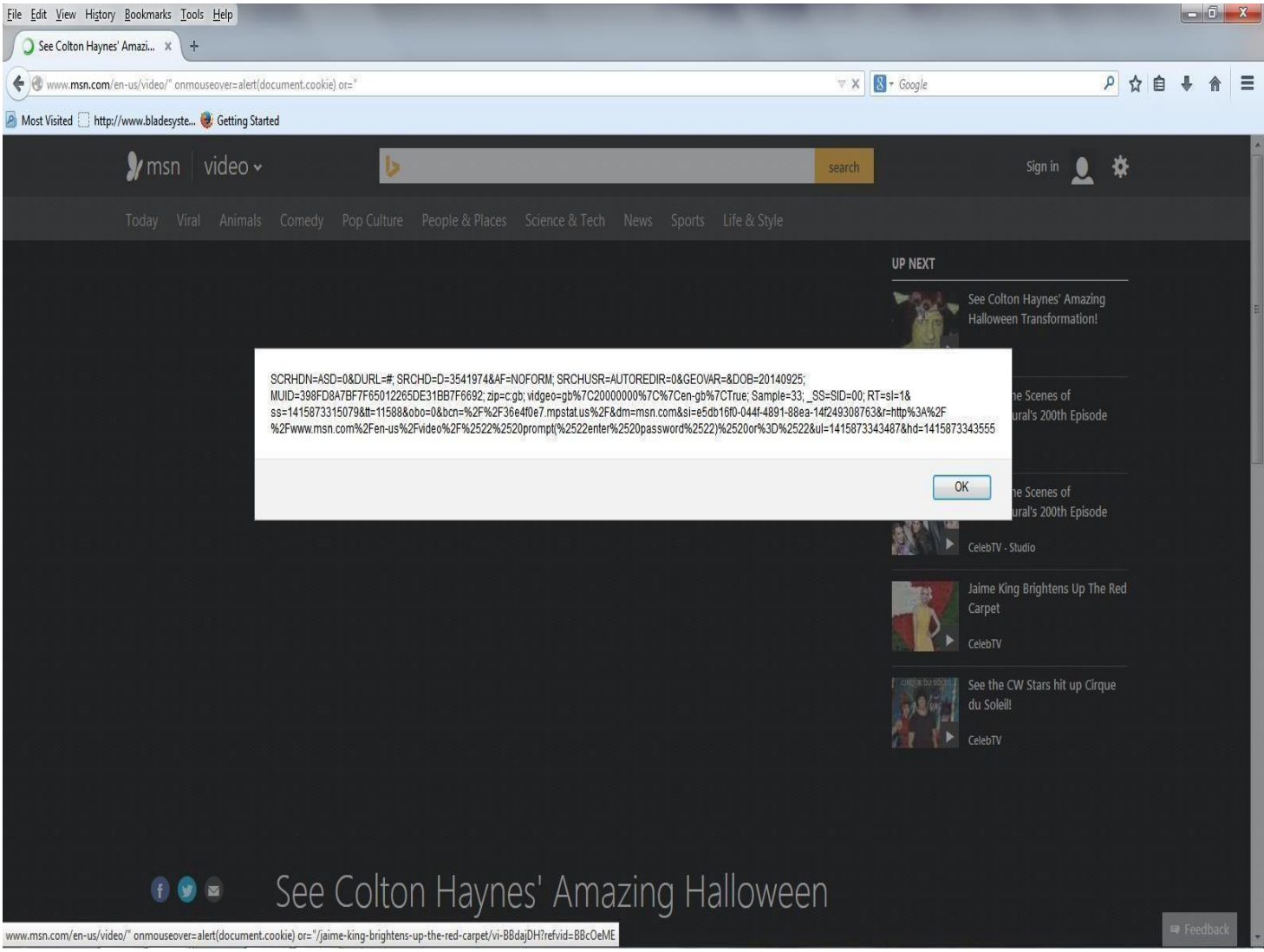
Proof of Concept Image 3



Description

Launch of software installed locally on the visitor's Operating System, by injecting commands via URI schemes. In the above example Outlook is launched with certain parameters.

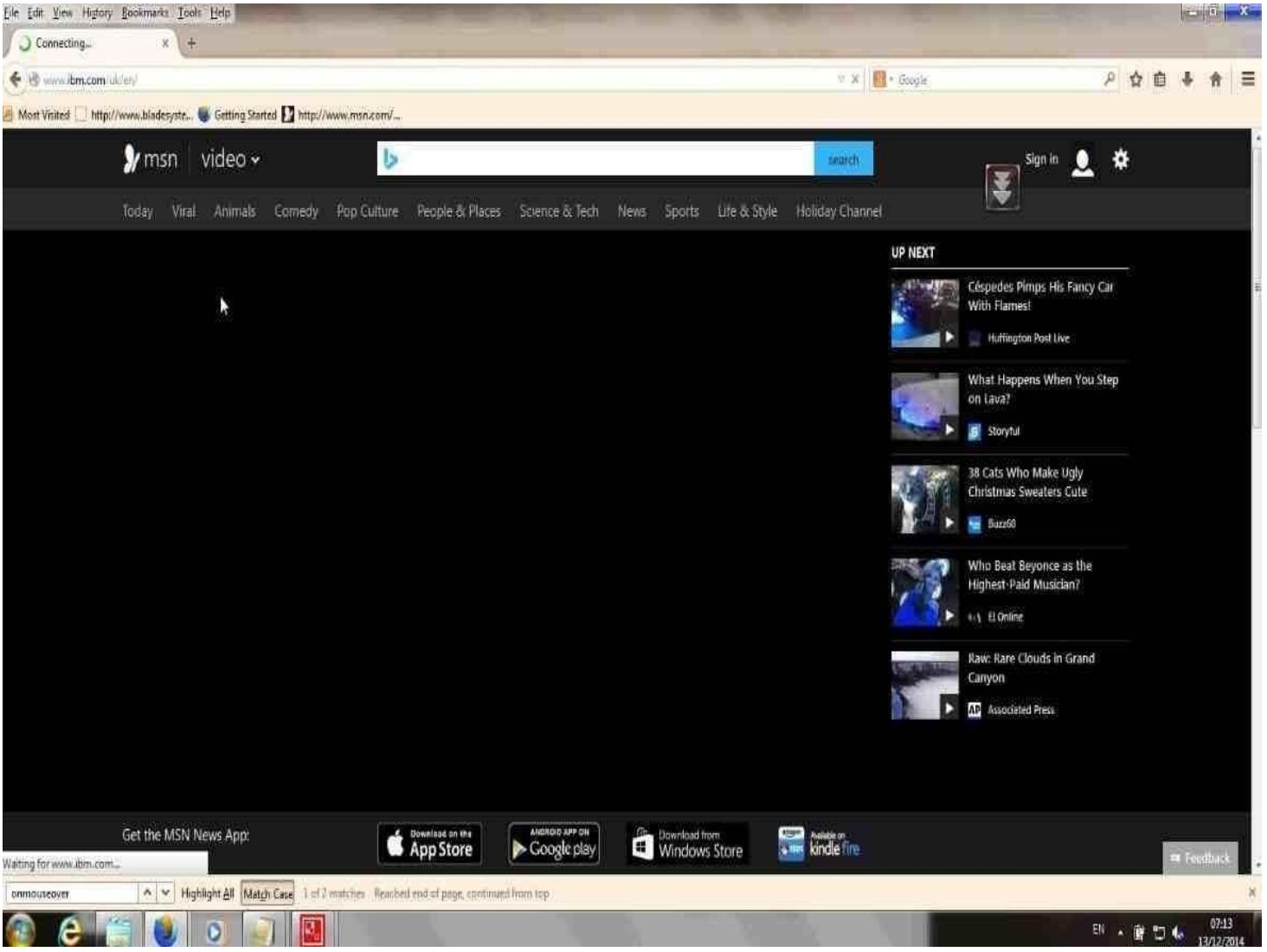
Proof of Concept Image 4



Description

Unauthenticated Cross-Site Scripting with preview of document. Cookie.

Proof of Concept Image 5



Description

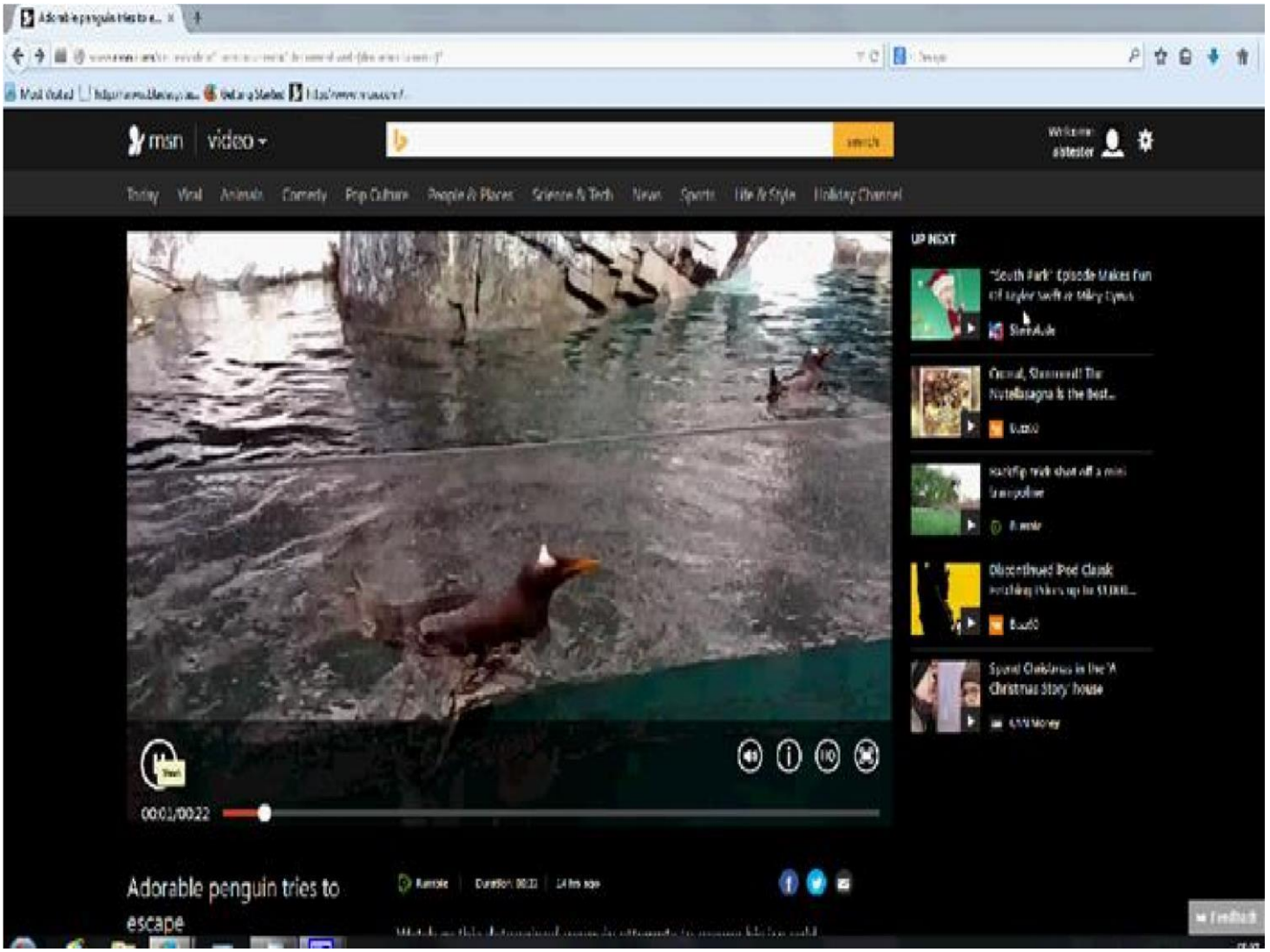
A malicious user could escalate the attack, by redirecting to a malicious website with an embedded payload. In a web-based attack scenario, an attacker could host a specially crafted website to leverage the attack surface. [3] Proof of Concept redirection to a third-party website ("www.ibm.com").

Proof of Concept Image 6

Description

A malicious user could escalate the attack, by redirecting to a malicious website with an embedded payload. In a web-based attack scenario, an attacker could host a specially crafted website to leverage the attack surface. [3] Proof of Concept redirection to a third-party website ("www.ibm.com").

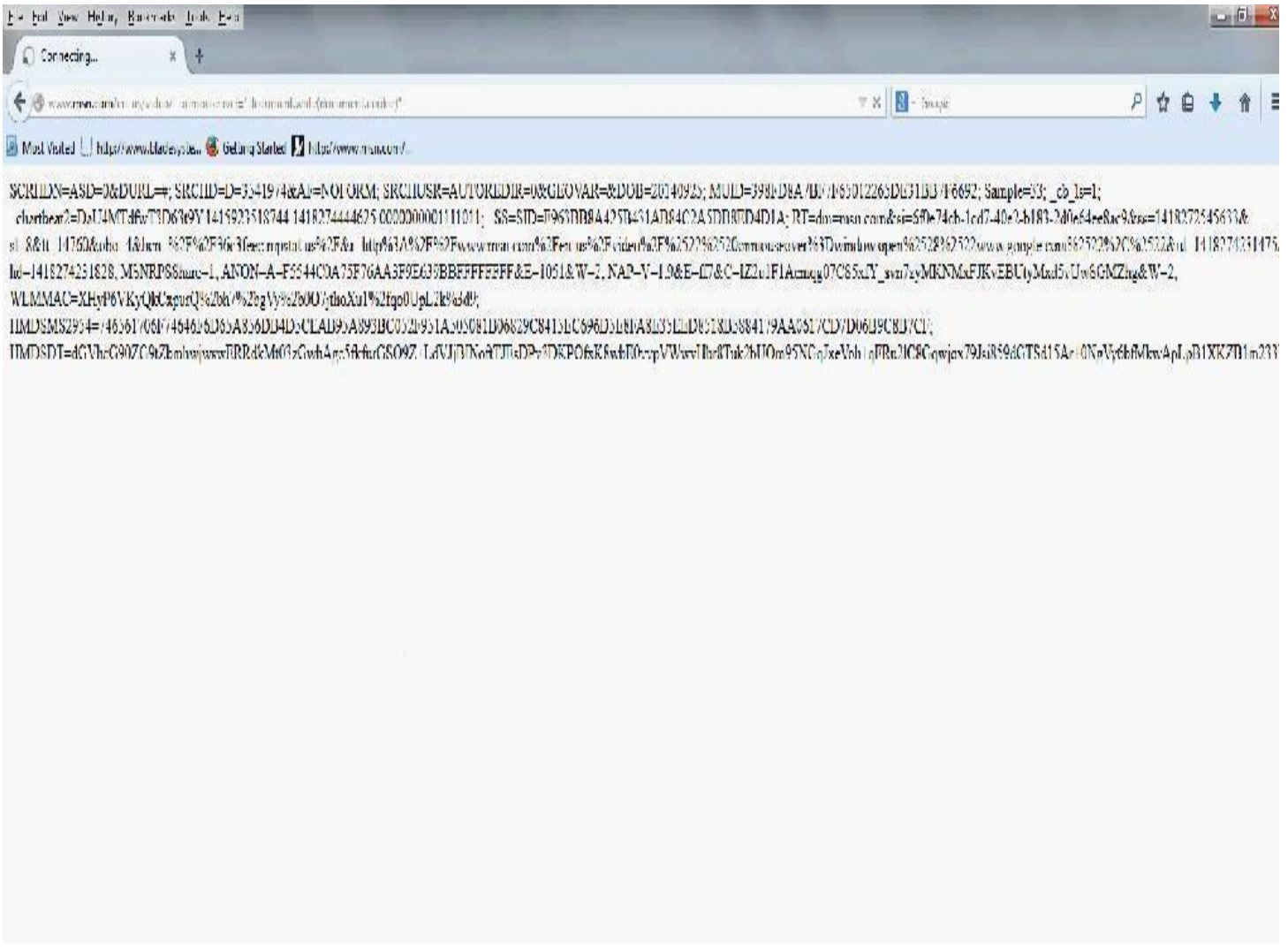
Proof of Concept Image 7



Description

Authenticated Cross-Site Scripting with preview of (document.cookie).

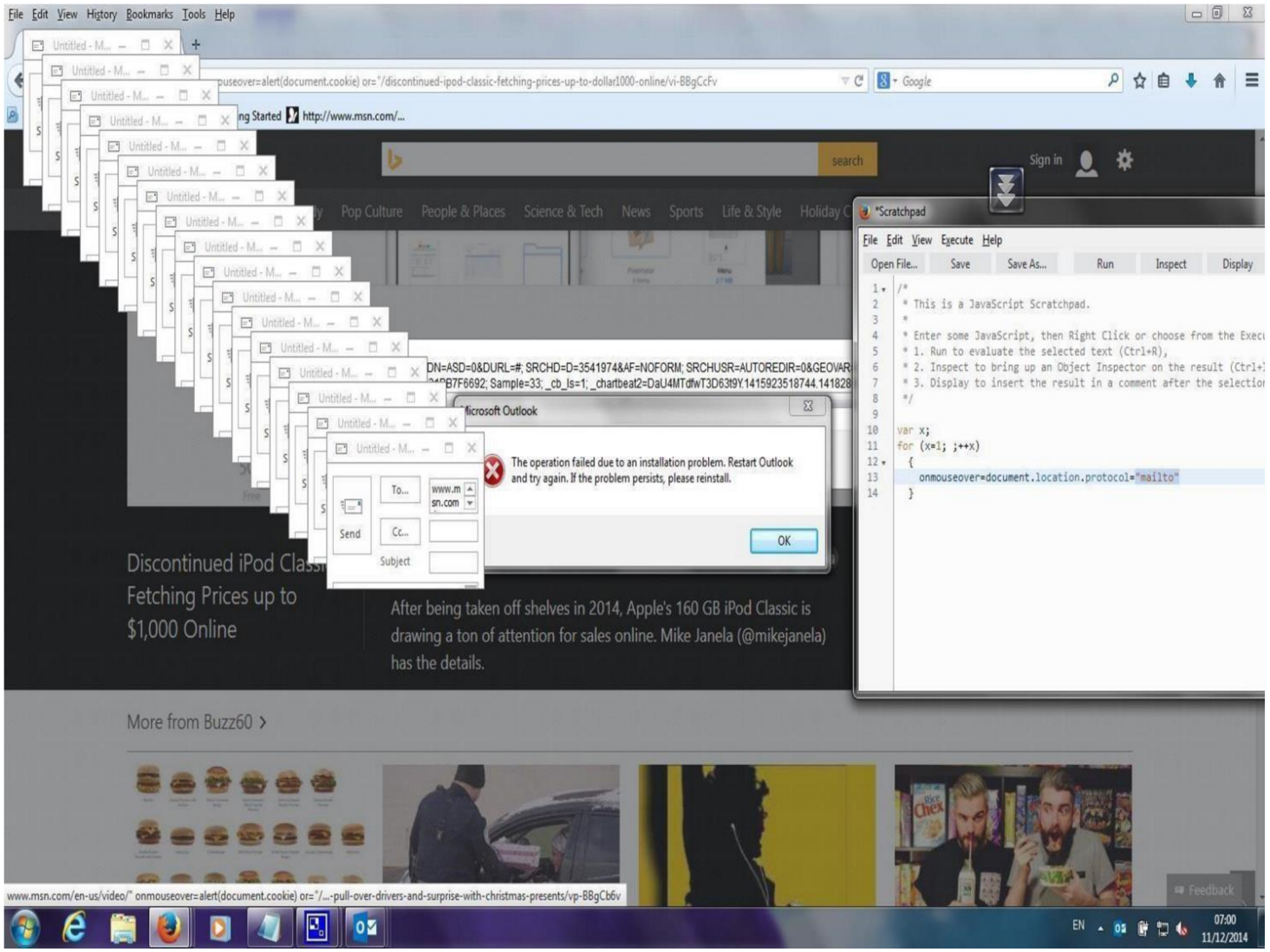
Proof of Concept Image 8



Description

Authenticated Cross-Site Scripting with preview of document.write (document.cookie).

Proof of Concept Image 9



Description

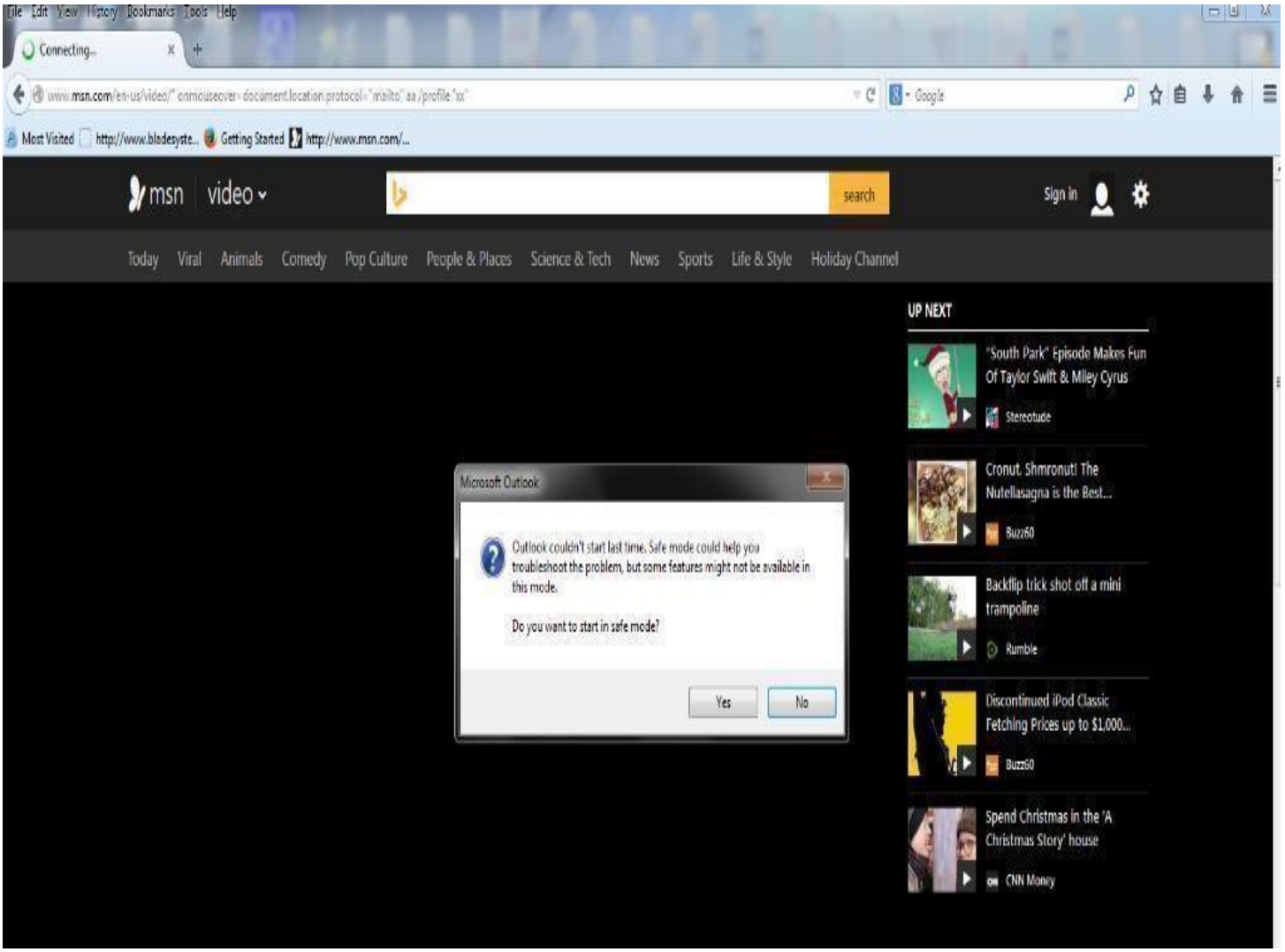
Denial of Service attack of local programs and O/S resource exhaustion on the visitor's operating system.

Proof of Concept Image 10

Description

Image demonstrating the possibility of document.write and user content fabrication by a malicious user.

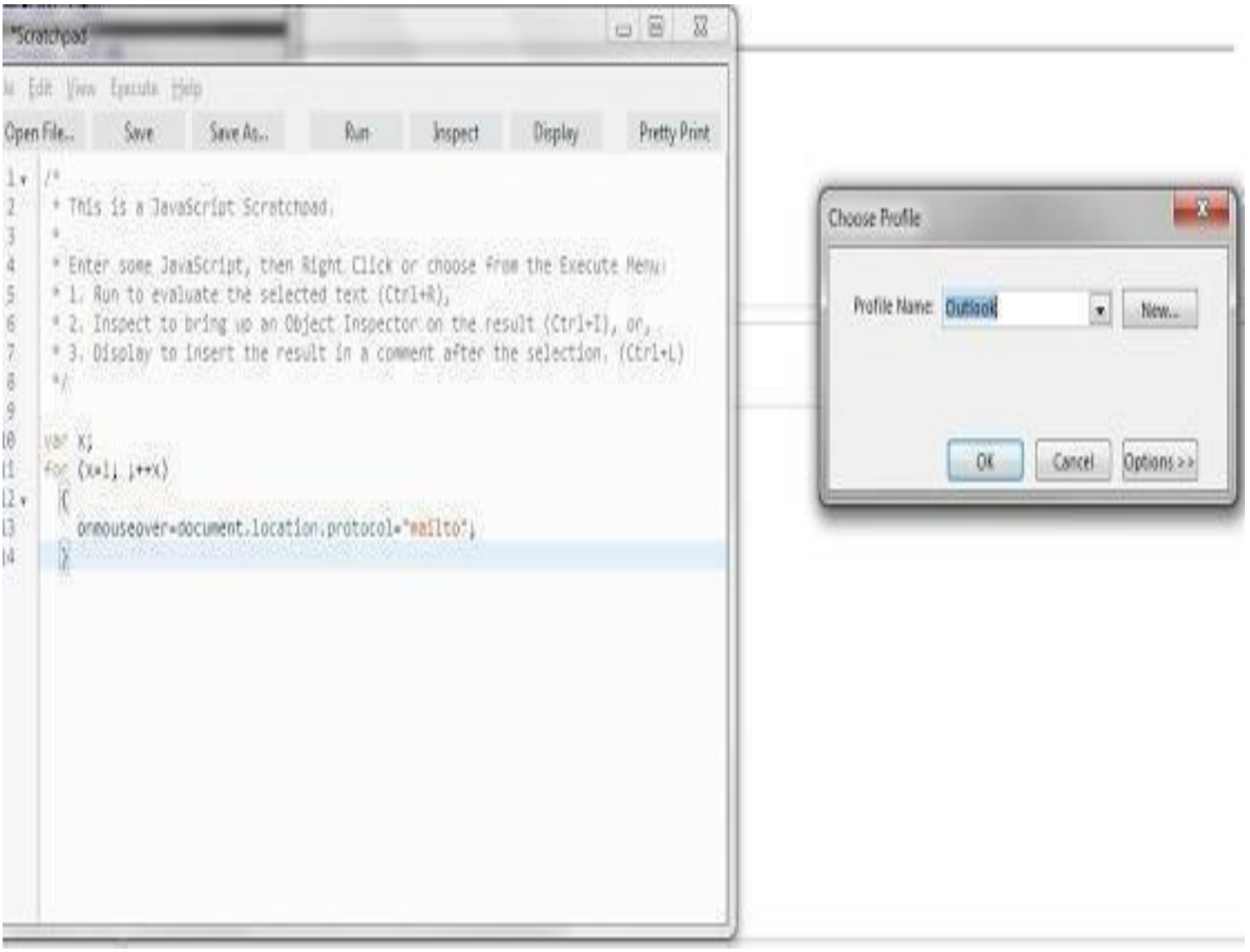
Proof of Concept Image 11



Description

Attempts to load Microsoft Outlook with different parameters. In this Proof of Concept the parameters used are **/safe** and **/profile**.

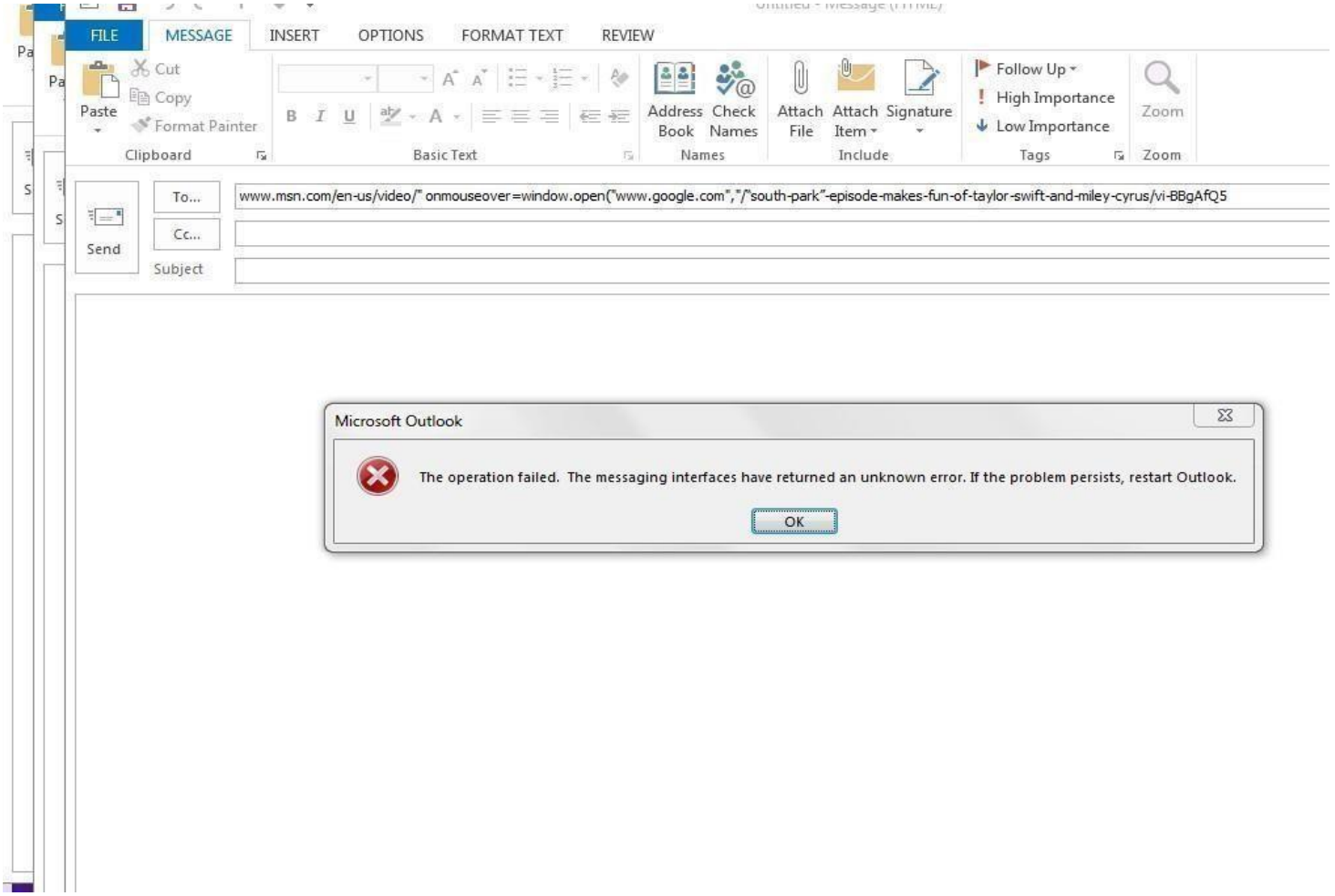
Proof of Concept Image 12



Description

Unexpected behavior caused by local command injections. The above picture demonstrates an Outlook profile corruption, as a result of certain parameters parsed to the called program.

Proof of Concept Image 13



Description

Unexpected behavior caused by local command injections. The above picture demonstrates an Outlook profile corruption, as a result of certain parameters parsed to the called program.

Appendices

Microsoft Corporation was prompt to circulate a remediation for the issue. Sincere thanks to Microsoft Corporation for the excellent cooperation and prompt response to the issue.

References

[1] Microsoft Corporation (2015). *December 2014*, Security *Researcher Acknowledgments - Microsoft Online Services | TechNet*. [Online] Available at: http://technet.microsoft.com/en-us/security/cc308589.aspx [Last Accessed 6 Jan. 2015]

[2] Microsoft Corporation, (2015). *URI schemes (Windows)*. [Online] Available at: http://msdn.microsoft.com/enus/library/windows/apps/jj655406.aspx [Last Accessed 6 Jan. 2015]

[3] Microsoft Corporation, 2015. 'Microsoft Security Bulletin MS14-021 - Critical'. https://technet.microsoft.com/enus/library/security/ms14-021.aspx [Last Accessed 6 Jan. 2015]

[4] Microsoft News Site. 2015. http://news.microsoft.com/download/presskits/msn/docs/msnfactsheet.docx. [Last Accessed 6 Jan. 2015]