

Information Technology
Information and Systems Security/Compliance
Information Security Vulnerability Assessment Program
Version: 1.3

Refer all questions and recommendations concerning this document to:
Information & Systems Security/Compliance
E-mail: security@northwestern.edu
Phone: 847-467-3569

Revisions

Date Version Modified By Comments

06/28/07 1.0 D. Kovarik Initial publication
7/11/08 1.1 J. Holland and D. Kovarik
4/17/2012 1.2 T. LeKan and D. Kovarik
10/8/2015 1.3 T.LeKan and D. Kovarik
Updated to reflect changes in ISS/C Staffing and Software

Contacts

Tim LeKan,
t-lekan@northwestern.edu
Office: 847-467-3569

Roger Safian,
r-safian@northwestern.edu
Office: 747-467-6437

Mary Carp
mary.carp@northwestern.edu
Office: 847-467-5996

Dave Kovarik
david-kovarik@northwestern.edu
Office: 847-467-5930

Table of Contents

Revisions.....	1
Contacts.....	1
Overview.....	3
What is a Vulnerability Assessment?.....	3
Focus of Assessment	4
How to Request a Vulnerability Assessment.....	4
Reports and Remediation	4
Resources/References	5

Overview

To help properly secure the University's information technology assets, Information & Systems Security Compliance (ISS/C) has developed the Vulnerability Assessment Program to help University departments assess the security of their networked assets. The activities involved in the Vulnerability Assessment Program may include the scanning of desktops, laptops, servers, Websites, and other computer systems owned by the University, or otherwise attached to the University network. Assessments may be performed on a regular (scheduled) or ad hoc basis to discover vulnerabilities that may be present on these systems.

The scanning of Northwestern's networked devices for vulnerabilities is driven by the information security standards adopted by Northwestern that call for periodic and methodical assessments (i.e., scans) capable of producing comparable and reproducible results; NUIT's Vulnerability Assessment Program complies with these standards.

Armed with the knowledge of these vulnerabilities, departments can apply security fixes or other compensating controls to improve security. The program provides for a menu of services for selection by the client, including:

- review of the Client's network infrastructure through review of documents, configurations, and network diagrams;
- network-based assessment of workstations, servers, and devices;
- network-based assessment of web applications;
- general and technical security consulting before, during and after the Assessment;
- documentation and reports, with additional consulting as needed; educational presentations relevant to the Assessment (e.g., vulnerability reduction)

While there is no charge to the Client for these assessment services, there is the expectation that the Client will take appropriate action to resolve high-risk vulnerabilities in a timely manner to prevent their exploitation. ISS/C can provide technical assistance in the remediation effort.

What is a Vulnerability Assessment?

A Vulnerability Assessment is a collaborative process, performed at the direction of the Client, that helps determine whether a network device or an application is susceptible to a known vulnerability, primarily through reconnaissance activities (e.g., testing for specific ports that are listening, identifying the operating system and patch levels, etc.). The Assessment does not actually exploit a vulnerability, rather it identifies the presence of a known vulnerability so that remedial action may be taken by the Client. While every attempt is made not to disrupt operations during the course of an Assessment, there is a possibility of adverse impact (e.g., system crash, lack of or slow response, etc.), most notably in instances where the system is poorly configured or has a high degree of vulnerability.

Focus of Assessment

The focus of the Vulnerability Assessment Program is a University-wide program with special attention and prioritization given to the following:

- Clients receiving a feed of NetIDs and passwords for their departmental Domain Controller.
- Clients that process University data identified and classified as “Legally/Contractually Restricted” (e.g., FERPA, HIPAA, FISMA, etc.).
- Clients requesting additional assistance with auditing/assessing their network infrastructure or specific devices for vulnerabilities.
- Other instances where high-value data is existent.

How to request a Vulnerability Assessment (VA)

The following outlines how to request an assessment and what information is needed:

- A client may request a VA be performed through an informal written request. A suggestion by ISS/C to conduct an assessment on a system may also be sufficient.
- Identify the target of the scan; this is the range of IP addresses assigned to or “owned” by the Client and/or URLs for owned websites.
- Permit the appropriate network and/or physical access to the Client networks and resources, e.g. firewall rules, user accounts for “Authenticated Scans”, etc.
- Confirm the date and time of the scan. Recurring or scheduled scans can also be established.
- Establish the contact list for setup and remediation.
 - Individual systems owners, systems Admins and other support personnel as appropriate.

Reports and Remediation

Documentation of the results will be provided to the Client. Where necessary, a remediation plan will be discussed with the Client along with scheduling subsequent assessments.

See Appendices for sample reporting.

Resources/References

Policies, Standards and Bench Marks

- Center for Internet Security - <http://www.cisecurity.org>
- SANS – System Administration and Security
 - Sample Policies - <http://www.sans.org/resources/policies/>
 - Misc Resources - http://www.sans.org/free_resources.php
- CERT Vulnerability Remediation - <http://www.cert.org/vuls/>
- OWASP - http://www.owasp.org/index.php/Main_Page
- NUIT - <http://policies.northwestern.edu/policies-by-category.html>
- ISO – www.iso.org
- PCI DSS - <https://www.pcisecuritystandards.org/>

References

- [1] SANS Analyst Program, *“Penetration Testing: Assessing Your Overall Security Before Attackers Do”*, Northcutt S., Shenk J., Shacklefor D., Rosenberg T., Siles R., Mancini S., June 2006,
http://www.coresecurity.com/files/attachments/SANS_Penetration_Testing.pdf
- [2] Northwestern University Data Access and Classification Policy
<http://www.it.northwestern.edu/policies/dataaccess.html>
- [3] ISO Standards 27002-2005, 4.1 *“Assessing Security Risks”*
http://www.iso.org/iso/catalogue_detail?csnumber=50297
- [4] ISO Standards 27002-2013, 12.6.1 *“Management of technical vulnerabilities”*
http://www.iso.org/iso/catalogue_detail?csnumber=54533

Appendices – Sample Reporting

This report was generated with an evaluation version of QualysGuard

Report Summary	
User Name:	Paul Klahn
Login Name:	quays_pk25
Company:	Qualys
User Role:	Manager
Address:	1600 Bridge Parkway
City:	Redwood Shores
State:	California
Zip:	94065
Country:	United States of America
Created:	06/13/2012 at 22:15:31 (GMT)
Template Title:	JF - Confirmed Patchable and Exploitable Level 4 and 5
Asset Groups:	-
IPs:	10.10.10.220
Tags:	-
Sort by:	Host
Trend Analysis:	Latest report
Date Range:	N/A
Active Hosts:	1
Hosts Matching Filters:	1

Summary of Vulnerabilities

Vulnerabilities Total	222	Security Risk (Avg)	 4.3	Business Risk	 45/100
-----------------------	-----	---------------------	---	---------------	--

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	76	-	-	76
4	146	-	-	146
3	0	-	-	0
2	0	-	-	0
1	0	-	-	0
Total	222	-	-	222

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Windows	85	-	-	85
Local	70	-	-	70
Office Application	39	-	-	39
Internet Explorer	15	-	-	15
Security Policy	6	-	-	6
Total	215	-	-	215


Detailed Results

Vulnerabilities Total	222	Security Risk		4.3
-----------------------	-----	---------------	---	-----

by Severity				
Severity	Confirmed	Potential	Information Gathered	Total
5	76	-	-	76
4	146	-	-	146
3	0	-	-	0
2	0	-	-	0
1	0	-	-	0
Total	222	-	-	222

5 Biggest Categories				
Category	Confirmed	Potential	Information Gathered	Total
Windows	85	-	-	85
Local	70	-	-	70
Office Application	39	-	-	39
Internet Explorer	15	-	-	15
Security Policy	6	-	-	6
Total	215	-	-	215

Vulnerabilities (222)

 5 Microsoft Internet Explorer Cumulative Security Update (MS07-027) CVSS: - Active

QID: 100046 CVSS Base: 9.3
 Category: Internet Explorer CVSS Temporal: 7.3
 CVE ID: [CVE-2007-0942](#), [CVE-2007-0944](#), [CVE-2007-0945](#), [CVE-2007-0946](#), [CVE-2007-0947](#), [CVE-2007-2221](#)
 Vendor Reference: [MS07-027](#)
 Bugtraq ID: -
 Service Modified: 11/19/2007
 User Modified: -
 Edited: No
 PCI Vuln: Yes

First Detected: 10/01/2011 at 07:36:07 (GMT) Last Detected: 01/14/2012 at 08:26:08 (GMT) Times Detected: 15

CVSS Environment:

Asset Group: -
 Collateral Damage Potential: -
 Target Distribution: -
 Confidentiality Requirement: -
 Integrity Requirement: -
 Availability Requirement: -

SOLUTION:

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Microsoft Internet Explorer 5.01 Service Pack 4 on Windows 2000 Service Pack 4 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=67AE3381-16B2-4B34-B95C-69EE7D58B357>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=67AE3381-16B2-4B34-B95C-69EE7D58B357>
 Microsoft Internet Explorer 6 Service Pack 1 when installed on Windows 2000 Service Pack 4 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=03FC8E0C-DEC5-48D1-9A34-3B639F185F7D>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=03FC8E0C-DEC5-48D1-9A34-3B639F185F7D>
 Microsoft Internet Explorer 6 for Windows XP Service Pack 2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=EFC6BE04-0D6B-4639-8485-DA1525F6BC52>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=EFC6BE04-0D6B-4639-8485-DA1525F6BC52>
 Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=A077BE20-C379-4386-B478-80197A4A4ABC>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=A077BE20-C379-4386-B478-80197A4A4ABC>
 Microsoft Internet Explorer 6 for Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=D249089D-BB8E-4B86-AB8E-18C52844ACB2>


(<http://www.microsoft.com/downloads/details.aspx?FamilyId=D249089D-BB8E-4B86-AB8E-18C52844ACB2>)
 Microsoft Internet Explorer 6 for Windows Server 2003 with SP1 for Itanium based Systems and Windows Server 2003 with SP2 for Itanium based Systems :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=D52C0AFD-CC3A-4A5C-B91B-E006D497BC26>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=D52C0AFD-CC3A-4A5C-B91B-E006D497BC26>
 Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=94B83BDD-2BD1-43E4-BABF-68135D253293>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=94B83BDD-2BD1-43E4-BABF-68135D253293>
 Windows Internet Explorer 7 for Windows XP Service Pack 2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=7A778D93-9D85-4217-8CC0-5C494D954CA0>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=7A778D93-9D85-4217-8CC0-5C494D954CA0>
 Windows Internet Explorer 7 for Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=29938ED4-F8BB-4793-897C-966BA7F4830C>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=29938ED4-F8BB-4793-897C-966BA7F4830C>
 Windows Internet Explorer 7 for Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 :
<http://www.microsoft.com/downloads/details.aspx?FamilyId=0F173D60-6FD0-4C92-BB2A-A7A78707E35F>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=0F173D60-6FD0-4C92-BB2A-A7A78707E35F>
 For a complete list of patch download links, please refer to Microsoft Security Bulletin MS07-027
<http://www.microsoft.com/technet/security/bulletin/MS07-027.mspx>.

Virtual Patches:

 **Trend Micro Virtual Patching**

Virtual Patch #1000103: Microsoft Internet Explorer COM Object Instantiation Memory Corruption Vulnerability (Group 1)
 Virtual Patch #1000994: Microsoft Windows Media Server MDSAAuth.DLL ActiveX Control Remote Code Execution

EXPLOITABILITY:

 **The Exploit-DB**

Reference: CVE-2007-2221
 Description: MS Internet Explorer
 Link: <http://www.exploit-db.com/exploits/3892>

RESULTS:

HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB931768 is missing
 HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP0\KB931768-IE7 is missing
 %windir%\System32\wininet.dll Version is 6.0.3790.630

 **5 Cumulative Security Update for Internet Explorer (MS07-069)**

CVSS: - Active

QID:	100054	CVSS Base:	9.3
Category:	Internet Explorer	CVSS Temporal:	7.3
CVE ID:	CVE-2007-3902 , CVE-2007-3903 , CVE-2007-5344 , CVE-2007-5347		
Vendor Reference:	MS07-069		
Bugtraq ID:	-		
Service Modified:	12/12/2007		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		

First Detected: 10/01/2011 at 07:36:07 (GMT) Last Detected: 01/14/2012 at 08:26:08 (GMT) Times Detected: 15

CVSS Environment:

Asset Group: -
 Collateral Damage Potential: -
 Target Distribution: -
 Confidentiality Requirement: -
 Integrity Requirement: -
 Availability Requirement: -

SOLUTION:

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows 2000 Service Pack 4 (Microsoft Internet Explorer 5.01 Service Pack 4):
<http://www.microsoft.com/downloads/details.aspx?FamilyId=B3BD16EA-5D69-4AE3-84B3-AB773052CEEB>
<http://www.microsoft.com/downloads/details.aspx?FamilyId=B3BD16EA-5D69-4AE3-84B3-AB773052CEEB>
 Microsoft Windows 2000 Service Pack 4 (Microsoft Internet Explorer 6 Service Pack

1):<http://www.microsoft.com/downloads/details.aspx?FamilyId=BC8EDF05-262A-4D1D-B196-4FC1A844970C>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=BC8EDF05-262A-4D1D-B196-4FC1A844970C)
 Windows XP Service Pack 2 (Microsoft Internet Explorer
 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=6E4EBAFC-34C3-4DC7-B712-152C611D3F0A>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=6E4EBAFC-34C3-4DC7-B712-152C611D3F0A)
 Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 (Microsoft Internet Explorer
 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=F5A5AF23-30FB-4E47-94BD-3B05B55C92F2>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=F5A5AF23-30FB-4E47-94BD-3B05B55C92F2)
 Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 (Microsoft Internet Explorer
 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=BF466060-A585-4C2E-A48D-70E080C3BBE7>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=BF466060-A585-4C2E-A48D-70E080C3BBE7)
 Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 (Microsoft Internet Explorer
 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=074697F2-18C8-4521-BBF7-1D0E7395D27D>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=074697F2-18C8-4521-BBF7-1D0E7395D27D)
 Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems (Microsoft Internet
 Explorer 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=B3F390A6-0361-4553-B627-5E7AD6BF5055>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=B3F390A6-0361-4553-B627-5E7AD6BF5055)
 Windows XP Service Pack 2 (Windows Internet Explorer
 7):<http://www.microsoft.com/downloads/details.aspx?FamilyId=B15A6506-02DD-43C2-AEF4-E10C1C76EE97>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=B15A6506-02DD-43C2-AEF4-E10C1C76EE97)
 Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 (Windows Internet Explorer
 7):<http://www.microsoft.com/downloads/details.aspx?FamilyId=C092A6BB-8E62-4D90-BDB1-5F3A15968F75>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=C092A6BB-8E62-4D90-BDB1-5F3A15968F75)
 Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 (Windows Internet Explorer
 7):<http://www.microsoft.com/downloads/details.aspx?FamilyId=34759C10-16A5-42A2-974D-9D532FB5A0A7>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=34759C10-16A5-42A2-974D-9D532FB5A0A7)
 For a complete list of patch download links, please refer to Microsoft Security Bulletin MS07-069
 (http://www.microsoft.com/technet/security/bulletin/MS07-069.mspx).

Virtual Patches:



Trend Micro Virtual Patching

Virtual Patch #1001247: Microsoft Internet Explorer DHTML Object Memory Corruption Vulnerability

Virtual Patch #1001261: Microsoft Internet Explorer Intuit Products AWAPI4.dll ActiveX Control Code Execution Vulnerabilities

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Internet Explorer Version = 6.0.3790.0

HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB942615\Filelist is missing

%windir%\System32\wininet.dll Version is 6.0.3790.630

5 Internet Explorer Cumulative Security Update (MS08-010)

CVSS: - Active

QID:	100055	CVSS Base:	9.3
Category:	Internet Explorer	CVSS Temporal:	7.3
CVE ID:	CVE-2008-0076 , CVE-2008-0077 , CVE-2008-0078 , CVE-2007-4790		
Vendor Reference:	MS08-010		
Bugtraq ID:	-		
Service Modified:	02/13/2008		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		

First Detected: 10/01/2011 at 07:36:07 (GMT) Last Detected: 01/14/2012 at 08:26:08 (GMT) Times Detected: 15

CVSS Environment:

Asset Group: -
 Collateral Damage Potential: -
 Target Distribution: -
 Confidentiality Requirement: -
 Integrity Requirement: -
 Availability Requirement: -

SOLUTION:

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows 2000 Service Pack 4 (Microsoft Internet Explorer 5.01 Service Pack 4):<http://www.microsoft.com/downloads/details.aspx?FamilyId=1032A039-468B-4C5F-8C1C-5E54C2832E41>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=1032A039-468B-4C5F-8C1C-5E54C2832E41)
 Microsoft Windows 2000 Service Pack 4 (Microsoft Internet Explorer 6 Service Pack 1):<http://www.microsoft.com/downloads/details.aspx?FamilyId=87E66DCE-5060-4814-8754-829B4E190359>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=87E66DCE-5060-4814-8754-829B4E190359)
 Windows XP Service Pack 2 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=BB2AA3CB-021F-4890-AB20-2A51F8E17554>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=BB2AA3CB-021F-4890-AB20-2A51F8E17554)
 Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=8989F576-8B30-4866-90EC-929D24F3B409>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=8989F576-8B30-4866-90EC-929D24F3B409)
 Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=429B7ED1-FE78-459A-B834-D0F3C69CB703>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=429B7ED1-FE78-459A-B834-D0F3C69CB703)
 Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=E989E23C-38BB-4FE7-A830-D7BDF7659392>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=E989E23C-38BB-4FE7-A830-D7BDF7659392)
 Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?FamilyId=5A097F7A-B696-48D0-B13F-337C5FD14E24>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=5A097F7A-B696-48D0-B13F-337C5FD14E24)
 Windows XP Service Pack 2 (Windows Internet Explorer 7):<http://www.microsoft.com/downloads/details.aspx?FamilyId=D4AA293A-6332-4C6C-B128-876F516BD030>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=D4AA293A-6332-4C6C-B128-876F516BD030)
 Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 (Windows Internet Explorer 7):<http://www.microsoft.com/downloads/details.aspx?FamilyId=B72AF1B6-6E23-4005-AEF6-82195B380153>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=B72AF1B6-6E23-4005-AEF6-82195B380153)
 Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 (Windows Internet Explorer 7):<http://www.microsoft.com/downloads/details.aspx?FamilyId=B2AA6562-881E-4FD6-BE1B-53426A0FF4A9>
 (http://www.microsoft.com/downloads/details.aspx?FamilyId=B2AA6562-881E-4FD6-BE1B-53426A0FF4A9)
 For a complete list of patch download links, please refer to Microsoft Security Bulletin MS08-010 (<http://www.microsoft.com/technet/security/bulletin/MS08-010.mspx>).

Virtual Patches:

 Trend Micro Virtual Patching

- Virtual Patch #1001088: Microsoft Internet Explorer Visual FoxPro ActiveX Object Memory Corruption
- Virtual Patch #1001636: Microsoft Internet Explorer HTML Rendering Memory Corruption Vulnerability
- Virtual Patch #1001821: Microsoft Internet Explorer Image Processing Argument Handling Memory Corruption

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

RESULTS:

HKLM\Software\Microsoft\Internet Explorer Version = 6.0.3790.0
 HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB944533\Filelist is missing
 %windir%\System32\wininet.dll Version is 6.0.3790.630

 5 Microsoft Internet Explorer Pointer Reference Memory Corruption (MS08-078)

CVSS: - Active

QID:	100065	CVSS Base:	9.3
Category:	Internet Explorer	CVSS Temporal:	6.9
CVE ID:	CVE-2008-4844		
Vendor Reference:	MS08-078		
Bugtraq ID:	32721		
Service Modified:	01/08/2009		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		

First Detected: 10/01/2011 at 07:36:07 (GMT) Last Detected: 01/14/2012 at 08:26:08 (GMT) Times Detected: 15

CVSS Environment:

- Asset Group: -
- Collateral Damage Potential: -
- Target Distribution: -
- Confidentiality Requirement: -
- Integrity Requirement: -

Availability Requirement: -

SOLUTION:

Patch:

Following are links for downloading patches to fix the vulnerabilities:

Microsoft Windows 2000 Service Pack 4 (Microsoft Internet Explorer 5.01 Service Pack 4):<http://www.microsoft.com/downloads/details.aspx?familyid=d3e18732-47f1-40ce-999c-d1fd283bf138>
(<http://www.microsoft.com/downloads/details.aspx?familyid=d3e18732-47f1-40ce-999c-d1fd283bf138>)
Microsoft Windows 2000 Service Pack 4 (Microsoft Internet Explorer 6 Service Pack 1):<http://www.microsoft.com/downloads/details.aspx?familyid=124c14b6-9323-4f6f-902b-727aa56444bc>
(<http://www.microsoft.com/downloads/details.aspx?familyid=124c14b6-9323-4f6f-902b-727aa56444bc>)
Windows XP Service Pack 2 and Windows XP Service Pack 3 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?familyid=1d83e0af-46fa-4bfc-ba57-635435a7ef2d>
(<http://www.microsoft.com/downloads/details.aspx?familyid=1d83e0af-46fa-4bfc-ba57-635435a7ef2d>)
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?familyid=a585cb73-2c1a-4fa8-862a-ad6aeaeaf2f8>
(<http://www.microsoft.com/downloads/details.aspx?familyid=a585cb73-2c1a-4fa8-862a-ad6aeaeaf2f8>)
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?familyid=d81e9cf9-ce0c-463a-a359-49a348cb89ae>
(<http://www.microsoft.com/downloads/details.aspx?familyid=d81e9cf9-ce0c-463a-a359-49a348cb89ae>)
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2 (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?familyid=015df302-d79f-43a1-b5c5-32ac04de0510>
(<http://www.microsoft.com/downloads/details.aspx?familyid=015df302-d79f-43a1-b5c5-32ac04de0510>)
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems (Microsoft Internet Explorer 6):<http://www.microsoft.com/downloads/details.aspx?familyid=18016305-7f72-47f6-ab4c-94282289bf5f>
(<http://www.microsoft.com/downloads/details.aspx?familyid=18016305-7f72-47f6-ab4c-94282289bf5f>)
Windows XP Service Pack 2 and Windows XP Service Pack 3 (Windows Internet Explorer 7):<http://www.microsoft.com/downloads/details.aspx?familyid=0190a289-164e-41a7-8c01-fa1aaed3f531>
(<http://www.microsoft.com/downloads/details.aspx?familyid=0190a289-164e-41a7-8c01-fa1aaed3f531>)
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2 (Windows Internet Explorer 7):<http://www.microsoft.com/downloads/details.aspx?familyid=9ba71e23-8cef-4399-b215-983b0dcf5cb5>
(<http://www.microsoft.com/downloads/details.aspx?familyid=9ba71e23-8cef-4399-b215-983b0dcf5cb5>)
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2 (Windows Internet Explorer 7):<http://www.microsoft.com/downloads/details.aspx?familyid=388847ec-817e-45cf-8fa7-32c7e1f57f80>
(<http://www.microsoft.com/downloads/details.aspx?familyid=388847ec-817e-45cf-8fa7-32c7e1f57f80>)
For a complete list of patch download links, please refer to Microsoft Security Bulletin MS08-078 (<http://www.microsoft.com/technet/security/bulletin/MS08-078.mspx>).

Virtual Patches:



Trend Micro Virtual Patching

Virtual Patch #1003129: Pointer Reference Memory Corruption Vulnerability

Virtual Patch #1003133: Pointer Reference Memory Corruption Vulnerability Domain Blocker

EXPLOITABILITY:



Core Security

Reference: CVE-2008-4844

Description: Microsoft Internet Explorer XML Buffer Overflow Exploit - Core Security Category : Exploits/Client Side



Immunity

Reference: CVE-2008-4844

Description: MS Internet Explorer XML Parsing Vulnerability - Immunity Ref : ms08_078

Link: http://qualys.immunityinc.com/home/exploitpack/CANVAS/ms08_078/qualys_user



Metasploit

Reference: CVE-2008-4844

Description: Internet Explorer Data Binding Memory Corruption - Metasploit Ref : /modules/exploit/windows/browser/ms08_078_xml_corruption

Link: http://www.metasploit.com/modules/exploit/windows/browser/ms08_078_xml_corruption



The Exploit-DB

Reference: CVE-2008-4844

Description: MS Internet Explorer XML Parsing Remote Buffer Overflow Exploit 0day - The Exploit-DB Ref : 7403

Link: <http://www.exploit-db.com/exploits/7403>

Reference: CVE-2008-4844

Description: MS Internet Explorer XML Parsing Buffer Overflow Exploit (vista) 0day - The Exploit-DB Ref : 7410

Link: <http://www.exploit-db.com/exploits/7410>

Reference: CVE-2008-4844

Description: Internet Explorer Data Binding Memory Corruption - The Exploit-DB Ref : 16583

Link: <http://www.exploit-db.com/exploits/16583>



ExploitKits

Reference: CVE-2008-4844

Description: Internet Explorer 7 XML Exploit

Link: <http://contagiodump.blogspot.com/2010/06/overview-of-exploit-packs-update.html>

RESULTS:

HKLM\Software\Microsoft\Internet Explorer Version = 6.0.3790.0

HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB960714 is missing

%windir%\System32\mshtml.dll Version is 6.0.3790.630



5 Microsoft Windows GDI+ Remote Code Execution Vulnerability (MS08-052)

CVSS: - **Active**

QID: 90454

CVSS Base: 9.3

Category: Windows

CVSS Temporal: 7.7

CVE ID: [CVE-2007-5348](#), [CVE-2008-3012](#), [CVE-2008-3013](#), [CVE-2008-3014](#), [CVE-2008-3015](#)

Vendor Reference: [MS08-052](#)

Bugtraq ID: -

Service Modified: 11/17/2009

User Modified: -

Edited: No

PCI Vuln: Yes

First Detected: 07/27/2011 at 19:27:53 (GMT) Last Detected: 01/14/2012 at 08:26:08 (GMT) Times Detected: 25

CVSS Environment:

Asset Group: -

Collateral Damage Potential: -

Target Distribution: -

Confidentiality Requirement: -

Integrity Requirement: -

Availability Requirement: -

SOLUTION:

Refer to Microsoft Security Bulletin MS08-052 (<http://www.microsoft.com/technet/security/bulletin/MS08-052.msp>) for more information on this issue.

Microsoft has rated this vulnerability as Critical.

Virtual Patches:



Trend Micro Virtual Patching

Virtual Patch #1002758: Microsoft Windows GDI+ VML Buffer Overrun Vulnerability

Virtual Patch #1003083: Microsoft GDI+ GIF Parsing Vulnerability

Virtual Patch #1002762: Microsoft Windows GDI+ WMF Buffer Overrun Vulnerability

Virtual Patch #1002757: Microsoft Windows GDI+ BMP Integer Overflow Vulnerability

EXPLOITABILITY:



Core Security

Reference: CVE-2008-3014

Description: Microsoft Windows GDI Plus WMF Buffer Overflow Exploit (MS08-052) - Core Security Category : Exploits/Client Side



The Exploit-DB

Reference: CVE-2007-5348

Description: MS Internet Explorer GDI+ Proof of Concept (MS08-052) - The Exploit-DB Ref : 6619

Link: <http://www.exploit-db.com/exploits/6619>



Scan Report

08 Oct 2015

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Tim LeKan
nrthw_tl

Northwestern University
1800 Sherman Ave Suite 209
Evanston, Illinois 60201
United States of America

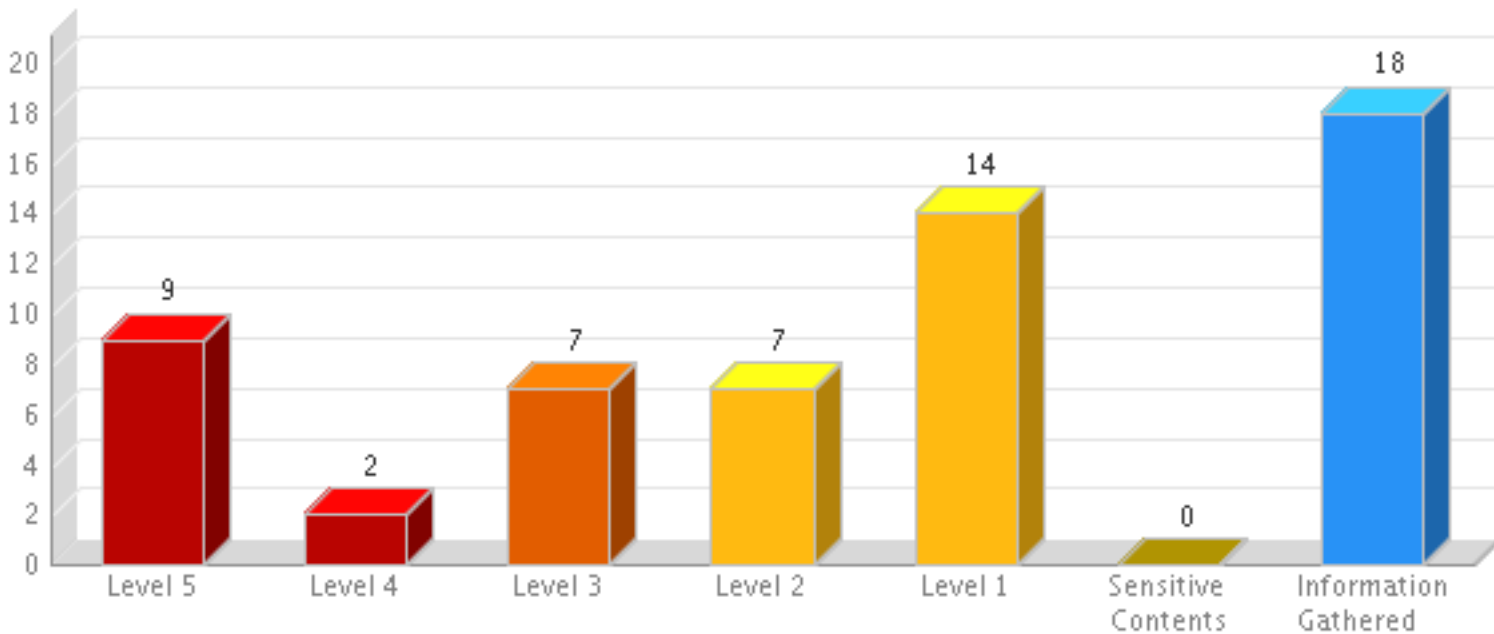
Target and Filters

Scans (1)	Web Application Vulnerability Scan - Test Web Site 2 - 2015-10-08
Web Applications (1)	Test Web Site 2
Status	New, Active, Re-Opened

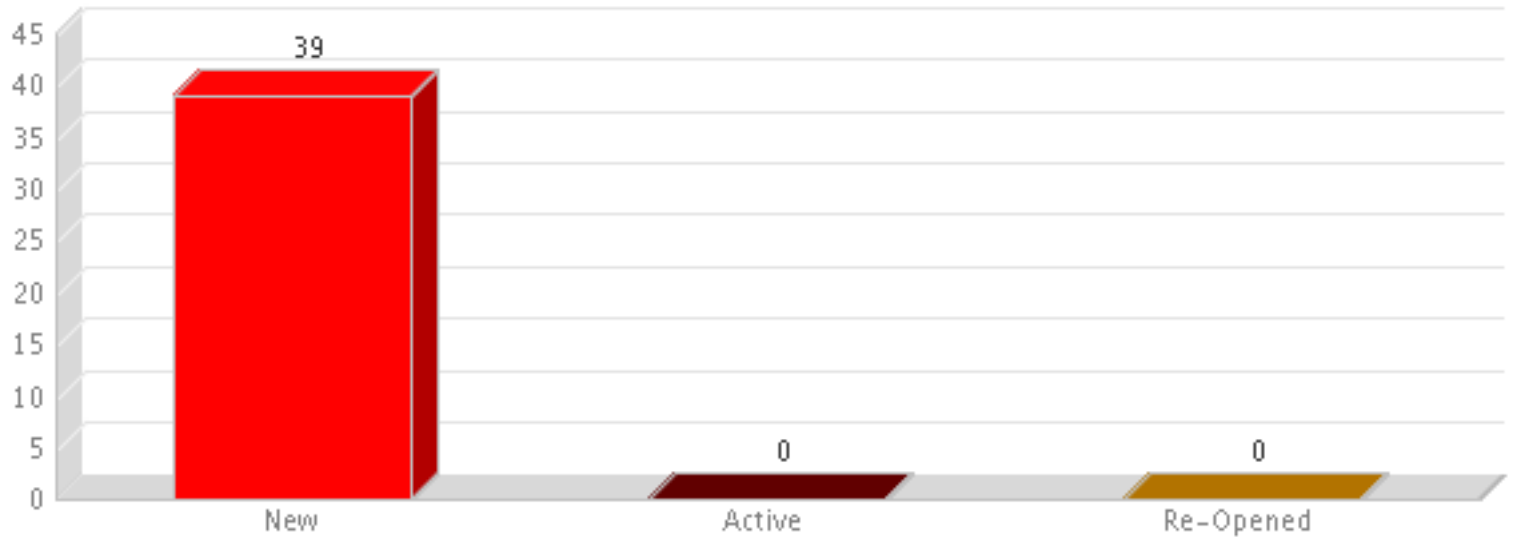
Summary

Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
HIGH	39	0	18

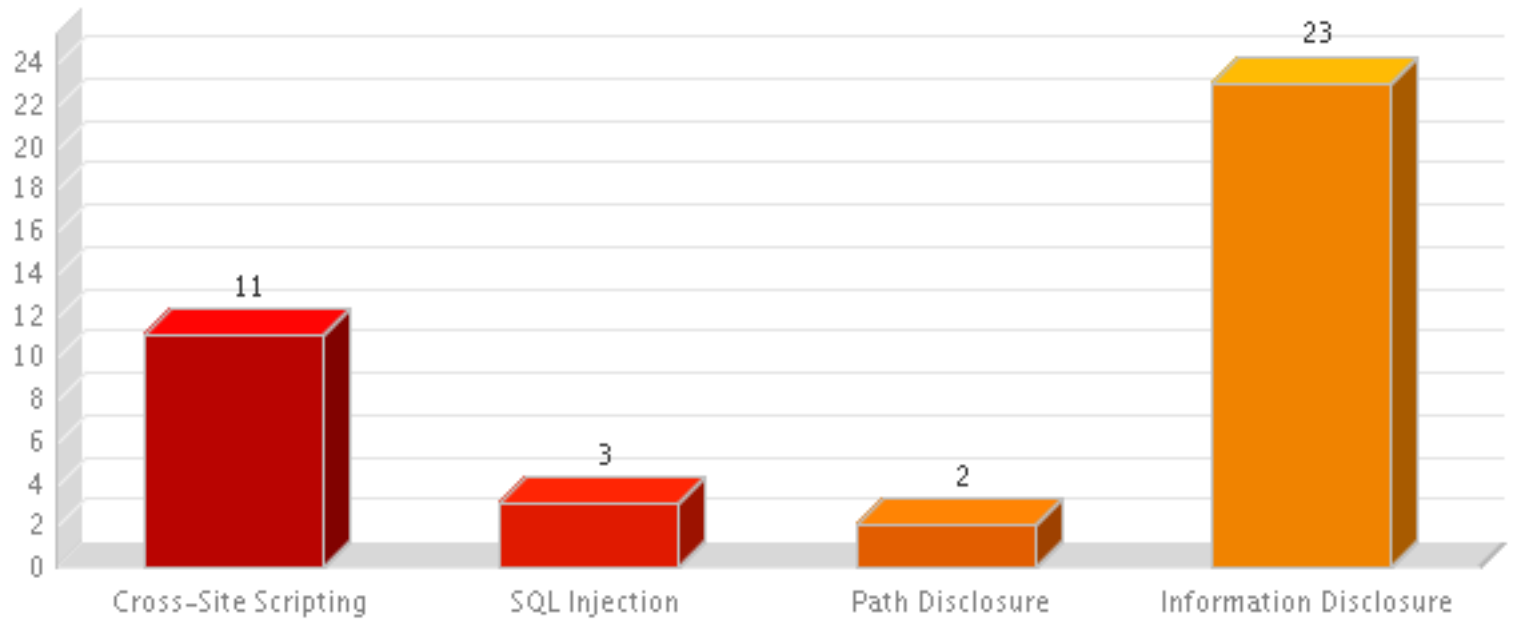
Findings by Severity



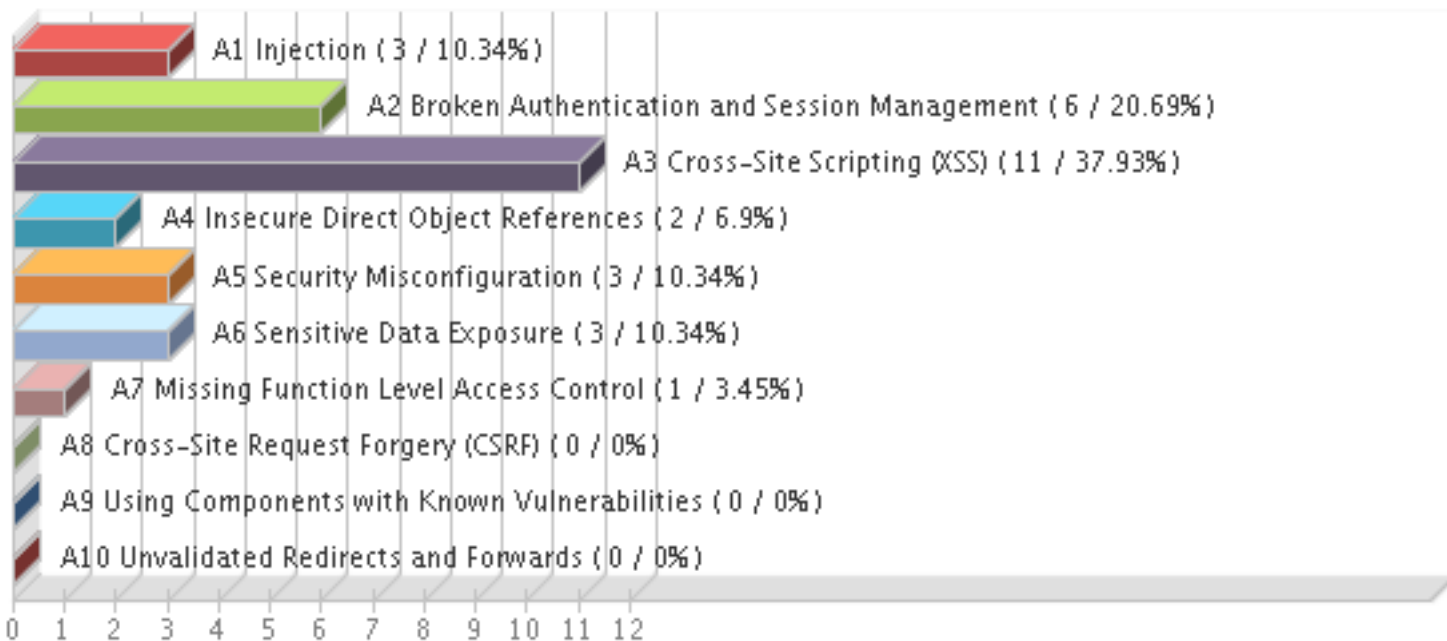
Vulnerabilities by Status



Vulnerabilities by Group



OWASP Top 10 2013 Vulnerabilities



Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Web Application Vulnerability Scan - Test Web Site 2 - 2015-10-08	08 Oct 2015 10:10 GMT-0600	9	2	7	7	14	0	18

Results(57)

Vulnerability (39)

Cross-Site Scripting (11)

 150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities (4)

150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities

New

URL: <http://demo.testfire.net/comment.aspx>

Finding #	4849952(474978225)	First Time Detected	08 Oct 2015 10:10 GMT-0600
Group	Cross-Site Scripting	Last Time Detected	08 Oct 2015 10:10 GMT-0600
CWE	CWE-79	Last Time Tested	08 Oct 2015 10:10 GMT-0600
OWASP	A3 Cross-Site Scripting (XSS)	Times Detected	1
WASC	WASC-8 Cross-Site Scripting		
CVSS Base	4.3	CVSS Temporal	3.9

Details

Threat

XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

Impact

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

Solution

Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

Detection Information

Parameter	It has been detected by exploiting the parameter name of the form located in URL http://demo.testfire.net/feedback.aspx The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

<http://demo.testfire.net/>
<http://demo.testfire.net/feedback.aspx>

Payloads

#1 Request

Payload ""<qss%20a=@REQUESTID@>
Request POST http://demo.testfire.net/comment.aspx

#1 Referer: http://demo.testfire.net/

#2 Cookie: lang=; amSessionId=15130676; ASP.NET_SessionId=vvdt2455rgmjcz312m2mamep;

Click this [link](#) to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
ef="default.aspx?content=inside_careers.htm">Careers</a></li>
</ul>
</td>
<td valign="top" colspan="3" class="bb">
```

```
<div class="fl" style="width: 99%;">
```

```
<h1>Thank You</h1>
```

```
<p>Thank you for your comments, ""<qss a=X149637348Y2Z>. They will be reviewed by our Customer Service staff and given the full attention that they deserve.</p>
```

```
</div>
```

```
</td>
</tr>
</table>
```

```
</div>
```

```
<div id="footer" style="width: 99%;">
<a id="_ctl0__ctl0_HyperLink5
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities

New

URL: <http://demo.testfire.net/bank/login.aspx>

Finding #	4849971 (474978244)	First Time Detected	08 Oct 2015 10:10 GMT-0600
Group	Cross-Site Scripting	Last Time Detected	08 Oct 2015 10:10 GMT-0600
CWE	CWE-79	Last Time Tested	08 Oct 2015 10:10 GMT-0600
OWASP	A3 Cross-Site Scripting (XSS)	Times Detected	1
WASC	WASC-8 Cross-Site Scripting		
CVSS Base	4.3	CVSS Temporal	3.9

Details

Threat

XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

Impact

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

Solution

Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

Detection Information

Parameter	It has been detected by exploiting the parameter uid of the form located in URL http://demo.testfire.net/bank/login.aspx The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

<http://demo.testfire.net/>

Payloads

#1 Request

Payload uid=%22%3E%3Cqss%3E&passw=password&btnSubmit=Login

Request POST http://demo.testfire.net/bank/login.aspx

#1 Referer: http://demo.testfire.net/

#2 Cookie: lang=; amSessionId=15130676; ASP.NET_SessionId=vvdt2455rgmjcz312m2mamep;

Click this [link](#) to try to reproduce the vulnerability using above payload. Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

/p>

```
<form action="login.aspx" method="post" name="login" id="login" onsubmit="return (confirminput(login));">
<table>
<tr>
<td>
Username:
</td>
<td>
<input type="text" id="uid" name="uid" value=""><qss>" style="width: 150px;">
</td>
</tr>
<tr>
<td>
Password:
</td>
<td>
<input type="password" id="passw" name="passw" style="width: 150px;">
</td>
</tr>
```

* The reflected string on the response webpage indicates that the vulnerability test was successful

150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities

New

URL: <http://demo.testfire.net/notfound.aspx?asperrorpath=/Privacypolicy.aspx>

Finding #	4849979(474978252)	First Time Detected	08 Oct 2015 10:10 GMT-0600
Group	Cross-Site Scripting	Last Time Detected	08 Oct 2015 10:10 GMT-0600
CWE	CWE-79	Last Time Tested	08 Oct 2015 10:10 GMT-0600
OWASP	A3 Cross-Site Scripting (XSS)	Times Detected	1
WASC	WASC-8 Cross-Site Scripting		
CVSS Base	4.3	CVSS Temporal	3.9

Details

Threat

XSS vulnerabilities occur when the Web application echoes user-supplied data in an HTML response sent to the Web browser. For example, a Web application might include the user's name as part of a welcome message or display a home address when confirming a shipping destination. If the user-supplied data contain characters that are interpreted as part of an HTML element instead of literal text, then an attacker can modify the HTML that is received by the victim's Web browser.

The XSS payload is echoed in HTML document returned by the request. An XSS payload may consist of HTML, JavaScript or other content that will be rendered by the browser. In order to exploit this vulnerability, a malicious user would need to trick a victim into visiting the URL with the XSS payload.

Impact

XSS exploits pose a significant threat to a Web application, its users and user data. XSS exploits target the users of a Web application rather than the Web application itself. An exploit can lead to theft of the user's credentials and personal or financial information. Complex exploits and attack scenarios are possible via XSS because it enables an attacker to execute dynamic code. Consequently, any capability or feature available to the Web browser (for example HTML, JavaScript, Flash and Java applets) can be used to as a part of a compromise.

Solution

Filter all data collected from the client including user-supplied content and browser content such as Referrer and User-Agent headers.

Any data collected from the client and displayed in a Web page should be HTML-encoded to ensure the content is rendered as text instead of an HTML element or JavaScript.

Detection Information

Parameter	It has been detected by exploiting the parameter asperrorpath The payloads section will display a list of tests that show how the param could have been exploited to collect the information
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

<http://demo.testfire.net/>
http://demo.testfire.net/default.aspx?content=inside_careers.htm
<http://demo.testfire.net/Privacypolicy.aspx?sec=Careers&template=US>

Payloads