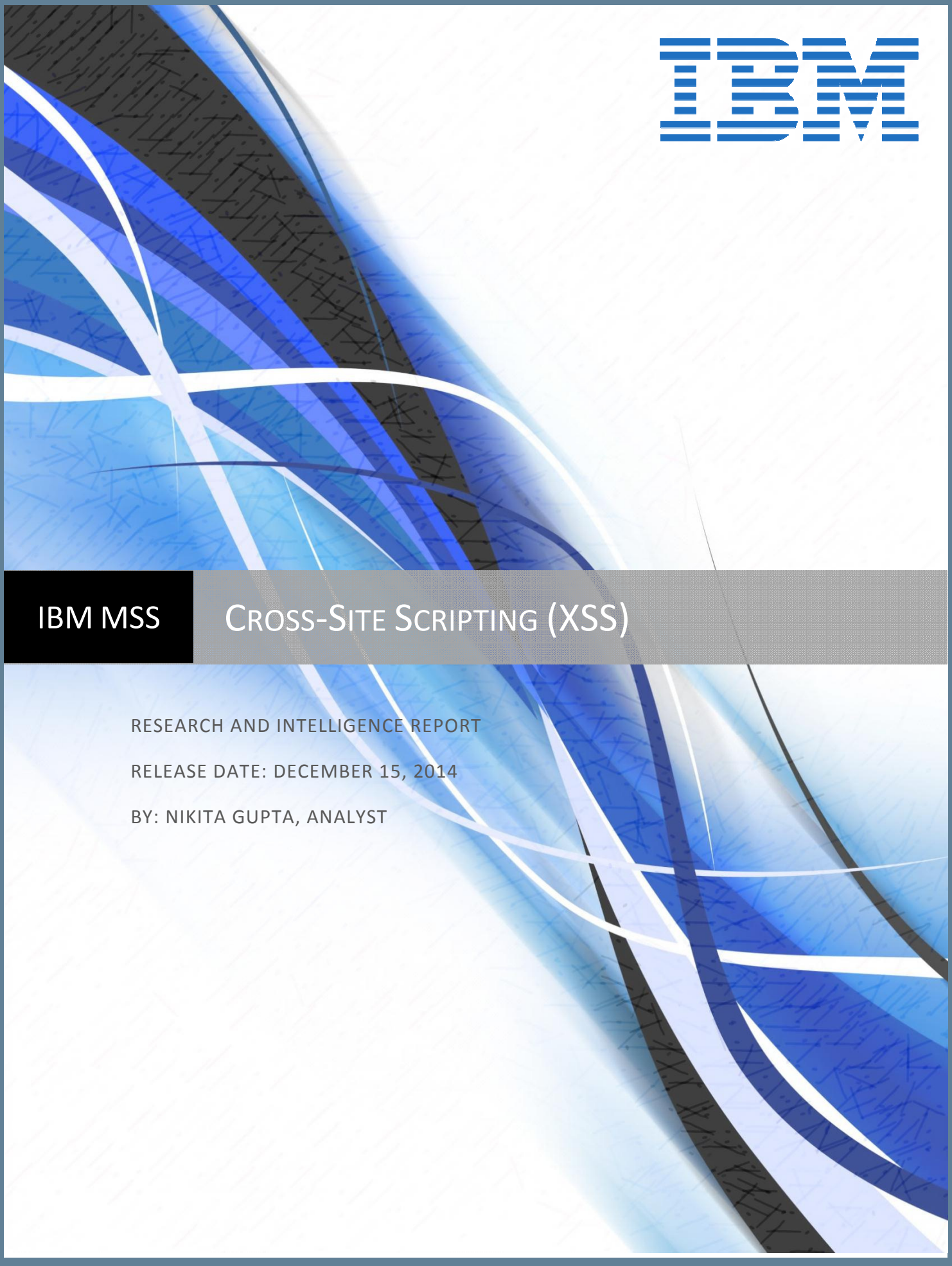


IBM MSS

CROSS-SITE SCRIPTING (XSS)

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: DECEMBER 15, 2014

BY: NIKITA GUPTA, ANALYST

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

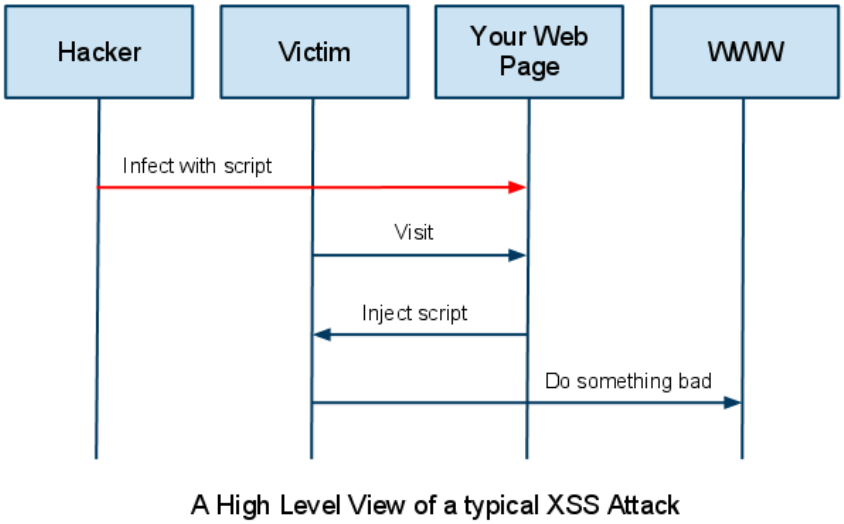
One of the major vulnerability categories often found in web applications is cross-site scripting (XSS). Today, in the digital world, many transactions occur online such as banking, shopping, E-trading, and travel booking. According to statistics gathered by IBM's Hosted Application Scanning Management (HASM) team, in over 900 dynamic web application scans, 17% were vulnerable to XSS. While this may not sound like a very high percentage, take into account that this data sample comes from organizations that have extremely mature and established security practices. Researchers have found these vulnerabilities to exist even on some of the most common and popular websites like Facebook, Amazon, Google, and PayPal. According to White Hat Security, as of today, they are seeing a 47.9% likelihood of a site being susceptible to Cross Site Scripting attacks.

In 1995, the early days of the Internet, Netscape introduced JavaScript. People learned fast that they can do many interesting things with it. Attackers learned that they could trick a user to load any website with iframes and use JavaScript to navigate between the websites. Hence, this led to the name Cross-site Scripting (XSS). In 2005, the Samy worm exploiting a XSS vulnerability on MySpace.com led to downing the whole website for 2.5 hours. In less than 20 hours, this worm affected about a million users registering itself as one of the fastest propagating worms in history.

So should organizations be concerned about cross-site scripting? Well, if an organization's website accepts user input then it may be vulnerable to cross-site scripting attacks and concern is indeed warranted.

WHAT IS XSS?

When a website is accepting user input without validation, the website is vulnerable to cross-site scripting attacks. When a browser renders a user input as a browser script that is known as cross-site scripting. Examples include the browser executing commands to display malicious content or the intent may be to steal the victim's user credentials or personal information.



A High Level View of a typical XSS Attack

Illustration 1. Source: Acunetix (http://www.acunetix.com/websitesecurity/cross-site-scripting/)

The illustration above gives a high level view of a typical cross-site scripting attack. Attacker injects a malicious script on a website. When a victim visits that website, the browser renders the attacker's script interpreting it as benign, but this script can do terrible things on the victim's browser.

The browser renders anything written inside HTML tags on the client side. So if an attacker crafts an input to the website in the form of HTML tags or browser script, the browser will think it is a part of the website and will try and render the result. This leads to cross-site scripting attacks. There are different types of XSS attacks. Some examples are Stored, Reflected, and DOM based XSS.

Stored: These attacks are those in which injected script is stored in the server or the database. Whenever that page is loaded, the script is loaded from the storage area and infects the machine loading the page.

Reflected: Reflected XSS are parts of search results, error messages, etc., which are sent to the browser through a different route than the actual website page. Social engineering is most commonly used to trick the user into clicking on specially crafted forms or web links which send the malicious script to the browser. The browser, assuming that it is coming from a trusted source, executes the script. This type of XSS is also known as non-persistent XSS.

DOM based: These attacks are executed by modifying the DOM environment in the

victim's browser. The HTTP response in the page does not change, but the client side code in the page executes differently.

It's a common misunderstanding that a read only site is secure from XSS attack, but that is not true. Most XSS attacks steal the user's cookies, session, files, or they even try and install Trojans. XSS attacks can hide against web application filters by using character encoding for example the <script> tag can be encoded as &ltscript&gt. Even encoding the content and adding a meta tag to the DOM can prevent XSS detection. Iframes help in importing HTML to your page which consequently, helps in aiding in XSS attacks.

CONSEQUENCES OF XSS ATTACKS

An attacker can do a lot of damage with XSS attacks:

- ✓ Identity theft is one of the major concerns. An attacker can steal personal information about a victim, such as victim's credentials and session details, and then impersonate the victim. For example, by obtaining a victim's online banking session details and personal information, an attacker can transfer money to his account.
- ✓ Through XSS an attacker can deface websites, spy on users accessing that website, or cause a denial of service attack.
- ✓ Attackers can gain access to sensitive or restricted information. For example the attacker can get hold of the database where login information is stored.
- ✓ Attacker can obtain free access to otherwise paid for content.
- ✓ An XSS attack not only affects users of the website, but it also affects the company running the vulnerable website. Brand reputation is at stake. These types of incidents result in a loss of customer trust and may also have a financial impact.

XSS ATTACK METRICS

In terms of web application vulnerabilities disclosed, the 1Q 2014 edition of the IBM X-Force Threat Intelligence Quarterly reported a significant drop in XSS vulnerabilities for 2013 from 2012. This could be a possible explanation of a notable decrease in XSS attack activity this year compared to the previous. At the time of this report, IBM's Managed

Security Services has observed a 31 percent decrease in XSS attack activity as compared to 2013 as illustrated in Figure 1 below.

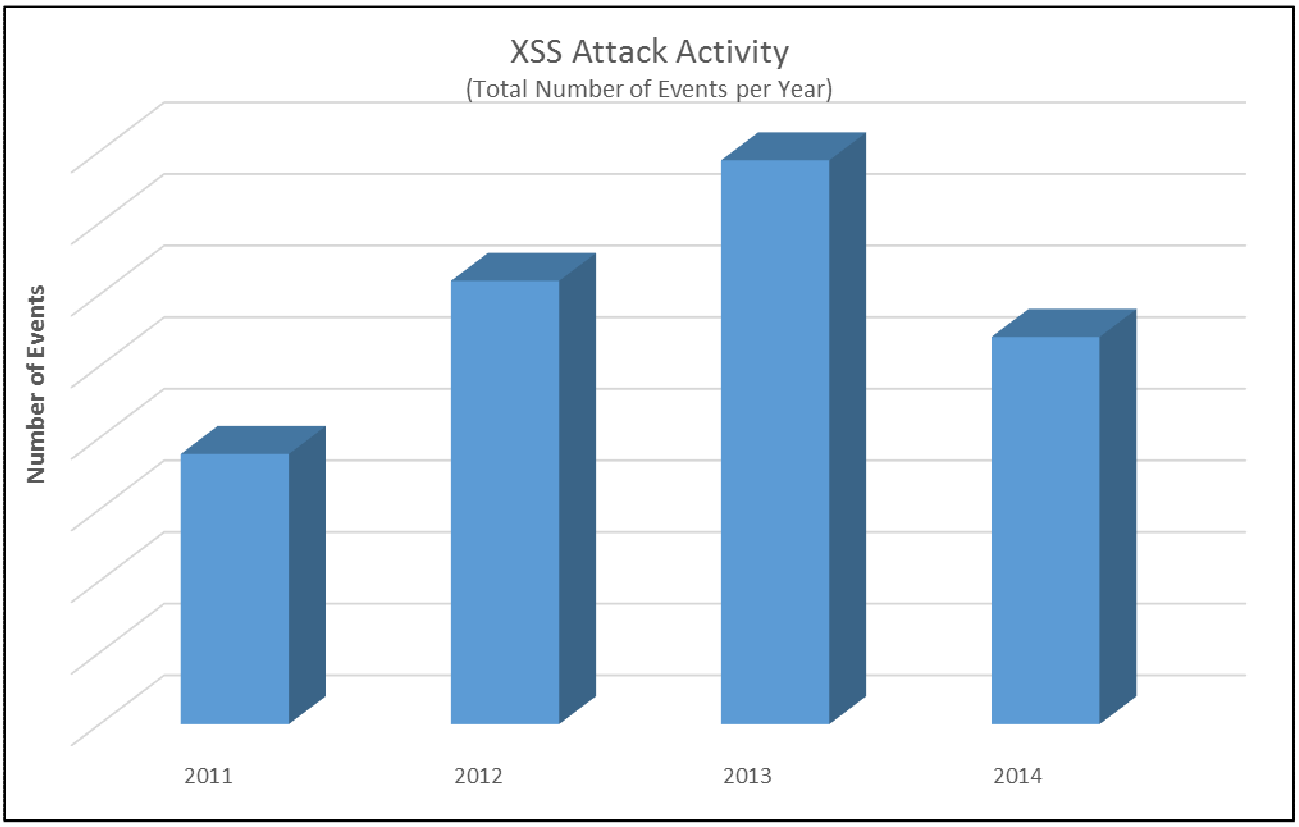


Figure 1. XSS Attack Activity as observed by IBM's Managed Security Services, 2011 – 2014.

Fewer reported vulnerabilities however, doesn't necessarily equate to less attack activity. Attackers have been known to utilize older vulnerabilities to exploit sites because they know that organizations are often slow to patch less critical vulnerabilities, such as those allowing cross-site scripting. Why go through the trouble of developing a new exploit for the latest vulnerability, when the existing exploits in an attacker's arsenal already do the trick?

Figure 2 below offers a view of XSS attack activity over the last four years. There is some positive news to be gleamed from this chart. Attack activity for 2014 is trending downward. Attack activity this low has not been observed since 2011. Will this trend continue in 2015? If vulnerability patch management continues to improve and fewer and fewer cross-site scripting vulnerabilities are reported, then a continued downward trend is possible.

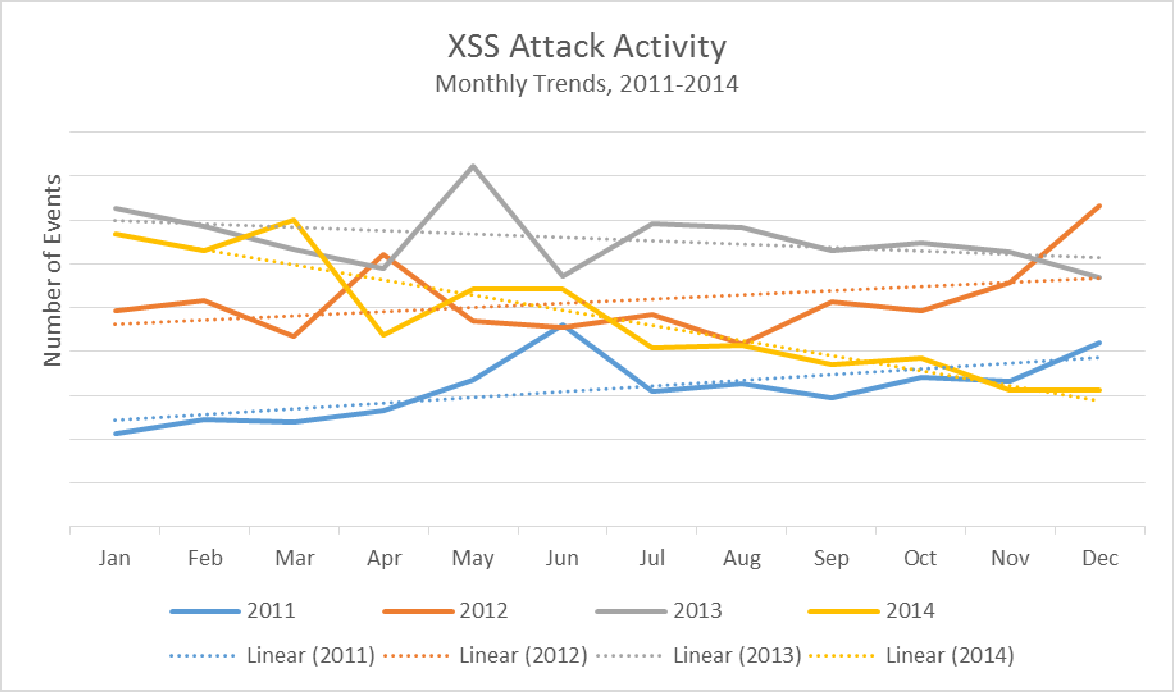


Figure 2. XSS Attack Activity as observed by IBM's Managed Security Services, 2011 – 2014.

RECOMMENDATIONS/MITIGATION TECHNIQUES

While organizations should be concerned with higher profile attacks and threats, they can also not ignore the more common vulnerabilities found in web applications. According to the 1Q 2014 edition of the IBM X-Force Threat Intelligence Quarterly, cross-site scripting was the second most prevalent consequence of exploitation at 18 percent. Attackers take advantage of companies that are focusing solely on putting out the major fires and target their low hanging fruit vulnerabilities. Cross-site scripting falls in this category. There are several steps organizations can take to mitigate this type of threat. Some steps require the website administrator's participation and others fall under user education:

- ✓ Input sanitizing is the best method to prevent XSS attacks.
- ✓ Performing a thorough code review is a must. Check from where user or HTTP request input can make its way to HTML output.
- ✓ Even if document.cookie function of JavaScript is disabled, an attacker can find the cookie information of the user through the server. Hence, HTTP trace should also be disabled.
- ✓ By following links to different websites from the main website you are vulnerable to

XSS attacks. If you are on a particular website and it supposedly links Google's website, instead of following that link directly, type in Google's URL in the browser.

- ✓ Being vigilant to social engineering attacks will also prevent XSS attacks. All user input should be treated as text by the browser instead of executable browser script.

IDPS SIGNATURES

Where possible, we recommend that customers enable the signatures listed below and analyze any events generated by them. In addition, ensure that any related security patches and anti-virus solutions are up-to-date. These signatures may not be enabled by default.

IBM PROVENTIA

adobe-asfunction-protocol-xss
adobe-navigatetourl-xss
Apache.HTTPD.mod_proxy_balancer.XSS
Apache.Tomcat.Host.Manager.Name.XSS
Apache.Tomcat.Sendmail.Examples.XSS
CGI.Bonsai./cvslog.cgi.XSS
cPanel.FILEOP.Parameter.Multiple.XSS
CSS_IE_Expression_Sanitization_XSS
CSS_IE_HTML_Sanitization_XSS
CSS_Moz_Binding_Cross_Domain_Scripting
DHTML_IE_JavaScript_XSS
DokeosMultipleXSS
Email_iNotes_Math_XSS
Email_iNotes_Svg_XSS
Email_OWA_Header_XSS
Email_OWA_XSS
firefox-character-encoding-xss
Flash_NavigateToURL_XSS
GZIP_Filename_Script_Char_Exec
HTML_Asp_Dot_Net_XSS
HTML_Cisco_Injection
HTML_Exchange_OWA_Script_Injection
HTML_Firefox_Sidebar_Panel_XSS
HTML_IE7_Navigation_Cancelled_XSS
HTML_Lotus_Webaccess_JS_XSS
HTML_MMc_XSS

HTML_Pdf_XSS
HTML_SharePoint_Username_XSS
HTML_SrcDoc_XSS
HTML_XSS_Attempt
HTML_XSS_ViewSource_JavaScript
HTTP_Apache_Expect_XSS
HTTP_Apache_OnError_XSS
HTTP_BEA_Admin_Console_XSS
HTTP_MSSCOM_Cross_Site_Scripting
HTTP_OpenView_nnmvalidate_XSS
HTTP_PHP_Transfer_XSS
HTTP_QueryName_XSS
HTTP_Response_Set_Cookie_XSS
HTTP_SharePoint_Admin_GetArg_XSS
HTTP_SharePoint_GetArg_XSS
HTTP_Sharepoint_Inplview_XSS
HTTP_SharePoint_XSS_JavaScript_Injection
HTTP_Share_Point_XSS
HTTP_Symantec_WebGateway_Console_XSS
HTTP_Tivoli_WebReports_Cross_Site_Scripting
HTTP_XSS_JavaScript_Function_Exec
IBM.System.Storage.DS.Storage.Manager.XSS
php-phpinfo-function-xss
Script_IE_toStaticHTML_XSS
SIP_Header_XSS

AKAMAI

Cross-site Scripting (XSS) Attack
IE XSS
IE XSS Fil
IE XSS Filters - Attack
IE XSS Filters - Attack Detected
IE XSS Filters - Attack Detected.
Inbound Anomaly Score Exceeded (Total Score: %(WAF_CRS_TOTAL_ANOMALY_SCORE), SQLi=%(WAF_CRS_SQL_INJECTION
Inbound Anomaly Score Exceeded (Total Score: %{TX.ANOMALY_SCORE}, SQLi=%{TX.SQL_INJECTION_SCORE}, XSS=%{TX.XSS
Persistent Universal PDF XSS attack
Possible XSS Attack Detected - HTML Tag Handler
UPDF/XSS injection Attack
XSS Attack Detected

XSS Filter - Category 1: Script Tag Vector
XSS Filter - Category 2: Event Handler Vector

CHECKPOINT

Acrobat Reader UXSS Java Script Code Execution
Acrobat Reader UXSS Remote Code Execution
Apple Safari webarchive File Format UXSS
B-net Software Content Management System shout.php name Parameter XSS - Ver2
CFORM XSS Alert
Google Chrome XSSAuditor Filter Security Policy Bypass
Internet Explorer Navigation Cancel Page XSS - Ver2
Internet Explorer toStaticHTML API XSS (MS10-035)
Internet Explorer XSS Filter JavaScript Information Disclosure (MS11-089)
Internet Explorer XSS Filter JavaScript Information Disclosure (MS11-099)
InterWoven WorkDocs XSS Cross-Site Scripting
Joomla! HTTP-Referrer XSS
Microsoft AntiXSS Library Bypass Information Disclosure (MS12-007)
Microsoft SharePoint Reflected List Parameter XSS (MS12-050)
Microsoft SharePoint XSS scriptresx.ashx Elevation of Privilege (MS12-050)
Microsoft Visual Studio Team Foundation Server XSS (MS12-061)
Oracle GlassFish Enterprise Server Multiple Reflected XSS Vulnerabilities
SAP Internet Transaction Server wgate.dll service Parameter XSS - Ver2
User Defined XSS Alert
XSS Attacks - IPS-1 - General Settings
XSS invalid configuration

CISCO IDS

5232.1 - URL with XSS
5431.1 IIS W3Who Vulnerabilties
5432 Script Embeded in HTTP Header
5551.0 - Outlook Web Access Cross Site Scripting Vulnerability
5757 - Microsoft Exchange Server Cross-Site Scripting
5770 - Cisco Secure ACS XSS
5807.0 Indexing Service Cross Site Scripting Vulnerability
5817.0 ASP .NET Cross Site Scripting
5848.0 Content Management Service Cross-site Scripting
5903 MS SharePoint XSS

6007 - Management Console Cross-Site Scripting
Ajax Availability Calendar Id_Item Parameter XSS Vulnerability
AxisInternet VoIP Manager Contacts.cgi XSS Vulnerability
BitDefender Internet Security 2009 XSS
Check Point UTM-1 Edge and Safe Diagnostic Command XSS Vulnerability
Cisco ASA WebVPN XSS
Cisco Common Services Framework Help Servlet XSS Vulnerability
Cisco Secure ACS XSS
Cisco UCCX XSS
Cisco Unified MeetingPlace Stored XSS
ElproLOG MONITOR XSS Vulnerability
Flogr Index.php XSS Vulnerability
Google Chrome XSSAuditor Filter Security Policy Bypass Vulnerability
HTTP DaloRADIUS Mng-search.php XSS Vulnerability
IBM Lotus Domino XSS Vulnerability
IBM Lotus Notes Traveler Address Parameter XSS Vulnerability
IBM Lotus Notes Traveler UserId Parameter XSS Vulnerability
IBM Lotus Notes TravelerRedirectURL Parameter XSS Vulnerability
IBM Tivoli Endpoint Manager XSS Vulnerability
IBM Websphere Application Server XSS
Internet Explorer 8 XSS Attack
Interspire Email Marketer Index.php XSS Vulnerability
InterWoven WorkDocs XSS Vulnerability
Jahia xCM XSS Vulnerability
Jaow CMS XSS Vulnerability
JCore Path Parameter XSS Vulnerability
JForum Action Parameter XSS Vulnerabiity
Kajona GetAllPassedParams Function Absender_Name Parameter XSS Vulnerability
Kajona GetAllPassedParams Function Action Parameter XSS Vulnerability
Kajona GetAllPassedParams Function Comment_Name Parameter XSS Vulnerability
Kajona GetAllPassedParams Function Module Parameter XSS Vulnerability
ManageEngine Applications Manager MyPage.do Forpage Parameter XSS Vulnerability
ManageEngine Applications Manager ProcessTemplates.do Templatetype Parameter XSS Vulnerability
ManageEngine Applications Manager ShowCustom.do Monitorname Parameter XSS Vulnerability
ManageEngine Applications Manager Showresource.do Type Parameter XSS Vulnerability
Media Player Classic WebServer Browser.html Path Parameter XSS Vulnerability
Microsoft Forefront Unified Access Gateway Default Reflected XSS
Microsoft Forefront Unified Access Gateway XSS Vulnerability
Microsoft IE 8 toStaticHTML XSS
Microsoft Internet Explorer 8 XSS
Microsoft Remote Desktop Web Access XSS

Microsoft SharePoint Server XSS Vulnerability
Microsoft Sharepoint XSS
Microsoft Sharepoint XSS Elevation of Privilege
Microsoft Sharepoint XSS Vulnerability
Microsoft System Center Configuration Manager Reflected XSS
Microsoft Visual Studio Cross Site Scripting (XSS) Vulnerability
Microsoft Visual Studio Team Web Access XSS Vulnerability
MS Internet Explorer 8 XSS
MS SharePoint XSS
MyBB Game Section Plugin XSS Vulnerability
Nagios XI Reflected XSS Vulnerability
Nagios XI VisApi.Php Div Parameter XSS Vulnerability
NetArt Media Car Portal CMS 3.0 XSS Vulnerabilities
NetGear DGN1000B Wireless Router h_skeyword XSS Vulnerability
NetGear DGN1000B Wireless Router Service_name Parameter XSS Vulnerability
NetGear DGN1000B Wireless Router Ssid_name Parameter XSS Vulnerability
NetIQ Access Manager Multiple XSS Vulnerability
Open-Xchange Server Ajax Mail Json Parameter XSS Vulnerability
Open-Xchange Server TestServlet XSS Vulnerability
OpenX Plugin-Index.php XSS Vulnerabilitiy
Oracle GlassFish Server AuditModules.jsf XSS Vulnerability
Oracle GlassFish Server JmsHosts.jsf XSS Vulnerability
Oracle GlassFish Server Key XSS Vulnerability
Oracle GlassFish Server Realms.jsf XSS Vulnerability
Oracle GlassFish Server Stored XSS Vulnerability
Outlook Web Access XSS
Quick.Cms and Quick.Cart XSS Vulnerability
RTTucson Quotations Database Quote_search.php XSS Vulnerability
SAP Web Application Server XSS
Sharepoint Server 2007 XSS
Siemens WinCC WebNavigator DownloadComponents.asp HTTP Referer XSS
Siemens WinCC WebNavigator DownloadSelect.asp XSS
Siemens WinCC WebNavigator MainControl.asp XSS
Siemens WinCC WebNavigator Project.asp XSS
Siemens WinCC WebNavigator Unsupported.asp Agent Parameter XSS
Siemens WinCC WebNavigator WebClient.asp XSS
Siemens WinCC WebNavigator WNStandart.asp XSS
Slash CMS Index.php XSS Vulnerability
SolarWinds Orion IP Address Manager IPAM Search.aspx XSS Vulnerability
Stradus CMS XSS Vulnerability
Subrion CMS Group Parameter XSS Vulnerability

Subrion CMS Id Parameter XSS Vulnerability
Symantec Web Gateway XSS Vulnerability
Telnet Failure Log XSS
URL with XSS
VoipNow Professional Nsextt Parameter XSS Vulnerability
WebKit Cross Site Scripting Filter XSSAuditor.cpp Security Bypass Vulnerability
WordPress ABC Test Plugin Id Parameter XSS Vulnerability
WordPress Church_Admin Id Parameter XSS Vulnerability
WordPress Count Per Day Plugin Datemin Parameter XSS Vulnerability
WordPress Count Per Day Plugin Page Parameter XSS Vulnerability
WordPress Design Approval System Plugin XSS Vulnerability
WordPress Featurific For WordPress Plugin Snum Parameter XSS Vulnerability
WordPress Flashnews Theme Src Parameter XSS Vulnerability
WordPress Flashnews Theme Test.php Parameter XSS Vulnerability
WordPress Floating Tweets XSS Vulnerability
Wordpress Indianic Faqs Manager Plugin 1.0 XSS Vulnerability
WordPress Platinum SEO XSS Vulnerability
WordPress Pretty Link Plugin XSS Vulnerability
WordPress RokNewsPager Plugin XSS
WordPress Token Manager Plugin Tid Parameter XSS Vulnerability
WordPress Traffic Analyzer Plugin aoid Parameter XSS Vulnerability
WordPress Video Lead Form Plugin ErrMsg Parameter XSS Vulnerability
WordPress WP Socializer Val Parameter XSS Vulnerability
XAVi X7968 Host Name Txtbox Parameter XSS Vulnerability
XAVi X7968 PvcName Parameter XSS Vulnerability
XSS in Cisco ACS Server
Zyxware Health Monitoring System Reflected XSS Vulnerability

FORTINET

HTTP.URI.Script.XSS
12Planet.ChatServer.XSS
1two.Livre.d.guestbook.php.XSS
Aardvark.Topsites.PHP.XSS.Vulnerability
Absolute.Image.Gallery.XE.XSS
ACART.admin.error.asp.msg.variable.XSS
ACART.admin.index.asp.msg.variable.XSS
ACART.category.asp.XSS.authentication.bypass
ACART.deliver.asp.msg.variable.XSS
ACART.error.asp.msg.Variable.XSS

Actinic.E-Commerce.Services.bb000001.pl.XSS.Vulnerability
Actinic.E-Commerce.Services.ca000001.pl.hop.Variable.XSS
Actinic.E-Commerce.Services.ca000007.pl.REFPAGE.Variable.XSS
Adalis.D-Forum.Nav.PHP3.XSS
Adiscon.LogAnalyzer.index.php.Parameter.XSS.Vulnerability
Aditus.Consulting.JpGraph.Multiple.XSS.Vulnerabilities
Aditus.Consulting.JpGraph.MultipleXSS.Vulnerabilities
Adobe.Acrobat.Plugin.XSS
Adobe.ColdFusion.cfadminUserId.XSS.Vulnerability.APSB10-11
Adobe.ColdFusion.logintowizard.cfm.XSS
Adobe.ColdFusion.Multiple.XSS.Vulnerabilities.APSB09-12
Adobe.ColdFusion.probe.cfm.XSS
Adobe.ColdFusion.Scheduleedit.Cfm.XSS.Authentication.Bypass
Adobe.ColdFusion.Searchlog.XSS
Adobe.Flash.Player.ActiveX.iframe.XSS
Adobe.Flash.Player.Asfunction.Protocol.XSS
Adobe.Flash.Player.ExternalInterface.XSS
Adobe.Flash.Player.PCRE.XSS
Adobe.Flash.Player.Unescaped.JS.String.XSS
Adobe.Flash.Player.Unescaped.String.XSS
Adobe.Flash.Player.XSS
Adobe.Flex.History.Management.XSS
Adobe.Reader.Input.validation.XSS
ADODB.Tmssql.php.XSS
AdPeeps.XSS.and.HTML.Injection.Vulnerabilities
Advantech.WebAccess.gUpdate.asp.XSS
Advantech.WebAccess.HMI.SCADA.Software.XSS
Aestiva.HTML.OS.error.message.XSS
Aestiva.HTML.OS.XSS
AfterLogic.WebMail.Pro.Multiple.XSS
Aktivate.Shopping.System.catgy.cgi.desc.Variable.XSS
Alan.Ward.A-Cart.MSG.XSS.Vulnerability
Annuaire.1Two.XSS
Apache.1.3.HTTP.Server.Expect.Header.XSS
Apache.ActiveMQ.XSS
Apache.Archiva.Multiple.Cross-Site.Request.Forgery.and.XSS.Vuln
Apache.DoS.And.XSS.Attack
Apache.Expect.Header.XSS
Apache.Geronimo.XSS
Apache.Hadoop.Jetty.XSS
Apache.HTML.Injection.And.UTF7.XSS

Apache.HTTP.Server.413.Error.HTTP.Request.Method.XSS
Apache.HTTP.Server.Error.Page.Host.XSS
Apache.HTTP.Server.Error.Pages.XSS
Apache.httpd.mod_imap.module.XSS
Apache.Jakarta.Results.JSP.XSS
Apache.Mod.Perl.Status.XSS
Apache.Mod.Proxy.Ftp.Undefined.Charset.UTF7.XSS
Apache.Mod.Proxy.Ftp.Wildcard.Characters.XSS
Apache.Mod.Status.Status.Pages.XSS
Apache.MOD_IMAGEIMAP.Module.XSS
Apache.mod_negotiation.Filename.Handling.XSS
Apache.mod_ssl.Wildcard.DNS.XSS
Apache.MyFaces.Tomahawk.JSF.Framework.XSS
Apache.OFBiz.Webslinger.Component.XSS
Apache.printenv.XSS
Apache.Struts.cookbook.processSimple.do.Multiple.XSS.Vuln
Apache.Struts.Error.Response.XSS
Apache.Struts.struts-examples.upload-submit.do.Multiple.XSS
Apache.Struts.struts2-showcase.edit-person.action.XSS.Vuln
Apache.Struts.XSS
Apache.Tomcat.3.0.to.3.2.1.XSS
Apache.Tomcat.4.1.XSS
Apache.Tomcat.4.and.5.Multiple.XSS
Apache.Tomcat.4.Sendmailer.Servlet.Web.Application.XSS
Apache.Tomcat.5.implicit-objects.jsp.XSS
Apache.Tomcat.Cal2.JSP.XSS
Apache.Tomcat.Calendar.Application.XSS
Apache.Tomcat.DOS.Device.Name.XSS
Apache.Tomcat.Example.XSS
Apache.Tomcat.Host.Manager.XSS
Apache.Tomcat.HTML.Manager.Interface.XSS
Apache.Tomcat.Jsp.Examples.XSS
Apache.Tomcat.Manager.XSS
Apple.CUPS.Web.Interface.URL.Handling.XSS
Apple.QuickTime.Darwin.Streaming.Server.Parse_XML.CGI.XSS
Apple.Safari.Feed.URI.Input.Validation.XSS
Apple.Safari.Parent.Top.Property.XSS
applications: Fusebox.Index.CFM.XSS
Arbor.Networks.Peakflow.SP.index.XSS
AskSam.Web.Publisher.As_web4.XSS
ASP.Net.Unicode.Conversion.XSS

ASP.Portal.XSS
ASP.topics.asp.CATIT.Parameter.XSS
Asterisk.Recording.Interface.XSS
Asus.Routers.Reflected.XSS.and.Authentication.Bypass.Vuln
Atlassian.Confluence.Error.Page.XSS
Atlassian.Confluence.Prior.to.3.4.8.Multiple.XSS
Atlassian.JIRA.c0-id.Parameter.XSS
Atlassian.JIRA.Multiple.XSS.Vulnerabilities..2007.12.24
Atlassian.JIRA.ViewProfile.Page.XSS.Vulnerability.2008.10.29
Atlassian.JIRA.XSS.HTTP.Header.Injection.Vulns.2009.04.02
Atlassian.JIRA.XSS.Vulnerability.in.Issue.Actions.2008.02.21
AtMail.WebMail.Email.Body.HTML.Injection.and.Multiple.XSS.Vuln
Atmail.XSS.Vulnerability
AutoInde.search.parameter.XSS
AWStats.awstats.pl.URL.Handling.XSS
AXIGEN.Mail.Server.XSS
Axon.Virtual.PBX.logon.Multiple.Parameter.XSS.Vulnerabilities
Aztek.Forum.forum_2.php.XSS
Bandmin.1.4.XSS
BASE.base_local_rules.php.dir.Parameter.XSS
Basit.CMS.XSS
BEA.WebLogic.InteractiveQuery.jsp.XSS
BEA.WebLogic.Server.Express.XSS
BEA.Weblogic.XSS
BitDefender.Internet.Security.2009.File.Name.XSS
BlackBoard.5.login.pl.url.Parameter.XSS
BLOB.Blog.System.bpost.php.XSS.Vulnerability
Blog.Torrent.BTDownload.PHP.XSS
BMC.Remedy.Knowledge.Management.Multiple.XSS
BNET.Software.HTML.XSS
BreakCalendar.XSS
BreakCalendar.XSS.Flaw
Bugzilla.Multiple.XSS.and.Information.Disclosure.Vuln
Bugzilla.Multiple.XSS.Vulnerabilities
Bugzilla.XSS.and.CRLF.Multiple.Vulnerabilities
Bugzilla.XSS.And.Insecure.Temporary.Filenames
BuildBot.Web.Status.XSS.Vulnerability
Cacti.0.8.7e.Multiple.XSS.and.Arbitrary.Command.Execution
Cacti.Prior.to.0.8.7g.Multiple.XSS.Vulnerabilities
CactuShop.XSS.SQL.Injection.Vulns
Cart32.GetLatestBuilds.XSS

Caucho.Resin.Data.Handling.XSS
Caucho.Resin.Multiple.HTML.Injection.and.XSS
cc_guestbook.pl.XSS
CGI.Ceilidh.XSS
CGI.Happymall.ECommerce.NormalHTML.cgi.XSS
CGI.Referer.XSS
CGIEmail.1.4.Cgisco.query.Variable.XSS.Vulnerability
CGIEmail.1.6.Cgisco.query.Variable.XSS.Vulnerability
CGIWrap.cgiwrap.XSS
Chance.i.DiViS.Web.DVR.System.XSS
Check.Point.VPN1.UTM.Edge.Login.Page.XSS
Cherokee.Error.Page.XSS
Chimara.Web.Portal.Mutiple.Inputs.XSS
Chimera.Web.Portal.Multiple.Inputs.XSS
Chipmunk.Guestbook.AddEntry.PHP.XSS
Cisco.ACS.UCP.CSuserCGI.XSS
Cisco.Collaboration.Server.LoginPage.jhtml.XSS.Vulnerability
Cisco.Common.Services.Devices.Center.XSS
Cisco.EPC3925.Goform.Quick.Setup.XSS
Cisco.Secure.ACS.LoginProxy.CGI.XSS
Cisco.Subscriber.Edge.Services.Manager.XSS.And.HTML.Injection
Cisco.Unified.Operations.Manager.Multiple.XSS
Cisco.Unified.Operations.Manager.XSS
Cisco.Unity.Express.XSS
Cisco.Wireless.Lan.Controller.XSS
Citrix.MetaFrame.XP.XSS.Vulnerability
Citrix.NFuse.launch.asp.NFuse_Application.Variable.XSS.Vuln
Citrix.NFuse.launch.jsp.NFuse_Application.Variable.XSS.Vuln
Citrix.NFuse.XSS.Vulnerability
CjOverkill.trade.php.XSS
ClanSphere.text.Parameter.XSS.Vulnerability
ClarkConnect.proxy.php.XSS
Claroline.add_course.XSS
ClearTrust.XSS
Clixint.DPI.Image.Hosting.Script.XSS.Vulnerability
CMS.Made.Simple.editprefs.php.XSS.Vulnerability
CodeMeter.WebAdmin.licenses.html.XSS.Vulnerability
collector.ch.myGesuad.Multiple.SQL.Injection.and.XSS
Comersus.Cart.XSS
Coppermine.Photo.Gallery.css.Parameter.XSS
Coppermine.Photo.Gallery.Multiple.XSS.Vulnerabilities

Coppermine.Photo.Gallery.XSS
COWS.CGI.Online.Worldweb.Shopping.Diagnose.CGI.XSS
Cpanel.Multiple.Script.XSS
CubeCart.multiple.PHP.files.XSS
CuteNews.index.php.XSS
CuteNews.show_news.php.XSS
Cyphor.footer.php.XSS
D-Link.DIR-300.tools_admin.php.XSS
D-Link.MDIR-645.Multiple.XSS
daloRADIUS.login.php.error.Parameter.XSS
database: Oracle.Reports.10g.test.jsp.XSS
Datenbank.Module.For.PHPBB.XSS
DCP-Portal.calendar.php.year.variable.XSS
Default.Monkey.Server.test2.pl.Unspecified.Variable.XSS.Vuln
Dell.OpenManage.Server.Administator.XSS.Vulnerability
DevoyBB.XSS.SQL.Injection.Vulns
DHCP.Discover.Hostname.XSS
DLink.DSL.redpass.cgi.XSS
DNS4Me.XSS
Dokeos.add_course.XSS
DotNetNuke.Prior.to.5.2.SearchResults.aspx.Search.parameter.XSS
DotNetNuke.Prior.to.5.3.SearchResults.aspx.Search.parameter.XSS
Drake.CMS.UI.DTA.PHP.XSS
Drupal.Forum.XSS
Drupal.Multiple.XSS.and.Access.Bypass.Vulns.SA-CORE-2013-001
DVBBS.7.1.XSS
DVBBS.showerr.asp.XSS
Eclipse.IDE.Help.Component.XSS
eFront.Multiple.Parameters.XSS.And.SQL.Injection
eGroupWare.XSS.Vulnerability
Ektron.CMS400.NET.id.Parameter.XSS
Ektron.CMS400.NET.reterror.aspx.XSS.Vulnerability
Email.Attachment.MIME.JPG.XSS
Escapade.Scripting.Engine.PAGE.Variable.XSS.Vulnerability
Expinion.Net.Member.Management.System.XSS.Vulnerability
Expinion.Net.MMS.Error.asp.XSS
Expinion.Net.MMS.XSS
eZ.Publish.ezjscore.Module.XSS
eZ.Publish.index.php.XSS.Vulnerability
ezPublish.2.27.Search.Parameter.XSS.Vulnerability
F-Secure.Policy.Manager.WebReporting.Multiple.XSS.Vuln

Faq-O-Matic.fom.cgi.cmd.XSS
Faq-O-Matic.fom.cgi.file.Vulnerablity.to.XSS
Faq-O-Matic.XSS
FastCGI.echo.exe.XSS.Vulnerability
FastCGI.echo.XSS.Vulnerability
FastCGI.echo2.exe.XSS.Vulnerability
FastCGI.echo2.XSS.Vulnerability
FastCGI.Samples.XSS
FeedList.Plugin.for.WordPress.Parameter.XSS
FireStats.WordPress.Plugin.Multiple.XSS.Authentication.Bypass
FlashCard.ID.Parameter.XSS
FlatNuke.help.php.or.footer.php.XSS
FlatNuke.index.php.XSS
Fork.CMS.XSS.and.Local.File.Inclusion.Vulnerabilities
Foro.Domus.Escribir.PHP.XSS
Fortigate.Firewall.dlg.Admin.Interface.XSS
Fortigate.Firewall.policy.Admin.Interface.XSS
Forum.Livre.Busca2.ASP.Palavra.XSS
FreePBX.Callmenum.Remote.Code.Execution.And.XSS
Fusebox.Index.CFM.XSS
FuseTalk.tombstone.cfm.ProfileID.XSS
Gallery.search.php.searchstring.Variable.XSS.Vulnerability
Gallery.XSS.Vulnerability
GeekLog.1.3.7.profiles.php.uid.variable.XSS.vulnerability
GeekLog.Comment.php.CID.Variable.XSS.Vulnerability
Generic.Referer.XSS.Attempt
Genium.CMS.Galerie.XSS
GForge.account.verify.php.confirm_hash.Parameter.XSS
GForge.help.tracker.php.helpname.Parameter.XSS
GlassFish.Enterprise.Server.Multiple.XSS.Vulns
GoAhead.WebServer.XSS
Google.Chrome.XSSAuditor.Filter.Security.Bypass
Goollery.XSS.Viewpic
GPhotos.affich.php.image.Parameter.XSS
GPhotos.diapo.php.rep.Parameter.XSS
Hastymail2.Background.CSS.Attribute.XSS.Vulnerability
HNS.title.cgi.XSS.Vulnerability
Horde.App.Framework.icon_browser.php.XSS.Vuln
Horde.Groupware.Webmail.Edition.Ingo.Filter.Post.Request.XSS
Horde.IMP.Multiple.XSS
Horde.IMP.XSS.Vulnerability

Horde.php.subdir.Parameter.XSS
HP.Insight.Diagnostics.XSS
HP.Network.Node.Manager.I.Multiple.XSS
HP.OpenView.Performance.Insight.XSS.Vulnerability
HP.Power.Manager.CSRF.And.XSS.Vulnerabilities
HP.SMH.Remote.XSS.Vulnerability
HP.System.Management.Homepage.XSS
htDig.htsearch.XSS
HTTP.Accept-Language.Header.XSS
HTTP.Malformed.Request.XSS
HTTP.Referer.Header.XSS
HTTP.Request.UserAgent.XSS
HTTP.URI.Script.XSS
HTTP.URI.XSS
IBM.Directory.Server.ldacgi.exe.XSS.Vulnerability
IBM.Lotus.Connections.Name.XSS
IBM.Lotus.Domino.HTTP.Response.Splitting.and.XSS.Vulns
IBM.Lotus.Domino.XSS
IBM.Lotus.Notes.XSS
IBM.Lotus.Sametime.Client.Potential.XSS
IBM.Lotus.Sametime.Server.Multiple.XSS.Vulnerabilities
IBM.Notes.Bypass.Restrictions.and.XSS.Vulnerabilities
IBM.Rational.Clearcase.Pathinfo.XSS
IBM.Tivoli.Directory.Server.XSS.Vulnerability
IBM.Tivoli.Endpoint.Manager.Web.Reports.ScheduleParam.XSS
IBM.Tivoli.Monitoring.Eclipse.Help.Server.XSS
IBM.WAS.Administration.Console.XSS.Vulnerability
IBM.Web.Traffic.Express.Caching.Proxy.HTTP.GET.Request.XSS
IBM.WebSphere.App.Server.Admin.Console.XSS.and.mod_ibm_ssl
IBM.Websphere.Application.Server.Webcontainer.XSS
IBM.WebSphere.Application.Server.XSS
iBoutique.page.Parameter.SQL.Injection.and.XSS.Vulnerabilities
IceWarp.Mail.Server.XSS.Vulns
IceWarp.Webmail.addressaction.html.XSS.vulnerability
IceWarp.XSS
IdeoContent.Manager.XSS
IIS5.Sample.App.XSS.Attack
IMP.Content-Type.XSS
Inktomi.Traffic.Server.XSS
InShop.InMail.XSS.Vulns
InterWoven.WorkDocs.XSS

Invision.Power.Board.BBCode.XSS.Vulnerability
Invision.Power.Board.Referer.XSS
Invision.Power.Board.SML.XSS
Invision.Power.Board.XSS
JelSoft.VBulletin.search.php.XSS
Jetty.JSP.Servlet.Engine.XSS.Vulnerability
Jetty.Persistent.XSS.in.Sample.Cookies.Application
JEUS.Web.Server.Input.Validation.Flaw.Permits.Remote.XSS
Jive.Openfire.User.Properties.XSS
Joomla!.JA_Purity.Template.XSS.Vulnerability
Joomla!.Komento.Component.Multiple.XSS.Vuln
Joomla!.Youtube.Gallery.Component.videofile.XSS.Vuln
Joomla.Currency.Converter.Module.XSS.Vulnerability
Joomla.Lyftenbloggie.XSS.Vulnerability
Joomla.Multiple.XSS.and.Information.Disclosure.Vulns
Joomla.Prior.to.1.6.4.Multiple.XSS
Joomla.URI.Index.php.XSS
JServ.Non-existent.JSP.File.XSS.Vulnerability
JServ.non-existent.jsp.XSS
JShop.E-Commerce.xSearch.XSS
Juniper.Networks.JUNOS.JWeb.Multiple.XSS.And.HTML.Injection
Kayako.ESupport.XSS.SQL.Injection.Vulns
Kayako.SupportSuite.Ticket.Subject.XSS.Vulnerability
KDE.Konqueror.KHTML.Library.Title.XSS
Keene.Digital.Media.Server.XSS
Kerio.MailServer.Buffer.Overflow.XSS.Vulns
Keyfax.Customer.Response.Management.Multiple.XSS
Kingsoft.Webshield.XSS
Led-Forums.Index.php.Topmessage.Variable.XSS.Vulnerability
LedForums.Forums.Index.php.Top_message.Variable.XSS
Link.Bank.Site.XSS
Linksys.WVC54GCA.Wireless-g.XSS
LiteSpeed.ConfMgr.PHP.M.XSS
Lotus.Domino.Server.XSS.Vulnerability
Lycos.htmlGEAR.Guestbook.XSS
Macromedia.ColdFusion.Missing.Template.XSS.Vulnerability
Macromedia.JRun.JMC.Interface.clusterframe.jsp.XSS.Attack
Macromedia.Sitespring.500error.jsp.et.Variable.XSS.Vuln
Mail.showmail.pl.folder.Variable.XSS.Vulnerability
MailEnable.Webmail.XSS
MailEnable.Webmail.XSS.Vulnerability

Mailman.listinfo.XSS.Vulnerability
Mailman.ml-name.Feature.Multiple.Variable.XSS
Mailman.Prior.to.2.1.14.Multiple.XSS..Vulnerabilities
Mailtraq.Browse.ASP.XSS
MakeBid.Auction.Deluxe.XSS
Mambo.administrator/upload.php.choice.XSS
Mambo.emailarticle.php.id.XSS
Mambo.emailfaq.php.id.Variable.XSS
Mambo.emailnews.php.id.Variable.XSS
Mambo.mambosimple.php.sitename.Variable.XSS
Mambo.Site.Server.gallery.php.XSS.Vulnerability
Mambo.Site.Server.navigation.php.XSS.Vulnerability
Mambo.Site.Server.upload.php.XSS.vulnerability
Mambo.Site.Server.uploadimage.php.XSS.Vulnerability
Mambo.Site.Server.view.php.Path.Variable.XSS.Vulnerability
ManageEngine.ADAudit.Plus.reportList.Param.XSS
ManageEngine.ADManager.Plus.computerName.Param.XSS
ManageEngine.ADManager.Plus.Multiple.XSS.Vulnerabilities
ManageEngine.ADSelfService.Plus.SearchString.XSS
ManageEngine.App.Manager.Multiple.XSS.and.SQL.Injection.Vuln
ManageEngine.ServiceDesk.Plus.SolutionSearch.do.XSS.Vuln
Mantis.Multiple.Unspecified.XSS
Mantis.Multiple.XSS.and.SQL.Injection
Mantis.view.all.set.php.XSS
MantisBT.Multiple.Local.File.Include.andXSS.Vulns
MantisBT.NuSOAP.XSS.Vulnerability
MantisBT.Prior.to.1.2.3.Multiple.XSS.Vulnerabilities
MantisBT.Prior.to.1.2.7.Multiple.XSS.Vulnerabilities
MantisBT.XSS.And.SQL.Injection
Max.Web.Portal.search.asp.Search.Variable.XSS
McAfee.ePolicy.Orchestrator.XSS.Vuln.KB78824
McAfee.WebShield.UI.dashboard.XSS.Vulnerability
McAfee.WebShield.UI.ProcessTextFile.XSS.Vulnerability
MDaemon.WorldClient.Prior.to.12.5.7.Multiple.XSS.Vuln
MediaWiki.AJAX.Index.PHP.XSS
MediaWiki.Backslash.Escaped.CSS.Comments.XSS
MediaWiki.CSS.Comments.XSS
MediaWiki.Parser.Script.Insertion.XSS
Mediawiki.SVG.XSS.and.Password.Reset.Vuln
MediaWiki.uselang.Parameter.XSS
MediaWiki.XSS.Vulnerability

MegaBook.admin.cgi.login.name.XSS.Vulnerability
MercuryBoard.f.Parameter.XSS
MercuryBoard.Index.Php.XSS
Mewsoft.NetAuction.auction.cgi.Term.Variable.XSS
MHonArc.SMTP.XSS
Microsoft.IIS.Redirect.Response.XSS.Vuln
Microsoft.Internet.Explorer.XSS.Filter.SCRIPT.Tag.XSS.Vuln
Microsoft.SharePoint.Services.Help.Page.cid0.Parameter.XSS
Microsoft.SharePoint.Upload.aspx.XSS.Vulnerability
Microsoft.Site.Server.Default.asp.XSS
Microsoft.Site.Server.formslogin.asp.url.Parameter.XSS
Mini.Web.Shop.Viewcategory.PHP.XSS
MiniBB.XSS.Vuln
MIT.Cgiemail.Cgicso.Query.Variable.XSS.Vulnerability
MODx.Evolution.CMS.SearchHighlight.Plugin.XSS.Vulnerability
MODx.Revolution.CMS.modahsh.Parameter.XSS.Vulnerability
MoniWiki.Wiki.PHP.XSS
Monkey.HTTP.Daemon.Sample.Script.XSS
Moodle.XSS
Mozilla.Browser.Zombie.Document.XSS
Mozilla.Browsers.CSS.Moz-binding.XSS
Mozilla.Firefox.IFRAME.XSS
Mozilla.Firefox.Javascript.BOM.Characters.XSS
Mozilla.Firefox.Javascript.Html.Escaped.Surrogates.XSS
Mozilla.Firefox.Locationbar.XSS
MoziloCMS.Local.File.Include.and.XSS
MS.Anti.XSS.Library.Bypass.Information.Disclosure
MS.AntiXSS.Lib.Info.Disclosure
MS.ASP.DotNET.XSS
MS.ASP.NET.Framework.XSS
MS.ASP.NET.XSS
MS.ASP.NET.XSS.B
MS.Dynamics.AX.Enterprise.Portal.XSS
MS.Exchange.OWA.From.XSS
MS.Exchange.OWA.HTML.Parse.XSS
MS.Exchange.OWA.XSS.Spoofing
MS.Exchange.Server.5.5.Outlook.Web.Access.XSS
MS.Exchange.Server.Outlook.Web.Access.XSS
MS.Forefront.UAG.Mobile.Portal.Website.XSS
MS.Forefront.UAG.Server.default.asp.XSS
MS.Forefront.UAG.Server.tableData.XSS

MS.Forefront.UAG.Server.XSS
MS.Forefront.UAG.Signurl.XSS
MS.Forefront.UAG.XSS
MS.Frontpage.Server.Extension.fpadmdll.dll.XSS
MS.IE.CSS.expression.Property.XSS
MS.IE.EUC.JP.Character.Encoding.Universal.XSS
MS.IE.FTP.Web.View.XSS
MS.IE.Malformed.Image.XSS
MS.IE.NavCancel.HTM.XSS
MS.IE.NavCancel.XSS
MS.IE.SharePoint.toStaticHTML.XSS
MS.IE.toStaticHTML.Function.XSS
MS.IE.TOSTATICHTML.HTML.Sanitization.XSS
MS.IE.Windows.MHTML.XSS
MS.IE.XSS.Filter.Information.Disclosure
MS.IE7.navcancl.htm.XSS
MS.IIS.Help.File.Search.XSS
MS.IIS.HTTP.Error.Page.XSS
MS.IIS.IDC.Extension.XSS
MS.IIS.IndexServer.Htw.XSS
MS.IIS.Redirection.Error.Page.XSS
MS.Indexing.Service.IIS.XSS
MS.ISA.Server.Forefront.TMG.Cookieauth.Dll.XSS
MS.Lync.Meeting.URL.XSS
MS.Mulitple.Server.CSS.Expressions.XSS
MS.Office.CDO.XSS
MS.Outlook.Web.Access.XSS
MS.Remote.Desktop.Web.Access.XSS
MS.Remote.Desktop.Web.Access.XSS.Vuln.MS11-061
MS.Report.Viewer.TimeMethod.XSS
MS.SCCM.XSS
MS.SCOM.Web.Console.XSS
MS.SharePoint.Calendar.CalendarData.XSS
MS.SharePoint.EditForm.TEXTFIELD.SPSAVE.XSS
MS.SharePoint.inplview.aspx.XSS
MS.SharePoint.Query.Iqy.XSS
MS.SharePoint.Reflected.List.Parameter.XSS
MS.SharePoint.Server.Filter.Aspx.XSS
MS.SharePoint.Server.Help.aspx.XSS
MS.SharePoint.Server.Lists.XSS
MS.Sharepoint.Server.PlaceHolderDialogBodySection.XSS

MS.SharePoint.Server.Remote.XSS
MS.SharePoint.Server.scriptresx.ashx.XSS
MS.SharePoint.Server.XSS
MS.SharePoint.themeweb.aspx.XSS
MS.SharePoint.Username.XSS
MS.SharePoint.Web.Analytics.XSS
MS.SharePoint.Wiki.Page.HTTP.Post.Request.XSS
MS.SharePoint.wizardlist.aspx.XSS
MS.SharePoint.Wizardlist.XSS
MS.SharePoint.XSS
MS.SQL.Injection.Table.XSS
MS.SqlServer.Reporting.Services.XSS
MS.Visual.Studio.Team.Server.Foundation.Multiple.XSS
MS.Windows.AD.Certificate.Service.XSS
MS.Windows.Management.Console.XSS
MS.Windows.MHTML.XSS
MS.Windows.MHTML.XSS.Attempt
MS.Windows.Remote.Desktop.Web.Access.XSS
MS.Windows.SharePoint.Services.and.SharePoint.Team.Services.XSS
MS.Windows.System.Center.Operations.Manager.Web.Console.XSS
My.Little.Forum.XSS
MyBB.Prior.to.1.6.1.Multiple.XSS.Vulnerabilities
MyBulletinBoard.XSS.and.SQL.Injection
MyBulletinBorad.1.0.0.XSS
myGuestBook.CGI.myguestbook.cgi.XSS
MySQL.Eventum.bugs.forgotpassword.php.email.variable.XSS
MySQL.Eventum.forgotpassword.php.email.Variable.XSS
MyWebServer.1.0.2.XSS.Vuln
MyWebServer.Long.URL.Error.Page.XSS
Nagios.XI.Alert.Cloud.XSS
Nagios.XI.Multiple.HTTP.XSS
NagiosQL.TxtSearch.Parameter.XSS
Namazu.namazu.cgi..multiple.XSS.Vulns
Naxtor.Edirectory.Message.ASP.XSS
Neoteris.IVE.XSS
Nessus.Web.Server.XSS.Vulnerability
NetGear.FVS318.Filter.Log.XSS
Network.Query.Tool.XSS
NetworkActiv.Web.Server.XSS
Nokia.Electronic.Documentation.XSS
Novell.GroupWise.Prior.7.03HP2.8.0HP1.WebAccess.Multi.XSS

Novell.GroupWise.WebAccess.Login.User.lang.Param.XSS
Novell.QuickFinder.Server.XSS
Nuke.Bookmarks.XSS
Nuked-Klan.Multiple.XSS.Vulns
Ocean12.Guestbook.XSS
ocPortal.Arbitrary.File.Disclosure.and.XSS.Vulnerabilities
OmniHTTPD.redir.exe.CGI.parameter.XSS
OmniHTTPd.test.php.Sample.Application.XSS
OmniHTTPd.test.shtml.Sample.Application.XSS
OneCMS.index.php.XSS.Vulnerability
Open.WebMail.Logindomain.Parameter.XSS.Vuln
OpenAdmin.Tool.for.Informix.informixserver.Parameter.XSS
OpenBB.board.php.XSS
OpenBB.member.php.XSS
OpenWebMail.Content-Type.XSS
Opera.Command.Execution.and.XSS.Vulnerability
Opera.Web.Browser.HTML.Injection.and.XSS
Oracle.Application.Server.Bpel.XSS
Oracle.Application.Server.Portal.XSS
Oracle.BEA.Weblogic.Linked.XSS
Oracle.BEA.Weblogic.Server.Console-help.Portal.XSS
Oracle.BPM.Process.Administrator.tips.jsp.XSS.Vulnerability
Oracle.Business.Intelligence.Enterprise.Edition.XSS
Oracle.GlassFish.Server.Malformed.Username.XSS
Oracle.GlassFish.Server.XSS
Oracle.HTTP.Server.Isqlplus.XSS
Oracle.HTTP.Server.XSS
Oracle.OpenSSO.XSS.POST.Injection
Oracle.Portal.JSP.tc.Parameter.Handling.XSS
Oracle.Reports.10g.test.jsp.XSS
Oracle.Reports.Server.XSS
Oracle.Reports.Web.Cartridge.RWCGI60.XSS
Oracle.Secure.Backup.Administration.Server.login.php.XSS
Oracle.Secure.Enterprise.Search.Linked.XSS
Oracle.Secure.Enterprise.Search.XSS
Oracle.WebCenter.Content.Component.XSS.Vulnerability
Oracle.Workflow.WfMonitor.XSS
Oracle.Workflow.Wfroute.XSS
Oracle9iAS.iSQLplus.XSS
Oracle9iAS.mod_plsql.XSS
osCommerce.default.php.error_message.XSS.Vulnerability

osCommerce.default.php.info_message.XSS.Vulnerability
OTRS.Prior.to.3.0.7.Multiple.XSS.Vulnerabilities
Owl.Intranet.Engine.XSS.SQL.Injection.Vulns
P2P.Server.Xedus.XSS
Palo.Alto.Firewall.Role.XSS
PeopleSoft.JMS.Listening.Connector.Activity.Param.XSS
Perception.LiteServe.Directory.Index.XSS
Phorum.Search.Script.XSS
PhotoADay.Pad_selected.Parameter.XSS
PhotoPost.PHP.Pro.XSS
PHP-Fusion.Homepage.Address.XSS
PHP-Nuke.comments.php.subject.Variable.XSS.Vulnerability
PHP-Nuke.download.php.dcategory.Variable.XSS.Vulnerability
PHP-Nuke.friend.php.fname.Variable.XSS.Vulnerability
PHP-Nuke.Viewpage.php.XSS.Vuln
PHP-Nuke.Your_Account.avatarcategory.XSS
PHP.CMS.Made.Simple.Index.php.XSS
PHP.CSS.Parameter.Remote.XSS
PHP.CSS.Parameter.XSS
PHP.FlatNuke.XSS
PHP.Guppy.XSS
PHP.index.php.SEARCH.Parameter.XSS
PHP.Index.php.Shard.Parameter.XSS
PHP.Invision.Power.Board.Multiple.XSS
PHP.phpinfo.3.Multiple.Method.User.Supplied.Array.XSS
PHP.phpinfo.Multiple.Method.User.Supplied.Array.XSS
PHP.PHPWCMS.XSS
PHP.PostNuke.TTitle.XSS
PHP.preview.php.FILE.Parameter.XSS
php.Reactor.Comments.Section.browse.php.go.Variable.XSS.Vuln
php.Reactor.Forums.Section.browse.php.go.Variable.XSS.Vuln
PHP.Riverdark.rss.php.XSS
PHP.upload.php.PATH.Parameter.XSS
PHP.WHM.AutoPilot.XSS
PHP.XSS.magic_quotes.vulnerabilities
PHP.Zeroboard.XSS
PhpAdsNew.configuration.file.XSS
phPay.search.php.lookfor.variable.XSS
phpBB.viewtopic.php.highlight.variable.XSS
phpBB.viewtopic.php.topic_id.variable.XSS
phpBook.guestbook.php.XSS

PHPCMS.parser.php.XSS
phpCMS.Parser.XSS
phpCommunityCalendar.XSS
Phpgroupware.Addressbook.Index.php.Name.Variable.XSS.Vuln
Phpgroupware.index.php.Surname.Variable.XSS.Vulnerability
PhpGroupWare.XSS.and.SQL.Injection.Issues
PHPImageView.phpimageview.php.pic.variable.XSS
PHPKIT.include.php.contact_email.Variable.XSS.Vulnerability
PhpMyAdmin.Convcharset.XSS
PHPMyAdmin.Error.php.XSS
PHPMyAdmin.Multiple.Libraries.And.Themes.Remote.XSS
phpMyAdmin.Multiple.XSS.Vulnerabilities.PMASA-2011-13
phpMyAdmin.Multiple.XSS.Vulnerabilities.PMASA-2011-18
phpMyAdmin.Multiple.XSS.Vulnerabilities.PMASA-2011-19/20
phpMyAdmin.Multiple.XSS.Vulnerabilities.PMASA-2012-4
phpMyAdmin.Prior.to.3.5.3.Multiple.XSS
phpMyAdmin.read_dump.php.XSS
phpMyAdmin.setup.php.Verbose.Server.Name.XSS.Vulnerability
PHPMyAdmin.XSS
PhpNuke.user.php.XSS.vulnerability
phpPgAdmin.Prior.5.0.3.Multiple.XSS.Vulnerabilities
PHPRaid.View.PHP.XSS
PHProxy.Error.Parameter.XSS
PHPSiteSearch.XSS
phpWebSite.0.8.3.article.php.sid.Variable.XSS.Vulnerability
phpWebSite.fatcat.Module.fatcat_id.Parameter.XSS
phpWebSite.Pagemaster.Module.PAGE_id.Parameter.XSS
phpWebSite.Search.Module.PDA_limit.Parameter.XSS
Pinnacle.Systems.ShowCenter.SettingsBase.PHP.XSS
Pivot.Multiple.XSS.HTML.Injection
PivotX.Prior.to.2.2.2.Multiple.XSS.Vulnerabilities
Piwigo.Photo.Gallery.Project.LocalFiles.Editor.Plugin.XSS
PmWiki.Search.XSS
PostNuke.index.php.catid.Variable.XSS.Vulnerability
PostNuke.user.php.img.src.Variable.XSS
Powie.PForum.Username.XSS
Project.Woodstock.UTF-7.404.Page.XSS
PsychoStats.Login.XSS
PunBB.IMG.Tag.Client.Side.Scripting.XSS
PunBB.Install.PHP.XSS
PunBB.Profile.PHP.XSS

PunBB.URL.Quote.Tag.XSS
Quick.Post.Widget.Plugin.XSS
raSMP.Index.PHP.User.Agent.XSS
Red.Hat.Apache.HTTP.Server.Multiple.XSS
Red.Hat.GNU.Mailman.Subscribe.XSS
ReviewPost.PHP.Pro.2.84.XSS
Revize.CMS.HTTPTranslatorServlet.XSS
Ricoh.Web.Image.Monitor.XSS
Rockliffe.MailSite.HTTP.Mail.Management.XSS
Ruby.on.Rails.Multiple.XSS.Vulns
RWAuction.Pro.Search.ASP.XSS
S9Y.Serendipity.Remote.XSS
Sage.CMS.mod.Variable.XSS.Vulnerability
Sambar.Server.create.stm.path.Variable.XSS
Sambar.Server.edit.stm.name.Variable.XSS
Sambar.Server.edit.stm.path.Variable.XSS
Sambar.Server.environ.pl.param1.Variable.XSS
Sambar.Server.findata.stm.host.Variable.XSS
Sambar.Server.findata.stm.user.Variable.XSS
Sambar.Server.ftp.stm.path.Variable.XSS
Sambar.Server.htaccess.stm.path.Variable.XSS
Sambar.Server.iecreate.stm.path.Variable.XSS
Sambar.Server.ieedit.stm.name.Variable.XSS
Sambar.Server.ieedit.stm.path.Variable.XSS
Sambar.Server.index.stm.wwwsite.Variable.XSS
Sambar.Server.info.stm.name.Variable.XSS
Sambar.Server.info.stm.path.Variable.XSS
Sambar.Server.ipdata.stm.ipaddr.Variable.XSS
Sambar.Server.mkdir.stm.path.Variable.XSS
Sambar.Server.Multiple.XSS
Sambar.Server.rename.stm.name.Variable.XSS
Sambar.Server.rename.stm.path.Variable.XSS
Sambar.Server.search.dll.query.Variable.XSS.Vulnerability
Sambar.Server.search.stm.path.Variable.XSS
Sambar.Server.search.stm.query.Variable.XSS
Sambar.Server.sendmail.stm.name.Variable.XSS
Sambar.Server.sendmail.stm.path.Variable.XSS
Sambar.Server.showfnc.stm.pkg.Variable.XSS
Sambar.Server.showfncs.stm.pkg.Variable.XSS
Sambar.Server.showfunc.stm.func.Variable.XSS
Sambar.Server.stmex.stm.bar.Variable.XSS.nikto.003254

Sambar.Server.stmex.stm.foo.Variable.XSS.nikto.003255
Sambar.Server.template.stm.path.Variable.XSS
Sambar.Server.testcgi.exe.XSS
Sambar.Server.Testisa.dll.Check1.Variable.XSS.Vulnerability
Sambar.Server.update.stm.name.Variable.XSS
Sambar.Server.update.stm.path.Variable.XSS
Sambar.Server.vccheckin.stm.name.Variable.XSS
Sambar.Server.vccheckin.stm.path.Variable.XSS
Sambar.Server.vccreate.stm.name.Variable.XSS
Sambar.Server.vccreate.stm.path.Variable.XSS
Sambar.Server.vchist.stm.name.Variable.XSS
Sambar.Server.vchist.stm.path.Variable.XSS
Sambar.Server.Whodata.Sitename.Variable.XSS.Vulnerability
SAP.CFolders.XSS
SAP.Crystal.Reports.Server.logonAction.Parameter.XSS
SAP.Crystal.Reports.viewreport.asp.XSS
SAP.Internet.Transaction.Server.Multiple.XSS
SAP.Internet.Transaction.Server.wgate.dll.XSS
SAP.Internet.Transaction.Server.XSS
SAP.Web.Application.Server.Webgui.XSS
SelectaPix.XSS
Semantic.Enterprise.Wiki.XSS.vulnerability
Seo.Panel.XSS.Vulnerability
Serendipity.comment.php.XSS
Serendipity.XSS.Vulnerability
sgdynamo.exe.XSS.Vuln
SHOUTcast.Server.logfiles.XSS
SilverStripe.Forums.Module.Search.Parameter.XSS
SimpleGroupware.export.Parameter.XSS.Vuln
SIP.Header.Remote.XSS
SIP.Header.XSS
Sitecore.CMS.sc_error.Parameter.XSS.Vulnerability
Siteframe.search.php.searchfor.Variable.XSS.Vulnerability
Siteman.Page.Parameter.XSS
SixCMS.List.PHP.XSS
Snitz.Forums.2000.members.asp.SQL.Injection.and.XSS.Vuln
Snitz.Forums.Search.ASP.XSS
SNMP.XSS.Attempt
Sockso.Registration.Persistent.XSS.Vuln
SolarWinds.Orion.IPAM.Reflected.XSS
Sophos.Web.Protection.Appliance.XSS

Sphinx.Mobile.Web.Server.XSS.Vulnerability
Splunk.4.x.Prior.4.1.3.404.Response.XSS
Splunk.Prior.to.5.0.8.Unspecified.XSS.Vuln.SP-CAAAKQX
Splunk.Reflected.XSS.Vulnerability.SP-CAAAHXG
SQLiteManager.dbsel.And.nsextt.Parameters.Multiple.XSS.Vuln
SQLiteManager.Main.PHP.XSS
SQLiteManager.main.php.XSS.Vulnerability
SquirrelMail.addressbook.php.multiple.variable.XSS
SquirrelMail.help.php.chapter.variable.XSS
SquirrelMail.options.php.optpage.variable.XSS
SquirrelMail.read.body.php.XSS
SquirrelMail.search.php.multiple.variable.XSS
Stalker.CommuniGate.Pro.WebMail.URI.Parsing.XSS
Sun.AnswerBook2.Documentation.Search.Function.XSS
Sun.Application.Server.Error.Message.XSS
Sun.Cobalt.RaQ.message.cgi.info.variable.XSS
Sun.iPlanet.Admin.Server.XSS
Sun.iPlanet.WebServer.Admin.Server.XSS
Sun.Java.Calendar.Server.Command.Shtml.Multiple.XSS.Vuln
Sun.Java.Calendar.Server.Command.Shtml.XSS
Sun.Java.Communications.Express.UWCMain.XSS
Sun.Java.System.Identity.Manager.activeControl.XSS
Sun.Java.System.Portal.Server.Multiple.XSS.Vuln
Sun.Java.Web.Console.help.JSP.Scripts.Multiple.XSS
Sun.Solaris.Tomcat.Directory.Traversal.and.XSS.251986
SurgeLDAP.User.CGI.XSS
SurgeMail.surgeweb.XSS
Symantec.Endpoint.Protection.Mgr.XSS.and.CSRF.Vulnerability
Symantec.IM.Manager.Multiple.XSS
Symantec.SecurityExpressions.Audit.and.Compliance.Server.XSS
Symantec.Web.Gateway.Blacklist.PHP.XSS
Symantec.Web.Gateway.Multiple.PHP.Pages.XSS
Symantec.Web.Gateway.XSS
Sympoll.index.php.vo.Variable.XSS.Vulnerability
Syneto.Unified.Threat.Management.Index.php.XSS
TclHttpd.debug.module.dbg.XSS
TclHttpd.debug.module.echo.XSS
TclHttpd.debug.module.errorInfo.XSS
TclHttpd.debug.module.showproc.XSS
TechSmith.Camtasia.swf.cspreloader.XSS
Teekais.Tracking.Online.XSS

Telnet.Login.Remote.XSS
Telnet.Login.XSS
TemaTres.SQL.Injection.and.XSS.Vulnerabilities
TestLink.login.php.req.Parameter.XSS
TheWebForum.twf.Register.PHP.XSS
Tiki.Wiki.CMS.Groupware.snarf_ajax.php.XSS.Vulnerability
TikiWiki.Multiple.XSS
TikiWiki.tiki-error.php.XSS
Tiny.Web.Gallery.Index.PHP.XSS
TinyPHPForum.Action.PHP.XSS
TippingPoint.Web.Interface.Reverse.DNS.Lookup.XSS
TMax.Jeus.url.jsp.XSS
Tomcat.Calendar.App.cal2.jsp.time.Parameter.XSS
Tomcat.Documentation.Sample.Multiple.XSS.Vulnerabilities
Tomcat.JSP.Examples.Web.Application.Multiple.XSS
Tomcat.Manager.Host.Manager.Upload.Script.XSS
Topic.Calendar.calendar_scheduler.XSS
Trend.Micro.InterScan.Messaging.Security.Suite.XSS
TrendMicro.InterScan.Messaging.Security.Suite.XSS
TWiki.Multiple.XSS.Vulnerabilities
TWiki.newtopic.Parameter.XSS.Vulnerability.
TWiki.organization.XSS.Vulnerability
Twitter.Feed.for.WordPress.Plugin.XSS.Vulnerability
Typo3.BodyTag.URI.XSS
UBBCentral.UBB.threads.XSS.Vulns
Ultimate.HelpDesk.Index.ASP.XSS
Ultraseek.Multiple.Buffer.Overflows.and.XSS
Unobtrusive.Ajax.Star.Rating.Bar.rpc.php.q.Variable.XSS
URI.Request.XSS
UseModWiki.Wiki.PL.XSS
Vbulletin.2.2.9.memberlist.php.XSS
vBulletin.3.0.7.XSS
vBulletin.3.0.9.XSS
vBulletin.before.3.0.9.XSS
VCard.Pro.Create.PHP.XSS
ViewCVS.CGI.viewcvs.cgi.url.Parameter.XSS
ViewCVS.CGI.viewcvs.cgi/viewcvs/.cvsroot.Parameter.XSS
ViewCVS.XSS.Vuln
ViewVC.viewvc.cgi.Search.Parameter.XSS.Vulnerability
Vignette.Server.Var.Parameter.XSS.vulnerability
VP-ASP.Shopping.Cart.shopadmin.asp.UserName.Variable.XSS

W3C.Jigsaw.Server.Error.Page.XSS
WackoWiki.XSS.Vuln
WBBlog.Parameter.Remote.XSS
Web.Authoring.Tools.Flash.Files.XSS
Web.Server.XSS
Web.Server.Zeus.XSS
Web.Wiz.Forums.forum_members.asp.XSS.Vulnerability
Web.Wiz.Forums.Members.Asp.XSS.Vulnerability
Web.Wiz.Forums.Multiple.pm_buddy_list.asp.XSS
Web.Wiz.Forums.XSS.Vulnerability
WebCalendar.colors.php.color.XSS
Webcalendar.week.php.url.Parameter.XSS
WebCalendar.week.php.user.XSS
WebChat.XSS.Vuln
Webmi.Cgi.Page.Parsing.XSS
Webmin.Search.Parameter.XSS
web_app: Inktomi.Traffic.Server.XSS
web_app: URI.Request.XSS
web_client: Mozilla.Browsers.CSS.moz-binding.XSS
web_server: HTTP.URI.Script.XSS
WordPress.All-in-One.Event.Calendar.Plugin.XSS.Vulnerabilities
WordPress.cformsII.Plugin.rs.and.rsargs.XSS
Wordpress.Count.per.Day.Plugin.Multiple.XSS.Vulns
WordPress.Count.Per.Day.Plugin.XSS
Wordpress.Default.Theme.Admin.XSS
WordPress.mb.miniAudioPlayer.Plugin.XSS.Vulnerabilities
WordPress.Occasions.Plugin.XSS
Wordpress.PHP.Application.XSS
WordPress.Platinum.SEO.Pack.Plugin.s.Parameter.XSS.Vuln
WordPress.post.php.XSS
WordPress.Prior.to.3.5.2.Multiple.XSS.Vulnerabilities
WordPress.RSS.Feed.Generator.self_link.HTTP_HOST.XSS
WordPress.Simply.Poll.Plugin.XSS
WordPress.TinyMCE.Color.Picker.Plugin.XSS.and.Bypass.Vuln
WordPress.Traffic.Analyzer.Plugin.aoid.Parameter.XSS.Vuln
WordPress.WP-Cumulus.Plugin.tagcloud.swf.XSS
WordPress.WP.Banners.Lite.Plugin.XSS
WordPress.WP.E.Commerce.Plugin.cart.message.XSS
WordPress.Wptitle.XSS
WordPress.XSS.HTML.Injection.SQL.Injection
WordPress.XSS.SQL.Injection

WordPress.XSS.Vulnerability
WowBB.XSS.SQL.Injection
Wrensoft.Zoom.Search.Engin.search.php.zoom_query.Variable.XSS
XAMPP.for.Windows.Multiple.XSS.and.SQL.Injection
Xitami.XSS.Vulnerability
XMB.XSS
XOOPS.Dictionary.Module.XSS
Xoops.glossaire-aff.php.XSS
XOOPS.misc.php.Query.String.XSS
Xoops.myheader.php.URL.XSS
Xoops.Viewtopic.php.XSS
XSS.Vulnerabilities.In.Common.Shockwave.Flash.Files
YaBB.index.php.Password.Field.XSS.Vulnerability
YaBB.pl.XSS.And.Administrative.Commands
YACY.Peer-To-Peer.Search.Engine.XSS
Yoast.Google.Analytics.For.WordPress.Plugin.XSS
Zeroboard.XSS
Zeus.4.2r2.vs_diag.cgi.server.variable.XSS.vulnerability
Zeus.Admin.Server.index.fcgi.section.Parameter.XSS
ZOHO.ManageEngine.ADSelfService.Plus.SearchString.XSS

INTRUSHIELD

HTTP: Adobe Flash Player Adobe Flash Player XSS Exceptions Vulnerability (CVE-2014-0531)
HTTP: Adobe Flash Player Adobe Flash Player XSS Marshalling Data Vulnerability (CVE-2014-0533)
HTTP: Adobe Flash Player XSS Vulnerability
HTTP: Adobe Flash Player XSS vulnerability (CVE-2014-0509)
HTTP: Adobe Flash Player XSS Vulnerability(CVE-2014-0503)
HTTP: Adobe Reader FDF After Before XSS Vulnerability
HTTP: Advantech WebAccess HMI and SCADA Software XSS
HTTP: Apache SSI XSS Exploit
HTTP: Apache Wicket XSS Vulnerability
HTTP: Cross Site Scripting - Adobe Reader Firefox XSS Vulnerability
HTTP: Cross Site Scripting - Apache SSI XSS Exploit
HTTP: Cross Site Scripting - Apache Tomcat Servlet Mapping XSS Scripting
HTTP: Cross Site Scripting - Microsoft Forefront UAG Mobile Portal XSS Vulnerability
HTTP: Cross Site Scripting - Microsoft Forefront UAG Signurl XSS Vulnerability
HTTP: Cross Site Scripting - Microsoft Forefront UAG XSS Vulnerability

HTTP: Cross Site Scripting - Microsoft FrontPage Server Extensions XSS Scripting Vulnerability
HTTP: Cross Site Scripting - WordPress RSS Feed Generator self_link HTTP_HOST XSS Scripting
HTTP: HTTP SCCM XSS Javascript Injection
HTTP: Internet Explorer Navigation Cancel Page XSS
HTTP: InterWoven WorkDocs XSS Vulnerability
HTTP: Microsoft AntiXSS Library Bypass Vulnerability
HTTP: Microsoft Default Reflected XSS Vulnerability
HTTP: Microsoft ExcelTable Reflected XSS Vulnerability
HTTP: Microsoft ExcelTable Response Splitting XSS Vulnerability
HTTP: Microsoft Exchange OWA XSS and Spoofing Vulnerability
HTTP: Microsoft IE XSS Filter Information Disclosure Vulnerability
HTTP: Microsoft IIS Form_JScript.asp XSS
HTTP: Microsoft Internet Explorer Print Table of Links Local Zone XSS Vulnerability
HTTP: Microsoft Internet Explorer Shift_JIS Encoding XSS Vulnerability
HTTP: Microsoft Lync Server XSS Vulnerability (CVE-2014-1823)
HTTP: Microsoft Report Viewer Control XSS Vulnerability
HTTP: Microsoft Sharepoint Contact Details XSS Elevation of Privilege Vulnerability
HTTP: Microsoft Sharepoint XSS Elevation of Privilege Vulnerability
HTTP: Microsoft Sharepoint XSS Elevation of Privilege Vulnerability II
HTTP: Microsoft SharePoint XSS in inplview.aspx Vulnerability
HTTP: Microsoft SharePoint XSS in Scriptresx.ashx Vulnerability
HTTP: Microsoft SharePoint XSS in themeweb.aspx Vulnerability
HTTP: Microsoft SharePoint XSS in wizardlist.aspx Vulnerability
HTTP: Microsoft SQL Server Reflected XSS Privilege Escalation
HTTP: Microsoft Windows Remote Desktop Web Access XSS Vulnerability
HTTP: Opera historysearch XSS
HTTP: POST XSS Vulnerability
HTTP: Visual Studio XSS Vulnerability Privilege Elevation
HTTP: XSS Vulnerability In SharePoint (CVE-2014-1754)
SIP: SIP header XSS Injection Vulnerabilty
SMTP: IBM Lotus Notes XSS Vulnerability
TELNET: XSS Attempt via Telnet User Name Detected
HTTP: Apache SSI XSS Exploit (0x40217300)
HTTP: IIS Index Server Cross-site Scripting (0x4022d700)
HTTP: Information Disclosure in ASP.NET 2.0
HTTP: Microsoft FrontPage Server Extensions Cross Site Scripting Vulnerability (0x4022b500)
MTIS07-174-A MS SharePoint XSS
SMTP: MS06-029 Outlook Web Access Cross-Site Scripting (0x4040ab00)
SMTP:Microsoft Outlook Web Access Cross Site Scripting

NETSCREEN

APP:ACPROXY-XSS-INJECT
APP:CISCO:VIDEO-SURVEILANCE-XSS
APP:HP-LASERJET-EWS-XSS
APP:HPOV:NNM-XSS
APP:IBM:LOTUS-NOTES-XSS
APP:IBM:TIV-SCHEDULEPARAM-XSS
APP:MCAFEE-EPOLICY-XSS
APP:ORACLE:ISQL-XSS
APP:ORACLE:RAPID-WEBSRV-XSS
APP:PROXY:ACPROXY-XSS-INJECT
APP:SAP:WEBAPP-SERV-XSS
APP:SYMC:MGM-CONSOLE-XSS
APP:TMIC:INTERSCAN-XSS
APP:TRENDMICRO-ISMSS-XSS
CHAT:YIM:XSS
CHAT:YIM:YHOO-XSS
HTTP: XSS: HTML-SCRIPT-IN-URL-PRM
HTTP:APACHE:TOMCAT-CAL2JSP-XSS
HTTP:CGI:OMNIHTTPD-REDIR-XSS
HTTP:CHKP:VPN1-UTM-XSS
HTTP:CISCO:CSUSERCGIXSS
HTTP:CISCO:LINKSYS-WRT54GL-XSS
HTTP:CISCO:UNIFIED-XSS
HTTP:CISCO:UNIFIED-XSS-2
HTTP:COBALT:SERVICE-CGI-XSS
HTTP:COLDFUSION:MX7-XSS
HTTP:FRONTPAGE:FP-XSS
HTTP:IIS:ASP-XSS-FLAW
HTTP:IIS:MS-RD-WEB-ACCESS-XSS
HTTP:IIS:MS-REPORT-VIEWER-XSS
HTTP:IIS:SHAREPOINT-2010-XSS
HTTP:IIS:SHAREPOINT-MUL-XSS
HTTP:IIS:SHAREPOINT-XSS
HTTP:IIS:SP-SCRIPTRESX-XSS
HTTP:IIS:XSS-IIS-ASP
HTTP:MCAFEE-EPOLICY-XSS
HTTP:ORACLE:GLASSFISH-MUL-XSS
HTTP:OWA:OWA-CSS
HTTP:PHP:OPEN-REALITY-XSS-SQLI
HTTP:PHP:PHPNUKE:BOOKMARKS-XSS
HTTP:PHP:STRIP-TAGS-XSS

HTTP:PKG:IPLANET-XSS-ROOT
HTTP:SQL:INJ:ORA-REPT-XSS
HTTP:SQL:INJECTION:ORA-REPT-XSS
HTTP:STC:ADOBE:ACROBAT-XSS
HTTP:STC:ADOBE:FLASH-PLAYER-XSS
HTTP:STC:ADOBE:PDF-GOTO-XSS
HTTP:STC:ADOBE:PDF-XML-XSS
HTTP:STC:ADOBE:SWF-FILE-XSS
HTTP:STC:ADOBE:SWF-UNVRSL-XSS
HTTP:STC:HTML-HTW-XSS
HTTP:STC:IE:8-XSS-FILTER
HTTP:STC:IE:ANTIXSS-INFO-DISC
HTTP:STC:IE:BACKTOJPU-XSS
HTTP:STC:IE:CSS-XSS
HTTP:STC:IE:DHTML-EDIT-XSS
HTTP:STC:IE:EUC-JP-XSS
HTTP:STC:IE:HTML-XSS
HTTP:STC:IE:OWA-XSS
HTTP:STC:IE:TOSTATIC-XSS
HTTP:STC:IE:UNIV-XSS
HTTP:STC:IE:XSS-FILTER-DISC
HTTP:STC:MCAFEE:EPOLICY-XSS
HTTP:STC:MOZILLA:RSS-SCRIPT-INJ
HTTP:STC:OPERA:LINKS-PANEL-XSS
HTTP:STC:SAFARI:WEBKIT-XSS
HTTP:STC:SHAREPOINT-XSS
HTTP:TOMCAT:SC-XSS
HTTP:WEBLOGIC:BEA-ADMIN-CON-XSS
HTTP:XSS:ADOBE-COLDF-SEARCHLOG
HTTP:XSS:ADOBE-COLDFUSION
HTTP:XSS:AFTERLOGIC-WEBMAIL-PRO
HTTP:XSS:ANWIKI-XSS
HTTP:XSS:APACHE-MOD-NEGOTIATION
HTTP:XSS:APACHE-SSI-XSS
HTTP:XSS:ASP-REQ-VALIDATION
HTTP:XSS:ATUTOR-ACONTENT
HTTP:XSS:AWAUCTIONSCRIPT-CMS
HTTP:XSS:AWSTATS-EXEC
HTTP:XSS:AXIS-M10-CAMERA
HTTP:XSS:BEA-ADMIN-CONSOLE
HTTP:XSS:CA-SITEMINDER-OLUNICDE

HTTP:XSS:CISCO-CSDC
HTTP:XSS:CISCO-CSUSERCGIXSS
HTTP:XSS:CISCO-IOS-ADMIN
HTTP:XSS:CISCO-SESM
HTTP:XSS:CISCO-XSS
HTTP:XSS:CISCOWORKS-CSFHS
HTTP:XSS:CISCOWORKS-CSFHS-1
HTTP:XSS:CMSQLITE-ID
HTTP:XSS:COLDFUSION-MX7
HTTP:XSS:CPANEL-FILEOP
HTTP:XSS:CPANEL-MODULES
HTTP:XSS:CSS-HEAP
HTTP:XSS:DRUPAL-CUMULAS
HTTP:XSS:DYNAMICAX-PORTAL-XSS
HTTP:XSS:E2-PHOTO-GALLERY
HTTP:XSS:FOREFRONT-SIGNURL
HTTP:XSS:FRONTPAGE-EXT
HTTP:XSS:HDR-REFERRER
HTTP:XSS:HP-INSIGHT-ONLINE
HTTP:XSS:HP-INTELLIGENT-MNGT
HTTP:XSS:HP-SEARCH-XSS
HTTP:XSS:HTML-HTW
HTTP:XSS:HTML-SCRIPT-IN-AE
HTTP:XSS:HTML-SCRIPT-IN-AL
HTTP:XSS:HTML-SCRIPT-IN-COOKIE
HTTP:XSS:HTML-SCRIPT-IN-HOST
HTTP:XSS:HTML-SCRIPT-IN-POST
HTTP:XSS:HTML-SCRIPT-IN-UA
HTTP:XSS:HTML-SCRIPT-IN-URL-PRM
HTTP:XSS:HTML-SCRIPT-IN-URL-PTH
HTTP:XSS:HTML-SCRIPT-IN-URL-VAR
HTTP:XSS:HTW-XSS
HTTP:XSS:IBM-LOTUS-DOMINO-XNSF
HTTP:XSS:IBM-LOTUS-NOTES-TRAV
HTTP:XSS:IBM-LOTUS-SIMPLESEARCH
HTTP:XSS:IBM-OPEN-ADMIN
HTTP:XSS:IBM-RATIONAL-CLEARCASE
HTTP:XSS:IE-BACKTOJPU
HTTP:XSS:IE-DHTML-EDIT
HTTP:XSS:IE7-XSS
HTTP:XSS:IIS-ASP

HTTP:XSS:INMAGIC-DBTWPUB
HTTP:XSS:IPLANET-ROOT
HTTP:XSS:ISA-AUTH-XSS
HTTP:XSS:JAVA-COM-EXP
HTTP:XSS:JAVA-IDENTITY-MGR
HTTP:XSS:JOOMLA-CITY
HTTP:XSS:JOOMLA-COM-RESMAN
HTTP:XSS:LDAP-ACCOUNT-MGR
HTTP:XSS:LINKSYS-WIRELESS
HTTP:XSS:MAILMAN-ADMIN
HTTP:XSS:MAILMAN-OPTIONS
HTTP:XSS:MC-CONTENT-MANAGER
HTTP:XSS:MERCURY-BOARD
HTTP:XSS:MS-CS
HTTP:XSS:MS-FOREFRONT-DEFAULT
HTTP:XSS:MS-FOREFRONT-EXCEL-TBL
HTTP:XSS:MS-FOREFRONT-INFO-DISC
HTTP:XSS:MS-IE-TOSTATICHTML
HTTP:XSS:MS-LYNC-SERVER
HTTP:XSS:MS-OUTLOOK-REDIR-ASP
HTTP:XSS:MS-REPORT-MANAGER
HTTP:XSS:MS-REPORT-VIEWER
HTTP:XSS:MS-SCCM-REFLECTED
HTTP:XSS:MS-SCOM-WEB-CONSOLE
HTTP:XSS:MS-SHAREPOINT-PARAM
HTTP:XSS:MS-VSTWAC-TFS
HTTP:XSS:MS-W3WHO-XSS
HTTP:XSS:MUL-RECORDPRESS
HTTP:XSS:NAGIOS-XI-ALERT-CLOUD
HTTP:XSS:NASA-TRACE
HTTP:XSS:NOVELL-QUICKFINDER
HTTP:XSS:OMNIHTTPD-REDIR
HTTP:XSS:ORACLE-BIEE-XSS
HTTP:XSS:ORACLE-GLASSFISH
HTTP:XSS:ORACLE-RAPID-WEBSRV
HTTP:XSS:ORACLE-REPORT-SVR
HTTP:XSS:OUTLOOK-WEB
HTTP:XSS:OUTLOOK-WEB-ACCESS
HTTP:XSS:PACER-EDITION-EMAIL
HTTP:XSS:PHPNUKE-BOOKMARKS
HTTP:XSS:PHPWEBSITE-PAGE-ID

HTTP:XSS:REALPLAYER-SMIL
HTTP:XSS:ROBOHELP-XSS
HTTP:XSS:SERVICE-CGI
HTTP:XSS:SHARE-XSS
HTTP:XSS:SHAREPOINT-CALLBACK
HTTP:XSS:SHAREPOINT-COMMAND
HTTP:XSS:SHAREPOINT-EDITFORM
HTTP:XSS:SHAREPOINT-INPLVIEW
HTTP:XSS:SHAREPOINT-LIST-XSS
HTTP:XSS:SHAREPOINT-THEMEWEB
HTTP:XSS:SHAREPOINT-USER
HTTP:XSS:SHAREPOINT-WIZARDLIST
HTTP:XSS:SHAREPOINT-XSS
HTTP:XSS:SHAREPOINT-XSS-2
HTTP:XSS:SUBRION-CMS
HTTP:XSS:SUSPICIOUS-SCAN
HTTP:XSS:SYM-GATEWAY-PHP-PAGE
HTTP:XSS:SYM-IM-MANAGER
HTTP:XSS:SYMANTEC-WG
HTTP:XSS:SYNDEO-CMS-ADDONS
HTTP:XSS:TECHSMITH-SWF
HTTP:XSS:TM-REQUEST-FORGERY
HTTP:XSS:TOMCAT-JSP
HTTP:XSS:URL-IMG-XSS
HTTP:XSS:US-ROBOTICS-FIRMWARE
HTTP:XSS:VBULLETIN-SORT
HTTP:XSS:VBULLETIN-SORTORDER
HTTP:XSS:WEB-VIEW-DOC-SCR-INJ
HTTP:XSS:WEBPAGE-URL
HTTP:XSS:WHITE-LABEL-CMS
HTTP:XSS:WP-AJAX-CALENDAR
HTTP:XSS:WP-AJAX-CATEGORY
HTTP:XSS:WP-AJAX-RECENT-POSTS
HTTP:XSS:WP-COMICPRESS
HTTP:XSS:WP-DAILY-MAUI-PHOTO
HTTP:XSS:WP-ESHOP
HTTP:XSS:WP-GAZETTE-THEME
HTTP:XSS:WP-IGIT-POSTS
HTTP:XSS:WP-INLINE-GALLERY
HTTP:XSS:WP-LAZYEST-GALLERY
HTTP:XSS:WP-LIVE-WIRE-THEME

HTTP:XSS:WP-LOCAL-MARKET-EXP
HTTP:XSS:WP-PHOTO-ALBUM
HTTP:XSS:WP-PHOTORACER
HTTP:XSS:WP-PHOTOSMASH-GAL
HTTP:XSS:WP-PLACESTER
HTTP:XSS:WP-RATING-WIDGET
HTTP:XSS:WP-SERMON-BROWSER
HTTP:XSS:WP-SOCIALGRID
HTTP:XSS:WP-STATS-DASHBOARD
HTTP:XSS:WP-UNIVERSAL-POST
HTTP:XSS:WP-WOOTHEMES
HTTP:XSS:WP-YT-AUDIO
HTTP:XSS:WP-ZOTPRESS
HTTP:XSS:X-FORWARDED-FOR-INJ
HTTP:XSS:XOOPS-MULT
HTTP:XSS:XOOPS-VIEW-PHOTOS-PHP
HTTP:XSS:YOAST-WP
HTTP:XSS:ZEN-CART
SCAN:DARKD0RK3R-XSS
SCAN:RPVS:XSS-URL
SMTP:HTML-VAL-XSS
SMTP:IBM-LOTUS-NOTES-XSS
SMTP:MAL:SQM-CONTENT-XSS
SMTP:MAL:XSS-URL-IN-EMAIL
SMTP:OUTLOOK:OWA-XSS
SMTP:OVERFLOW:SQRLMAIL-HDR-INJ
SSL:MGM-CONSOLE-XSS

PALO ALTO

Adobe Coldfusion XSS Vulnerabily
Adobe Coldfusion 8 XSS Vulnerabily
Adobe Coldfusion 8 XSS Vulnerabily(32525)
Adobe Coldfusion XSS Vulnerabily
Adobe Coldfusion XSS Vulnerabily(32526)
Adobe Flash Player MovieClipLoader XSS Vulnerability
Adobe Flash Player MovieClipLoader XSS Vulnerability(34378)
Adobe Flash Player XSS Vulnerability
Apache SSI Error Page XSS Vulnerability
Apache SSI Error Page XSS Vulnerability(31910)

Apache Wicket Unspecified XSS Vulnerability
Cisco Unified Operations Manager Common Services Device Center XSS Vulnerability
CiscoWorks Common Services Framework Help Servlet XSS Vulnerability
Generic prompt XSS vulnerability
InterWoven WorkDocs XSS Vulnerability(31064)
Microsoft ASP.Net 1.1 XSS Protection Bypass Vulnerability
Microsoft ASP.Net 1.1 XSS Protection Bypass Vulnerability(31943)
Microsoft Dynamics AX Enterprise Portal XSS Vulnerability
Microsoft Dynamics AX Enterprise Portal XSS Vulnerability(34825)
Microsoft Exchange OWA XSS and Spoofing Vulnerability
Microsoft Exchange OWA XSS and Spoofing Vulnerability(31176)
Microsoft Forefront Unified Access Gateway Default Reflected XSS Vulnerability
Microsoft Forefront Unified Access Gateway Default Reflected XSS Vulnerability(34479)
Microsoft Forefront Unified Access Gateway ExcelTable Response Splitting XSS Vulnerability
Microsoft Forefront Unified Access Gateway ExcelTable Response Splitting XSS Vulnerability(34482)
Microsoft IIS 5.0 Form_JScript.asp XSS Vulnerability
Microsoft IIS 5.0 Form_JScript.asp XSS Vulnerability(32775)
Microsoft Internet Explorer Navigation Cancel Page XSS Vulnerability
Microsoft Internet Explorer Navigation Cancel Page XSS Vulnerability(33464)
Microsoft Internet Explorer Print Table XSS Vulneraiblity
Microsoft Internet Explorer Print Table XSS Vulneraiblity(34302)
Microsoft SharePoint inplview.aspx XSS Vulnerability
Microsoft SharePoint inplview.aspx XSS Vulnerability(34620)
Microsoft SharePoint themeweb.aspx XSS Vulnerability
Microsoft SharePoint themeweb.aspx XSS Vulnerability(34621)
Microsoft SharePoint wizardlist.aspx XSS Vulnerability
Microsoft SharePoint wizardlist.aspx XSS Vulnerability(34623)
Microsoft SQL Server Reporting Services Reflected XSS Vulnerability
Microsoft SQL Server Reporting Services Reflected XSS Vulnerability(35060)
Microsoft System Center Configuration Manager XSS Vulnerability
Microsoft System Center Configuration Manager XSS Vulnerability(34998)
Microsoft System Center Operations Manager Web Console XSS Vulnerability
Microsoft Unified Access Gateway Mobile Portal Website XSS Vulnerability
Microsoft Unified Access Gateway Mobile Portal Website XSS Vulnerability(33567)
Microsoft Unified Access Gateway Signurl.asp XSS Vulnerability
Microsoft Unified Access Gateway Signurl.asp XSS Vulnerability(33568)
Microsoft Unified Access Gateway XSS Allows Escalation of Privileges Vulnerability
Microsoft Unified Access Gateway XSS Allows Escalation of Privileges Vulnerability(33564)
Microsoft Windows MHTML Mime-Formatted Request XSS Vulnerability
Microsoft Windows MHTML Mime-Formatted Request XSS Vulnerability(34109)
Oracle GlassFish Enterprise Server XSS Vulnerability

SAP Internet Transaction Server wgate.dll ~service Parameter XSS Vulnerability
SAP Internet Transaction Server wgate.dll ~service Parameter XSS Vulnerability
SAP Internet Transaction Server wgate.dll ~service Parameter XSS Vulnerability(31937)
Symantec Messaging Gateway Management Console XSS Vulnerability
Yahoo Web Email XSS Vulnerability
Yahoo Web Email XSS Vulnerability(32534)

SNORT

ATTACK-RESPONSES successful cross site scripting forced download attempt
APP-DETECT Acunetix web vulnerability scanner base64 XSS attempt
APP-DETECT Acunetix web vulnerability scanner XSS attempt
BROWSER-CHROME Google Chrome net-internals uri fragment identifier XSS attempt
BROWSER-IE Microsoft Internet Explorer 8 XSS in toStaticHTML API attempt
BROWSER-IE Microsoft Internet Explorer invalid Shift_JIS character xss attempt
BROWSER-IE Microsoft Internet Explorer toStaticHTML XSS attempt
BROWSER-IE Microsoft Internet Explorer XSRF timing attack against XSS filter
BROWSER-IE Microsoft multiple product toStaticHTML XSS attempt
FILE-OTHER Microsoft Windows MHTML XSS attempt
OS-WINDOWS Microsoft Certification service XSS attempt
OS-WINDOWS Microsoft ForeFront UAG ExcelTable.asp XSS attempt
OS-WINDOWS Microsoft SCCM ReportChart xss attempt
OS-WINDOWS Microsoft Windows MHTML XSS attempt
PROTOCOL-VOIP Call-ID header XSS injection attempt
PROTOCOL-VOIP Contact header XSS injection attempt
PROTOCOL-VOIP From header XSS injection attempt
PROTOCOL-VOIP Subject header XSS injection attempt
PROTOCOL-VOIP To header XSS injection attempt
SERVER-MAIL Microsoft Windows Exchange OWA XSS and spoofing attempt
SERVER-OTHER McAfee ePolicy Orchestrator XSS attempt
SERVER-OTHER Palo Alto Networks Firewall editUser.esp XSS attempt
SERVER-WEBAPP Devellion CubeCart multiple parameter XSS vulnerability
SERVER-WEBAPP Drupal VideoWhisper Webcam plugin XSS attempt
SERVER-WEBAPP HP Insight Diagnostics XSS attempt
SERVER-WEBAPP Jive Software Openfire audit-policy.jsp XSS attempt
SERVER-WEBAPP Jive Software Openfire group-summary.jsp XSS attempt
SERVER-WEBAPP Jive Software Openfire log.jsp XSS attempt
SERVER-WEBAPP Jive Software Openfire logviewer.jsp XSS attempt
SERVER-WEBAPP Jive Software Openfire muc-room-edit-form.jsp XSS attempt
SERVER-WEBAPP Jive Software Openfire server-properties.jsp XSS attempt
SERVER-WEBAPP Jive Software Openfire user-properties.jsp XSS attempt

SERVER-WEBAPP LongTail Video JW Player XSS attempt link param
SERVER-WEBAPP Microsoft ASP.NET improper comment handling XSS attempt
SERVER-WEBAPP Microsoft Office SharePoint Javascript XSS attempt
SERVER-WEBAPP Microsoft Office SharePoint XSS vulnerability attempt
SERVER-WEBAPP Microsoft SharePoint XSS
SERVER-WEBAPP raSMP User-Agent XSS injection attempt
SERVER-WEBAPP WordPress XSS fs-admin.php injection attempt
WEB-CLIENT IBM Tivoli Endpoint Manager Web Reports xss attempt

SOURCEFIRE

ATTACK-RESPONSES successful cross site scripting forced download attempt
WEB-MISC Quicktime User-Agent buffer overflow attempt
WEB-PHP modules.php access
WEB-CGI Emumail emumail.fcgi access
WEB-MISC sresult.exe access
WEB-MISC sambar /search/results.stm access
APP-DETECT Acunetix web vulnerability scanner prompt XSS attempt
BROWSER-IE Microsoft Internet Explorer 8 toStaticHTML XSS attempt
BROWSER-IE Microsoft Internet Explorer XSS mouseevent PII disclosure attempt
EXPLOIT IE8 XSS in toStaticHTML API attempt
EXPLOIT javascript handler in URI XSS attempt
EXPLOIT Microsoft Forefront UAG javascript handler in URI XSS attempt
EXPLOIT Microsoft Internet Explorer 8 XSS in toStaticHTML API attempt
EXPLOIT Microsoft Internet Explorer XSRF timing attack against XSS filter
EXPLOIT Microsoft Sharepoint Javascript XSS attempt
EXPLOIT Microsoft SharePoint XSS
EXPLOIT Microsoft Sharepoint XSS vulnerability attempt
FILE-FLASH Adobe Flash Player marshallException through JavaScript XSS attempt
FILE-FLASH Adobe Shockwave Flash Flex authoring tool XSS exploit attempt
FILE-OFFICE Microsoft Office SharePoint XSS attempt
FILE-OTHER Microsoft MHTML XSS attempt
ORACLE BPEL process manager XSS injection attempt
OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt
OS-WINDOWS Microsoft Forefront UAG URL XSS alternate attempt
OS-WINDOWS Microsoft Report Viewer reflect XSS attempt
OS-WINDOWS Microsoft Windows Forefront UAG URL XSS attempt
OS-WINDOWS Microsoft Windows Help Centre escape sequence XSS attempt

SERVER-ORACLE BPEL process manager XSS injection attempt
SERVER-OTHER IBM Tivoli Endpoint Manager Web Reports xss attempt
SERVER-OTHER Microsoft SharePoint XSS attempt
SERVER-WEBAPP Cisco Common Services Device Center XSS attempt
SERVER-WEBAPP Cisco Common Services Help servlet XSS attempt
SERVER-WEBAPP IBM System Storage DS storage manager profiler XSS attempt
SERVER-WEBAPP JavaScript tag in User-Agent field possible XSS attempt
SERVER-WEBAPP Microsoft Office SharePoint query.iqy XSS attempt
SERVER-WEBAPP Microsoft Office SharePoint scriptresx.ashx XSS attempt
SERVER-WEBAPP Microsoft Office SharePoint themeweb.aspx XSS attempt
SERVER-WEBAPP Microsoft Office SharePoint XSS attempt
SERVER-WEBAPP Microsoft SharePoint chart webpart XSS attempt
SERVER-WEBAPP Microsoft Sharepoint ThemeOverride XSS Attempt
SPECIFIC-THREATS Microsoft Exchange OWA XSS and spoofing attempt
WEB-CLIENT Adobe Shockwave Flash Flex authoring tool XSS exploit attempt
WEB-CLIENT Forefront UAG URL XSS alternate attempt
WEB-CLIENT Forefront UAG URL XSS attempt
WEB-CLIENT Micrisoft Windows Forefront UAG URL XSS attempt
WEB-CLIENT Microsoft Certification service XSS attempt
WEB-CLIENT Microsoft Forefront UAG URL XSS alternate attempt
WEB-CLIENT Microsoft IE XSS mouseevent PII disclosure attempt
WEB-CLIENT Microsoft Internet Explorer 8 toStaticHTML XSS attempt
WEB-CLIENT Microsoft Internet Explorer XSS mouseevent PII disclosure attempt
WEB-CLIENT Microsoft MHTML XSS attempt
WEB-CLIENT Microsoft Report Viewer reflect XSS attempt
WEB-CLIENT Microsoft Windows Forefront UAG URL XSS attempt
WEB-CLIENT Microsoft Windows Help Centre escape sequence XSS attempt
WEB-CLIENT Palo Alto Networks Firewall editUser.esp XSS attempt
WEB-MISC Cisco Common Services Device Center XSS attempt
WEB-MISC Cisco Common Services Help servlet XSS attempt
WEB-MISC Microsoft ForeFront UAG ExcelTable.asp XSS attempt
WEB-MISC Microsoft SharePoint chart webpart XSS attempt
WEB-MISC Microsoft Sharepoint themeweb.aspx XSS attempt
WEB-MISC Microsoft Sharepoint XSS attempt
WEB-MISC Microsoft Windows Sharepoint XSS attempt

TIPPING POINT

HTTP: Microsoft SharePoint calendar.aspx XSS Vulnerability
HTTP: Microsoft SharePoint NewForm.aspx XSS Vulnerability

HTTP: Microsoft SharePoint Picker.aspx XSS Vulnerability
HTTP: Microsoft SharePoint Query XSS Vulnerability
HTTP: Microsoft DynamicsAx XSS Vulnerability
HTTP: Microsoft SharePoint XSS Vulnerability
HTTP: Microsoft Visual Studio Team Web Access XSS Vulnerability
HTTP: Kerio MailServer WebMail Cross-Site Scripting
HTTP: Kerio MailServer WebMail Cross-Site Scripting
HTTP: Adobe Acrobat XSS Vulnerability
SMTP: Adobe Acrobat XSS Vulnerability
HTTP: Apache Host Header XSS Vulnerability
HTTP: PHP File Include Exploit via XSS
HTTP: cPanel Multiple Module Cross Site Scripting
HTTP: Microsoft SharePoint Cross Site Scripting Vulnerability
SMTP: XSS Vulnerability in Cascading Style Sheets
SMTP: XSS Vulnerability in From: Header
HTTP: Mozilla IFrame XSS
HTTP: Microsoft Sharepoint Help.aspx XSS Vulnerability
HTTP: Oracle Secure Enterprise Search Cross Site Scripting

TREND MICRO

Apple Safari Webarchive File Format UXSS Vulnerability
Flash Authoring Flex SWF Files XSS
Generic Cross Site Scripting(XSS) Prevention
IBM Tivoli Endpoint Manager Web Reports XSS Vulnerability
Internet Explorer XSS Filter Bypass Vulnerability
MailEnable Enterprise Multiple XSS Injection Vulnerabilities
Mozilla Firefox "HTML escaped low surrogates" XSS Attack
Multiple XSS Vulnerabilities In Sun Communications Express

REFERENCES

- ✓ IBM X-Force Quarterly Reports (2Q 2014): https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-ASEAN_WEB-ORG_Cross&S_PKG=ov24066&S_TACT=102PW99W
- ✓ IBM Hosted Application Security Management (HASM): A cloud-based solution for dynamic testing of web applications using IBM Security AppScan® in both preproduction and production environments. HASM services include a dedicated security analyst to configure and manage the testing.
- ✓ White Hat Security: https://www.whitehatsec.com/

- ✓ XSS: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)
- ✓ I'll never get caught. I'm Popular., 10/04/05, -samy: http://namb.la/popular/
- ✓ XSS: http://www.acunetix.com/websitesecurity/xss/
- ✓ Origin of XSS: http://jeremiahgrossman.blogspot.com/2006/07/origins-of-cross-site-scripting-xss.html
- ✓ MySpace worm: http://www.techspot.com/news/24226-myspace-speaks-about-samy-kamkars-sentencing.html

CONTRIBUTORS

Michelle Alvarez - Researcher/Editor, Threat Research Group
Nick Bradley - Practice Lead, Threat Research Group
David McMillen, Senior Threat Researcher
Leslie Horacek - X-Force Threat Response Manager

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. The data contained herein describing tactics, techniques and procedures is classified Confidential for the benefit of IBM MSS clients only. This information is provided "AS IS," and without warranty of any kind.