

SAINTwriter Assessment Report

Report Generated: January 7, 2010

1.0 Introduction

On January 7, 2010, at 3:35 PM, a sql/xss vulnerability assessment was conducted using the SAINT 7.2.2 vulnerability scanner. The scan discovered a total of one live host, and detected one critical problem, one area of concern, and zero potential problems. The hosts and problems detected are discussed in greater detail in the following sections.

2.0 Summary

The following vulnerability severity levels are used to categorize the vulnerabilities:

CRITICAL PROBLEMS

Vulnerabilities which pose an immediate threat to the network by allowing a remote attacker to directly gain read or write access, execute commands on the target, or create a denial of service.

AREAS OF CONCERN

Vulnerabilities which do not directly allow remote access, but do allow privilege elevation attacks, attacks on other targets using the vulnerable host as an intermediary, or gathering of passwords or configuration information which could be used to plan an attack.

POTENTIAL PROBLEMS

Warnings which may or may not be vulnerabilities, depending upon the patch level or configuration of the target. Further investigation on the part of the system administrator may be necessary.

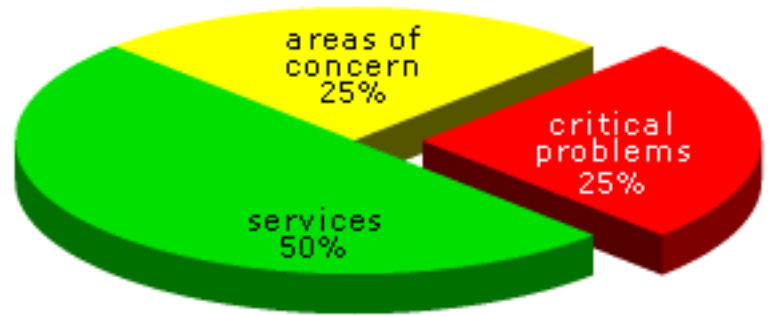
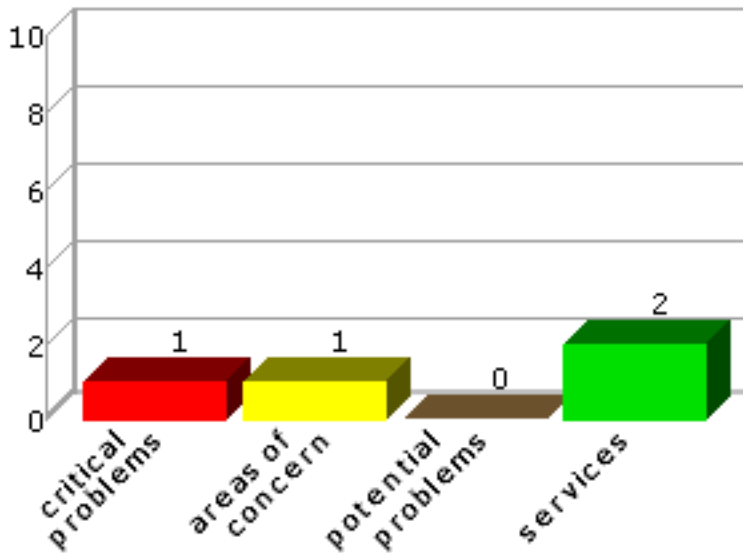
SERVICES

Network services which accept client connections on a given TCP or UDP port. This is simply a count of network services, and does not imply that the service is or is not vulnerable.

The sections below summarize the results of the scan.

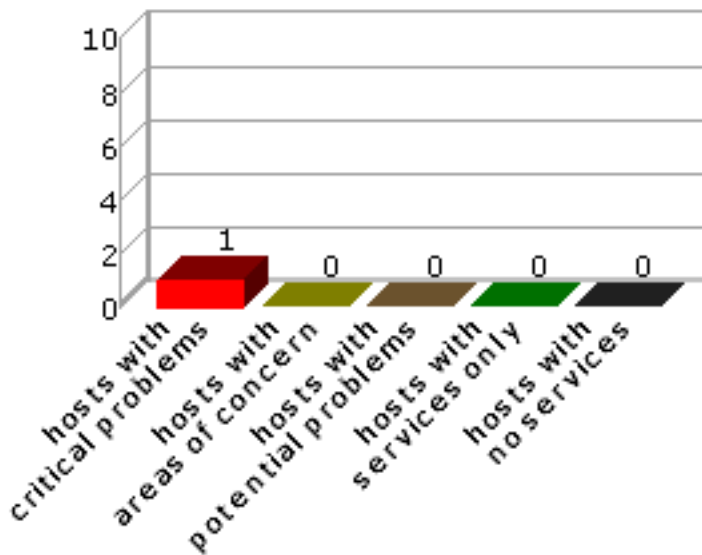
2.1 Vulnerabilities by Severity

This section shows the overall number of vulnerabilities and services detected at each severity level.



2.2 Hosts by Severity

This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host.

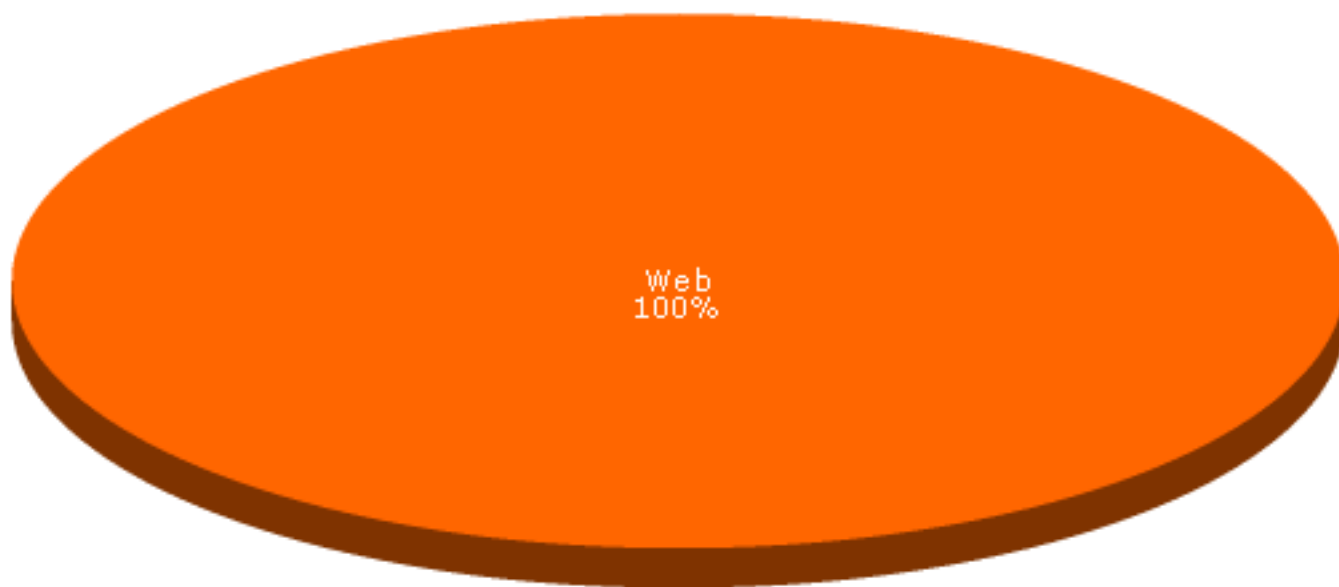
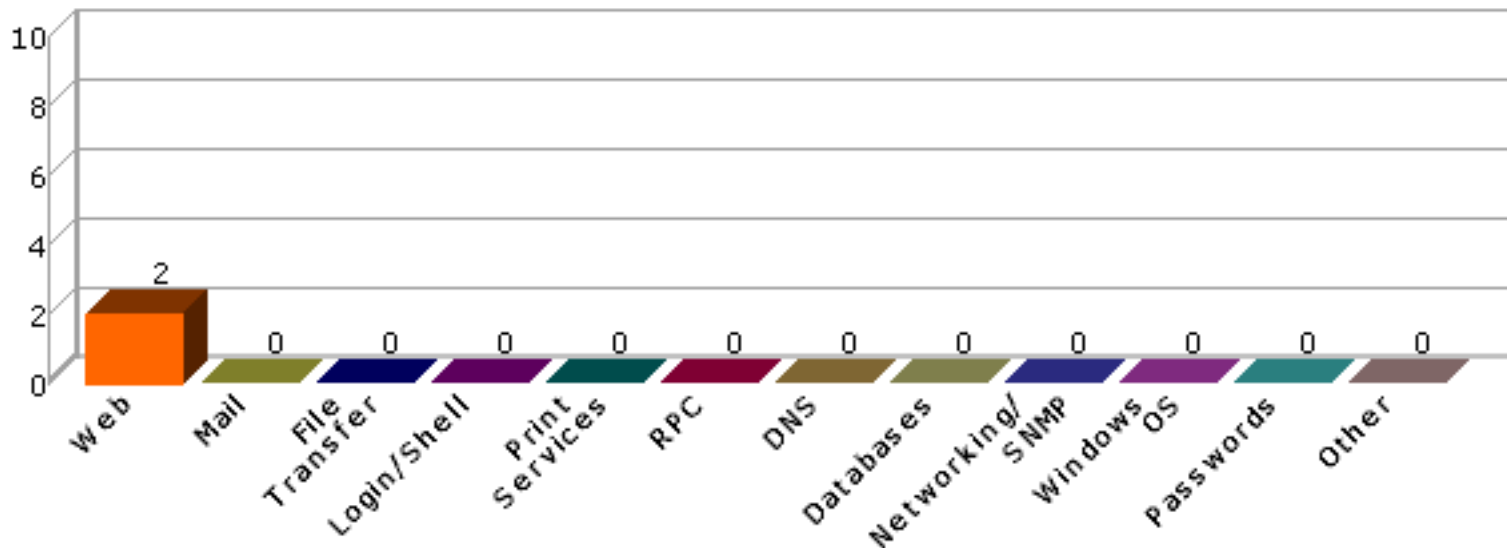


2.3 Vulnerabilities by Class

This section shows the number of vulnerabilities detected in each of the following classes.

Class	Description
Web	Vulnerabilities in web servers, CGI programs, and any other software offering an HTTP interface
Mail	Vulnerabilities in SMTP, IMAP, POP, or web-based mail services
File Transfer	Vulnerabilities in FTP and TFTP services
Login/Shell	Vulnerabilities in ssh, telnet, rlogin, rsh, or rexec services
Print Services	Vulnerabilities in lpd and other print daemons
RPC	Vulnerabilities in Remote Procedure Call services

DNS	Vulnerabilities in Domain Name Services
Databases	Vulnerabilities in database services
Networking/SNMP	Vulnerabilities in routers, switches, firewalls, or any SNMP service
Windows OS	Missing hotfixes or vulnerabilities in the registry or SMB shares
Passwords	Missing or easily guessed user passwords
Other	Any vulnerability which does not fit into one of the above classes



3.0 Overview

The following tables present an overview of the hosts discovered on the network and the vulnerabilities contained therein.

3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
172.16.1.2		172.16.1.2		1	1	0

3.2 Vulnerability List

This table presents an overview of the vulnerabilities detected on the network.

Host Name	Severity	Vulnerability / Service	Class	CVE	Exploit Available?
172.16.1.2	critical	SQL injection in id parameter to search.jsp	Web		no
172.16.1.2	concern	Cross-site scripting vulnerability in Username parameter to login.php	Web		no
172.16.1.2	service	WWW			no
172.16.1.2	service	WWW (Secure)			no
172.16.1.2	info	Web Directory: /ecatalog/			no
172.16.1.2	info	Web Directory: /php/			no
172.16.1.2	info	Web Directory: /products/			no
172.16.1.2	info	Web Directory: /projects/			no
172.16.1.2	info	Web Directory: /register/			no
172.16.1.2	info	Web Directory: /software/			no
172.16.1.2	info	Web Directory: /view/			no

4.0 Details

The following sections provide details on the specific vulnerabilities detected on each host.

4.1 172.16.1.2

IP Address: 172.16.1.2

Scan time: Jan 07 15:35:35 2010

SQL injection in id parameter to search.jsp

Severity: Critical Problem

Impact

A remote attacker could execute SQL commands on the back-end database, possibly leading to password retrieval, authentication bypass, unauthorized data access, or unauthorized data modification.

Resolution

All user-supplied parameters should be checked for illegal characters, such as a single quote ('), before being used in an SQL query. See the references below for fix information for specific products.

Where can I read more about this?

For more information on SQL injection, see the [white paper](#) from SPI Dynamics.

For more information on specific SQL injection vulnerabilities, see the following references:

- MaxWebPortal forum.asp SQL Injection Vulnerability (CVE 2009-3436)
- PHP-Nuke 'main/tracking/userLog.php' SQL Injection Vulnerability (CVE 2009-1842)
- PHP-Nuke Search Module (CVE 2005-3792)
- gCards vulnerability (CVE 2005-3408)
- Basic Analysis and Security Engine vulnerability (CVE 2005-3325)
- search.php (phpBB2) (CVE 2003-1216)
- search.php (phpBB2) (CVE 2004-2350)
- viewtopic.php (phpBB2) (CVE 2003-0486)
- privmsg.php (phpBB2)
- ProductCart (CVE 2003-0522)
- VP-ASP shopexd.asp (CVE 2003-0560)
- VP-ASP shopsearch.asp/shopdisplayproducts.asp
- VP-ASP shopcurrency.asp (CVE 2006-2263)
- VP-ASP shopproductselect.asp (CVE 2004-2413)
- phpWebSite calendar module (CVE 2003-0735 *Related: CVE 2003-0736 CVE 2003-0737 CVE 2003-0738*)
- phpWebSite calendar module (CVE 2004-1654)
- phpWebSite Index.PHP Multiple SQL Injection Vulnerabilities
- phpWebSite topics.php (CVE 2006-0973)
- phpWebSite friend.php (CVE 2006-1330)
- phpWebSite links.php (CVE 2008-6266)
- DeskPRO (CVE 2003-0874)
- My Classifieds SQL
- Land Down Under auth.php (CVE 2003-1315)
- osCommerce create_account_process.php and other scripts
- PHP-Nuke Web_Links, Downloads, and Sections modules (CVE 2004-0269)
- PHP-Nuke admin.php (CVE 2004-1932)
- Event Calendar for PHP-Nuke (CVE 2004-1530)
- ASP Portal index.asp *Related: multiple asp (CVE 2006-1353)*
- YaBB SE (double decoding) (CVE 2006-3275)
- Spider Sales (CVE 2004-0348 *Related: CVE 2004-0350 CVE 2004-0351*)
- Invision Gallery (CVE 2004-1835)
- Invision Gallery (rating parameter) (CVE 2005-1948)
- Invision Gallery (album parameter) (CVE 2006-5206 *Related: CVE 2006-5205*)
- CactuShop (CVE 2004-1881)
- NukeCalendar (CVE 2004-1914)
- Tiki CMS (CVE 2004-1925)
- TUTOS
- Advanced Guestbook (CVE 2004-1952)
- Advanced Guestbook (index.php) (CVE 2005-1548)
- phpBugTracker (CVE 2004-1519)
- OpenBB (CVE 2004-1966)
- OpenBB (read.php) (CVE 2005-2566)
- PHP-Nuke viewsdownload
- PHP-Nuke Journal
- PHP-Nuke Search (CVE 2004-0732)
- PHP-Nuke Search (CVE 2004-0738)
- Zen Cart (CVE 2004-2023)
- JPortal print (CVE 2004-2036)
- JPortal Search (CVE 2005-3052)
- JPortal (forum.php)
- e107 (CVE 2004-2042)
- Invision Power Board (ssi.php)

- Invision Power Board (Post) (CVE 2004-1531)
- Arcade module for Invision Power Board (CVE 2004-1536)
- Invision Power Board (Members) (CVE 2005-1070)
- Web Center (CVE 2004-2561)
- HelpBox
- Nucleus CMS (CVE 2004-2056)
- phpMyWebHosting (CVE 2004-2218)
- Ulog-php (CVE 2005-0463)
- Password Protect (CVE 2004-1647)
- getInternet
- Subjects (CVE 2004-1668)
- aspWebCalendar, aspWebAlbum (CVE 2004-1552 CVE 2004-1553)
- BroadBoard (CVE 2004-1555)
- PHP-Fusion 1 2 3 4 5 (CVE 2004-2437 CVE 2005-3740 CVE 2005-4005 CVE 2006-2330 CVE 2006-2459)
- CubeCart (CVE 2004-1579 CVE 2004-1580)
- SalesLogix Web Client (CVE 2004-1608)
- Phorum (CVE 2004-2240)
- Phorum (follow.php) (CVE 2004-1518)
- antiboard.php (CVE 2004-2062)
- miniBB (CVE 2004-2456)
- PHPKIT print.php (CVE 2004-1538)
- last.php for vBulletin (CVE 2004-1515)
- phpGedView (CVE 2004-0065)
- ikonboard.cgi (CVE 2004-1406)
- MyBB 1.0.0 RC4 (CVE 2005-0282)
- MyBB 1.0.3 (CVE 2006-0638)
- Sgallery for PHP-Nuke (CVE 2005-0377)
- PeriDesk (kb.cgi) (CVE 2005-0343)
- MercuryBoard (CVE 2005-0414)
- MercuryBoard (User-Agent header) (CVE 2005-2028)
- PostNuke (Download search function) (CVE 2005-0617)
- PostNuke (getArticles) (CVE 2005-0615)
- PostNuke (article) (CVE 2005-1048)
- CopperExport (xp_publish.php) (CVE 2005-0697)
- paFileDB (CVE 2005-0781)
- paFileDB (pafiledbcookie) (CVE 2005-2723)
- Bugtraq (CVE 2005-0805)
- CoolForum (register.php) (CVE 2005-0858)
- PHP-Nuke Bookmarks module (CVE 2005-0902)
- PHP-Nuke Downloads module (CVE 2005-0996)
- PHP-Nuke WebLinks module (CVE 2005-0997)
- PHP-Nuke Top module (CVE 2005-0999)
- PHP-Nuke (name POST argument) (CVE 2005-3304)
- PHP-Nuke mainfile.php
- AspApp
- PortalApp (ad_click.asp) (CVE 2005-0948)
- E-XOOPS (CVE 2005-0911)
- ESMI PayPal Storefront (pages.php) (CVE 2005-0935)
- album_search.php (CVE 2005-1114)
- zOOm Media Gallery (CVE 2005-1079)
- LiteCommerce (CVE 2005-1032)
- kb.php (CVE 2005-1196)
- Auction (CVE 2005-1234)

- PHP-Calendar search (CVE 2005-1397)
- MetaCart e-Shop (CVE 2005-1363)
- Claroline (userInfo.php) (CVE 2005-1375)
- CodeThatShoppingCart (catalog.php) (CVE 2005-1594)
- NPDS (comments.php) (CVE 2005-1637)
- Help Center Live (faq/index.php) (CVE 2005-1673)
- Calendarix 1 2 (CVE 2005-1865 CVE 2006-3094)
- UBB Threads (CVE 2005-2058)
- Cacti (graph.php) (CVE 2005-2148)
- optReviewReadExec (CVE 2005-2190)
- Contrexx (CVE 2005-2415)
- MidiCart ASP (item_show.asp) (CVE 2005-2601)
- MidiCart ASP (item_list.asp) (CVE 2006-6209)
- MyBulletinBoard (misc.php) (CVE 2005-2888)
- Tunez (CVE 2005-3833 CVE 2005-3834)
- WebCalendar (CVE 2005-3949)
- Mercury CMS (page parameter) (CVE 2005-4406)
- Cerberus Helpdesk (CVE 2005-4427)
- NewsPHP (CVE 2006-0413)
- NewsPHP (id) (CVE 2006-3358 CVE 2006-3359)
- VBZoom 1 2 3 (CVE 2005-4729 CVE 2006-1132 CVE 2006-1133 CVE 2006-3054 CVE 2006-3055 CVE 2006-3056)
- PHPKIT include.php (CVE 2006-1773)
- ZixForum settings.asp (CVE 2006-2541)
- ZixForum ReplyNew.asp (CVE 2006-4612)
- MyNewsletter (CVE 2006-2887)
- PHPKIT faq.php (CVE 2006-7115)
- LDU-Seditio polls.php (CVE 2006-6268)
- cpCommerce (CVE 2007-2890 CVE 2007-2959 CVE 2007-2968)
- paFileDB categories (CVE 2007-3808)
- CandyPress (ajax_optInventory.asp) (CVE 2008-0546)
- WordPress Adserve plugin (adclick.php) (CVE 2008-0507)
- Joomla Glossary (CVE 2008-0514)
- WordPress fGallery plugin (fim_rss.php) (CVE 2008-0491)
- WordPress WP-Cal plugin (editevent.php) (CVE 2008-0490)
- Customer Testimonials Add-on for osCommerce Online Merchant (customer_testimonials.php) (CVE 2008-0719)
- Xoops classifieds module cid parameter for Adsvie action (CVE 2008-0873)
- PHP-Nuke WebLinks module cid parameter (CVE 2008-0879)
- Joomla Showcase catid parameter

Technical Details

```
Service: http
SENT: GET /search.jsp?Username=default&id='&submit=default HTTP/1.0
Host: 172.16.1.2:80
RECEIVED: error in your SQL syntax
```

Cross-site scripting vulnerability in Username parameter to login.php

Severity: Area of Concern

Impact

A malicious web site could cause arbitrary commands to run on a client through a specially crafted link to the vulnerable server. In some cases, this could result in the compromise of the client's cookies, leading to unauthorized access to web applications.

Resolution

Cross-site scripting can be fixed either by creating a customized error page which does not display the URI, or by applying one of the following fixes:

- **ASP Fast Forum:** Upgrade to a version created after 1 NOV 2005.
- **PHP-Nuke:** ([11/13/08](#)) [Upgrade](#) PHP-Nuke to a version higher than 8.1.
- **FlatNuke:** [Upgrade](#) to FlatNuke version 2.5.7
- **RSA Security:** Upgrade to RSA Security RSA Authentication Agent to a version higher than 5.3 or RSA Security ACE/Agent for Web to a version higher than 5.1.1 when they become available
- **Lotus Domino:** Upgrade to version 5.0.9 when it becomes available.
- **Microsoft ISA 2000:** Refer to [Microsoft Security Bulletin 01-045](#).
- **NetWare Web Search:** ([04/19/02](#)) Apply NetWare 6 Service Pack 1.
- **ColdFusion MX:** ([06/25/02](#)) Apply the patch referenced in [Macromedia Security Bulletin 02-03](#).
- **Apache Tomcat:** ([07/12/02](#)) [Upgrade](#) to version 4.1.4 or higher, and unmap the "invoker" servlet (mapped to `/servlet/`), which executes anonymous servlet classes that have not been defined in a `web.xml` file. The entry for this can be found in the `<tomcat-install-dir>/conf/web.xml` file.
- **Apache printenv program** ([12/30/02](#)) Remove the `cgi-bin/printenv` program. Although this program outputs the `text/plain` MIME type which shouldn't be susceptible to cross-site scripting, some browsers do not correctly handle this type and would therefore be vulnerable.
- **Microsoft Content Management Server 2001** ([01/23/03](#)) Apply the cumulative patch referenced in [Microsoft Security Bulletin 03-002](#), or apply Microsoft Content Management Server 2001 Service Pack 2 if available.
- **WebCalendar** ([09/22/03](#)) [Upgrade](#) to a WebCalendar version newer than 0.9.42.
- **VP-ASP (Shopping Cart)** ([12/22/03](#) [06/22/04](#) [11/30/05](#)) See the [VP-ASP security fixes](#).
- **Bitfolge sniff** ([12/22/03](#)) [Upgrade](#) to sniff 1.2.7 or later.
- **osCommerce** ([12/23/03](#)) [Upgrade](#) to osCommerce 2.2 milestone 3.
- **IBM Net.Data db2www** ([02/04/04](#)) Use `DTW_DEFAULT_ERROR_MESSAGE` feature (or `DTW_DEFAULT_MACRO` feature on zOS and iServer) to ensure that error messages do not include user input in their response. For example, in the Net.Data configuration file `db2www.ini`, insert an entry such as:
`DTW_DEFAULT_ERROR_MESSAGE This Web Site is experiencing problems. Check back later.`
- **ASP Portal** ([02/27/04](#)) Upgrade your version.
- **phpBB2** ([03/24/04](#)) [Upgrade](#) to phpBB 2.0.7 or higher.
- **ZWiki** ([12/01/04](#)) [Upgrade](#) to 0.37 or higher when available or 0.37.0rc1, or apply the fix described [here](#).
- **ht://Dig** ([02/14/05](#)) [Upgrade](#) to higher than 3.2.0b6, or install a fixed package from your operating system vendor.
- **DotNetNuke** ([05/26/05](#)) [Upgrade](#) to 3.0.12 or higher.
- **Apache Struts** ([12/07/05](#)) [Upgrade](#) to 1.2.8 or higher.
- **phpMyChat** ([12/09/05](#)) [Upgrade](#) to higher than version 0.14.5 .
- **Cerberus Helpdesk** ([01/04/06](#)) [Upgrade](#) to 2.7.0 or higher.
- **Apache Geronimo** ([01/27/06](#)) [Upgrade](#) to version 1.0.1 or 1.1 when available.
- **Ashnews** ([02/10/06](#)) [Upgrade](#) to a version higher than 0.83 when available.
- **QwikiWiki** ([02/27/06](#)) [Upgrade](#) to a version higher than 1.51 when available.
- **vCard** ([03/23/06](#)) [Upgrade](#) to a version higher than 2.9.
- **Contrex** ([03/24/06](#)) [Patch](#) version 1.0.8 or [upgrade](#) to a version higher than 1.0.8 .

- **phpCOIN** (04/05/06) [upgrade](#) to version 1.2.3 .
- **PHPKIT** (04/05/06) [upgrade](#) to 1.6.1 Release 2.
- **phpAdsNew/phpPgAds** (04/06/06) [upgrade](#) [phpAdsNew](#) or [phpPgAds](#) to version 2.0.8.
- **Confixx** (04/23/06) [Upgrade](#) to a version higher than 3.1.2 when available.
- **phpLDAPadmin** (05/01/06) [Upgrade](#) to version 0.9.8.2 or higher.
- **Boardsolution** (05/02/06) [Upgrade](#) to version 1.13 or higher.
- **Pivot** (07/24/06) [Upgrade](#) to version 1.30 Final or higher.
- **XOOPS** (10/25/06) [Upgrade](#) to version higher than 2.0.15 when it becomes available (2.2 track has been discontinued).
- **XOOPS packs** (11/17/06) [Upgrade](#) [CommunityPack](#), [PersonalPack](#), and [IntranetPack](#) to a version higher than 1.0 or fix as [described](#).
- **cPanel** (11/06/06) [Upgrade](#) to 10.9.0 (Build CURRENT)-56 tree.
- **OsTicket** (01/02/07) [Upgrade](#) to 2.0 when available.
- **PHP iCalendar** (01/04/07) [Upgrade](#) to version 2.23 or later when available.
- **Citrix MetaFrame** (03/07/08) Apply a fix as described in [Document ID CTX101996](#).
- **Campus Bulletin Board** (05/29/08) [Upgrade](#) to a version higher than 3.4 when available.
- **Apache Roller** (01/27/09) Apply the fix described in Revision 668737.
- **All other products:** Retrieve an upgrade or a patch from the vendor. See the posting to [Bugtraq](#) for information about specific types of web servers. See references below. If a fix is unavailable, then work around the problem by creating a customized error page.

Where can I read more about this?

For more information on cross-site scripting, and, more generally, on malicious **HTML** tags embedded in client requests, see [CERT Advisory 2000-02](#) and Microsoft's [Information on Cross-Site Scripting](#).

For more information on cross-site scripting vulnerabilities in specific products, see the following:

- [PHP-Nuke \(Downloads Module\)](#)
- [PHP-Nuke \(Nuke League Module\)](#)
- [NetWare Web Search](#)
- [Apache printenv](#)
- [Apache printenv](#)
- [Microsoft Content Management Server 2001](#)
- [Microsoft Content Management Server 2001](#)
- [ProductCart](#)
- [WebCalendar](#)
- [WebCalendar \(view_entry.php\)](#)
- [VP-ASP shopdisplayproducts.asp](#)
- [VP-ASP shopdisplayproducts.asp \(update\)](#)
- [VP-ASP Shopping Cart](#)
- [Bitfolge sniff index.php](#)
- [osCommerce](#)
- [osCommerce \(contact_us.php\)](#)
- [IBM Net.Data db2www](#)
- [phpBB \(topic_id\)](#)
- [phpBB \(postorder\)](#)
- [phpBB \(postdays and topicdays\)](#)
- [Invision Power Board](#)
- [Invision Power Board referer](#)
- [PHP-Nuke \(body tag\)](#)
- [PHP-Nuke \(user parameter\)](#)
- [PHP-Nuke](#)
- [PHP-Nuke \(encoded\)](#)

- [PHP-Nuke \(Journal module\)](#)
- [PHP-Nuke \(NewLinks and NewDownloads\)](#)
- [CactuShop](#)
- [NukeCalendar](#)
- [Tiki CMS](#)
- [e107](#)
- [e107 \(error.php\)](#)
- [e107 \(search.php\)](#)
- [ArbitroWeb](#)
- [CuteNews](#)
- [CuteNews](#)
- [Cart32 GetLatestBuilds](#)
- [phpBB cat_title and faq.php](#)
- [phpBB search.php](#)
- [PostNuke Reviews](#)
- [PostNuke user.php](#)
- [PostNuke RSS module](#)
- [PostNuke Xanthia module](#)
- [Phorum \(search.php\)](#)
- [JShop](#)
- [phpWebSite](#)
- [Xedus](#)
- [Password Protect](#)
- [PSnews](#)
- [DNS4Me](#)
- [PHP-Fusion](#)
- [PHP-Fusion \(additional\)](#)
- [W-Agora](#)
- [DCP-Portal](#)
- [DCP-Portal \(additional\)](#)
- [DCP-Portal \(send page\)](#)
- [Turbo Traffic Trader](#)
- [GoSmart Message Board](#)
- [CoolPHP](#)
- [MoniWiki](#)
- [Horde \(help.php\)](#)
- [MailPost](#)
- [MailPost](#)
- [Bugtraq](#)
- [PHPKIT popup.php](#)
- [YaBB shadow tags](#)
- [YaBB usersrecentposts](#)
- [phpCMS](#)
- [Advanced Guestbook](#)
- [phpGedView](#)
- [CVSTrac](#)
- [Namazu](#)
- [Eventum](#)
- [Eventum \(view.php\)](#)
- [ht://Dig](#)
- [ht://Dig \(sort\)](#)
- [CubeCart](#)
- [MercuryBoard](#)
- [paFileDB](#)

- paFileDB (sortby parameter)
- CoolForum (avatar.php)
- PHP-Nuke Bookmarks module
- ESMI PayPal Storefront
- SonicWall SOHO/10
- calendar_scheduler.php
- RSA Authentication Agent
- Claroline
- osTicket
- osTicket (e)
- Help Center Live (faq/index.php)
- DotNetNuke
- MetaCart (productsByCategory.asp)
- X-Cart
- cPanel
- Hosting Controller (error.asp)
- Simple Message Board
- Fusebox
- Open WebMail (openwebmail-main.pl)
- MIVA Merchant (merchant.mvc)
- phpMyFAQ (footer.php)
- RSA Security
- FlatNuke
- Apache Struts
- PHP-Nuke
- ASP Fast Forum
- phpMyChat
- Cerberus Helpdesk
- Apache Geronimo
- QwikiWiki
- Ashnews
- PHP-Nuke Header.php
- vCard
- vCard(toprated.php)
- Contrexx
- phpCOIN
- phpAdsNew/phpPgAds
- PHPKIT (include.php)
- Confixx
- Confixx (additional)
- phpLDAPadmin
- Boardsolution
- BlueDragon
- Pivot
- XOOPS
- cPanel scripts
- Netquery (nquser.php)
- XOOPS packs (newlist.php)
- PHPNews (link_temp.php)
- PHP iCalendar
- VP-ASP shopcustadmin
- Open WebMail vulnerabilities (multiple)
- OpenBSD BGPD (/cgi-bin/bgplg)
- Citrix MetaFrame Web Manager 'login.asp'

- [Campus Bulletin Board](#)
- [Apache Roller](#)

Technical Details

Service: http

GET /login.php?Username=<script>alert('SAINT')</script> HTTP/1.0

Host: 172.16.1.2:80

User-Agent: Mozilla/4.0

Received:

<form method="post" id="Login" action="/login.php?Username=<script>alert('SAINT')</script>">

WWW

Severity: Service

Technical Details

HTTP/1.1 200 OK

Date: Thu, 07 Jan 2010 20:34:39 GMT

Server: Apache/2.2.8 (Mandriva Linux/PREFORK-6mdv2008.1)

X-Powered-By: PHP/5.2.5

Connection: close

Content-Type:

WWW (Secure)

Severity: Service

Technical Details

<?xml version="1.0" encoding="ISO-8859-1"?>