



Detailed Scan Report

Scan of http://192.168.1.100:80/

Scan details

Scan information	
Starttime	27/10/2009 23:27:45
Finish time	28/10/2009 0:20:51
Scan time	53 minutes, 5 seconds
Profile	default

Server information	
Responsive	True
Server banner	Apache/2.0.55 (Unix) PHP/5.1.2
Server OS	Unix
Server technologies	ASP,ASP.NET,PHP,Perl,mod_ssl,mod_perl,mod_python,OpenSSL,FrontPage,JRun,Ruby

Threat level



Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	12
High	8
Medium	2
Low	1
Informational	1

Knowledge base

List of open TCP ports

There are **6** open TCP ports on the remote host.

Port **21** - **[ftp]** is open.

Port banner:

OOPS: could not bind listening IPv4 socket

Port **25** - **[smtp]** is open.

Port banner:

slax.example.net ESMTP Sendmail 8.13.7/8.13.7; Tue, 27 Oct 2009 06:28:42 GMT

Port **22** - **[ssh]** is open.

Port banner:

SSH-1.99-OpenSSH_4.3

Port **80** - **[http]** is open.

Port banner:

HTTP/1.1 200 OK: Tue, 27 Oct 2009 06:30:30 GMT: Apache/2.0.55 (Unix) PHP/5.1.2Powered-By: PHP/5.1.2Length: 1983:
closeType: text/html

```
<style> {  
: black url(background.jpg) no-repe ...
```

Port **110** - **[pop3]** is open.

Port banner:

+OK

Port **143** - **[imap]** is open.

Port banner:

* OK [CAPABILITY IMAP4REV1 LITERAL+ SASL-IR LOGIN-REFERRALS STARTTLS AUTH=LOGIN] [192.168.1.100]
IMAP4rev1 2004.357 at Tue, 27 Oct 2009 06:32:33 +0000 (GMT)

IMAP server running

An IMAP server is running on TCP port 143.

POP3 server running

A POP3 server is running on TCP port 110.

SSH server running

A SSH server is running on TCP port 22.

SSH server information:

Server key fingerprint: ababa8ada2f2fdc26f0599694054ec10 version: SSH2 algorithm client to server: AES128 CTR algorithm
server to client: AES128 CTR algorithm client to server: HMAC with SHA-256 digest algorithm server to client: HMAC with
SHA-256 digest key algorithm: Certificate is signed using RSA digital signature with MD2 digest

SMTP server running

A SMTP server is running on TCP port 25. Information gathered from this service:

EHLO returns:

250-slax.example.net Hello [192.168.1.2], pleased to meet you

-ENHANCEDSTATUSCODES

-PIPELINING

-8BITMIME

-SIZE

-DSN

-ETRN

-AUTH DIGEST-MD5 CRAM-MD5

-DELIVERBY

HELP returns:

214-2.0.0 This is sendmail version 8.13.7

-2.0.0 Topics:

-2.0.0

-2.0.0

-2.0.0

-2.0.0

-2.0.0 For more info use "HELP <topic>".

-2.0.0 To report bugs in the implementation see

-2.0.0 [://www.sendmail.org/email-addresses.html](http://www.sendmail.org/email-addresses.html)

-2.0.0 For local information send email to Postmaster at your site.

2.0.0 End of HELP info

Alerts summary

Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerability	
Affects	Variations
Web Server	1
PHP HTML Entity Encoder Heap Overflow Vulnerability	
Affects	Variations
PHP	1
PHP version older than 5.2.1	
Affects	Variations
PHP	1
PHP version older than 5.2.3	
Affects	Variations
PHP	1
PHP version older than 5.2.5	
Affects	Variations
PHP	1
PHP version older than 5.2.6	
Affects	Variations
PHP	1
PHP Zend_Hash_Del_Key_Or_Index vulnerability	
Affects	Variations
PHP	1
Proxy accepts CONNECT requests	
Affects	Variations
Server	1
Apache 2.x version older than 2.0.61	
Affects	Variations
Web Server	1
Apache 2.x version older than 2.0.63	
Affects	Variations
Web Server	1
TRACE Method Enabled	
Affects	Variations
Web Server	1
Email address found	
Affects	Variations
/index2.php	1

Alert details

❗ Apache Mod_Rewrite Off-By-One Buffer Overflow Vulnerability

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

Apache mod_rewrite is prone to an off-by-one buffer-overflow condition. The vulnerability arising in the mod_rewrite module's ldap scheme handling allows for potential memory corruption when an attacker exploits certain rewrite rules.

Affected Apache versions:

- Apache 1.3.28 - 1.3.36 with mod_rewrite
- Apache 2.2.0 - 2.2.2 with mod_rewrite
- Apache 2.0.46 - 2.0.58 with mod_rewrite

Impact

An attacker may exploit this issue to trigger a denial-of-service condition. Reportedly, arbitrary code execution may also be possible.

Recommendation

Upgrade Apache to the latest version.

Affected items

Web Server
Details
Current version is Apache/2.0.55

❗ PHP HTML Entity Encoder Heap Overflow Vulnerability

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

Stefan Esser reported some vulnerabilities in PHP, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system. The vulnerabilities are caused due to boundary errors within the "htmlentities()" and "htmlspecialchars()" functions. If a PHP application uses these functions to process user-supplied input, this can be exploited to cause a heap-based buffer overflow by passing specially crafted data to the affected application. Successful exploitation may allow execution of arbitrary code, but requires that the UTF-8 character set is selected. For a detailed explanation of the vulnerability read the referenced article.

Vendor has released PHP 5.2.0 which fixes this issue.

Affected PHP versions (up to 4.4.4/5.1.6).

Impact

Denial of service, remote code execution.

Recommendation

Upgrade PHP to the latest version.

Affected items

PHP
Details
Current version is PHP/5.1.2

❗ PHP version older than 5.2.1

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

This release is a major stability and security enhancement of the 5.X branch, and all users are strongly encouraged to upgrade to it as soon as possible.

Security Enhancements and Fixes in PHP 5.2.1:

- Fixed possible `safe_mode` & `open_basedir` bypasses inside the session extension.
- Prevent search engines from indexing the `phpinfo()` page.
- Fixed a number of input processing bugs inside the filter extension.
- Fixed `unserialize()` abuse on 64 bit systems with certain input strings.
- Fixed possible overflows and stack corruptions in the session extension.
- Fixed an underflow inside the internal `sapi_header_op()` function.
- Fixed allocation bugs caused by attempts to allocate negative values in some code paths.
- Fixed possible stack overflows inside zip, imap & sqlite extensions.
- Fixed several possible buffer overflows inside the stream filters.
- Fixed non-validated resource destruction inside the shmop extension.
- Fixed a possible overflow in the `str_replace()` function.
- Fixed possible clobbering of super-globals in several code paths.
- Fixed a possible information disclosure inside the wddx extension.
- Fixed a possible string format vulnerability in `*print()` functions on 64 bit systems.
- Fixed a possible buffer overflow inside `mail()` and `ibase_{delete,add,modify}_user()` functions.
- Fixed a string format vulnerability inside the `odbc_result_all()` function.
- Memory limit is now enabled by default.
- Added internal heap protection.
- Extended filter extension support for `$_SERVER` in CGI and apache2 SAPIs.

Affected PHP versions (up to 5.2.0).

Impact

Denial of service or ultimately arbitrary code execution.

Recommendation

Upgrade PHP to the latest version.

Affected items

PHP
Details
Current version is PHP/5.1.2

❗ PHP version older than 5.2.3

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

The PHP development team would like to announce the immediate availability of PHP 5.2.3. This release continues to improve the security and the stability of the 5.X branch as well as addressing two regressions introduced by the previous 5.2 releases. These regressions relate to the timeout handling over non-blocking SSL connections and the lack of HTTP_RAW_POST_DATA in certain conditions. All users are encouraged to upgrade to this release.

Security Enhancements and Fixes in PHP 5.2.3:

- Fixed an integer overflow inside chunk_split() (by Gerhard Wagner, CVE-2007-2872)
- Fixed possible infinite loop in imagecreatefrompng. (by Xavier Roche, CVE-2007-2756)
- Fixed ext/filter Email Validation Vulnerability (MOPB-45 by Stefan Esser, CVE-2007-1900)
- Fixed bug #41492 (open_basedir/safe_mode bypass inside realpath()) (by bugs dot php dot net at chsc dot dk)
- Improved fix for CVE-2007-1887 to work with non-bundled sqlite2 lib.
- Added mysql_set_charset() to allow runtime altering of connection encoding.

Affected PHP versions (up to 5.2.2).

Impact

Denial of service or ultimately arbitrary code execution.

Recommendation

Upgrade PHP to the latest version.

Affected items

PHP
Details
Current version is PHP/5.1.2

❗ PHP version older than 5.2.5

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

The PHP development team would like to announce the immediate availability of PHP 5.2.5. This release focuses on improving the stability of the PHP 5.2.x branch with over 60 bug fixes, several of which are security related. All users of PHP are encouraged to upgrade to this release.

Security Enhancements and Fixes in PHP 5.2.5:

- Fixed dl() to only accept filenames. Reported by Laurent Gaffie.
- Fixed dl() to limit argument size to MAXPATHLEN (CVE-2007-4887). Reported by Laurent Gaffie.
- Fixed htmlentities/htmlspecialchars not to accept partial multibyte sequences. Reported by Rasmus Lerdorf
- Fixed possible triggering of buffer overflows inside glibc implementations of the fnmatch(), setlocale() and glob() functions. Reported by Laurent Gaffie.
- Fixed "mail.force_extra_parameters" php.ini directive not to be modifiable in .htaccess due to the security implications. Reported by SecurityReason.
- Fixed bug #42869 (automatic session id insertion adds sessions id to non-local forms).
- Fixed bug #41561 (Values set with php_admin_* in httpd.conf can be overwritten with ini_set()).

Affected PHP versions (up to 5.2.4).

Impact

Denial of service or ultimately arbitrary code execution.

Recommendation

Upgrade PHP to the latest version.

Affected items

PHP
Details
Current version is PHP/5.1.2

❗ PHP version older than 5.2.6

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

The PHP development team would like to announce the immediate availability of PHP 5.2.6. This release focuses on improving the stability of the PHP 5.2.x branch with over 120 bug fixes, several of which are security related. All users of PHP are encouraged to upgrade to this release.

Security Enhancements and Fixes in PHP 5.2.6:

- Fixed possible stack buffer overflow in the FastCGI SAPI identified by Andrei Nigmatulin.
- Fixed integer overflow in printf() identified by Maksymilian Arciemowicz.
- Fixed security issue detailed in CVE-2008-0599 identified by Ryan Permeh.
- Fixed a safe_mode bypass in cURL identified by Maksymilian Arciemowicz.
- Properly address incomplete multibyte chars inside escapeshellcmd() identified by Stefan Esser.
- Upgraded bundled PCRE to version 7.6

Affected PHP versions (up to 5.2.5).

Impact

Denial of service or ultimately arbitrary code execution.

Recommendation

Upgrade PHP to the latest version.

Affected items

Acunetix Website Audit

PHP

Details

Current version is [PHP/5.1.2](#)

❗ PHP Zend_Hash_Del_Key_Or_Index vulnerability

Severity	High
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

Stefan Esser had discovered a weakness within the depths of the implementation of hashtables in the Zend Engine. This vulnerability affects a large number of PHP applications. It creates large new holes in many popular PHP applications. Additionally many old holes that were disclosed in the past were only fixed by using the `unset()` statement. Many of these holes are still open if the already existing exploits are changed by adding the correct numerical keys to survive the `unset()`. For a detailed explanation of the vulnerability read the referenced article.

Affected PHP versions (up to 4.4.2/5.1.3).

Impact

Possible code execution, SQL injection, ...

Recommendation

Upgrade PHP to the latest version.

Affected items

PHP

Details

Current version is [PHP/5.1.2](#)

❗ Proxy accepts CONNECT requests

Severity	High
Type	Configuration
Reported by module	Scripting

Description

The remote proxy server can be used to send CONNECT requests. The proxy allows everyone to perform CONNECT HTTP requests to arbitrary ports, such as: [www.acunetix.com:25](#)

This may allow attackers to bypass your firewall and connect to sensitive ports like 23 (telnet), 25 (sendmail) using the proxy. A spammer may be using your proxy to send bulk email.

Impact

Firewall bypass, possible information disclosure

Recommendation

Restrict proxy access to valid users and/or hosts. Deny CONNECT requests.

Affected items

Server
Details
The proxy server is running on TCP port 80.

🚩 Apache 2.x version older than 2.0.61

Severity	Medium
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

Fixed in Apache httpd 2.0.61:

- **moderate** : mod_proxy crash CVE-2007-3847

A flaw was found in the Apache HTTP Server mod_proxy module. On sites where a reverse proxy is configured, a remote attacker could send a carefully crafted request that would cause the Apache child process handling that request to crash. On sites where a forward proxy is configured, an attacker could cause a similar crash if a user could be persuaded to visit a malicious site using the proxy. This could lead to a denial of service if using a threaded Multi-Processing Module.

- **moderate** : mod_status cross-site scripting CVE-2006-5752

A flaw was found in the mod_status module. On sites where the server-status page is publicly accessible and ExtendedStatus is enabled this could lead to a cross-site scripting attack. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.

- **moderate** : Signals to arbitrary processes CVE-2007-3304

The Apache HTTP server did not verify that a process was an Apache child process before sending it signals. A local attacker with the ability to run scripts on the HTTP server could manipulate the scoreboard and cause arbitrary processes to be terminated which could lead to a denial of service.

- **moderate** : mod_cache proxy DoS CVE-2007-1863

A bug was found in the mod_cache module. On sites where caching is enabled, a remote attacker could send a carefully crafted request that would cause the Apache child process handling that request to crash. This could lead to a denial of service if using a threaded Multi-Processing Module.

Affected Apache versions (up to 2.0.60).

Impact

Check references for details about every vulnerability.

Recommendation

Upgrade Apache 2.x to the latest version.

Affected items

Web Server
Details
Current version is <i>Apache/2.0.55</i>

🚩 Apache 2.x version older than 2.0.63

Severity	Medium
Type	Configuration
Reported by module	Version check

Description

This alert was generated using only banner information. It may be a false positive.

Fixed in Apache httpd 2.0.63:

- **low** : mod_proxy_ftp UTF-7 XSS CVE-2008-0005

A workaround was added in the mod_proxy_ftp module. On sites where mod_proxy_ftp is enabled and a forward proxy is configured, a cross-site scripting attack is possible against Web browsers which do not correctly derive the response character set following the rules in RFC 2616.

- **moderate** : mod_status XSS CVE-2007-6388

A flaw was found in the mod_status module. On sites where mod_status is enabled and the status pages were publicly accessible, a cross-site scripting attack is possible. Note that the server-status page is not enabled by default and it is best practice to not make this publicly available.

- **moderate** : mod_imap XSS CVE-2007-5000

A flaw was found in the mod_imap module. On sites where mod_imap is enabled and an imagemap file is publicly available, a cross-site scripting attack is possible.

Affected Apache versions (up to 2.0.62).

Impact

Check references for details about every vulnerability.

Recommendation

Upgrade Apache 2.x to the latest version.

Affected items

Web Server
Details
Current version is Apache/2.0.55

TRACE Method Enabled

Severity	Low
Type	Validation
Reported by module	CGI Tester

Description

HTTP TRACE method is enabled on this web server. In the presence of other cross-domain vulnerabilities in web browsers, sensitive header information could be read from any domains that support the HTTP TRACE method.

Impact

Attackers may abuse HTTP TRACE functionality to gain access to information in HTTP headers such as cookies and authentication data.

Recommendation

Disable TRACE Method on the web server.

Affected items

Web Server
Details
No details are available.
Request
TRACE /TRACE_test HTTP/1.0 Accept: /*/* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322) Host: 192.168.1.100 Connection: Close Pragma: no-cache Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)

Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED

Response

HTTP/1.1 200 OK
Date: Tue, 27 Oct 2009 06:29:07 GMT
Server: Apache/2.0.55 (Unix) PHP/5.1.2
Connection: close
Content-Type: message/http

Email address found

Severity	Informational
Type	Informational
Reported by module	Text search

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

Affected items

/index2.php

Details

We found
[marym@herot.net@herot.net@herot.net@herot.net@herot.net@herot.net@herot.net@herot.net@herot.net@herot.net](#)

Request

GET /index2.php HTTP/1.0
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1.1.4322)
Host: 192.168.1.100
Referer: http://192.168.1.100/
Accept-Language: es
Connection: keep-alive
Acunetix-Product: WVS/5.1 (Acunetix Web Vulnerability Scanner - NORMAL)
Acunetix-Scanning-agreement: Third Party Scanning PROHIBITED
Acunetix-User-agreement: http://www.acunetix.com/wvs/disc.htm

Response

HTTP/1.1 200 OK
Date: Tue, 27 Oct 2009 06:28:29 GMT
Server: Apache/2.0.55 (Unix) PHP/5.1.2
X-Powered-By: PHP/5.1.2
Content-Length: 2796
Keep-Alive: timeout=15, max=98
Connection: Keep-Alive
Content-Type: text/html