Scan report for www.cc-emblavez.fr

Scanned on 2015-02-03 08:47:40

SQL Error

Description
Your website contains one or more SQL-error(s). Make sure to remove them or have them fixed as soon as possible.

CVSS
5.9

URL
http://www.cc-emblavez.fr/pages/evenements/affiche_detail_manif_menu.php

Match

```
</a>/
              D&eacute;tail de l'&eacute;v&egrave;nement<br>
              <br>
              </font></p>
             Erreur SQL !<br><br>You have an error in your SQL syntax; check the manual
that corresponds to your MySQL
```

74 x Potential Vulnerabilities In The Web Server

Description
The web server is leaking information about which version of the web server is running. The specific version used have been looked up for known vulnerabilities and are listed below. Note though that these are just potential vulnerabilities and have not been verified.

CVSS
5.6

URL
http://www.cc-emblavez.fr/

Name
CVE-2006-4110

Match
```
Apache 2.2.3
```

```
Apache 2.2.2, when running on Windows, allows remote attackers to read source code of CGI programs via a request that contains uppercase (or alternate case) characters that bypass the case-sensitive ScriptAlias directive, but allow access to the file on case-insensitive file systems.
```

URL
http://www.cc-emblavez.fr/

Name
CVE-2006-5752

Match
```
Apache 2.2.3
```

```
Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when ExtendedStatus is enabled and a public server-status page is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving charsets with browsers that perform "charset detection" when the content-type is not specified.
```

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-1741

Match
```
Apache 2.2.3
```

```
Multiple race conditions in suexec in Apache HTTP Server (httpd) 2.2.3 between directory and file validation, and their usage, allow local users to gain privileges and execute arbitrary code by renaming directories or performing symlink attacks. NOTE: the
```

researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-1742

Match
Apache 2.2.3

suexec in Apache HTTP Server (httpd) 2.2.3 uses a partial comparison for verifying whether the current directory is within the document root, which might allow local users to perform unauthorized operations on incorrect directories, as demonstrated using "html_backup" and "htmleditor" under an "html" directory. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-1743

Match
Apache 2.2.3

suexec in Apache HTTP Server (httpd) 2.2.3 does not verify combinations of user and group IDs on the command line, which might allow local users to leverage other vulnerabilities to create arbitrary UID/GID owned files if /proc is mounted. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root." In addition, because this is dependent on other vulnerabilities, perhaps this is resultant and should not be included in CVE.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-4465

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in mod_autoindex.c in the Apache HTTP Server before 2.2.6, when the charset on a server-generated page is not defined, allows remote attackers to inject arbitrary web script or HTML via the P parameter using the UTF-7 charset. NOTE: it could be argued that this issue is due to a design limitation of browsers that attempt to perform automatic content type detection.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-5000

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in the (1) mod_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod_imagemap module in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-6203

Match
Apache 2.2.3

Apache HTTP Server 2.0.x and 2.2.x does not sanitize the HTTP Method specifier header from an HTTP request when it is reflected back in a "413 Request Entity Too Large" error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated via an HTTP request containing an invalid Content-length value, a similar issue to CVE-2006-3918.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-6388

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-6420

Match
Apache 2.2.3

Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod_proxy_balancer for Apache HTTP Server 2.2.x allows remote attackers to gain privileges via unspecified vectors.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-6421

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in balancer-manager in mod_proxy_balancer in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via the (1) ss, (2) wr, or (3) rr parameters, or (4) the URL.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-6422

Match
Apache 2.2.3

The balancer_handler function in mod_proxy_balancer in the Apache HTTP Server 2.2.0 through 2.2.6, when a threaded Multi-Processing Module is used, allows remote authenticated users to cause a denial of service (child process crash) via an invalid bb variable.

URL
http://www.cc-emblavez.fr/

Name
CVE-2007-6750

Match

Apache 2.2.3

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

URL
http://www.cc-emblavez.fr/

Name
CVE-2008-0455

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

URL
http://www.cc-emblavez.fr/

Name
CVE-2008-2168

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in Apache 2.2.6 and earlier allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded URLs that are not properly handled when displaying the 403 Forbidden error page.

URL
http://www.cc-emblavez.fr/

Name
CVE-2008-2939

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.

URL
http://www.cc-emblavez.fr/

Name
CVE-2009-1195

Match
Apache 2.2.3

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

URL
http://www.cc-emblavez.fr/

Name
CVE-2009-2699

Match
Apache 2.2.3

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

URL
http://www.cc-emblavez.fr/

Name
CVE-2009-3555

Match
Apache 2.2.3

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

URL
http://www.cc-emblavez.fr/

Name
CVE-2010-0408

Match
Apache 2.2.3

The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

URL
http://www.cc-emblavez.fr/

Name
CVE-2010-0434

Match
Apache 2.2.3

The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

URL
http://www.cc-emblavez.fr/

Name
CVE-2010-1452

Match
Apache 2.2.3

The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

URL

http://www.cc-emblavez.fr/

Name
CVE-2011-0419

Match
Apache 2.2.3

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

URL
http://www.cc-emblavez.fr/

Name
CVE-2011-3348

Match
Apache 2.2.3

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

URL
http://www.cc-emblavez.fr/

Name
CVE-2011-3368

Match
Apache 2.2.3

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

URL
http://www.cc-emblavez.fr/

Name
CVE-2011-3607

Match
Apache 2.2.3

Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

URL
http://www.cc-emblavez.fr/

Name
CVE-2011-3639

Match
Apache 2.2.3

The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

URL
http://www.cc-emblavez.fr/

Name
CVE-2011-4317

Match
Apache 2.2.3

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

URL
http://www.cc-emblavez.fr/

Name
CVE-2012-0031

Match
Apache 2.2.3

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

URL
http://www.cc-emblavez.fr/

Name
CVE-2012-0053

Match
Apache 2.2.3

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

URL
http://www.cc-emblavez.fr/

Name
CVE-2012-2687

Match
Apache 2.2.3

Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

URL
http://www.cc-emblavez.fr/

Name
CVE-2012-3499

Match
Apache 2.2.3

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

URL
http://www.cc-emblavez.fr/

Name
CVE-2012-4558

Match
Apache 2.2.3

Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

URL
http://www.cc-emblavez.fr/

Name
CVE-2014-0098

Match
Apache 2.2.3

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

URL
http://www.cc-emblavez.fr/

Name
CVE-2013-1862

Match
Apache 2.2.3

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

URL
http://www.cc-emblavez.fr/

Name
CVE-2013-1896

Match
Apache 2.2.3

mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

URL
http://www.cc-emblavez.fr/

Name
CVE-2013-6438

Match
Apache 2.2.3

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

URL
https://www.cc-emblavez.fr/

Name
CVE-2006-4110

Match
Apache 2.2.3

Apache 2.2.2, when running on Windows, allows remote attackers to read source code of CGI programs via a request that contains uppercase (or alternate case) characters that bypass the case-sensitive ScriptAlias directive, but allow access to the file on case-insensitive file systems.

URL
https://www.cc-emblavez.fr/

Name
CVE-2006-5752

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when ExtendedStatus is enabled and a public server-status page is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving charsets with browsers that perform "charset detection" when the content-type is not specified.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-1741

Match
Apache 2.2.3

Multiple race conditions in suexec in Apache HTTP Server (httpd) 2.2.3 between directory and file validation, and their usage, allow local users to gain privileges and execute arbitrary code by renaming directories or performing symlink attacks. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-1742

Match
Apache 2.2.3

suexec in Apache HTTP Server (httpd) 2.2.3 uses a partial comparison for verifying whether the current directory is within the document root, which might allow local users to perform unauthorized operations on incorrect directories, as demonstrated using "html_backup" and "htmleditor" under an "html" directory. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root."

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-1743

Match
Apache 2.2.3

suexec in Apache HTTP Server (httpd) 2.2.3 does not verify combinations of user and group IDs on the command line, which might allow local users to leverage other vulnerabilities to create arbitrary UID/GID owned files if /proc is mounted. NOTE: the researcher, who is reliable, claims that the vendor disputes the issue because "the attacks described rely on an insecure server configuration" in which the user "has write access to the document root." In addition, because this is dependent on other vulnerabilities, perhaps this is resultant and should not be included in CVE.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-4465

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in mod_autoindex.c in the Apache HTTP Server before 2.2.6, when the charset on a server-generated page is not defined, allows remote attackers to inject arbitrary web script or HTML via the P parameter using the UTF-7 charset. NOTE: it could be argued that this issue is due to a design limitation of browsers that attempt to perform automatic content type detection.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-5000

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in the (1) mod_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod_imagemap module in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-6203

Match
Apache 2.2.3

Apache HTTP Server 2.0.x and 2.2.x does not sanitize the HTTP Method specifier header from an HTTP request when it is reflected back in a "413 Request Entity Too Large" error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated via an HTTP request containing an invalid Content-length value, a similar issue to CVE-2006-3918.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-6388

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-6420

Match
Apache 2.2.3

Cross-site request forgery (CSRF) vulnerability in the balancer-manager in mod_proxy_balancer for Apache HTTP Server 2.2.x allows remote attackers to gain privileges via unspecified vectors.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-6421

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in balancer-manager in mod_proxy_balancer in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via the (1) ss, (2) wr, or (3) rr parameters, or (4) the URL.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-6422

Match
Apache 2.2.3

The balancer_handler function in mod_proxy_balancer in the Apache HTTP Server 2.2.0 through 2.2.6, when a threaded Multi-Processing Module is used, allows remote authenticated users to cause a denial of service (child process crash) via an invalid bb variable.

URL
https://www.cc-emblavez.fr/

Name
CVE-2007-6750

Match
Apache 2.2.3

The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

URL
https://www.cc-emblavez.fr/

Name
CVE-2008-0455

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server 2.2.6 and earlier in the 2.2.x series, 2.0.61 and earlier in the 2.0.x series, and 1.3.39 and earlier in the 1.3.x series allows remote authenticated users to inject arbitrary web script or HTML by uploading a file with a name containing XSS sequences and a file extension, which leads to injection within a (1) "406 Not Acceptable" or (2) "300 Multiple Choices" HTTP response when the extension is omitted in a request for the file.

URL
https://www.cc-emblavez.fr/

Name
CVE-2008-2168

Match

Apache 2.2.3

Cross-site scripting (XSS) vulnerability in Apache 2.2.6 and earlier allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded URLs that are not properly handled when displaying the 403 Forbidden error page.

URL
https://www.cc-emblavez.fr/

Name
CVE-2008-2939

Match
Apache 2.2.3

Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.

URL
https://www.cc-emblavez.fr/

Name
CVE-2009-1195

Match
Apache 2.2.3

The Apache HTTP Server 2.2.11 and earlier 2.2 versions does not properly handle Options=IncludesNOEXEC in the AllowOverride directive, which allows local users to gain privileges by configuring (1) Options Includes, (2) Options +Includes, or (3) Options +IncludesNOEXEC in a .htaccess file, and then inserting an exec element in a .shtml file.

URL
https://www.cc-emblavez.fr/

Name
CVE-2009-2699

Match
Apache 2.2.3

The Solaris pollset feature in the Event Port backend in poll/unix/port.c in the Apache Portable Runtime (APR) library before 1.3.9, as used in the Apache HTTP Server before 2.2.14 and other products, does not properly handle errors, which allows remote attackers to cause a denial of service (daemon hang) via unspecified HTTP requests, related to the prefork and event MPMs.

URL
https://www.cc-emblavez.fr/

Name
CVE-2009-3555

Match
Apache 2.2.3

The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a "plaintext injection" attack, aka the "Project Mogul" issue.

URL
https://www.cc-emblavez.fr/

Name
CVE-2010-0408

Match
Apache 2.2.3

The ap_proxy_ajp_request function in mod_proxy_ajp.c in mod_proxy_ajp in the Apache HTTP Server 2.2.x before 2.2.15 does not properly handle certain situations in which a client sends no request body, which allows remote attackers to cause a denial of service (backend server outage) via a crafted request, related to use of a 500 error code instead of the appropriate 400 error code.

URL
https://www.cc-emblavez.fr/

Name
CVE-2010-0434

Match
Apache 2.2.3

The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

URL
https://www.cc-emblavez.fr/

Name
CVE-2010-1452

Match
Apache 2.2.3

The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

URL
https://www.cc-emblavez.fr/

Name
CVE-2011-0419

Match
Apache 2.2.3

Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

URL
https://www.cc-emblavez.fr/

Name
CVE-2011-3348

Match
Apache 2.2.3

The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

URL
https://www.cc-emblavez.fr/

Name
CVE-2011-3368

Match
Apache 2.2.3

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

URL
https://www.cc-emblavez.fr/

Name
CVE-2011-3607

Match
Apache 2.2.3

Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

URL
https://www.cc-emblavez.fr/

Name
CVE-2011-3639

Match
Apache 2.2.3

The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character.
NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

URL
https://www.cc-emblavez.fr/

Name
CVE-2011-4317

Match
Apache 2.2.3

The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

URL
https://www.cc-emblavez.fr/

Name
CVE-2012-0031

Match
Apache 2.2.3

scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

URL
https://www.cc-emblavez.fr/

Name
CVE-2012-0053

Match
Apache 2.2.3

protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

URL
https://www.cc-emblavez.fr/

Name
CVE-2012-2687

Match
Apache 2.2.3

Multiple cross-site scripting (XSS) vulnerabilities in the make_variant_list function in mod_negotiation.c in the mod_negotiation module in the Apache HTTP Server 2.4.x before 2.4.3, when the MultiViews option is enabled, allow remote attackers to inject arbitrary web script or HTML via a crafted filename that is not properly handled during construction of a variant list.

URL
https://www.cc-emblavez.fr/

Name
CVE-2012-3499

Match
Apache 2.2.3

Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.

URL
https://www.cc-emblavez.fr/

Name
CVE-2012-4558

Match
Apache 2.2.3

Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.

URL
https://www.cc-emblavez.fr/

Name
CVE-2014-0098

Match
Apache 2.2.3

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

URL
https://www.cc-emblavez.fr/

Name
CVE-2013-1862

Match
Apache 2.2.3

mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

URL
https://www.cc-emblavez.fr/

Name
CVE-2013-1896

Match
Apache 2.2.3

mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.

URL
https://www.cc-emblavez.fr/

Name
CVE-2013-6438

Match
Apache 2.2.3

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

2 x Full Path Disclosure

Description

Typing in a series of unexpected characters into unprotected forms or parameters on a webpage could allow an attacker to retrieve the full directory path to a vulnerable script. It could also aid the attacker in mapping out strategic targets in the web servers file system. Strategic targets include but are not limited to vulnerable scripts and sensitive data.

The diclosure itself is considered as rather harmless but if used in conjunction other vulnerabilities it could increase the attackers success rate and boost their impact towards the server system.

CVSS

5

URL

https://www.cc-emblavez.fr/test/fcgi/test.fcgi?1422953723172[]=

Match

```
/usr/bin/
```

URL

https://www.cc-emblavez.fr/test/fcgi/test.fcgi?1422953735235[]=

Match

```
/usr/bin/
```

2 x Operating System Disclosure

Description

Your server discloses the name of its operating system. This information could help an attacker determine which attack-vector they are to use when targeting your system.

CVSS

5

URL

http://www.cc-emblavez.fr/

Match

```
Operating System: CentOS

Connection: close
Accept-Ranges: bytes
Content-Length: 2970
Content-Type: text/html
Date: Tue, 03 Feb 2015 08:56:09 GMT
ETag: "fc8f4a-b9a-13caf140"
Last-Modified: Thu, 04 Dec 2014 13:38:37 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PleskLin
```

URL

https://www.cc-emblavez.fr/

Match

```
Operating System: CentOS

Connection: close
Accept-Ranges: bytes
Content-Length: 7199
Content-Type: text/html
Date: Tue, 03 Feb 2015 08:56:09 GMT
ETag: "fc8f70-1c1f-8962cd80"
Last-Modified: Fri, 21 Feb 2014 15:47:18 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PleskLin
```

Missing DNSSEC

Description

Your domain is not configured to support DNSSEC. This opens up a man-in-the-middle scenario where remote attackers will be able to tamper with your DNS records by the use of cache poisoning techniques. You should ask your name provider for tips on how to enable DNSSEC for your domain.

CVSS

2.6

Domain

www.cc-emblavez.fr

Match

```
Record: A
```