Scan report for www.cc-emblavez.fr

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

3 x SQL Injection

Description
Could be abused to either extract specific data, possibly execute operating-system commands, read/write local files, or to put the server in a Denial- of Service condition.

CVSS
10

URL
http://www.cc-emblavez.fr/pages/evenements/affiche_detail_manif_menu.php?idevenement=1447"'`,%DE%7E%C7%1FY%00

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
```

URL
http://www.cc-emblavez.fr/pages/evenements/affiche_detail_manif.php?idevenement=1533"'`,%DE%7E%C7%1FY%00

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
```

URL
http://www.cc-emblavez.fr/pages/evenements/affiche_organisateur_manif.php?idasso=458"'`,%DE%7E%C7%1FY%00

Match
```
</a>/ Association organisatrice<br>
        <br>
        </font></p>


       Erreur SQL !<br><br>You have an error in your SQL syntax; check the manual that
corresponds to your MySQL
```

Blind SQL Injection

Description
Note: We are currently having problems with this module, and if you use a firewall such as ModSecurity we might encounter false-positive matches.

Could be abused for one or more of the following purposes: extracting specific data, possible execution of system commands, reading/writing local files or placing the target server in a Denial- of Service state.

CVSS
9.3

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

Match

```
Positive Probe: <tr>

  <td><a  href='affiche_manifs_jour_selectionne.php?date_debut_ang=2015-02-07'>samedi   7
fï¿½vrier 2015</a></td>

  <td>SAINT VINCENT</td>

  <td>BELOTE           <a           href='affiche_detail_manif.php?idevenement=485'><img
src='../../images/evenements/bouton_plus.jpg'           width='14'           height='14'
border='0'></a></td>

  <td>AMICALE       DES       SAPEURS       POMPIERS       SAINT       VINCENT       <a
href='affiche_organisateur_manif.php?idasso=164'><img
src='../../images/evenements/bouton_plus.jpg'           width='14'           height='14'
border='0'></a></td>

  </tr>
<tr>

  <td><a  href='affiche_manifs_jour_selectionne.php?date_debut_ang=2015-02-08'>dimanche
8 fï¿½vrier 2015</a></td>

  <td>BEAULIEU</td>

  <td>LOTO           <a           href='affiche_detail_manif.php?idevenement=1447'><img
src='../../images/evenements/bouton_plus.jpg'           width='14'           height='14'
border='0'></a></td>

  <td>A.P.E.              ECOLE              PRIVEE              BEAULIEU              <a
href='affiche_organisateur_manif.php?idasso=218'><img
src='../../images/evenements/bouton_plus.jpg'           width='14'           height='14'
border='0'></a></td>

  </tr>
<tr...

Negative Probe: </table>
             <p><font  face="Georgia,  Times  New  Roman,  Times,  serif"  size="2"><a
href="calendrier_manifs_evenements_principale.php"><img
src="../../images/evenements/bouton_retour.jpg" width="14" height="13" border="0"></a>
        Retour au <a href="calendrier_manifs_evenements_principale.php">choix
        des crit&egrave;res de s&eacute;lection</a>.</font></p>
```

```
      <p>  </p>
    </td>
  </tr>
</table>
</body>
</html>
```

POST

```
theme=2%26%27%3d%27%3d%22%3d%22&button=Afficher+les+%E9v%E8nements
```

16 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
9

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

Name
CVE-2006-4154

Match
`Apache 2.2.3`

`Format string vulnerability in the mod_tcl module 1.0 for Apache 2.x allows context-dependent attackers to execute arbitrary code via format string specifiers that are not properly handled in a set_var function call in (1) tcl_cmds.c and (2) tcl_core.c.`

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

Name
CVE-2007-6423

Match
`Apache 2.2.3`

`** DISPUTED **  Unspecified vulnerability in mod_proxy_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via a long URL.  NOTE: the vendor could not reproduce this issue.`

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

Name
CVE-2009-1890

Match
`Apache 2.2.3`

`The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.`

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

Name
CVE-2009-1891

Match
Apache 2.2.3

The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

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

Name
CVE-2010-0425

Match
Apache 2.2.3

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

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

Name
CVE-2011-3192

Match
Apache 2.2.3

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

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

Name
CVE-2012-0883

Match
Apache 2.2.3

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

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

Name
CVE-2013-2249

Match
Apache 2.2.3

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.

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

Name
CVE-2006-4154

Match
Apache 2.2.3

Format string vulnerability in the mod_tcl module 1.0 for Apache 2.x allows context-dependent attackers to execute arbitrary code via format string specifiers that are not properly handled in a set_var function call in (1) tcl_cmds.c and (2) tcl_core.c.

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

Name
CVE-2007-6423

Match
Apache 2.2.3

** DISPUTED ** Unspecified vulnerability in mod_proxy_balancer for Apache HTTP Server 2.2.x before 2.2.7-dev, when running on Windows, allows remote attackers to trigger memory corruption via a long URL. NOTE: the vendor could not reproduce this issue.

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

Name
CVE-2009-1890

Match
Apache 2.2.3

The stream_reqbody_cl function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server before 2.3.3, when a reverse proxy is configured, does not properly handle an amount of streamed data that exceeds the Content-Length value, which allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

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

Name
CVE-2009-1891

Match
Apache 2.2.3

The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

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

Name
CVE-2010-0425

Match
Apache 2.2.3

modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

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

Name
CVE-2011-3192

Match
Apache 2.2.3

The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

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

Name
CVE-2012-0883

Match
Apache 2.2.3

envvars (aka envvars-std) in the Apache HTTP Server before 2.4.2 places a zero-length directory name in the LD_LIBRARY_PATH, which allows local users to gain privileges via a Trojan horse DSO in the current working directory during execution of apachectl.

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

Name
CVE-2013-2249

Match
Apache 2.2.3

mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.