Multiple vulnerabilities in POSH web application

Description

Multiple Cross-Site Scripting vulnerabilities, a design vulnerability and an SQL vulnerability have been found in the last version of POSH < 3.2.1.

SQL injection

POSH allows applications to be added to an existing portal but failed at sanitizing a supplied parameter (rssurl) when processing the request, resulting in a potential database compromise.

Access Vector: remote

Security Risk: high

Vulnerability: CWE-89

CVE-ID: CVE-2014-2211

Proof of Concept

http://host/portal/addtoapplication.php?pid=0&rssurl=url,nbvariables,defvar%20FROM%20dir_item,dir_cat_item%20WHERE%201=0%20UNION%20SELECT%201,2,3,4,5,6,(select%20group_concat(username,':',email,':',md5pass)%20from%20users),8%23

Vulnerable code

The vulnerable code is located in */portal/addtoapplication.php*, line 71:

```
if ($_GET["pid"]==86)
{
    $DB->getResults($addtoapplication_getUserRssInfo,$DB->quote('rssurl='.$_GET["rssurl"]));
    $var="rssurl=".urlencode($_GET["rssurl"])."&";
}
else
{
    $DB->getResults($addtoapplication_getRssInfo,$_GET["rssurl"],$DB->escape($_GET["pid"]));
}
```

Solution

Escape `$_GET['rssurl']` with `$DB->quote()`.

Information leak (design vulnerability)

POSH provides a *remember me* feature that allows users to authenticate once and then use a dedicated cookie to prove their identity. POSH stores the username and md5 digest of the password in this cookie, with absolutely no protection, thus exposing user credentials through XSS.

Access Vector: remote

Security Risk: medium

Vulnerability: -

CVE-ID: CVE-2014-2212

Vulnerable code

The vulnerable code is located in */portal/scr_authentif.php*, line 79:

```
//login request
if (!empty($_COOKIE["autoi"]))
{
    $id = $_COOKIE["autoi"];
    $password = $_COOKIE["autop"];
    $md5 = true;
}
```

Solution

Use a per-user unpredictable token instead of storing the user's id and password in a cookie.

Cross-Site Scripting vulnerabilities

Many cross-site scripting vulnerabilities have been found in POSH:

```
http://host/includes/plugins/mobile/scripts/login.php?error=<script>alert('XSS')</script>
http://host/portal/openrssarticle.php?id=alert('XSS')
```

Access Vector: remote

Security Risk: low

Vulnerability: CWE-79

CVE-ID: CVE-2014-2213

Solution

Validate the *id* parameter (must be integer) and escape html-specific characters when displaying the error message.

Arbitrary URL redirection

POSH is prone to an arbitrary URL redirection vulnerability using POST requests, in its script in charge of sending reset password links to users:

```
POST /posh/portal/scr_sendmd5.php HTTP/1.1
Content-Length: 61
Content-Type: application/x-www-form-urlencoded
Host: <host>
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Accept: */*

redirect=%2f%2fwww.sysdream.com&update=Send&username=kjjascli
```

Access Vector: remote

Security Risk: low

Vulnerability: CWE-601

CVE-ID: CVE-2014-2214

Solution

Only allow redirection to known pages or remove any leading '/'.

Affected versions

- POSH <= 3.2.1

Credits

- Anthony BAUBE, Sysdream (a.baube -at- sysdream -dot- com)
- Damien CAUQUIL, Sysdream (d.cauquil -at- sysdream -dot- com)

Contact

- Website: http://www.sysdream.com
- Twitter: @sysdream