Security Advisory SWRX-2014-004

Open Web Analytics Reflected Cross-Site Scripting (XSS)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Open Web Analytics Reflected Cross-Site Scripting (XSS)
Advisory ID: SWRX-2014-004
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-004
Date published: Thursday, February 13, 2014
CVE: CVE-2014-1456
CVSS v2 base score: 5.0
Date of last update: Thursday, February 13, 2014
Vendors contacted: Open Web Analytics
Release mode: Coordinated
Discovered by: Dana James Traversie, Dell SecureWorks

Summary

Open Web Analytics (OWA) is open source web analytics software that can track and analyze how visitors use websites and applications. OWA is vulnerable to a reflected cross-site scripting (XSS) vulnerability due to insufficient input validation of a parameter on the login page. User-controllable input is not properly sanitized before being displayed in dynamically generated web content. Remote attackers could leverage this vulnerability to conduct reflected XSS attacks.

Affected products

This vulnerability affects Open Web Analytics v1.5.5 and v1.5.4. It may affect prior versions.

Vendor information, solutions, and workarounds

The vendor has released an updated version to address this vulnerability. OWA users should upgrade to version v1.5.6 or later.

Details

A reflected XSS vulnerability exists in Open Web Analytics v1.5.5 and v1.5.4 due to insufficient input validation of the 'owa_user_id' parameter on the login page. User-controllable input supplied to the affected parameter is not sanitized for illegal or malicious data before being returned to the user in dynamic web content. Remote attackers could leverage this issue to conduct reflected XSS attacks via specially crafted requests. When loaded, arbitrary script or HTML code injected into the affected parameter is executed in a target user's browser session in the security context of the vulnerable web application. Successful exploitation may allow an attacker to retrieve session information, steal recently submitted data, or launch additional attacks.

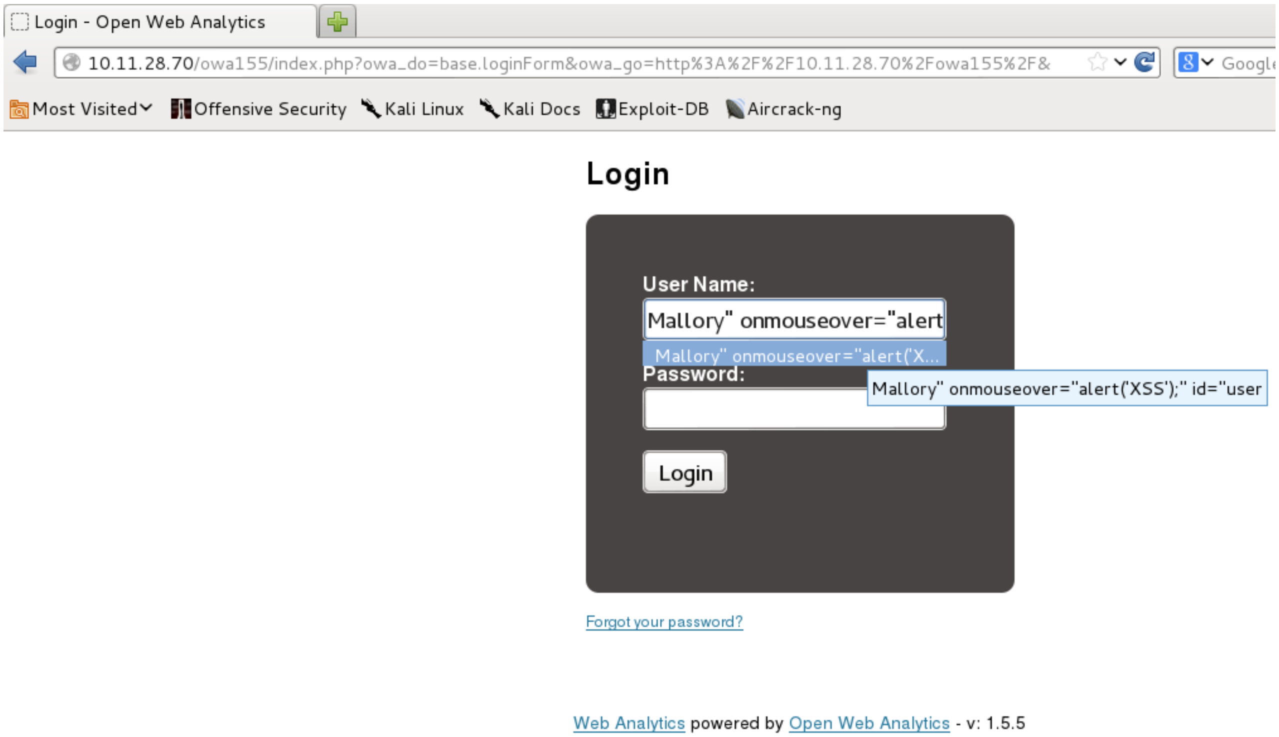
CVSS severity (version 2.0)

Access vector: Network
Access complexity: Low
Authentication: None
Impact type: Allows unauthorized modification
Confidentiality impact: None
Integrity impact: Partial
Availability impact: None
CVSS v2 base score: 5
CVSS v2 impact subscore: 2.9
CVSS v2 exploitability subscore: 10
CVSS v2 vector: (AV:N/AC:L/Au:N/C:N/I:P/A:N)

Proof of concept

The presence of this vulnerability can be confirmed on the OWA login page after entering the following string in the user name text field and clicking the login button (see Figures 1 and 2):

```
Mallory" onmouseover="alert('XSS');" id="user
```



10.11.28.70/owa155/index.php?owa_do=base.loginForm&owa_go=http%3A%2F%2F10.11.28.70%2Fowa155%2F&

Login

User Name: Mallory" onmouseover="alert

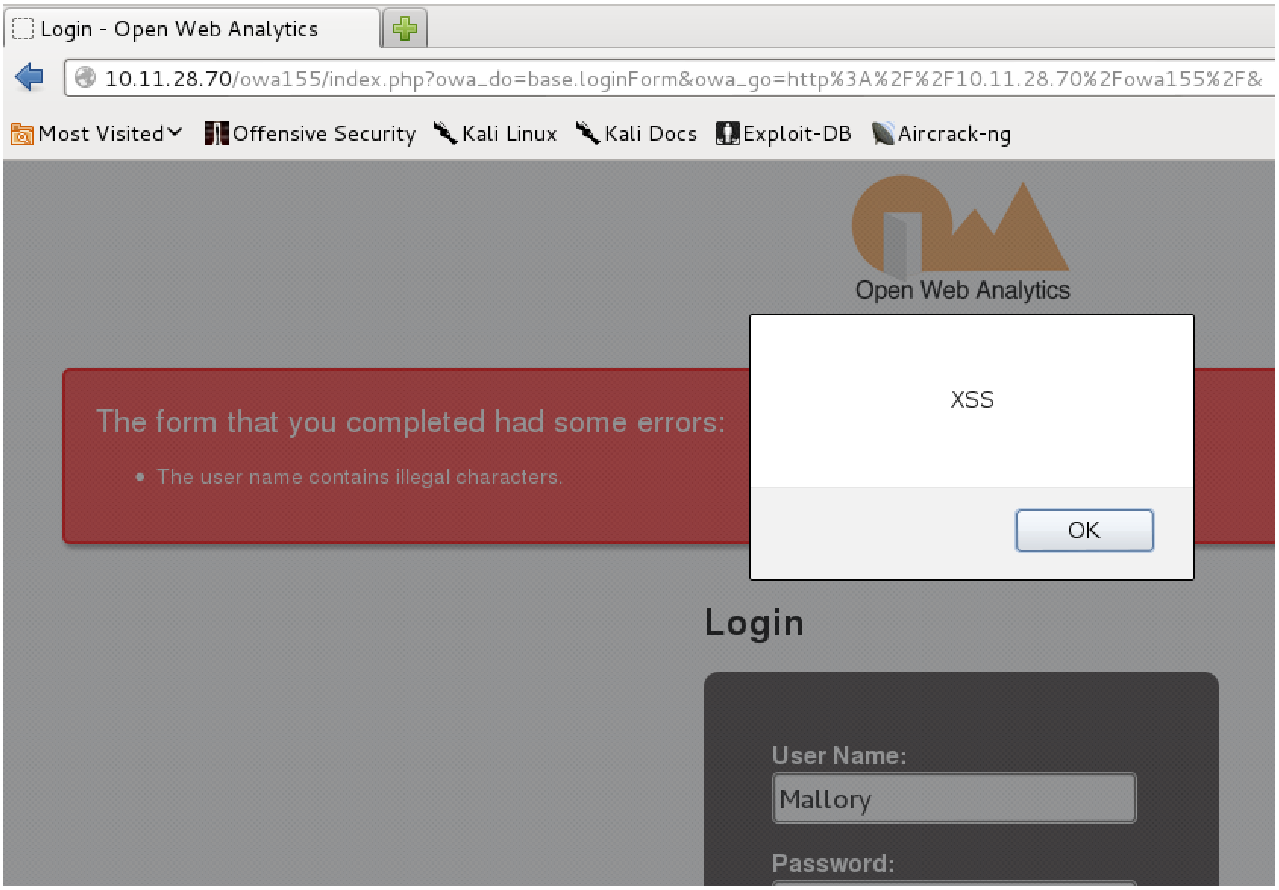
Mallory" onmouseover="alert('X...

Password:

Mallory" onmouseover="alert('XSS');" id="user

Web Analytics powered by Open Web Analytics - v: 1.5.5

Figure 1. Proof-of-concept string displayed on the login page before the login button is clicked. (Source: Dell SecureWorks)



10.11.28.70/owa155/index.php?owa_do=base.loginForm&owa_go=http%3A%2F%2F10.11.28.70%2Fowa155%2F&

The form that you completed had some errors:

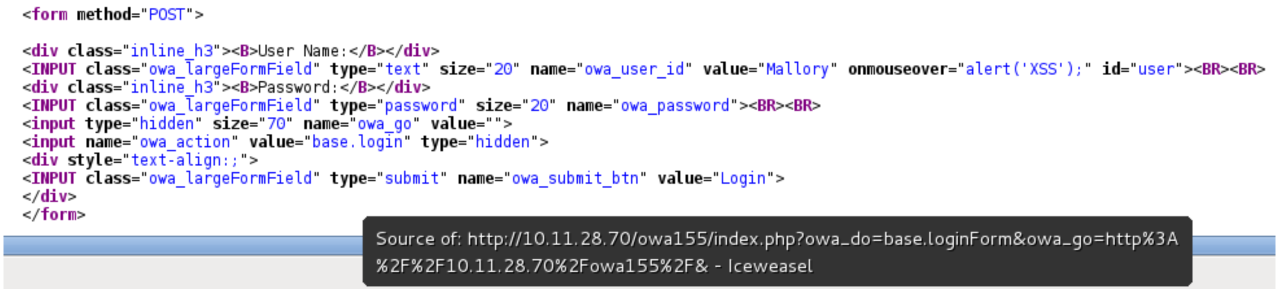
- The user name contains illegal characters.

XSS

Mallory

Figure 2. JavaScript popup displayed after the login button has been clicked and the mouse cursor is over the user name text field. (Source: Dell SecureWorks)

Figure 3 lists the web page source code after the proof-of-concept string has impacted the vulnerable HTML form element on the OWA login page.



```
<form method="POST">

<div class="inline_h3"><B>User Name:</B></div>
<INPUT class="owa_largeFormField" type="text" size="20" name="owa_user_id" value="Mallory" onmouseover="alert('XSS');" id="user"><BR><BR>
<div class="inline_h3"><B>Password:</B></div>
<INPUT class="owa_largeFormField" type="password" size="20" name="owa_password"><BR><BR>
<input type="hidden" size="70" name="owa_go" value="">
<input name="owa_action" value="base.login" type="hidden">
<div style="text-align:;">
<INPUT class="owa_largeFormField" type="submit" name="owa_submit_btn" value="Login">
</div>
</form>
```

Source of: http://10.11.28.70/owa155/index.php?owa_do=base.loginForm&owa_go=http%3A%2F%2F10.11.28.70%2Fowa155%2F& - Iceweasel

Figure 3. The web page source displayed after the login button has been clicked, showing the impact of the proof-of-concept string on the affected HTML form element. (Source: Dell SecureWorks)

Revision history

1.0 2014-02-13: Initial advisory release

PGP keys

This advisory has been signed with the Dell SecureWorks Counter Threat Unit™ PGP key, which is available for download at http://www.secureworks.com/SecureWorksCTU.asc.

About Dell SecureWorks

Dell Inc. listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information and IT security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

Disclaimer

This advisory may not be edited or modified in any way without the express written consent of Dell SecureWorks. Permission is hereby granted to link to this advisory via the Dell SecureWorks website or use in accordance with the fair use doctrine of U.S. copyright laws. See the Dell SecureWorks terms of use at http://www.secureworks.com/contact/terms_of_use/ for additional information.

The most recent version of this advisory may be found on the Dell SecureWorks website at http://www.secureworks.com. The contents of this advisory may change or be removed from the website without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. ANY USE OF THIS INFORMATION IS AT THE USER'S RISK. In no event shall Dell SecureWorks be liable for any damages whatsoever arising out of or in connection with the use or further publication or disclosure of this information.