

Redirection Vulnerability in wp-pass.php, WordPress 2.2.1

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-07/msg00039.html>

- *From:* "Nick S. Coblentz" <ncoblentz@xxxxxxxxxxxxxxxxx>
 - *Date:* Thu, 5 Jul 2007 10:14:20 -0500
-

The vulnerability found could allow an attacker to redirect victims to an arbitrary 3rd party site. This site could be a phishing site or contain malware allowing the attacker to steal account credentials or compromise hosts. This vulnerability can be found in Wordpress 2.2, however it is likely that it exists in previous versions as well.

Additional vulnerabilities may exist in the following areas due to the use of the problematic code:

wp-includes/pluggable.php (lines 282 to 292)
wp-includes/functions.php, wp_nonce_ays function (lines 1287 to 1313)

Description:

The wp-pass.php page can be used to redirect users to arbitrary third party sites. An attacker may use this vulnerability to redirect users to a phishing or malware site.

Relevant Code:

wp-pass.php (line 10)

```
wp_redirect(wp_get_referer());
```

wp-includes/functions.php (line 1040 to 1045)

```
function wp_get_referer() {  
    foreach ( array($_REQUEST['_wp_http_referer'],  
$_SERVER['HTTP_REFERER']) as $ref )  
        if ( !empty($ref) )  
            return $ref;  
    return false;  
}
```

Redirection Vulnerability in wp-pass.php, WordPress 2.2.1

Exploit:

`http://<WordpressSiteAddressHere>/wp-pass.php?_wp_http_referer=http://www.EvilPhishingOrMalwareSite.com`

Since the function uses the `$_REQUEST` variable, this attack could also be executed using a cookie or post parameter named `"_wp_http_referer"`

If this were a real attack, A link would be sent to users in an E-mail, IM, or other delivery message to trick users into visiting the link.

Versions Affected:

This vulnerability is likely present in several previous versions of Wordpress, however it was tested and verified in version 2.2.1

Vendor Response:

The Wordpress team is currently working on addressing this issue and others in the 2.2.2 release of its blogging software.

Disclosure Timeline:

2007-06-21 Discovery by Nick Coblenz of Security PS
(<http://www.securityps.com>)
2007-06-22 Vendor notification
2007-07-02 2nd Vendor notification
2007-07-05 Vendor response

Remediation:

Wordpress 2.2.2 will address this issue as well as others.

Credit:

This vulnerability was discovered by Nicholas Coblenz, a security consultant a Security PS (<http://www.securityps.com>). The vulnerability found could allow an attacker to redirect victims to an arbitrary 3rd party site. This site could be a phishing site or contain malware allowing the attacker to steal account credentials or compromise hosts. This vulnerability can be found in Wordpress 2.2, however it is likely that it exists in previous versions as well.

Additional vulnerabilities may exist in the following areas due to the use of the problematic code:

Redirection Vulnerability in wp-pass.php, WordPress 2.2.1

wp-includes/pluggable.php (lines 282 to 292)

wp-includes/functions.php, wp_nonce_ays function (lines 1287 to 1313)

Description:

The wp-pass.php page can be used to redirect users to arbitrary third party sites. An attacker may use this vulnerability to redirect users to a phishing or malware site.

Relevant Code:

wp-pass.php (line 10)

```
wp_redirect(wp_get_referer());
```

wp-includes/functions.php (line 1040 to 1045)

```
function wp_get_referer() {  
    foreach ( array($_REQUEST['_wp_http_referer'],  
        $_SERVER['HTTP_REFERER']) as $ref )  
        if ( !empty($ref) )  
            return $ref;  
    return false;  
}
```

Exploit:

http://<WordpressSiteAddressHere>/wp-pass.php?_wp_http_referer=http://www.EvilPhishingOrMalwareSite.com

Since the function uses the \$_REQUEST variable, this attack could also be executed using a cookie or post parameter named "_wp_http_referer"

If this were a real attack, A link would be sent to users in an E-mail, IM, or other delivery message to trick users into visiting the link.

Versions Affected:

This vulnerability is likely present in several previous versions of Wordpress, however it was tested and verified in version 2.2.1

Vendor Response:

The Wordpress team is currently working on addressing this issue and others in the 2.2.2 release of its blogging software.

Redirection Vulnerability in wp-pass.php, WordPress 2.2.1

Disclosure Timeline:

2007-06-21 Discovery by Nick Coblenz of Security PS

(<http://www.securityps.com>)

2007-06-22 Vendor notification

2007-07-02 2nd Vendor notification

2007-07-05 Vendor response

Remediation:

Wordpress 2.2.2 will address this issue as well as others.

Credit:

This vulnerability was discovered by Nicholas Coblenz, a security consultant at Security PS (<http://www.securityps.com>).