Published in System Weakness

Mayur Parmar Follow
Aug 30, 2020 · 2 min read · Listen

CVE-2020–24115

Use of hardcoded credentials in source code leads to admin panel access

# Exploit Title: Online Book Store 1.0 — Use of Hard-coded Credentials in source code leads to admin panel access
# Date: 2020–07–22
# Exploit Author: Mayur Parmar(th3cyb3rc0p)
# Vendor Homepage: https://projectworlds.in/free-projects/php-projects/online-book-store-project-in-php/
# Software Link: https://github.com/projectworlds32/online-book-store-project-in-php/archive/master.zip
# Version: 1.0
# Tested on Windows10
# CVE: CVE-2020-24115

Hardcoded Credentials:

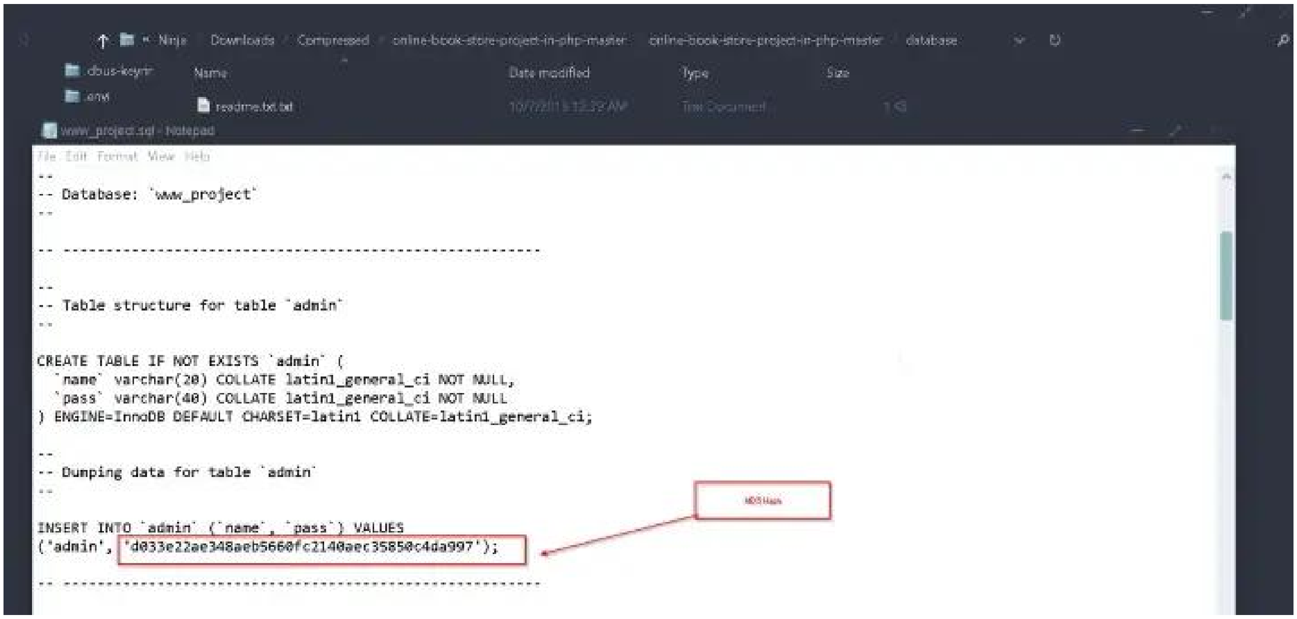
Hardcoded Passwords, also often referred to as Embedded Credentials, are plain text passwords or other secrets in source code. Password hardcoding refers to the practice of embedding plain text (non-encrypted) passwords and other secrets (SSH Keys, DevOps secrets, etc.) into the source code. Default, hardcoded passwords may be used across many of the same devices, applications, systems, which helps simplify set up at scale, but at the same time, poses a considerable cybersecurity risk.

Attack Vector:

An attacker can gain admin panel access using default credentials and do malicious activities.

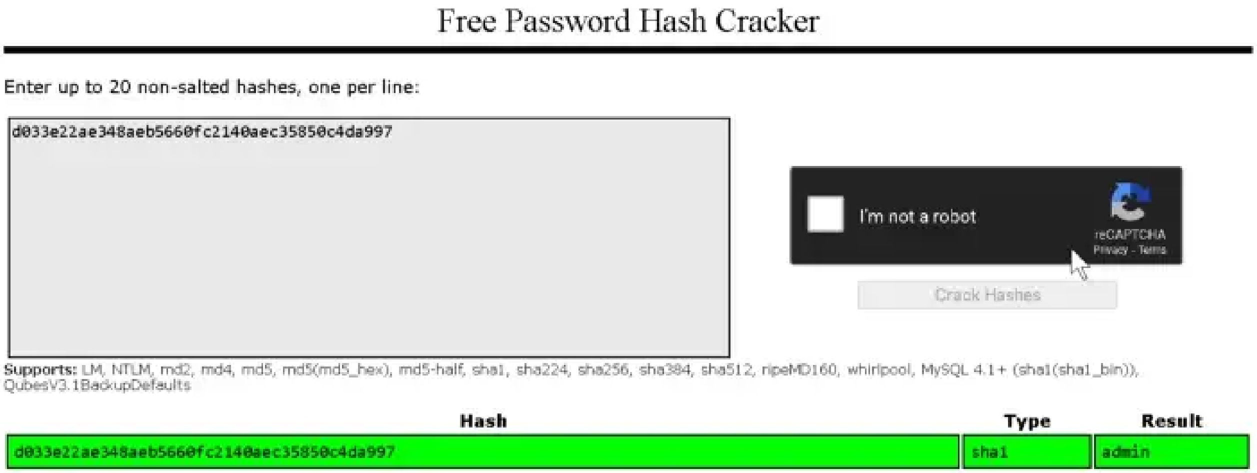
Steps to reproduce:

1. Download source code from https://projectworlds.in/free-projects/php-projects/online-book-store-project-in-php/
2. Now unzip it and goto the **Database** folder here we can see one SQL file.
3. Now open that file using Notepad and there we can see admin credentials. but the password is encrypted .from pattern I identified that this is MD5 hash. so we can easily decrypt using crackstation.net or any hash cracker tools like Hashcat, John the ripper.


Ninja / Downloads / Compressed / online-book-store-project-in-php-master / online-book-store-project-in-php-master / database
dbus-keyrr
.envi
Name
Date modified
Type
Size
readme.txt.txt
www_project.sql - Notepad
File Edit Format View Help
MD5 Hash

```
--
-- 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');

-- --------------------------------------------------------
```

Credentials



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

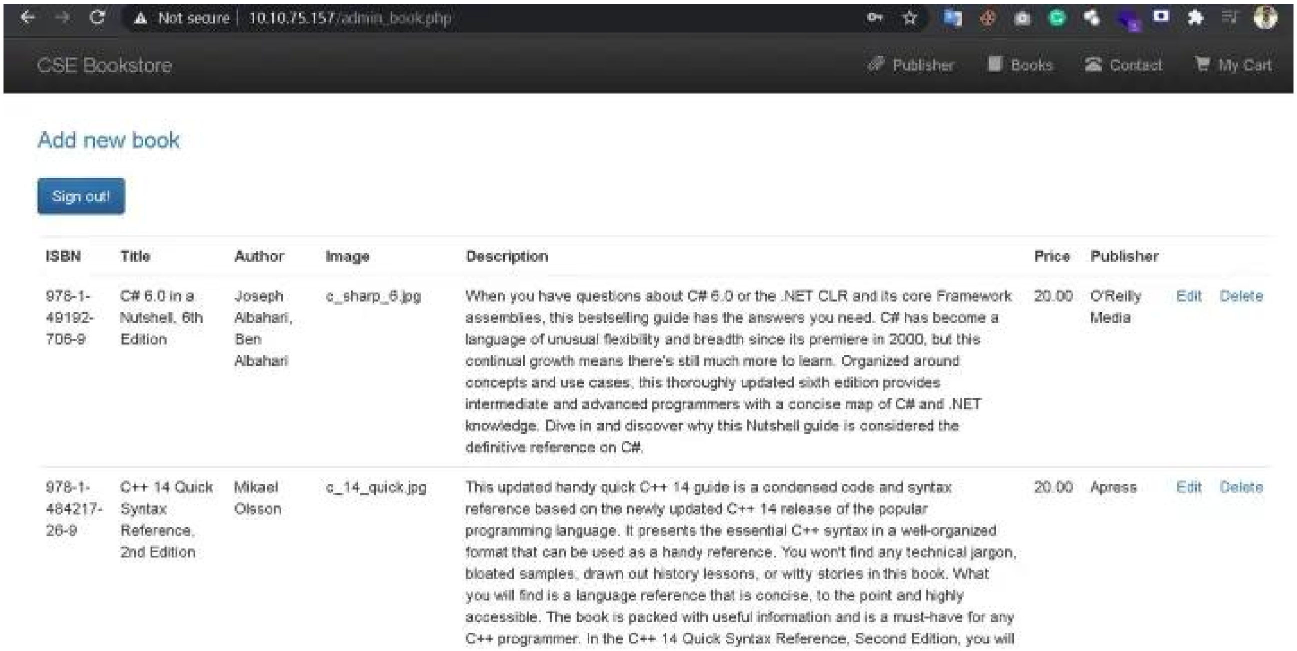
```
d033e22ae348aeb5660fc2140aec35850c4da997
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d033e22ae348aeb5660fc2140aec35850c4da997	sha1	admin

Cracked Credentials

4. Now we have Admin credentials so we can easily log in to the portal.



Add new book

ISBN	Title	Author	Image	Description	Price	Publisher		
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. Organized 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	O'Reilly Media	Edit	Delete
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. You 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. In the C++ 14 Quick Syntax Reference, Second Edition, you will	20.00	Apress	Edit	Delete

Admin Login

Mitigation:

- Always use a strong encryption algorithm like SHA-256 with SALT.
- Never use default credentials always change during installation time

> *Author at: https://systemweakness.com/*

Cve 2020 24115 Ctf Tryhackme Cyber Defecers Infosec