

Network Pentesting

Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

Pentesting Windows Endpoints: Software Based Vulnerabilities

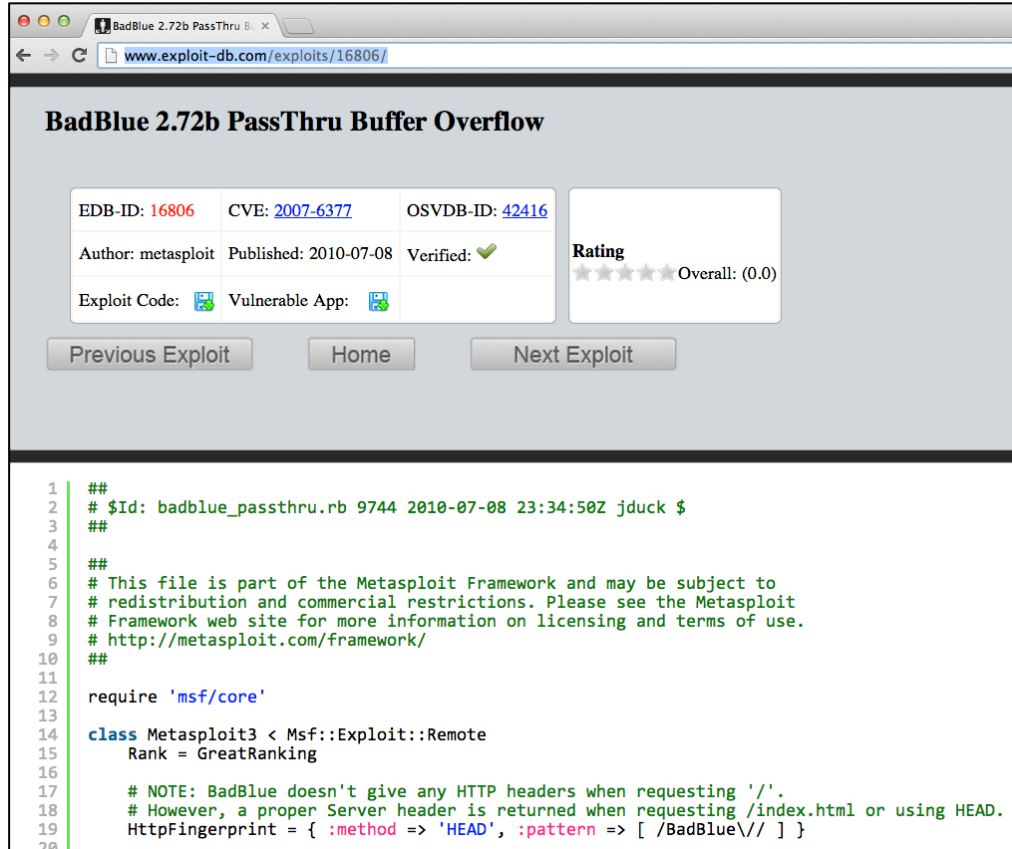
Basics of Vulnerabilities

- Metasploit course on Pentester Academy
- <http://PentesterAcademy.com/topics>

Lab Setup



BadBlue 2.72b



The screenshot shows a web browser window displaying the exploit details for 'BadBlue 2.72b PassThru Buffer Overflow' on the Exploit-DB website. The page includes a header with the exploit title, a metadata table with fields like EDB-ID, CVE, OSVDB-ID, Author, Published, and Verified, and a rating section. Below the metadata are navigation buttons for 'Previous Exploit', 'Home', and 'Next Exploit'. The main content area displays the raw exploit code in a monospaced font, starting with a comment block and a class definition for Metasploit3.

```
1  ##
2  # $Id: badblue_passthru.rb 9744 2010-07-08 23:34:50Z jduck $
3  ##
4
5  ##
6  # This file is part of the Metasploit Framework and may be subject to
7  # redistribution and commercial restrictions. Please see the Metasploit
8  # Framework web site for more information on licensing and terms of use.
9  # http://metasploit.com/framework/
10 ##
11
12 require 'msf/core'
13
14 class Metasploit3 < Msf::Exploit::Remote
15   Rank = GreatRanking
16
17   # NOTE: BadBlue doesn't give any HTTP headers when requesting '/'.
18   # However, a proper Server header is returned when requesting /index.html or using HEAD.
19   HttpFingerprint = { :method => 'HEAD', :pattern => [ /BadBlue\/ ] }
20
```

<http://www.exploit-db.com/exploits/16806/>

Penetrating Systems

- Software Bugs
 - Core Windows
 - 3rd Party
- Software Misconfiguration
- Social Engineering

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



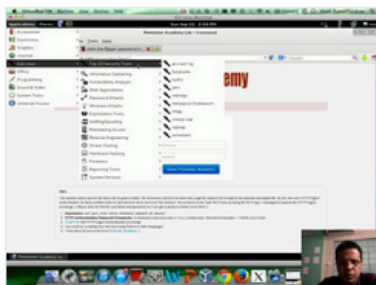
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Start Learning Today!

Latest Videos

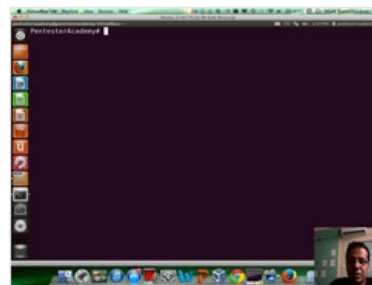
New content added weekly!



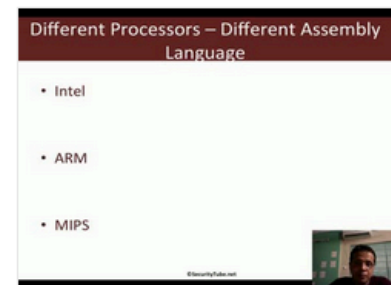
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux