Official Pwning Guide



Special CTF Edition

Visit hxp.io for more information!

This document was created for HXP CTF 2017...

Contents

1	Introduction	3
2	PDF	5

1 Introduction

Let someone else explain what this is about:

Capture the Flag (CTF) is a special kind of information security competitions. There are three common types of CTFs: Jeopardy, Attack-Defence and mixed.

Jeopardy-style CTFs has a couple of questions (tasks) in range of categories. For example, Web, Forensic, Crypto, Binary or something else. Team can gain some points for every solved task. More points for more complicated tasks usually. The next task in chain can be opened only after some team solve previous task. Then the game time is over sum of points shows you a CTF winer. Famous example of such CTF is Defcon CTF quals.

Well, attack-defence is another interesting kind of competitions. Here every team has own network(or only one host) with vulnarable services. Your team has time for patching your services and developing exploits usually. So, then organizers connects participants of competition and the wargame starts! You should protect own services for defence points and hack opponents for attack points. Historically this is a first type of CTFs, everybody knows about DEF CON CTF - something like a World Cup of all other competitions.

Mixed competitions may vary possible formats. It may be something like wargame with special time for task-based elements (like UCSB iCTF).

CTF games often touch on many other aspects of information security: cryptography, stego, binary analysis, reverse engeneering, mobile security and others. Good teams generally have strong skills and experience in all these issues.

- CTFTime.org

Okay, so apparently this is somehow about security challenges and flags. For this CTF you should be looking for some textual string like this:

hxp{this_is_not_the_flag}

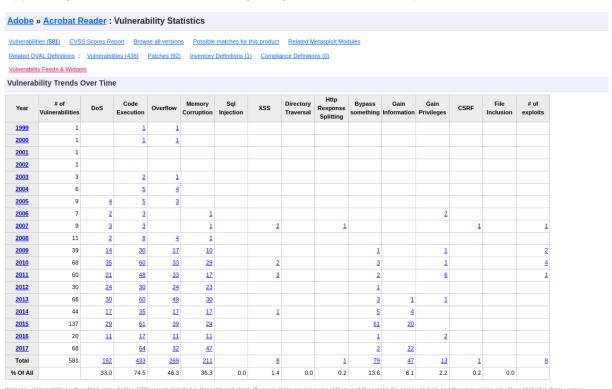
So let's get started!

2 PDF

PDF is a file-format invented by Adobe Inc. It offers unlimited possibilities to you! If you like it boring you can write a document with text and images and save it as PDF so others can read (as I do right now) it.

If belong to the cool people, you can use it to store your files in it, share your thoughts with your friends by adding annotations (did you know that they even support audio?).

Apparently the format is not that easy, they still seem to have problems with their Reader:



Just thought that this challenge is about Binary Exploitation? It isn't ;-) Just find the flag. Maybe this is of some help for you: PDF 1.7 Spec