Official Pwning Guide

Special CTF Edition

Visit `hxp.io` for more information!

This document was created for HXP CTF 2017...

it may contain cool stuff
and maybe a flag!

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:

Adobe » Acrobat Reader : Vulnerability Statistics

Vulnerabilities (581) CVSS Scores Report Browse all versions Possible matches for this product Related Metasploit Modules

Related OVAL Definitions : Vulnerabilities (438) Patches (92) Inventory Definitions (1) Compliance Definitions (0)

Vulnerability Feeds & Widgets

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	1		1	1											
2000	1		1	1											
2001	1														
2002	1														
2003	3		2	1											
2004	6		5	4											
2005	9	4	5	3											
2006	7	2	3		1							2			
2007	9	3	3		1		2		1				1		1
2008	11	2	8	4	1										
2009	39	14	30	17	10					1		1			2
2010	68	35	60	33	29		2			3		1			4
2011	60	21	48	33	17		3			2		6			1
2012	30	24	30	24	23					1					
2013	66	30	60	49	30					3	1	1			
2014	44	17	35	17	17		1			5	4				
2015	137	29	61	39	24					61	20				
2016	20	11	17	11	11					1		2			
2017	68		64	32	47					2	22				
Total	581	192	433	269	211		8		1	79	47	13	1		8
% Of All		33.0	74.5	46.3	36.3	0.0	1.4	0.0	0.2	13.6	8.1	2.2	0.2	0.0	

Warning : Vulnerabilities with publish dates before 1999 are not included in this table and chart. (Because there are not many of them and they make the page look bad; and they may not be actually published in those years.)

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