



HACK WORDPRESS



# Contents

- 1 Introduction
- 2 Mandatory part
- 3 Bonus part

# Chapter 1

## Introduction

The project is there to make you learn how a attack is prepared and thought.

You will have to be creative, methodologic, strategic & having a clarity of mind. What we ask of you is very simple, but can be tricky without the right tools. That's right you'll need to combine different kind of knowledges to find the best way to gain access to the wordpress website.

# Chapter 2

## Mandatory part

You need to fully retrieve everything on this website, code, database, contents..

<https://leetsec-c1f98d.ingress-bonde.ewp.live/>

(or the one above is down, use this one : <http://34.106.189.163/> (NO SSL))

You should be able to clone it to another server and retrieve information inside, like a secret page hidden somewhere...

This website is running on wordpress engine, by aware.

Find a way to get access to the any user account. (to the real website or clone, as long as they are the same)

To prove that you hacked it, find the secret text code in a secret page on the wordpress website

Git push the secret code into a file "secret.txt" in this folder :

<https://github.com/leetsec/phase1/wordpress-hack/{your login}/>



Tips:

Most backup wordpress plugin store theirs non-encrypted backups in the http server

Reminder: A script kiddie needs to know how to use google if you have any questions. If you're stuck, talk to other member of the club inside the discord at "INFOSEC > web-security" channel.

