WELCOME TO CLASS 2!

BLACK HAT PYTHON3

RALEIGH ISSA

LOGISTICS

- Web class Wednesdays 7:00 - 8:30 EDT
- Discord Channel to help each other https://discord.gg/WR23qUj
- Discord Office Hour Monday, 7:00 - 8:00
- Direct message on Discord or email: tim@reachtim.com
- GitHub Repo of class materials/updated code https://github.com/tiarno/bhp3_class

RECORDING FROM LAST CLASS

https://www.dropbox.com/s/a0sx0k69siy10ia/2018-07-18%2019.00%20Raleigh%20ISSA%20-%20Blackhat%20Python%20Class%201.mp4?dl=0

UPDATE

Make sure your repo is up to date on commits and push to github.

Then:

```
git remote add upstream https://github.com/tiarno/bhp3_class.g
git fetch upstream
git checkout master
git merge upstream/master
git add -A .
git commit -m "merged upstream changes"
git push
```

PREVIOUSLY

- `os.walk`
- lists, queues, deques
- threading

LET'S CODE!

- Target website uses a popular framework.
- enumerate that website for further attacks.

enumeration with mapper.py

Demo

HTTP STATUS CODES

https://www.restapitutorial.com/httpstatuscodes.html

LET'S CODE!

- Target website uses an unknown architecture.
- enumerate that website for further attacks.

TARGET

http://testphp.vulnweb.com/disclaimer.php

ONLINE WORDLISTS

https://github.com/DanMcInerney/Probable-Wordlists

https://github.com/danielmiessler/SecLists

(Discovery/Web-Content/SVNDigger)

KALI WORDLISTS

Demo

Activity

```
user@kali:/usr/share/wordlists
```

enumeration with dirfinder.py

Demo

try/except/else/finally

```
try:
  something that might cause an error
except SomeError as e:
  print(e)
  dosomething()
else:
  everything_is_fine()
finally:
  cleanup()
```

LET'S CODE!

- Target website is WordPress.
- Brute force the login page.

BytesIO

https://webkul.com/blog/using-io-for-creating-file-object/

BROWSER DEV TOOLS

Demo

Activity

http://boodelyboo.com/wordpress

lxml MODULE AND XPATH

```
parser = etree.HTMLParser()
tree = etree.parse(BytesIO(content), parser=parser)
for elem in tree.findall('//input'):
    # do stuff with elem
```

wp_killer.py

Demo

SUMMARY

- mapping an app
- word lists for enumeration
- word lists for password bruteforce
- browser tools
- `lxml` for web parsing

READING 1

- BHP, Chapter 5 (web hacking)
- GitHub Repo: https://github.com/tiarno/bhp3_class
- PEP-8: https://www.datacamp.com/community/tutorials/pep
tutorial-python-code

READING 2

- Requests http://docs.python-requests.org/en/master/
- Threading: https://docs.python.org/3.6/library/threading.html
- `BytesIO` https://webkul.com/blog/using-io-for-creating-file-object/

YOUR JOB

- populate your `bhp3_class/web` module
  - mapper.py
  - dirfinder.py
- Can you create a function to return words from a word list? That would let us simplify the dirfinder/wp_killer code.

PICK YOUR APP

https://www.makeuseof.com/tag/10-popular-content-management-systems-online/