

A laptop screen is shown in a dark, dimly lit environment. The screen displays a line graph with a blue line and a globe. The text is overlaid on the screen.

# Using a Dating Site as a Botnet Command and Control Server

Presented By Nathaniel 'We Can Do It In Python' Beckstead

# \$whoami



- ❑ Third year CSEC major
- ❑ Interests
  - ❑ Blue team
  - ❑ Automation
  - ❑ Collecting data and never using it
- ❑ Hobbies
  - ❑ Cooking
  - ❑ Hiking
  - ❑ Homelab
- ❑ Find me
  - ❑ Github - [becksteadn](#)
  - ❑ Blog - [scriptingis.life](#)





# The Website

[wordsofheart.com](https://wordsofheart.com)





# The Website

Went around Twitter  
on Valentine's Day.

Gained traction from  
a Motherboard  
article.



# FIND AND DATE PEOPLE WHO HAVE THE SAME PASSWORD

We believe that something as intimate as your password best describes your inner self.

LOGIN

REGISTER

DO NOT USE your real password here, especially a password for something important (banks, e-mail, Facebook)!



# REGISTER

**PHOTO (REQUIRED)**

If you want your potential dates to be able to contact you, provide at least one of the following:

**REGISTER**

# WE FOUND SOME MATCHES FOR YOU!



**tomek1**

Unfortunately, that user didn't leave any contact detail. You may be out of luck today.



**Kotesiek**

Unfortunately, that user didn't leave any contact detail. You may be out of luck today.



**kkkkkk**

Unfortunately, that user didn't leave any contact detail. You may be out of luck today.



**1@user.com**

Unfortunately, that user didn't leave any contact detail. You may be out of luck today.



**llakksl**

Unfortunately, that user didn't leave any contact detail. You may be out of luck today.



**daniel123**

Unfortunately, that user didn't leave any contact detail. You may be out of luck today.

# LEAVE A MESSAGE

Messages will be visible for everyone with the same password.

ADD

Suck a dick 8===D

rm -rf /

,

drop table comments.

omg u guys the message interface looks sooooo  
much nicer now  
WOOOwwwoOOoOOwWeeeEeee!!!

so no one here is actually legit



# Hmmmm

---

Only people with the same password can see profiles and comments.

Using a long complex password could result in a secret chat room.



# Automating Websites with Python

---

1. Record requests with a proxy
2. Translate to Python ``requests`` module
3. Get information using Beautiful Soup



# Demo



# Record Requests

---

#	Host	Method	URL	Params	Edited	Status
1	https://wordsofheart.com	GET	/			200
2	https://wordsofheart.com	GET	/user/register/			200
3	https://wordsofheart.com	POST	/user/register/	✓		302
4	https://wordsofheart.com	GET	/static/css/bootstrap.min.css.map			404
5	https://wordsofheart.com	GET	/user/find-matches/			200

---

# Record Requests

---

```
POST /user/login/ HTTP/1.1
Host: wordsofheart.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://wordsofheart.com/user/login/
Content-Type: application/x-www-form-urlencoded
Content-Length: 123
Cookie: _ga=GAL.2.654333245.1517934319; csrftoken=sst61CYL9JrvglBAvR49I7Czp25Ny2tLY0AbzSN05zqgeLy0NwcfJnR0v61aVNJB; _gid=GAL.2.823056923.1536852137; sessionId=u73p1058emhrx79a55ar3xs7lodepqeb;
_gat_gtag_UA_113220308_1=1
Connection: close
Upgrade-Insecure-Requests: 1
DNT: 1
```

```
csrfmiddlewaretoken=sH5XN9Ui28kZ01SNCuEpIGsGULZNscoAY3c2lpJVYjKYrPdUSMvLAH70PVaPOEq&username=sparsa_bot&password=sparsal23
```

```
VaPOEq&username=sparsa_bot&password=sparsal23
```

---



# Translate to Python

```
def user_register(name, passwd, email, twitter, facebook):  
    s = requests.Session()  
    s.headers = init_headers  
    s.proxies = {'http' : 'localhost:8080', 'https' : 'localhost:8080'} # Test with Burp Suite for now  
  
    r = s.get("https://wordsofheart.com/user/register/", verify=False)  
  
    # Craft POST information  
    register_files = { 'photo' : ('bot.jpg', open('bot.jpg', 'rb'), 'image/jpeg') }  
    register_data = {  
        "username" : name,  
        "password" : passwd,  
        # "photo" : "???????",  
        "email" : email,  
        "twitter" : twitter,  
        "facebook" : facebook  
    }  
    s.headers['Referer'] = "https://wordsofheart.com/user/register/"  
  
    r = s.post("https://wordsofheart.com/user/register/", data=register_data, files=register_files, verify=False)  
  
    # Go to 'homepage'  
    r = s.get("https://wordsofheart.com/user/find-matches/", verify=False)  
    save_page(r, register_matches.html )
```

# Find Content in Web Pages

— — —

```
▼ <div class="comment">
  gAAAAABbm-aGI-DoDggn4TYyCStsJGm8MsCGgcRUZZsF2HAcVk_SJ-
  OMZacJnCWds0DQdaVK5y6Bxyfn5aB3fTLIGti4sfZcKJBySck3EN8owl
</div>
▼ <div class="comment">
  gAAAAABbm-ZxIhmG-mAufwMt0ZuQxym8Ls_5PVEN651up3h1J6u5JMDa
  n1T6PBdVFevNcPBCqAEWSt4Q44vHgEnCvGkuKvotnHLnQpamHvdsCU=
</div>
▼ <div class="comment">
  gAAAAABbmun6hSDLzErxfAuWpFSnV0BrxdYdeFeq5BCB1hRgvkp-jMNM
</div>
▼ <div class="comment">
  gAAAAABbmoVfVgSnVbuIAZtiz9JyAqNI7QhaKm80qATvFxfZTGkSnemr
</div>
▼ <div class="comment">
  Shhh this is secret.
</div>
```

---

# Find Content in Web Pages

```
def read_messages(session_obj):
    s = session_obj
    r = s.get("https://wordsofheart.com/user/find-matches/")
    soup = BeautifulSoup(r.text, 'lxml')
    comments = soup.findAll("div", {"class" : "comment"})
    with open("data/comments.txt", "w") as f:
        for cmt in comments:
            new_cmt = cmt.text.strip()
            try:
                print(decrypt_message(new_cmt))
            except:
                print("[*] Couldn't decrypt: {}".format(new_cmt))
            f.write(new_cmt + "\n")
```

# Find Content in Web Pages

---

```
Getting fresh login page: 200
[*] Logged in, got matches.
[*] Messages:
echo "Second cmd"
echo "Hello world"
nc -nvlp 80
nc -nvlp 80
[*] Couldn't decrypt: Shhh this is secret.
```

---

# The Problems

---

- ❑ Relies on a single domain.
- ❑ Users (bots) need to be registered and are visible to everyone else.
- ❑ A whole lot else.





# Questions