

Jennings Zhang <jenni_zh@protonmail.com>

May 1, 2019

Wootton Cybersecurity Club

“Weird Flex but OK”



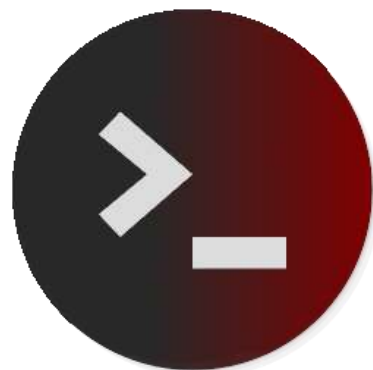
**Northeastern
University**

Computer Science/Biology



**Boston
Children's
Hospital**

Fetal-Neonatal
Neuroimaging and
Developmental Science
Center



2017

whoami

Impressed with your CTF results Inbox x



Thomas, Graham <G s@intuit.com>

to zhang.jenn+intuit@husky.neu.edu ▾

Thu, Mar 21, 10:28 AM



Hey Jenn,

Woke up this morning to find that someone absolutely demolished the ctf. Let me know if you want any help getting further.

Also, send me your resume and I'll forward it to my director if you want.

Graham Thomas | Software Engineer
INTUIT | simplify the business of life™



Jennings Zhang

Dear Thomas, Thank you for reaching out!

Thu, Mar 21, 11:36 AM



Thomas, Graham <G @intuit.com>

to me ▾

Thu, Mar 21, 12:06 PM



Hey Jennings,

Password managers and random string passwords are good practices! Here is your temp password: . Let me know if it works for you.

Also regarding cyber-security majors, most people on our team are either dropouts or have degrees that are completely irrelevant to the job. Cyber Security majors are just starting to pop up after all. Are you interested in working at Intuit in San Diego after college? If you are, when do you expect to graduate?

This url: <https://tango.intuit.com/googlece514814f4ad94c9.html> is actually the answer to "What does the blog say?". I should probably change the name to make that less confusing... Sorry

This URL <https://tango.intuit.com/j/> alludes to the last part of the CTF. I didn't expect any students to get there; it's definitely another caliber from the other challenges.

I'll forward your resume onto my director. Also, there is a slack channel on the home page of the CTF if you want to join to ask me questions on something other than through email. No one else is on it though lol...

Good luck!



npm test

- What is XSS?



xsser -h

We're in, boys

```
element.innerHTML = input; // BAD  
element.innerText = input; // OK
```

Advice:

- Keep dependencies up to date
- Never trust user input
- Don't push passwords to Github...



BuHub | Devpost

https://devpost.com/software/buhub

Hackathons For organizations

BuHub

BU students have trouble understanding graduation requirement. We

Like 1

STORY UPDATES

BuHub

Project Name: BU Hub Calculator

Link to our project: <http://3.16.111.249:8000/>

Input your major and AP credits to receive a selection which will fulfill remaining hub credits

File Edit View Search Terminal Help

```

auth_user_groups      django_content_type
auth_user_permissions django_migrations
courses_actuallhubcourse django_session
courses_apclasses
sqlite> SELECT * FROM auth_user;
1|pbkdf2_sha256$100000$0m6xchVwglVX$31r2FmavBgoVhYkNj4m7veaTurgcfUj38prl3Wxa5r0=|2019-01-27 02:55:41.655860|1|jinglin|jinglin@mit.edu|1|2019-01-27 02:55:26.225953|
sqlite> SELECT * FROM django_session;
7rh9qji0ib3b77gixd7tg1zy5ka240uc|NDUxMzQ1MmUxNTkwMzd1M2MyZmMwZWFL0GRjMmFiNTg1ZmY5NzM4ZTp7I19hdXR0X3VZXXJfawQioiIXIiw1X2F1dGhfdXNlc19iYWNRZW5kIjo1ZGphbmdvLmNvbnRyaWIuYXV0aC5iYWNRZW5kcy5Nb2RlY2t1bmQ1LCJfYXV0aF91c2VyX2hhc2giOiIzOGES5MmQ1MTk00WZjM2U4ZWE0MTYyMzIzYmI2ZmQ1NWFiYmI3NzM4In0=|2019-02-10 02:55:41.659026
sqlite>

```

Select ap classes to change

Django administration

WELCOME, FEDORA. [VIEW SITE](#) / [CHANGE PASSWORD](#) / [LOG OUT](#)

Home · Courses · Ap classes

The ap classes "APClasses object (42)" was changed successfully.

Select ap classes to change

ADD AP CLASSES +

Action: Go

0 of 41 selected

| <input type="checkbox"/> | EXAMINATION | SCORE | COURSE_EQUIVALENT | BU_HUB_AREA |
|-------------------------------------|--------------------------------|-------|--|-------------|
| <input checked="" type="checkbox"/> | Don't push passwords to Github | 4,5 | Nani the fudge did you just fudging iimasu about watashi, you ch | |
| <input checked="" type="checkbox"/> | United States History | 4,5 | HI-099 | |
| <input type="checkbox"/> | Statistics | 4,5 | MA-115 | QR II |
| <input checked="" type="checkbox"/> | Spanish Literature and Culture | 5 | LS-212,LS-307 | GCIL |
| <input type="checkbox"/> | | | | GCIL |
| <input type="checkbox"/> | | | | GCIL |

BuHub/settings.py at mas

GitHub, Inc. [US] https://github.com/moderatelyfunctional/BuHub/blob/master/buhub/buhu...

```

19 # Quick-start development settings - unsuitable for production
20 # See https://docs.djangoproject.com/en/2.0/howto/deployment/checklist/
21
22 # SECURITY WARNING: keep the secret key used in production secret!
23 SECRET_KEY = 'i-uu898lt4u+l4sc7wl)*668@-osvs!47+9sp070z%u@334#2z'
24
25 # SECURITY WARNING: don't run with debug turned on in production!
26 DEBUG = True
27
28 ALLOWED_HOSTS = ['ec2-3-16-111-249.us-east-2.compute.amazonaws.com', '127.0.0.1']
29
30

```

3.16.111.249:8000

AP classes you've taken

| | | |
|------------------------------------|-----|--|
| BC | 4,5 | MA-123+MA-124 |
| ry | 4,5 | CH131,CH171 |
| Language and Culture | 5 | LC212 |
| er Science A | 4,5 | CS-111 |
| er Science Principles | 4,5 | CS-101 |
| ush passwords to Github | 4,5 | Nani the fudge did you just fudging iimasu about watashi, you ch |
| ics: Macro | 4,5 | EC-102 |
| Economics: Micro | 4,5 | EC-101 |
| English Literature and Composition | 4,5 | EN-100,HU-101,HU-102,HU-103,WR-099 |
| Environmental Science | 4,5 | ES-107 |
| European History | 4,5 | HI-098 |

Next



```
journalctl -r -u sshd -u sshguard -n 300
```



Thamsk - jenni_zh@protonmail.com

Questions? Ask me anything!