Team: BUILDS

Who we are

- John-Nicholas Furst
- Allan Wirth
- Jeff Crowell
- Danny Cooper
- Andrew Mohn

Defense

- Read the install.sh
- Change default passwords
- Firewall -- It is your friend
- Read the logs
- Chroot
-

Directory Traversal on CafePress

- Noticed that CafePress wasn't sanitizing input properly, and created a file in a subdirectory below the .py file based on input.

- Specifically, the name of the file uploaded wasn't being cleaned well-- if we urlencoded our "../../../" it would get past the filter, and be decoded before opening

    -%2E%2E%2F !!!

Directory Traversal (contd.)

-This is good, but then we noticed something better!

-If we traverse up to somewhere we don't have access to, it crashes and takes us to a debug page

-Python shell for debugging enabled by default in flask!

Directory Traversal (other)

-Since we found this, we didn't need to try to do other interesting things, like overwrite files directly, but it would have been trivial to do so

-Overwrite database file to kill integrity, overwrite cafepress.py to have a backdoor (requires them to restart, but this happens)

Woot

- Admin=true
- Refresh your page
- PII!

MONp42FgntZBF28q1Y5d

MONp42FgntZBF28q1Y5d

- Monocle default credentials
- MySQL open on 3306.....
- select * from wordpress.wp_users;
- MONp42FgntZBF28q1Y5d
- Admin reset key!!!!!
- http://team12.ctf.csail.mit.edu/wp-login.php?action=rp&key=MONp42FgntZBF28q1Y5d&login=admin
- Howdy Admin

What to do with WP Admin

- Reset admin email
- Everyone can register
- All registrations are admin :)
- Disable plugins
- Edit themes
  - Add reverse shells
  - Add fork bombs
- When all else fails
  - Delete needed files

Come hangout with us

We have a space...

We love talking about security

We play in a lot of CTF's

We love beer