

# Boofuzz

Unknown macro: 'html'

Excuse the ads! We need some help to keep our site up.

Unknown macro: 'html'

## List

- [Boofuzz](#)
  - [Install](#)
  - [API](#)
- [Example](#)
  - [Install vsftpd.](#)
  - [Run fuzz](#)
    - [Source code](#)
    - [Run](#)
    - [Web](#)
- [Related site](#)

## Boofuzz

- **Boofuzz Network Protocol Fuzzing framework .**
- **Boofuzz Sully fuzzing framework .**
- **Boofuzz Sully .**
  - 
  - -
  - 
  -
- **Boofuzz Sully .**
  - 
  - 
  - , IP , UDP
  - .
  - CSV .
  -

## Install

Command

pip install boofuzz

 **Install**

- <http://boofuzz.readthedocs.io/en/latest/index.html#installation>

## API

- <http://boofuzz.readthedocs.io/en/latest/index.html#api-documentation>

## Example

### Install vsftpd.

Command

sudo apt-get install vsftpd

## Run fuzz

### Source code

<https://raw.githubusercontent.com/jtpereyda/boofuzz-ftp/master/ftp.py>

```
#!/usr/bin/env python
# Designed for use with boofuzz v0.0.1-dev3
from boofuzz import *

def main():
    session = Session(
        target=Target(
            connection=SocketConnection("127.0.0.1", 21, proto='tcp'))

    s_initialize("user")
    s_string("USER")
    s_delim(" ")
    s_string("anonymous")
    s_static("\r\n")

    s_initialize("pass")
    s_string("PASS")
    s_delim(" ")
    s_string("james")
    s_static("\r\n")

    s_initialize("stor")
    s_string("STOR")
    s_delim(" ")
    s_string("AAAA")
    s_static("\r\n")

    s_initialize("retr")
    s_string("RETR")
    s_delim(" ")
    s_string("AAAA")
    s_static("\r\n")

    session.connect(s_get("user"))
    session.connect(s_get("user"), s_get("pass"))
    session.connect(s_get("pass"), s_get("stor"))
    session.connect(s_get("pass"), s_get("retr"))

    session.fuzz()

if __name__ == "__main__":
    main()
```

### Run

#### Command

```
python ftp.py > fuzz-logs.txt
```

### Web

<http://127.0.0.1:26000/>

boofuzz Fuzz Control

Pause

Total: 863 of 11,716 [==

user: 863 of 2,929 [=====

7.366%

29.464%

Test Case #

Crash Synopsis

Captured Bytes



- <https://github.com/jtpereyda/boofuzz-ftp>
- <https://github.com/jtpereyda/boofuzz-http>

## Related site

- <http://boofuzz.readthedocs.io/en/latest/>



Unknown macro: 'html'