

Write Up COMPFEST 11

Artillery



Rexy Fahrezi
Gayu Gumelar

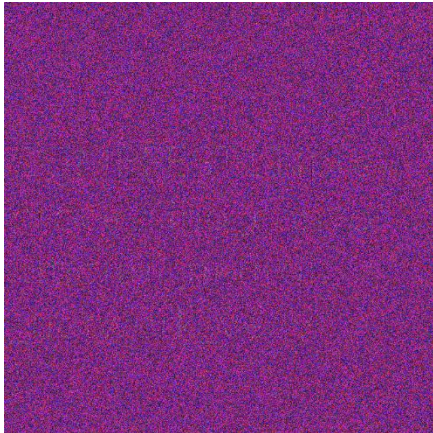
Universitas Teknokrat Indonesia

Forensic

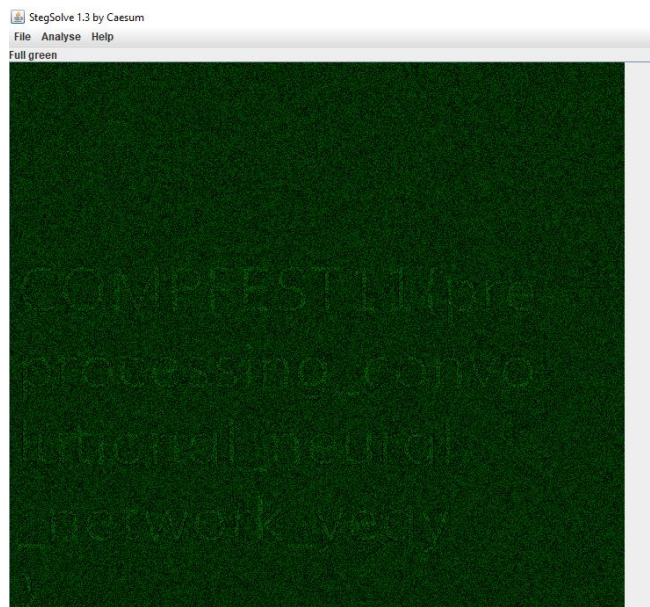
Cable News Network

Cara Pengerjaan

Diberikan sebuah file image



Lakukan analisis dengan Stegsolve,



Flag

COMPFEST11{preprocessing_convolutional_neural_network_yeay}

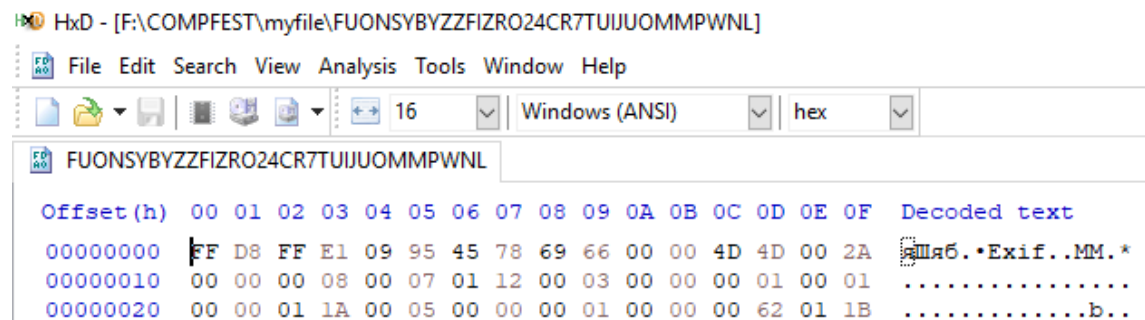
File Separation

Cara Pengerjaan

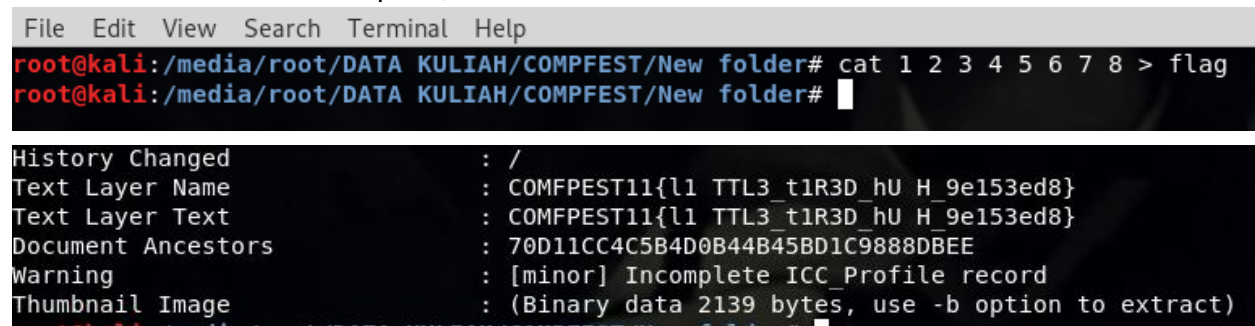
Diberikan file zip, lakukan extract

📁 _MACOSX	27/06/2019 10:13	File folder	
📄 5TJKUQMMHVSH6N26OVGYSEML7MR7X...	27/06/2019 10:11	File	119 KB
📄 7UEIMXOSXHB7QMAK7ESUJFZ6W4S73L2Y	27/06/2019 10:11	File	119 KB
📄 FUONSYBYZZFIZRO24CR7TUIJUOMMPW...	27/06/2019 10:11	File	119 KB
📄 L6MX2CYFKDEYXEZ5QWHHM4Q57H6W...	27/06/2019 10:11	File	119 KB
📄 LVF5LK4BNHVW2K5DBT4J7KIQJD4MQDQH	27/06/2019 10:11	File	119 KB
📄 MXXRYR7KVHCQYQCCPTC4YTTZI4CVR...	27/06/2019 10:11	File	119 KB
📁 myfile.zip	03/08/2019 15:14	WinRAR ZIP archive	734 KB
📄 O2KA5QQJO7SADZKP3REYQADUB7MR3...	27/06/2019 10:11	File	119 KB
📄 YUAE3MNDTWG67BGF4BKXLF2XNXW...	27/06/2019 10:11	File	119 KB

Analisis dengan hex editor



Dan mendapatkan clue exif yang berarti ini file image, yang di pecah kedalam beberapa bagian. Kami rename dari file 1 sampai 8, kemudian kami cat dan exiftool



Flag

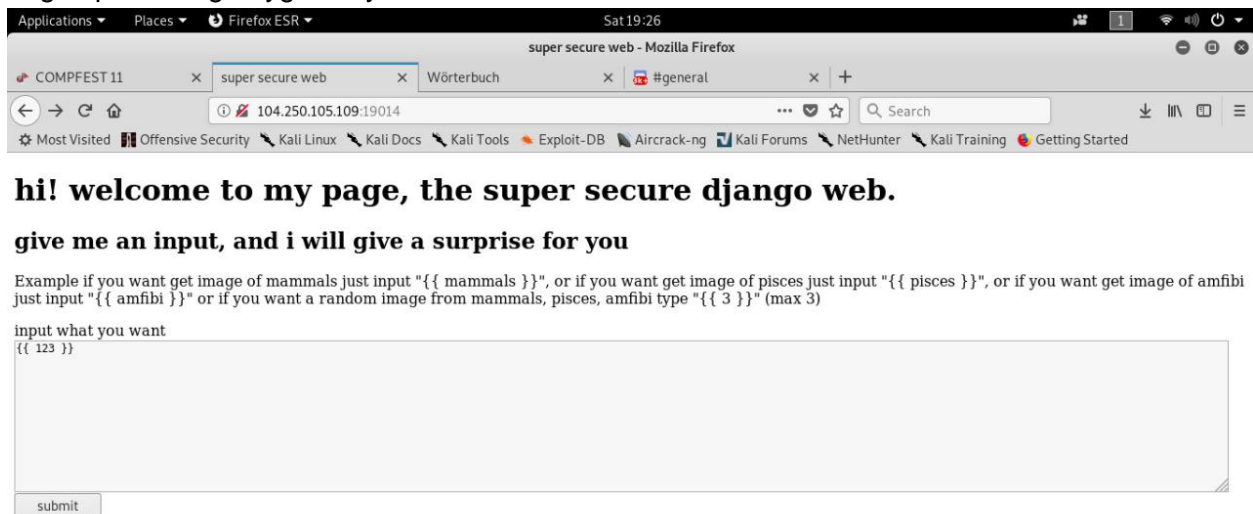
COMFPEST11{l1TTL3_t1R3D_hUH_9e153ed8}

Web

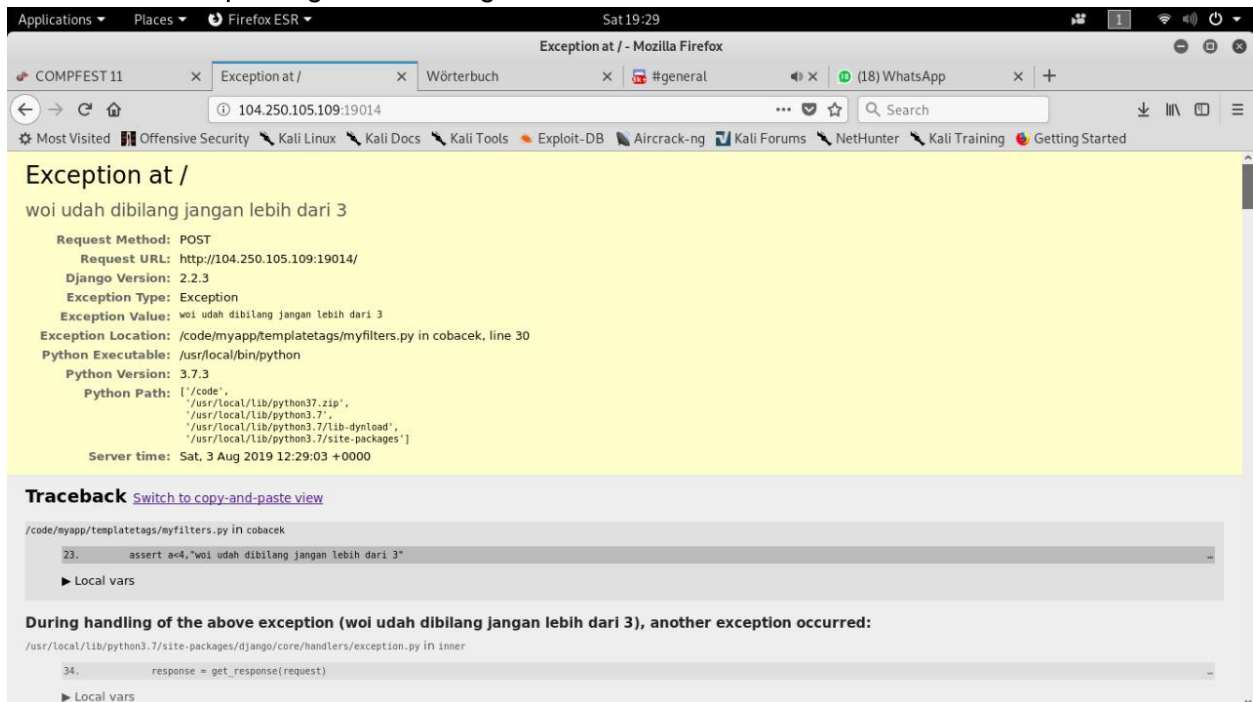
Super-Secure-Filter

Cara Pengerjaan

pertama kami coba menginputkan sesuai contoh disitu, ternyata yang outputnya sesuai dengan inputnya, ketika diinputkan `{{ mammals }}` maka akan terlihat gambar hewan mamalia (kucing), begitu pula dengan yg lainnya.



lalu kami coba input angka selain angka 3



dan ternyata muncul error pada halaman django, dan mentrigger fungsi `assert a<4`

```
Applications ▾ Places ▾ Firefox ESR ▾ Sat 19:30
Exception at / - Mozilla Firefox
COMPFEST 11 x Wörterbuch x #general x Exception at / x (18) WhatsApp x +
104.250.105.109:19014
Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums NetHunter Kali Training Getting Started

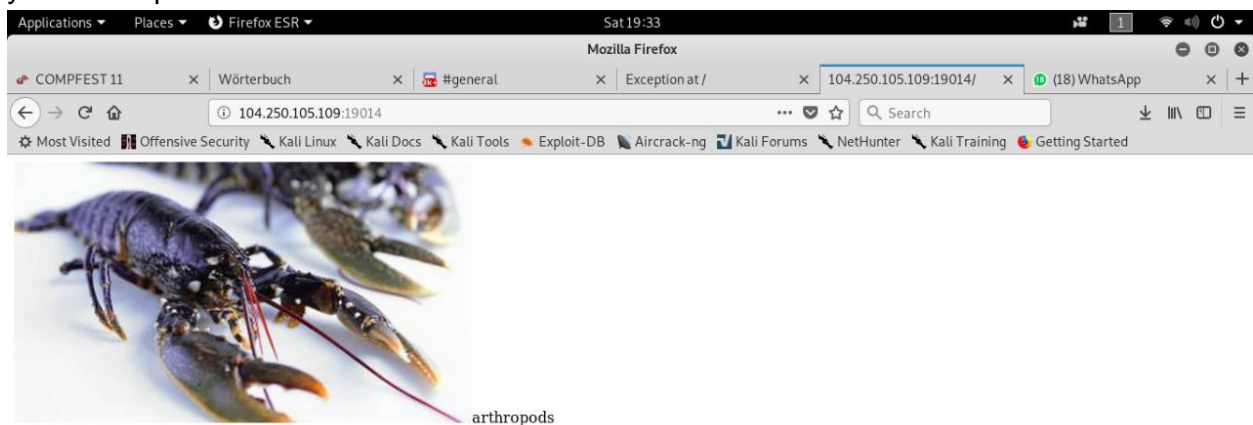
▶ Local vars
/usr/local/lib/python3.7/site-packages/django/core/handlers/base.py in _get_response
115. response = self.process_exception_by_middleware(e, request)

▶ Local vars
/usr/local/lib/python3.7/site-packages/django/core/handlers/base.py in _get_response
113. response = wrapped_callback(request, *callback_args, **callback_kwargs)

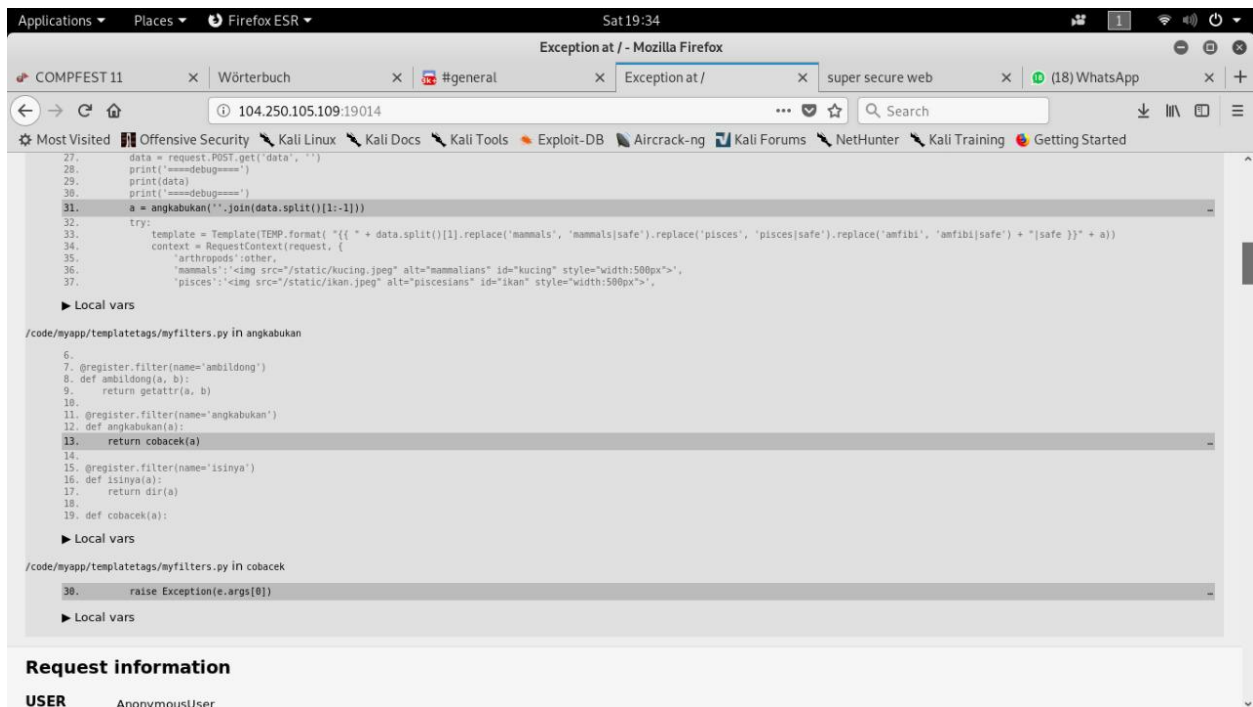
▶ Local vars
/code/myapp/views.py in homepage
24. if cek_cookies(request):
25.     return cek_cookies(request)
26. if request.method == "POST":
27.     data = request.POST.get('data', '')
28.     print('===debug===')
29.     print(data)
30.     print('===debug===')
31.     a = angkabukan(''.join(data.split()[1:-1]))
32.     try:
33.         template = Template(TMP.format('{{ ' + data.split()[1].replace('mammals', 'mammals|safe').replace('pisces', 'pisces|safe').replace('amfibi', 'amfibi|safe') + '|safe }}' + a))
34.         context = RequestContext(request, {
35.             'arthropods':data
36.             'mammals':',
37.             'pisces':',
▶ Local vars
/code/myapp/templatetags/myfilters.py in angkabukan
13. return cobacek(a)

▶ Local vars
/code/myapp/templatetags/myfilters.py in cobacek
38. raise Exception(e.args[0])
```

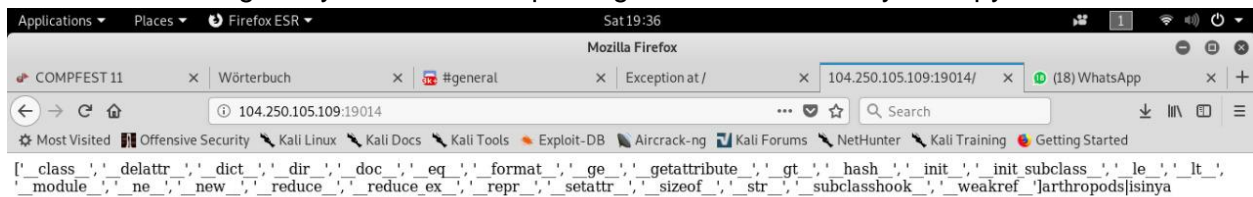
lalu saat di lihat dengan seksama, ternyata ada sesuatu yang janggal pada variable context. yaitu arthropods



ketika kami inputkan {{ arthropods }} benar saja, sebuah gambar muncul, tetapi keyword arthropods tidak tertera pada awal halaman seperti yang lainnya

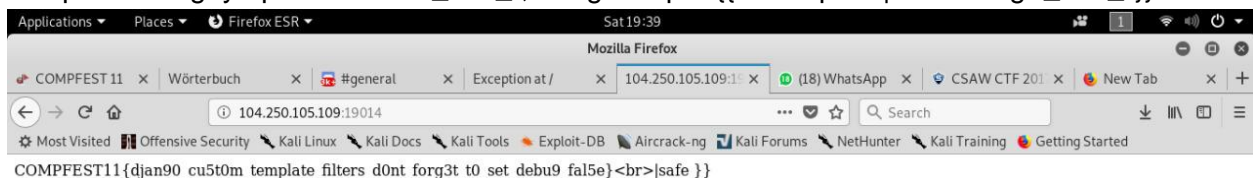


lalu kami check lagi ternyata ada beberapa fungsi custom filter di myfilters.py



lalu kami coba inputkan `{{ arthropods|isinya }}` dan benar saja, munculah beberapa atribut dari arthropods.

lalu kami menginputkan atributnya 1 per 1 menggunakan fungsi ambil dong , dan ternyata didapatkan flagnya pada atribut `_doc_` , dengan input `{{ arthropods|ambil_dong:"_doc_" }}`



Flag

COMPFEST11{djan90_cu5t0m_template_filters_d0nt_for3t_t0_set_debu9_fal5e}