Write Up COMPFEST 11

Artillery

Rexy Fahrezi
Gayu Gumelar

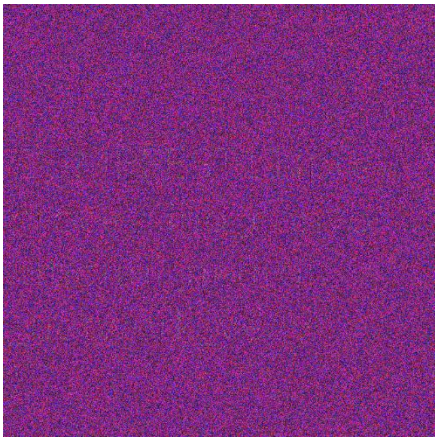
Universitas Teknokrat Indonesia

Forensic

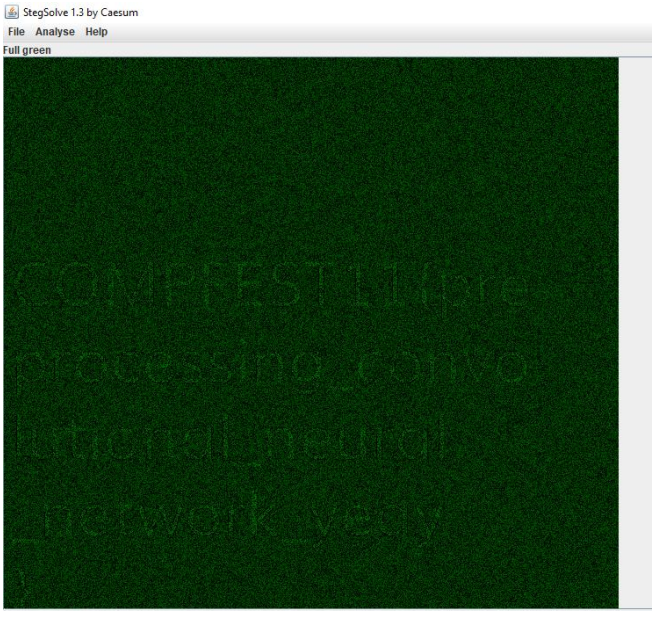
Cable News Network

Cara Pengerjaan

Diberikan sebuah file image



Lakukan analisis dengan Stegsolve,



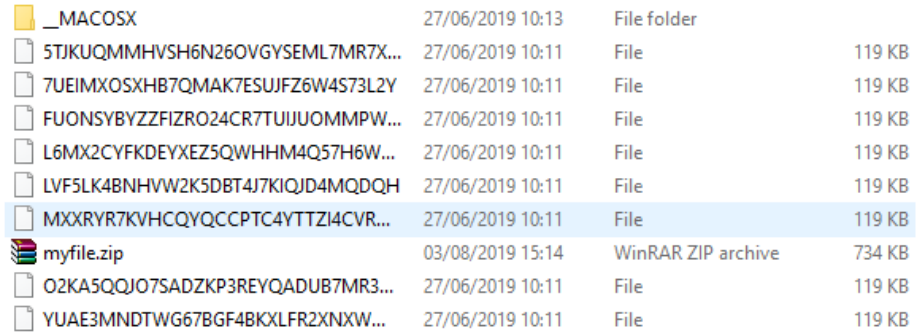
Flag

COMPFEST11{preprocessing_convolutional_neural_network_yeay}

File Separation

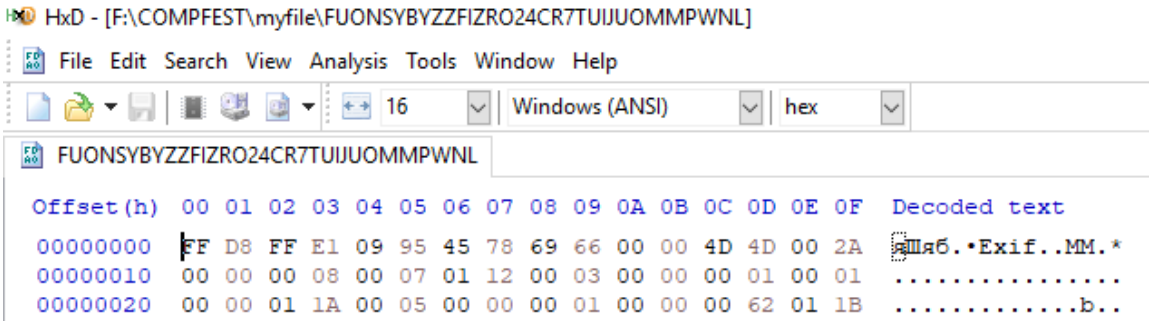
Cara Pengerjaan

Diberikan file zip, lakukan extract

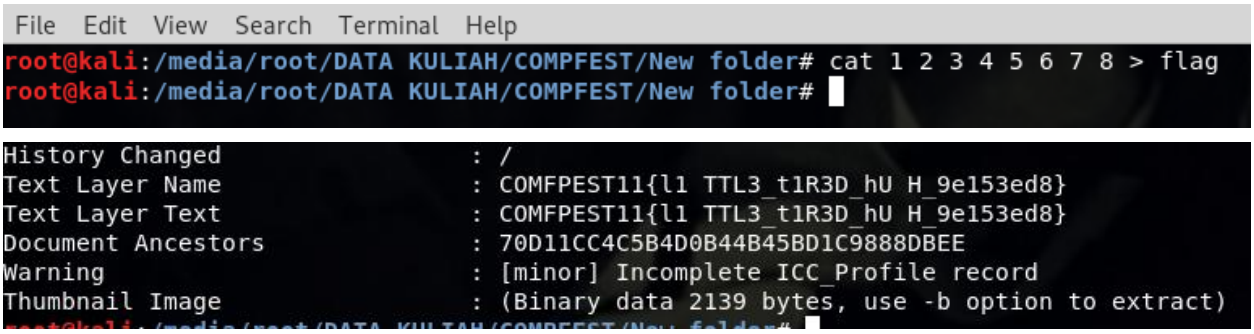


_MACOSX	27/06/2019 10:13	File folder	
5TJKUQMMHVSH6N26OVGYSEML7MR7X...	27/06/2019 10:11	File	119 KB
7UEIMXOSXHB7QMAK7ESUJFZ6W4S73L2Y	27/06/2019 10:11	File	119 KB
FUONSYBYZZFIZRO24CR7TUIJUOMMPW...	27/06/2019 10:11	File	119 KB
L6MX2CYFKDEYXEZ5QWHHM4Q57H6W...	27/06/2019 10:11	File	119 KB
LVF5LK4BNHVW2K5DBT4J7KIQJD4MQDQH	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
YUAE3MNDTWG67BGF4BKXLFR2XNXW...	27/06/2019 10:11	File	119 KB

Analisis dengan hex editor



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




```
History Changed                 : /
Text Layer Name                 : COMFPEST11{l1 TTL3_t1R3D_hU H_9e153ed8}
Text Layer Text                 : COMFPEST11{l1 TTL3_t1R3D_hU H_9e153ed8}
Document Ancestors              : 70D11CC4C5B4D0B44B45BD1C9888DBEE
Warning                         : [minor] Incomplete ICC_Profile record
Thumbnail Image                 : (Binary data 2139 bytes, use -b option to extract)
```

Flag

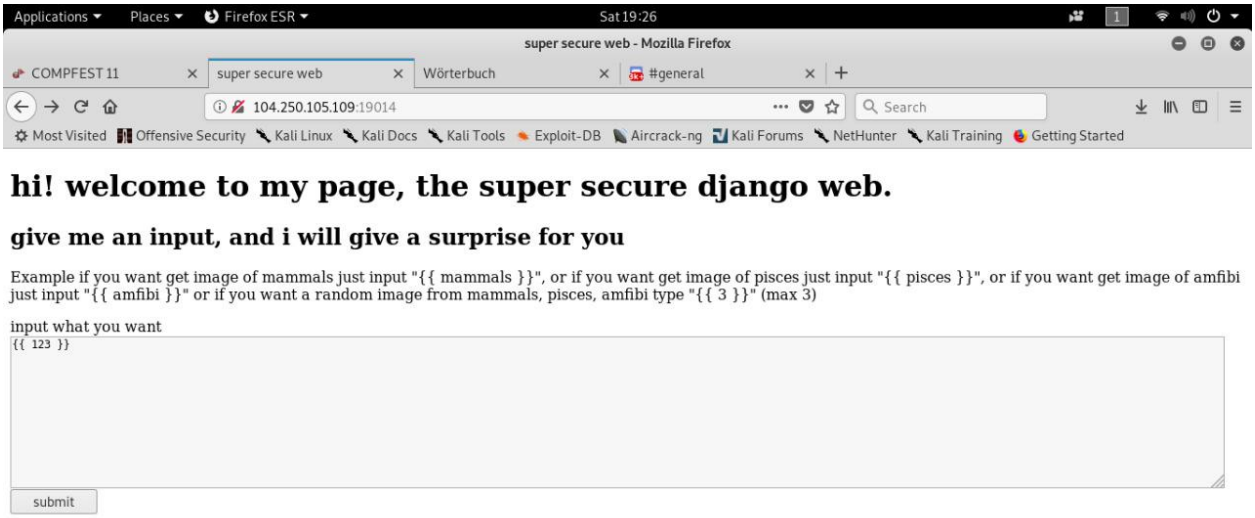
COMFPEST11{l1TTL3_t1R3D_hUH_9e153ed8}

Web

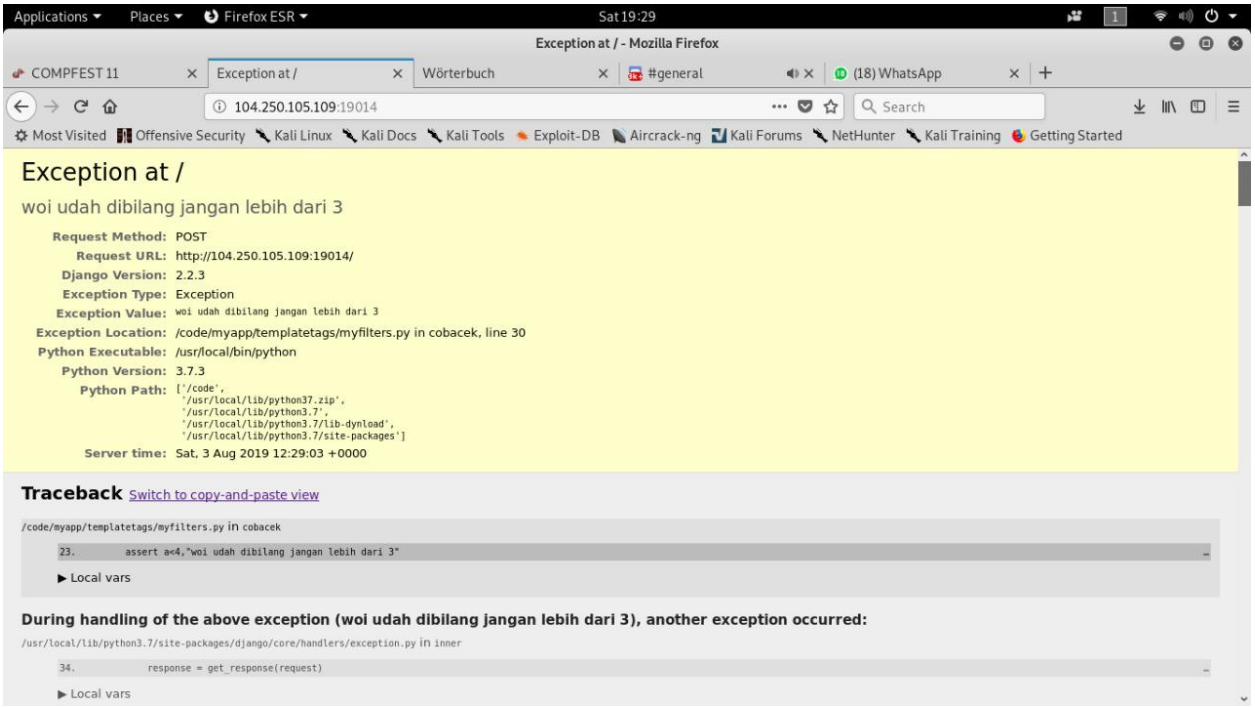
Super-Secure-Filter

Cara Pengerjaan

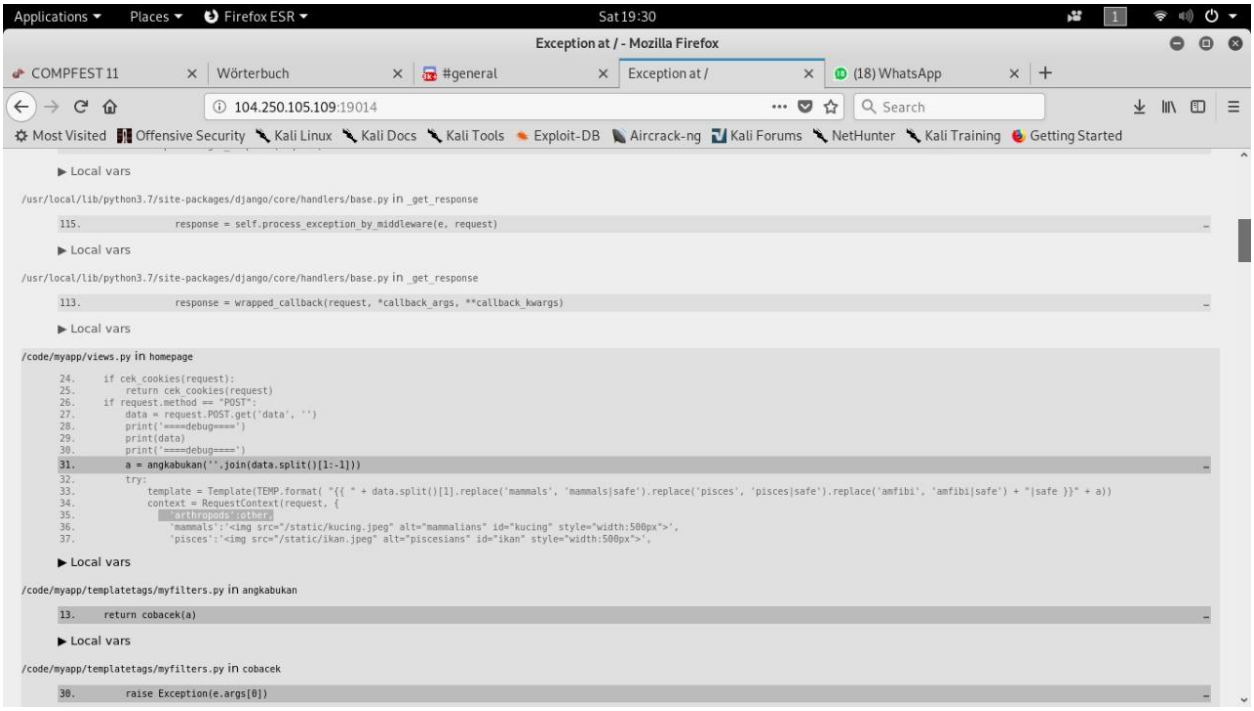
pertama kami coba menginputkan sesuai contoh disitu, ternyata yang outputnya sesuai dengan inputnya, ketika diinputkan {{ mammals }} maka akan terlihat gambar hewan mamalia (kucing), begitu pula dengan yg lainnya.



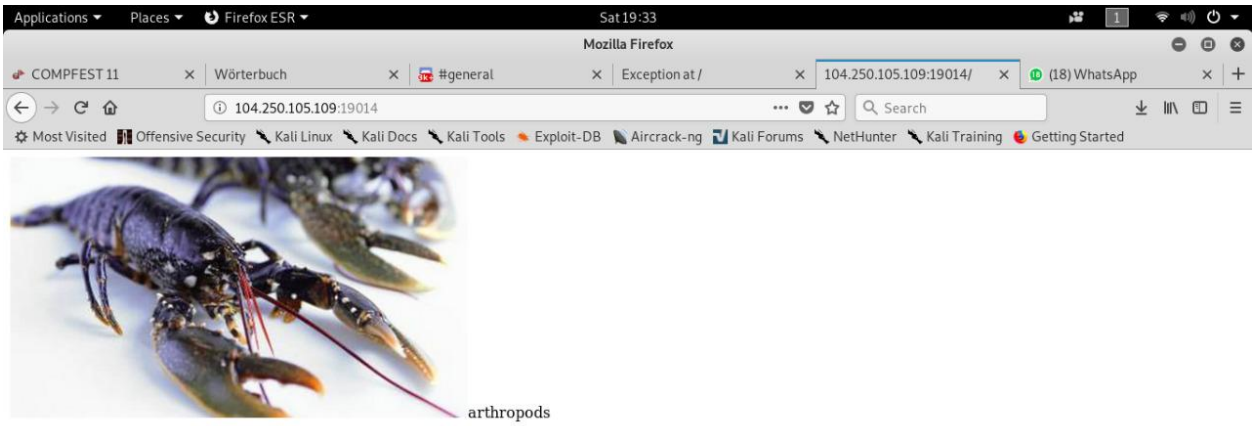
lalu kami coba input angka selain angka 3



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

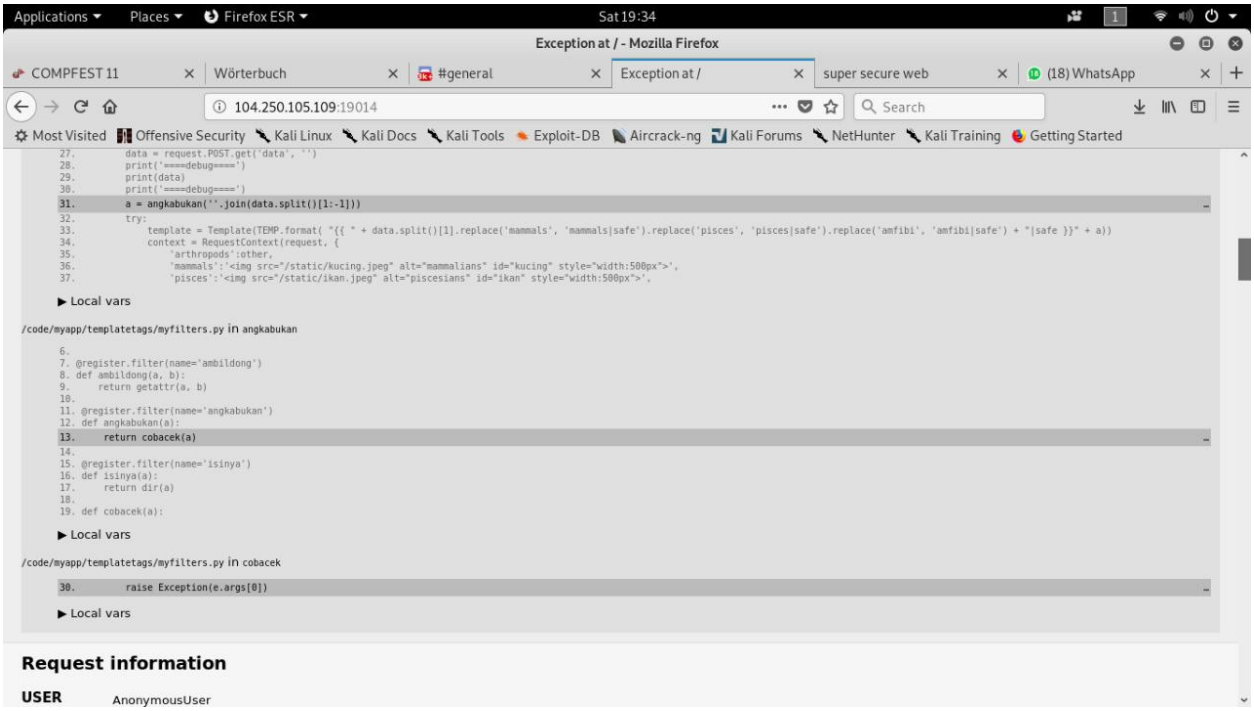


lalu saat di lihat dengan seksama, ternyata ada sesuatu yang janggal pada variable context. yaitu arthropods

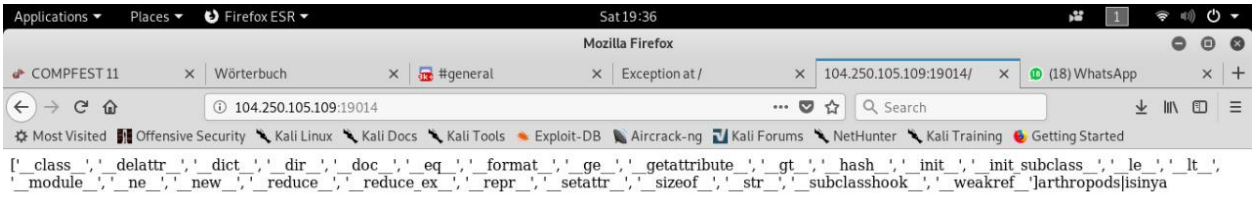


arthropods

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 attributnya 1 per 1 menggunakan fungsi ambil dong , dan ternyata didapatkan flagnya pada attribut _doc_ , dengan input {{ arthropods|ambildong:"_doc_"}}

Flag

COMPFEST11{djan90_cu5t0m_template_filters_d0nt_forg3t_t0_set_debu9_fal5e}