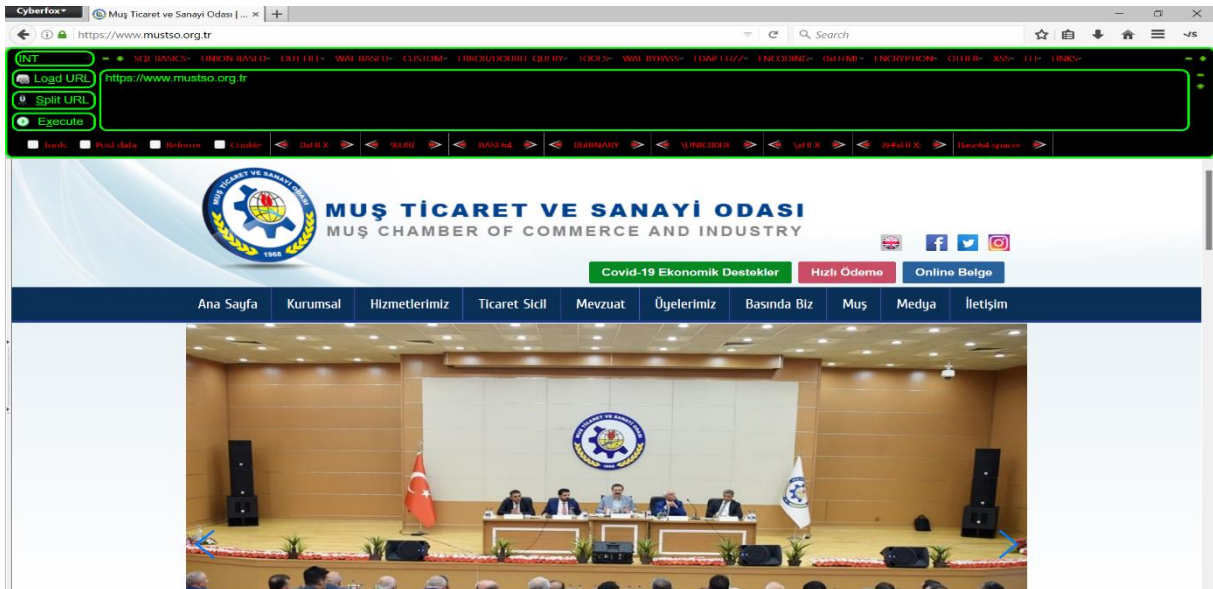


BİLGİ SİSTEMLERİ VE GÜVENLİĞİ DERSİ KİŞİSEL TARAMA RAPORU

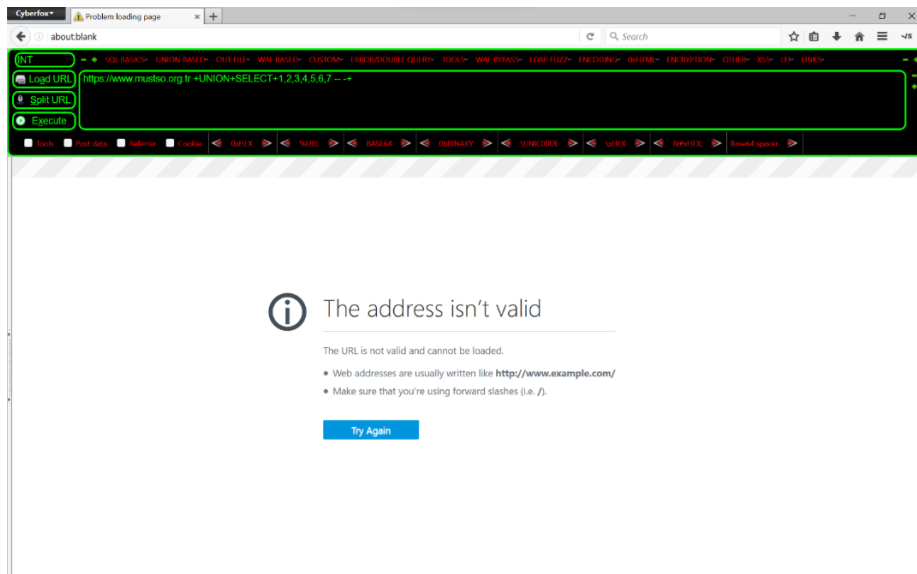
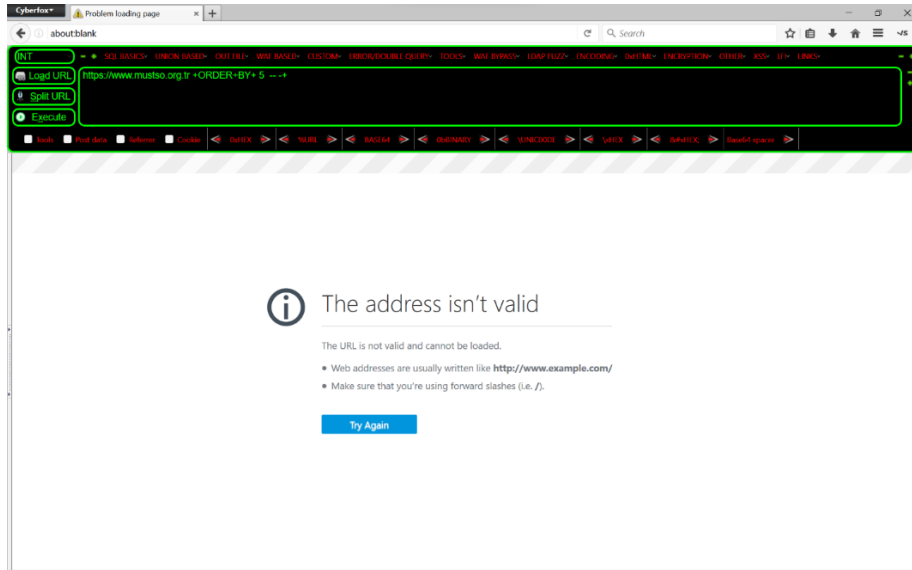
HALİL İBRAHİM YILDIZ – 16541072

HEDEF ADRES : MUSTSO.ORG.TR

- **HACKBAR:** Hackbar firefoxa bağlı bir eklentidir. Hackbar sayesinde Sql , Xss, Lfi gibi güvenlik zafiyetlerini kullanabiliyoruz.



- Kolon bulmak için 'ORDER BY' komutu ve 'UNION SELECT' komutunu kullandım fakat sql açığı olmadığından herhangi bir sonuç alamadım.



SKIPFISH:

- Aktif web uygulaması keşif aracı

```
kali@kali:~/Desktop
File Actions Edit View Help
skipfish version 2.10b by lcamtuf@google.com
- www.mustso.org.tr -

Scan statistics:
  Scan time : 0:04:16.060
  HTTP requests: 2642 (14.6/s), 12570 kB in, 1263 kB out (54.9 kB/s)
  Compression : 0 kB in, 0 kB out (0.0% gain)
  HTTP faults : 29 net errors, 0 proto errors, 0 retried, 0 drops
  TCP handshakes : 252 total (16.8 req/conn)
  TCP faults : 0 failures, 29 timeouts, 1 purged
  External links : 113 skipped
  Reqqs pending : 582

Database statistics:
  Pivots : 259 total, 5 done (1.93%)
  In progress : 207 pending, 31 init, 16 attacks, 0 dict
  Missing nodes : 6 spotted
  Node types : 1 serv, 141 dir, 9 file, 0 pinfo, 86 unkn, 22 par, 0 val
  Issues found : 33 info, 22 warn, 4 low, 2 medium, 0 high impact
  Dict size : 140 words (140 new), 9 extensions, 256 candidates
  Signatures : 77 total
```

Önemli satır 'Issues found' bu satırda kaç bilgi bulunduğu, kaç hatanın olduğu, Kaç düşük, orta, büyük kritik açık olduğunu gösteriyor. Fakat programı çalışmaya bıraktığımda en son 12 gün gösterdiği için Verileri alamadım Durdurma komutunu Kullanınca sistem tamamen duruyor ve bize hiçbir veri vermiyor.

- NMAP :

1. nmap -Pn --script vuln mustso.org.tr -d

```
kali@kali:~$ nmap -Pn --script vuln mustso.org.tr -d
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 13:50 EDT
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)

Timing report
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0

NSE: Using Lua 5.3.
NSE: Arguments from CLI:
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:50
NSE: Starting broadcast-avahi-dos.
NSE: [broadcast-avahi-dos] dns.query() got zero responses attempting to resolve query
: _services._dns-sd._udp.local
NSE: Finished broadcast-avahi-dos.
Completed NSE at 13:50, 10.09s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 13:50
Completed NSE at 13:50, 0.00s elapsed
mass_rdns: Using DNS server 192.168.1.1
Initiating Parallel DNS resolution of 1 host. at 13:51
mass_rdns: 0.01s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 13:51, 0.01s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR
: 1, CN: 0]
Initiating Connect Scan at 13:51
Scanning mustso.org.tr (151.80.40.80) [1000 ports]
Discovered open port 443/tcp on 151.80.40.80
Discovered open port 80/tcp on 151.80.40.80
Discovered open port 53/tcp on 151.80.40.80
Discovered open port 6003/tcp on 151.80.40.80
Discovered open port 1022/tcp on 151.80.40.80
Completed Connect Scan at 13:51, 7.34s elapsed (1000 total ports)
Overall sending rates: 272.30 packets / s.
NSE: Script scanning 151.80.40.80.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 13:51
NSE: Starting http-vuln-cve2012-1823 against mustso.org.tr (151.80.40.80:80).
NSE: Starting http-vuln-wnr1000-creds against mustso.org.tr (151.80.40.80:443).
NSE: Starting rsa-vuln-roca against mustso.org.tr (151.80.40.80:6003).
```

- host sisteminde aktif olan servislerin versiyon bilgilerini almanızı sağlar.
- 5 adet açık port bulunmuştur.(53-80-443-1022-6003/TCP)
- Güvenlik Duvarını ping temsil edebilir.
- Ping in IP adresini açıklamak için -Pn parametreleri kullanmalısınız.

2. nmap -p80 --script http-waf-detect mustso.org.tr

```
kali@kali:~$ nmap -p80 --script http-waf-detect mustso.org.tr
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 14:02 EDT
Nmap scan report for mustso.org.tr (151.80.40.80)
Host is up (0.082s latency).
rDNS record for 151.80.40.80: mirsoft.com.tr

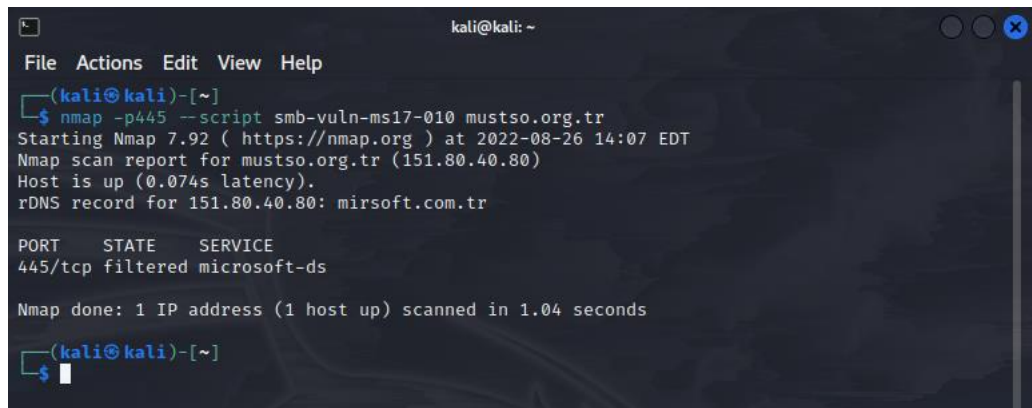
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds

(kali@kali)~$
```

- 1 Adet port bulunmuştur (80/TCP HTTP)
- Bir web sunucusunun bir IPS (İzinsiz Giriş Önleme Sistemi), IDS (İzinsiz Giriş Tespit Sistemi) veya WAF (Web Uygulaması Güvenlik Duvarı) tarafından korunup korunmadığını belirlemeye çalışır.

3. nmap -p445 --script smb-vuln-ms17-010 mustso.org.tr



```
kali@kali: ~  
File Actions Edit View Help  
~(kali@kali)-[~]  
$ nmap -p445 --script smb-vuln-ms17-010 mustso.org.tr  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 14:07 EDT  
Nmap scan report for mustso.org.tr (151.80.40.80)  
Host is up (0.074s latency).  
rDNS record for 151.80.40.80: mirsoft.com.tr  
  
PORT      STATE      SERVICE  
445/tcp    filtered  microsoft-ds  
  
Nmap done: 1 IP address (1 host up) scanned in 1.04 seconds  
  
~(kali@kali)-[~]  
$
```

- Hedef sistemde TCP\445 portuna erişilmesine rağmen MS17-010 zafiyetinin olmadığı düşünülüyorsa MS17-010 komutu kullanılır.
- 1 Adet port bulunmuştur (445/TCP)
- Bu zafiyet sayesinde zafiyeti sömüren kullanıcı, EternalBlue exploiti ile hedef sistem üzerinde uzaktan kod çalıştırabilme lüksüne sahip olabilmektedir

4. nmap -p445 --script vuln mustso.org.tr

```
(kali㉿kali)-[~]  
$ nmap -p445 --script vuln mustso.org.tr  
  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-26 14:12 EDT  
Nmap scan report for mustso.org.tr (151.80.40.80)  
Host is up (0.073s latency).  
rDNS record for 151.80.40.80: mirsoft.com.tr  
  
PORT      STATE      SERVICE  
445/tcp    filtered  microsoft-ds  
  
Nmap done: 1 IP address (1 host up) scanned in 11.34 seconds
```

- 1 Adet port bulunmuştur(445/TCP)
-
- Bellek bozulması güvenlik açığına karşı savunmasız olup olmadığını test eder.