Mustso.gov.tr - Ek Tarama ve Zaafiyet Bulma

Dipnot: Hocam bildiğiniz üzere Wireshark efektif kullanmak için aynı lat ağda bulunmamız gerekiyor Muş TSO ile, böyle bir imakanımız bulunmadığı için biz Wireshark'a dair elimizden geleni yaptık (**Wireshark - Musteso Final Raporu**) dosaysında ulaşabilirsiniz, ondan sonra faklı çeşitli araçlar deneme yaptık aşağıda yaptığımız çalışmalardan çeşitli verileri görebilirsiniz:

Shodan ile tarama yaptık ve bir kaç tane önemli bilgi yakaladık ve **en önemlisi bir tane açık bulduk**. Sonuçlar aşağıda verilmiştir.

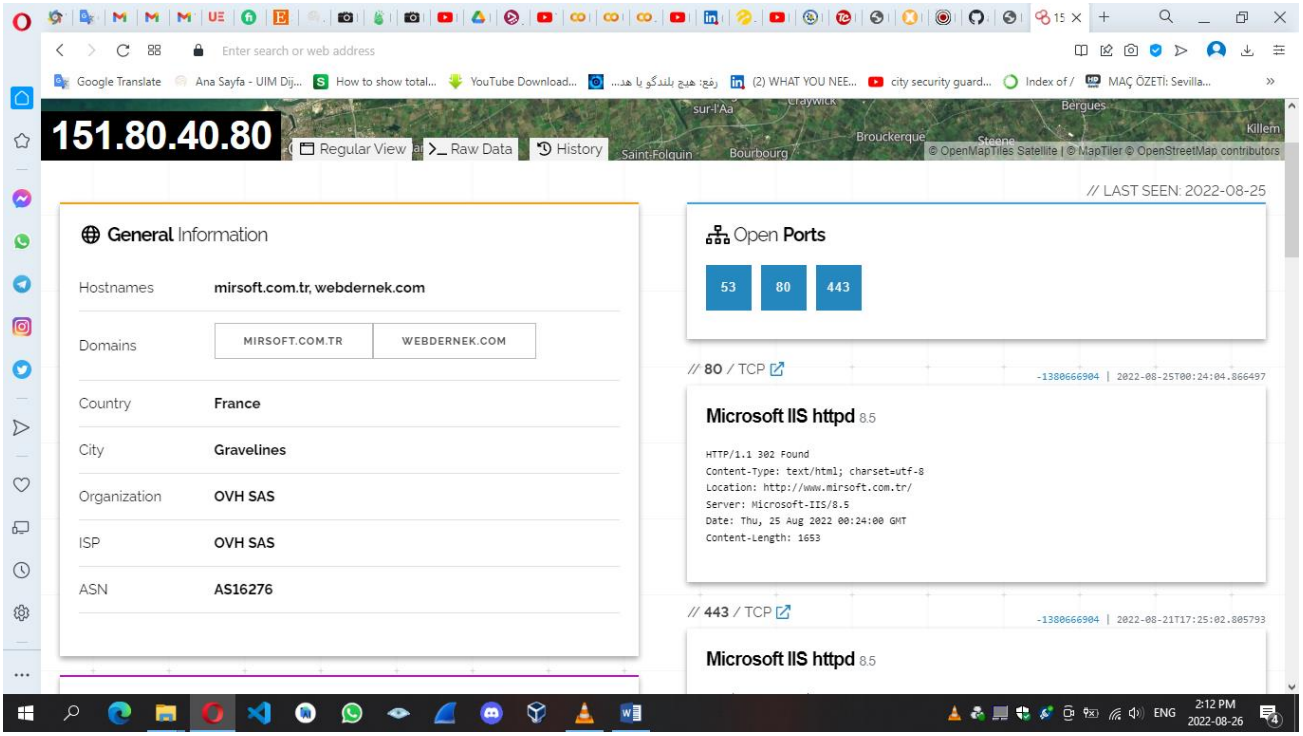
Açıklık: CVE-2014-4078 bu güvenlik numarası bu numara'da açıklık bulunuyor, bu açıklıkığı güncellemesi gerekiyor

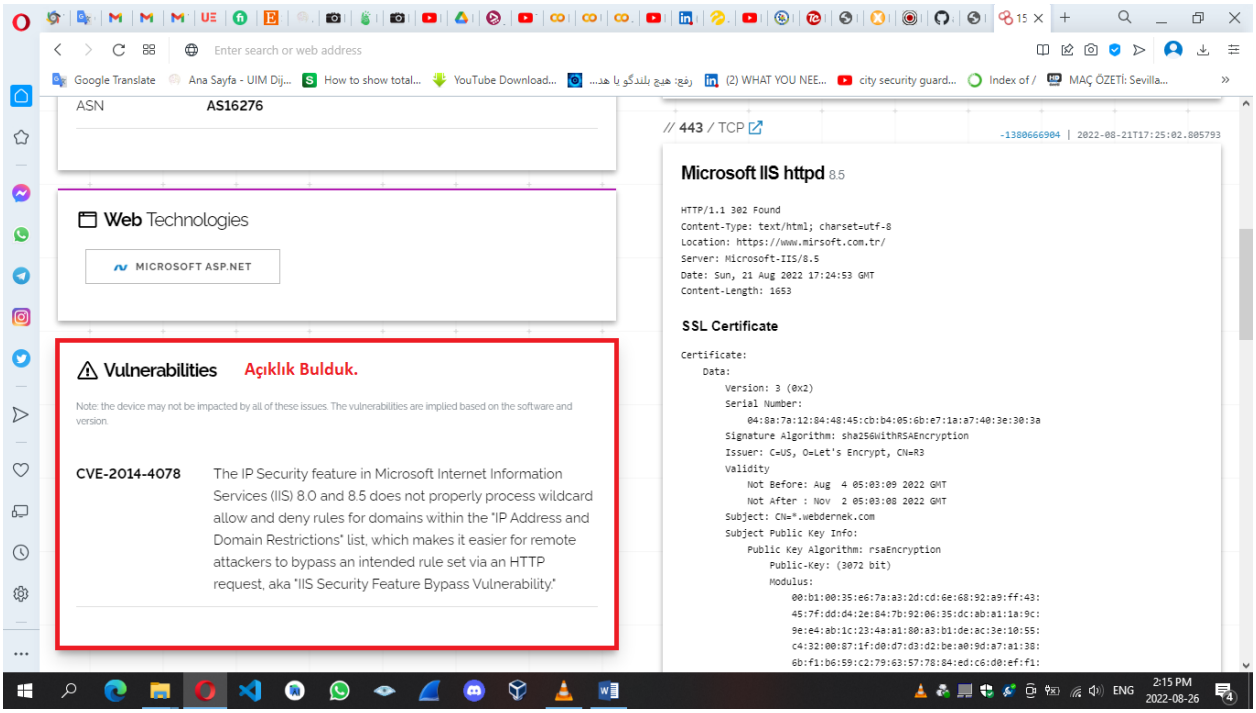
Mustso.gov.tr -> mirsoft.com.tr, webdernek.com web sitelerini aittir.

Sunucu frans'da bulunuyor, ASP.Net ile yazılmış.

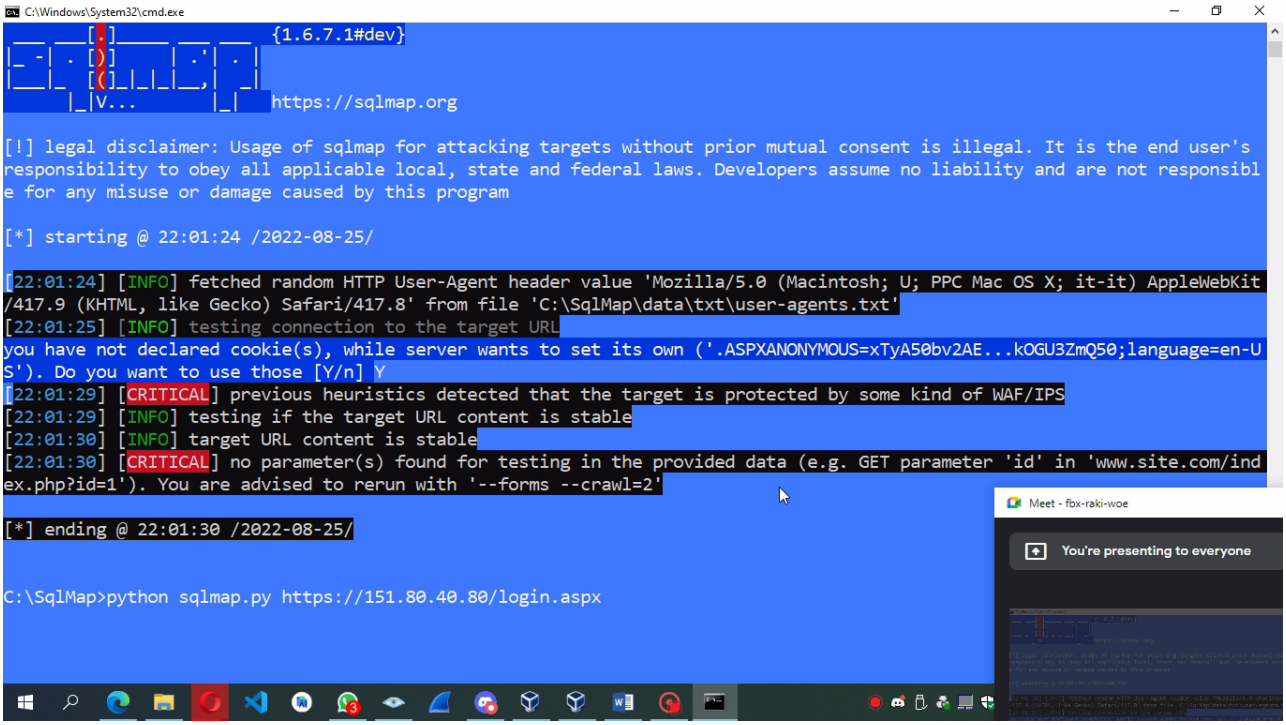
IIS/8.5 sürümünü kullanılıyor.

Web Site: https://www.shodan.io/host/151.80.40.80





SQL INJECTION (sqlmap) kullandık çeşitli denemeler yaptık (Meet üzerinden toplantı ile tüm grup üyeleri ile yaptık) aşağıda deneme yaptığımız görüntü mevcuttur:



SQLMAP denemelerimizden bazi sonuclar:

Microsoft Windows [Version 10.0.19044.1889]

(c) Microsoft Corporation. All rights reserved.

C:\SqlMap>python sqlmap.py -u "https://www.mustso.org.tr/BasındaBiz/Haber/tabid/17222/articleType/ArticleView/articleId/40695/Mirac-Kandiliniz-Kutlu-Olsun.aspx" --dbs

```
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.7.1#dev}
|_ -| . ["]     | .'| . |
|___|_  ['']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 21:59:25 /2022-08-25/

[21:59:26] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('.ASPXANONYMOUS=XGzXoEbv2AE...hZTg0MWE10;Article40695=1;language=en-US'). Do you want to use those [Y/n] y

[21:59:31] [INFO] checking if the target is protected by some kind of WAF/IPS

[21:59:31] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS

are you sure that you want to continue with further target testing? [Y/n] y

[21:59:34] [WARNING] please consider usage of tamper scripts (option '--tamper')

[21:59:34] [INFO] testing if the target URL content is stable

[21:59:35] [INFO] target URL content is stable

[21:59:35] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'

[21:59:35] [WARNING] HTTP error codes detected during run:

404 (Not Found) - 1 times

[*] ending @ 21:59:35 /2022-08-25/

C:\SqlMap>python sqlmap.py -u "https://www.mustso.org.tr/login.aspx" --dbs --random-agent

```
      ___
     __H__
 ___ ___[.]_____ ___ ___  {1.6.7.1#dev}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:01:24 /2022-08-25/

[22:01:24] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; U; PPC Mac OS X; it-it) AppleWebKit/417.9 (KHTML, like Gecko) Safari/417.8' from file 'C:\SqlMap\data\txt\user-agents.txt'

[22:01:25] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('.ASPXANONYMOUS=xTyA50bv2AE...kOGU3ZmQ50;language=en-US'). Do you want to use those [Y/n] Y

[22:01:29] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS

[22:01:29] [INFO] testing if the target URL content is stable

[22:01:30] [INFO] target URL content is stable

[22:01:30] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'

[*] ending @ 22:01:30 /2022-08-25/

C:\SqlMap>python sqlmap.py "https://151.80.40.80/login.aspx" --dbs --random-agent

```
      ___
     __H__
 ___ ___[.]_____ ___ ___  {1.6.7.1#dev}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:05:26 /2022-08-25/

[22:05:26] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_7; en-US) AppleWebKit/532.0 (KHTML, like Gecko) Chrome/3.0.198 Safari/532.0' from file 'C:\SqlMap\data\txt\user-agents.txt'

[22:05:26] [INFO] testing connection to the target URL

[22:05:27] [CRITICAL] page not found (404)

it is not recommended to continue in this kind of cases. Do you want to quit and make sure that everything is set up properly? [Y/n] y

[22:05:29] [WARNING] HTTP error codes detected during run:

404 (Not Found) - 1 times

[*] ending @ 22:05:29 /2022-08-25/

C:\SqlMap>python sqlmap.py -u "https://www.mustso.org.tr/BasındaBiz/Haber/tabid/17222/articleType/ArticleView/articleId/40739/HALK-BANKASINDAN-KADIN-GIRISIMCILERE-DESTEK.aspx" --dbs --random-agent

___

__H__

___ ___["]_____ ___ ___ {1.6.7.1#dev}

|_ -| . ["] | .'| . |

|___|_ ["]_|_|_|__,| _|

|_|V... |_| https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 22:07:10 /2022-08-25/

[22:07:10] [INFO] fetched random HTTP User-Agent header value 'Mozilla/4.0 (Compatible; MSIE 8.0; Windows NT 5.2; Trident/6.0)' from file 'C:\SqlMap\data\txt\user-agents.txt'

[22:07:10] [INFO] testing connection to the target URL

you have not declared cookie(s), while server wants to set its own ('.ASPXANONYMOUS=camPtUfv2AE...kZGQ2MWY00;Article40739=1;language=en-US'). Do you want to use those [Y/n] Y

[22:07:14] [INFO] checking if the target is protected by some kind of WAF/IPS

[22:07:15] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS

are you sure that you want to continue with further target testing? [Y/n] Y

[22:07:20] [WARNING] please consider usage of tamper scripts (option '--tamper')

[22:07:20] [INFO] testing if the target URL content is stable

[22:07:21] [INFO] target URL content is stable

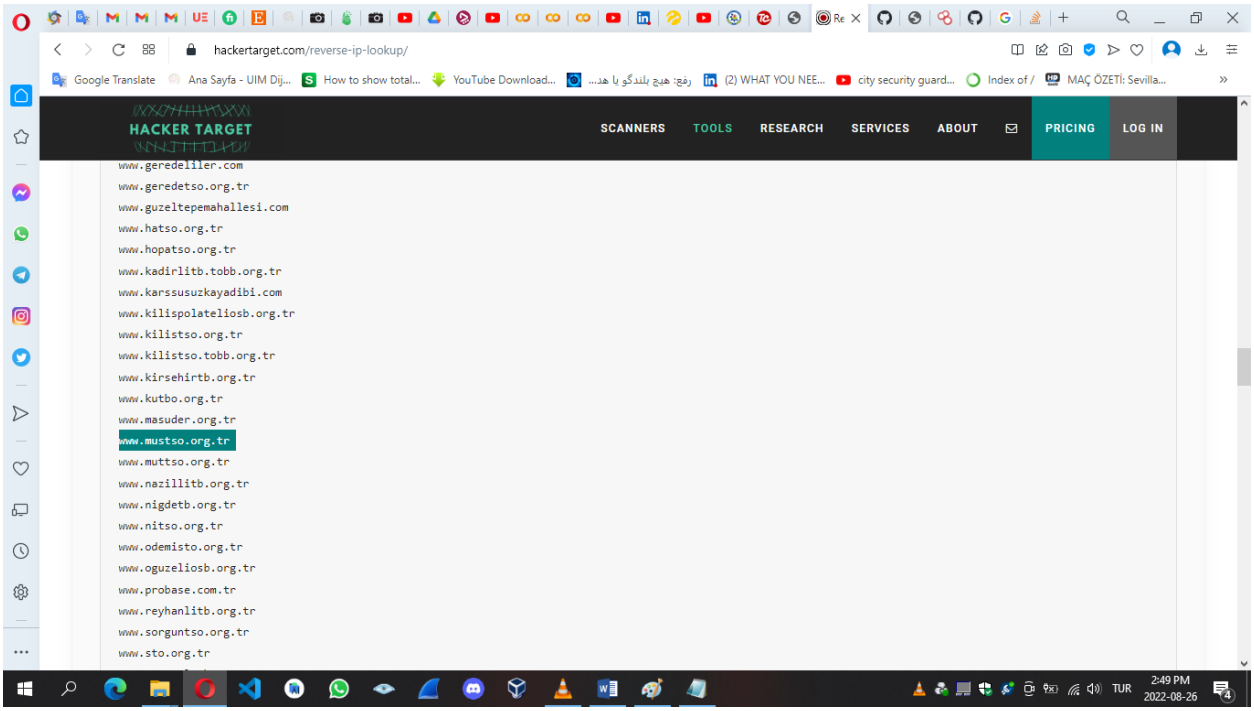
[22:07:21] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'

[22:07:21] [WARNING] HTTP error codes detected during run:

404 (Not Found) - 1 times

[*] ending @ 22:07:21 /2022-08-25/

Reverse IP Lookup (https://hackertarget.com/reverse-ip-lookup/) web sitesini kullandık, muş tso ile aynı sunucu'da bulunan **178** tanesi muş tso ile ayınıdır, ve hepsi nerdeyse aynı script'leri kullanılıyor. Deneme soncu 178 web sitenin listesini aşağıda verdik.



1. ahmetahi.com
2. akademi.bileciktso.org.tr
3. akademi.bulancak-tso.org.tr
4. akademi.nazillitb.org.tr

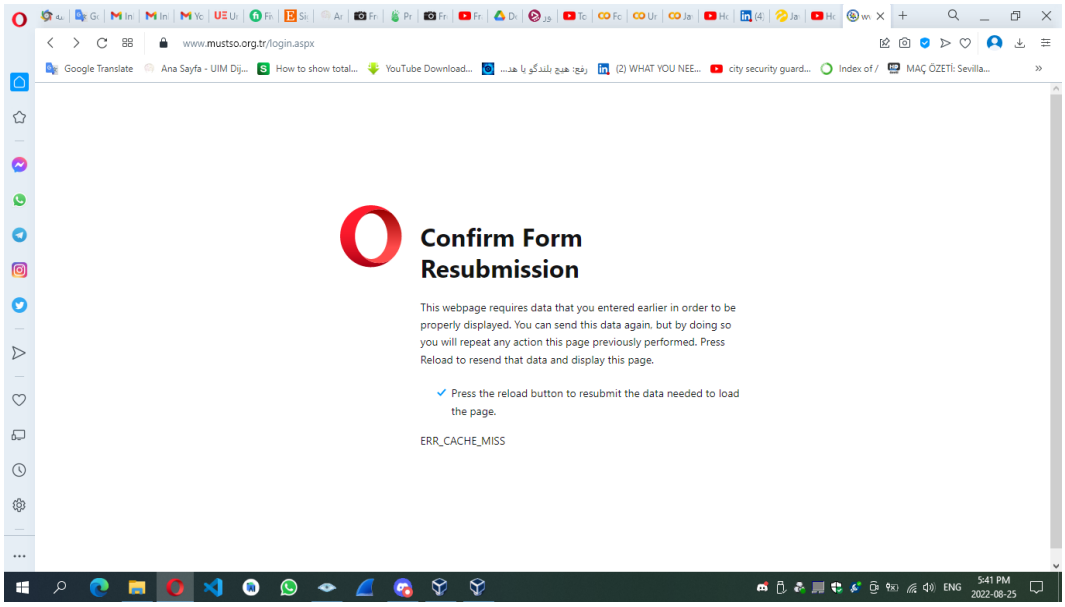
5. akademi.odemisto.org.tr
6. akademi.sto.org.tr
7. akademi.yuksekovatso.org.tr
8. akreditasyon.kutbo.org.tr
9. akreditasyon.nazillitb.org.tr
10. akreditasyon.nitso.org.tr
11. akyazitso.tobb.org.tr
12. alacatso.org.tr
13. animetakvimi.com
14. ankarapvctamiri.com
15. antakyatb.gov.tr
16. ardahantso.org.tr
17. b.site.probase.com.tr
18. baglum.site.probase.com.tr
19. baglumspor.com
20. basgimpa.site.probase.com.tr
21. bileciktso.org.tr
22. bintso.org.tr
23. bitlistso.org.tr
24. bogazliyantso.org.tr
25. bolulutahirusta.com
26. bozuyuk.site.probase.com.tr
27. bozuyuktso.org.tr
28. bucaktso.org.tr
29. bulancak-tso.org.tr
30. burmosan.com.tr
31. c.site.probase.com.tr
32. canakkaleliler.org
33. canakkaletso.org.tr
34. cankirigenclikdernegi.org
35. cankiritb.org.tr
36. cankiriyem.com.tr
37. catso.org.tr
38. cavdar.org.tr
39. cephe.site.probase.com.tr
40. ceyhantb.org.tr
41. ceyhantb.tobb.org.tr
42. ctso.site.probase.com.tr
43. demok.site.probase.com.tr
44. devrek.site.probase.com.tr
45. devrektso.org.tr
46. dnn.site.probase.com.tr
47. egerlibaskoy.org
48. ekremdoganayvakfi.com

49. en.bulancak-tso.org.tr
50. erdek.site.probase.com.tr
51. erdemlitso.org.tr
52. fransa3.probase.com.tr
53. gediz.site.probase.com.tr
54. gediztso.org.tr
55. gelibolutso.org.tr
56. genckalecikliler.com
57. geredeliler.com
58. geredetso.org.tr
59. geredetso.site.probase.com.tr
60. geredetso.tobb.org.tr
61. hatso.org.tr
62. hopatso.org.tr
63. ilgaz.bel.tr
64. islahiyeosb.org
65. islahiyeto.org.tr
66. kadirlitso.tobb.org.tr
67. kalite.bintso.org.tr
68. kalite.bulancak-tso.org.tr
69. kalite.hopatso.org.tr
70. kalite.sto.org.tr
71. kalite.yuksekovatso.org.tr
72. karssusuzkayadibi.com
73. karvak.com
74. karvak.site.probase.com.tr
75. kavrak.site.probase.com.tr
76. kilispolateliosb.org.tr
77. kilistso.org.tr
78. kirsehirtb.org.tr
79. kuantummedikal.com
80. kum.site.probase.com.tr
81. kumlucatb.org.tr
82. kutbo.org.tr
83. magicalchange.net
84. maltepe.site.probase.com.tr
85. masuder.org.tr
86. mayailaclama.com
87. mefkurede.site.probase.com.tr
88. mircekiraz.com
89. mirsoft.com.tr
90. muradiye.org.tr
91. muradiye.site.probase.com.tr
92. mustahsil.cankiritb.org.tr

93. mustso.org.tr
94. mutosb.org.tr
95. muttso.org.tr
96. muttso.site.probase.com.tr
97. nazillitb.org.tr
98. nigdetb.org.tr
99. nitso.org.tr
100. ns.bozuyuktso.tobb.org.tr
101. ns.ceyhantb.tobb.org.tr
102. ns1.probase.com.tr
103. ns3556883.ip-151-80-40.eu
104. odemisto.org.tr
105. oduldanismanlik.com
106. otelbaskent.com
107. panel.mirsoft.com.tr
108. platinsaglikhizmetleri.com
109. plugin.animetakvimi.com
110. privadomoda.com
111. probase.com.tr
112. pyl.animetakvimi.com
113. sitso.org.tr
114. sorguntso.org.tr
115. sto.org.tr
116. sungurlutb.org.tr
117. tarsustb.gov.tr
118. tarsustb.tobb.org.tr
119. termetb.org.tr
120. termetso.org.tr
121. uslu.site.probase.com.tr
122. webdernek.com
123. www.alacatso.org.tr
124. www.ankarapvctamiri.com
125. www.ardahantso.org.tr
126. www.bileciktso.org.tr
127. www.bintso.org.tr
128. www.bitlistso.org.tr
129. www.bogazliyantso.org.tr
130. www.bozuyuktso.org.tr
131. www.bozuyuktso.tobb.org.tr
132. www.bucaktso.org.tr
133. www.bulancak-tso.org.tr
134. www.burmosan.com.tr
135. www.cankiritb.org.tr
136. www.catso.org.tr

137. www.cavdar.org.tr
138. www.ceyhantb.org.tr
139. www.ekremdoganayvakfi.com
140. www.enkamuder.org.tr
141. www.erdemlitso.org.tr
142. www.eyaf.org.tr
143. www.gediztso.org.tr
144. www.genckalecikliler.com
145. www.geredeliler.com
146. www.geredetso.org.tr
147. www.guzeltepemahallesi.com
148. www.hatso.org.tr
149. www.hopatso.org.tr
150. www.kadirlitb.tobb.org.tr
151. www.karssusuzkayadibi.com
152. www.kilispolateliosb.org.tr
153. www.kilistso.org.tr
154. www.kilistso.tobb.org.tr
155. www.kirsehirtb.org.tr
156. www.kutbo.org.tr
157. www.masuder.org.tr
158. www.mustso.org.tr
159. www.muttso.org.tr
160. www.nazillitb.org.tr
161. www.nigdetb.org.tr
162. www.nitso.org.tr
163. www.odemisto.org.tr
164. www.oguzeliosb.org.tr
165. www.probase.com.tr
166. www.reyhanlitb.org.tr
167. www.sorguntso.org.tr
168. www.sto.org.tr
169. www.sungurlutb.org.tr
170. www.tarsustb.tobb.org.tr
171. www.tekmarglobal.com
172. www.termetb.org.tr
173. www.termetso.org.tr
174. www.yuksekovatso.org.tr
175. www.ziletb.org.tr
176. ytso.site.probase.com.tr
177. yuksekovatso.org.tr
178. ziletb.org.tr

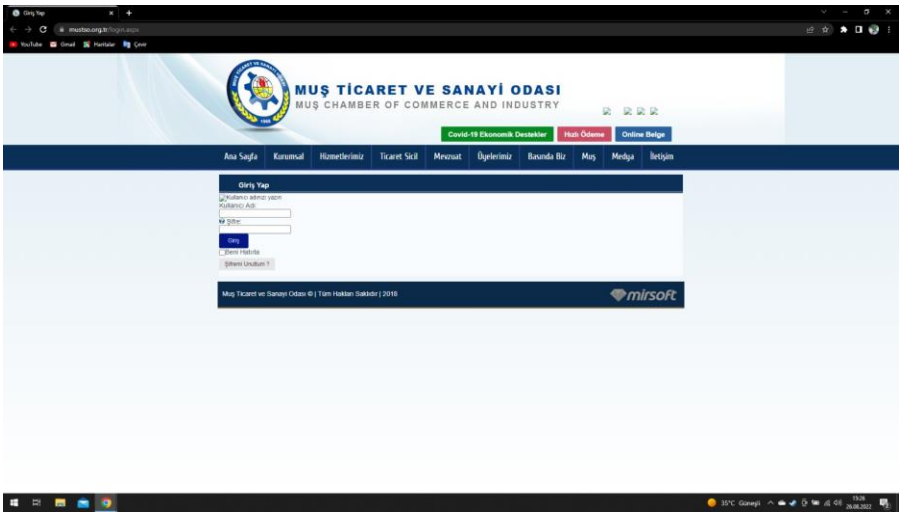
Mustso.gov.tr sayfasini yeniledikce bu hatayi bazen aliyorduk zaafiyet olarak gosterilebilir:



Giriş Sayfası: https://www.mustso.org.tr/login.aspx

Captcha: **Bir anti-spam aracı olarak oldukça etkilidir.** Ücretsizdir, kurulumu kolaydır ve web sitelerine 3 alanda ekstra bir güvenlik katmanı sağlar: Web sitesi kaydını işe yaramaz bilgiler ve bot hesapları almaktan korumak. Reklam ve istenmeyen mesajlar şeklinde yorum spam'ini önlemek.

Muş TSO'de **login.aspx** sayfasında **captcha** kullanmadından dolayı bu eksikliği zaafiyet olarak gosterilebilir ve bu zaafiyetin düzeltilemsi gerekiyor. Bizi captcha kullanımı öneriyoruz.



Bitiş: