

---

# Proyecto de Footprinting

AUDI

12 de Mayo del 2024

---

Jose Almirón López



---

# Índice

<b>1. Objetivo del documento.....</b>	<b>2</b>
<b>2. Información básica de la empresa.....</b>	<b>3</b>
<b>3. Infraestructura y reconocimiento DNS.....</b>	<b>3</b>
3.1. Rangos de redes descubiertos.....	3
3.2. Equipos descubiertos.....	4
3.3. Nombres de dominios y subdominios encontrados.....	8
3.4. Servidores de correo.....	17
3.5. Servidores de nombres.....	19
<b>4. Reconocimiento Web.....</b>	<b>25</b>
4.1. Reconocimiento manual del código.....	26
4.2. Hacking con buscadores.....	29
4.3. Análisis de ficheros.....	33
<b>5. Información personal y leaks.....</b>	<b>34</b>
5.1. Empleados.....	34
5.2. Contactos encontrados.....	37
<b>6. Conclusiones.....</b>	<b>37</b>

---

# 1. Objetivo del documento

Este informe tiene como objetivo realizar un estudio de footprinting o reconocimiento sobre Audi, una empresa líder en el sector automotriz. El footprinting es un proceso crucial en la evaluación de la seguridad informática que implica la recopilación sistemática de información sobre una red o sistema de información específico. A través de este proceso, se busca identificar activos, recursos, y posibles vulnerabilidades que podrían ser explotadas por terceros malintencionados.

La elección de Audi como objetivo de este informe se fundamenta en varios motivos:

- **Relevancia en la industria:** Audi es una marca de renombre mundial en el sector automotriz, reconocida por su innovación y tecnología avanzada en la fabricación de vehículos. Esta relevancia la convierte en un objetivo atractivo para posibles ataques cibernéticos, lo que resalta la importancia de evaluar su postura de seguridad.
- **Tecnología integrada:** Los vehículos modernos de Audi están equipados con una amplia gama de tecnologías informáticas y de comunicación, desde sistemas de entretenimiento hasta sistemas de asistencia al conductor. Explorar la infraestructura tecnológica de Audi permite comprender mejor los desafíos de seguridad asociados con la interconexión de dispositivos en el contexto de la industria automotriz.
- **Conciencia de ciberseguridad:** En un momento en que la ciberseguridad en el sector automotriz es una preocupación creciente, realizar una evaluación de seguridad en una empresa de renombre como Audi proporciona información valiosa sobre las posibles vulnerabilidades y amenazas que enfrenta la industria en general.
- **Énfasis en la responsabilidad ética:** Es fundamental destacar que este informe se realiza con un enfoque ético y responsable. La elección de Audi como objetivo subraya la importancia de llevar a cabo evaluaciones de seguridad de manera ética, sin comprometer la integridad de la empresa ni la privacidad de sus clientes.

---

## 2. Información básica de la empresa

En este informe, explicaremos información básica sobre esta empresa.

- **Nombre completo de la empresa:** Audi AG
- **Horario de apertura:** El horario de apertura de las sedes de Audi puede variar según la ubicación específica. Por ejemplo, la sede más cercana tiene un horario de atención al público de 10:00 a 14:00 y de 16:00 a 20:00
- **Dirección completa:** La sede central de Audi AG se encuentra en Ingolstadt, Alemania. Otras ubicaciones de Audi incluyen Audi Alemania, Audi Bruselas, Audi México, Audi Hungría, Audi China, Audi do Brasil, Audi India, Audi Eslovaquia, Audi España, Audi Rusia, entre otros.
- **Razón social:** Audi AG
- **CIF:** DE0006757008
- **Forma jurídica:** Aktiengesellschaft (AG) - que se traduce como "sociedad anónima" en español.

## 3. Infraestructura y reconocimiento DNS

### 3.1. Rangos de redes descubiertos

La red descubierta abarca desde 143.164.0.0 hasta 143.164.255.255.

```
(jose@kali)-[~]  
$ whois NET-AUDI -h whois.ripe.net | grep inetnum  
inetnum:      143.164.0.0 - 143.164.255.255
```

## 3.2. Equipos descubiertos

Utilizando el rango de direcciones IP obtenido, llevamos a cabo una búsqueda inversa que nos proporciona los nombres de los equipos junto con sus direcciones IP correspondientes.

```
└─$ dnsrecon -r 143.164.0.0-143.164.255.255 -t rv1 -d audi
[*] Performing Reverse Lookup from 143.164.0.0 to 143.164.255.255
[+] PTR dataproxy3.dev2.audi.de 143.164.47.49
[+] PTR dataproxy4.dev2.audi.de 143.164.47.50
[+] PTR dataproxy1.dev2.audi.de 143.164.47.47
[+] PTR dataproxy5.dev2.audi.de 143.164.47.51
[+] PTR dataproxy2.dev2.audi.de 143.164.47.48
[+] PTR kafka2.prod1.audi.de 143.164.47.72
[+] PTR kafka3.prod1.audi.de 143.164.47.73
[+] PTR kafka1.prod1.audi.de 143.164.47.71
[+] PTR kafka4.prod1.audi.de 143.164.47.74
[+] PTR kdc1.prod1.audi.de 143.164.47.80
[+] PTR kdc2.prod1.audi.de 143.164.47.81
[+] PTR kafka2.preprod1.audi.de 143.164.47.104
[+] PTR kafka1.preprod1.audi.de 143.164.47.103
[+] PTR kafka3.preprod1.audi.de 143.164.47.105
[+] PTR kdc1.preprod1.audi.de 143.164.47.111
[+] PTR kdc2.preprod1.audi.de 143.164.47.112
[+] PTR a57ulweb1b01.audi.de 143.164.97.1
[+] PTR irfwweb01.audi.de 143.164.97.3
[+] PTR n10h1web1b01.audi.de 143.164.97.2
[+] PTR irfwweb02.audi.de 143.164.97.4
[+] PTR irfwweb02n10-9.audi.de 143.164.97.6
[+] PTR irfwweb01a57-9.audi.de 143.164.97.5
[+] PTR aria.audi.de 143.164.97.215
[+] PTR shop.audi.de 143.164.97.213
[+] PTR shop-prelive.audi.de 143.164.97.212
[+] PTR extranet.audi.de 143.164.97.216
[+] PTR is0544.audi.de 143.164.97.217
[+] PTR is0542.audi.de 143.164.97.219
[+] PTR gebrauchtwagen.audi.de.164.143.in-addr.arpa 143.164.97.222
[+] PTR www.audi-a4.com 143.164.97.218
[+] PTR is0550.audi.de 143.164.97.221
[+] PTR is0548.audi.de 143.164.97.223
[+] PTR www.audi-fan.com 143.164.97.220
[+] PTR www.do-not-open.com 143.164.97.224
[+] PTR is0389.audi.de 143.164.97.228
```

```
[+] PTR is0532.audi.de 143.164.97.225
[+] PTR is0390.audi.de 143.164.97.227
[+] PTR www.audi-fan.de.164.143.in-addr.arpa 143.164.97.226
[+] PTR is0388.audi.de 143.164.97.229
[+] PTR is0387.audi.de 143.164.97.230
[+] PTR is0386.audi.de 143.164.97.231
[+] PTR is0385.audi.de 143.164.97.232
[+] PTR is0383.audi.de 143.164.97.234
[+] PTR is0384.audi.de 143.164.97.233
[+] PTR www.audi-tt.com 143.164.97.235
[+] PTR www.audi-partner.de 143.164.97.239
[+] PTR www.audi.hu 143.164.97.237
[+] PTR www.audi-servicenete.de 143.164.97.238
[+] PTR is0374.audi.de 143.164.97.241
[+] PTR www.audi.com 143.164.97.240
[+] PTR www.audi-marketing.com 143.164.97.236
[+] PTR is0369.audi.de 143.164.97.246
[+] PTR www-prelive.audi.de 143.164.97.247
[+] PTR is0370.audi.de 143.164.97.245
[+] PTR is0371.audi.de 143.164.97.244
[+] PTR is0372.audi.de 143.164.97.243
[+] PTR is0373.audi.de 143.164.97.242
[+] PTR konfigurator.audi.de 143.164.97.250
[+] PTR listen.audi.de 143.164.97.248
[+] PTR wap.audi.de 143.164.97.252
[+] PTR www.audi-allroad-quattro.com 143.164.97.251
[+] PTR www.audi-a2.com 143.164.97.249
[+] PTR www.sommerkonzerte.de 143.164.97.253
[+] PTR www.audi.de 143.164.97.254
[+] PTR irfwweb01a57-7.audi.de 143.164.98.3
[+] PTR irfwweb01.audi.de 143.164.98.1
[+] PTR irfwweb02.audi.de 143.164.98.2
[+] PTR irfwweb02n10-7.audi.de 143.164.98.4
[+] PTR irfwweb07.audi.de 143.164.98.5
[+] PTR is0353.audi.de 143.164.98.117
[+] PTR is0569.audi.de 143.164.98.116
[+] PTR is0352.audi.de 143.164.98.118
[+] PTR is0596.audi.de 143.164.98.120
[+] PTR is0595.audi.de 143.164.98.121
[+] PTR is0335.audi.de 143.164.98.123
[+] PTR is0597.audi.de 143.164.98.119
[+] PTR is0591.audi.de 143.164.98.122
[+] PTR is0334.audi.de 143.164.98.124
[+] PTR is0333.audi.de 143.164.98.125
[+] PTR irfwweb01.audi.de 143.164.98.129
```

```
[+] PTR is0332.audi.de 143.164.98.126
[+] PTR irfwweb07.audi.de 143.164.98.133
[+] PTR irfwweb02.audi.de 143.164.98.130
[+] PTR irfwweb01a57-8.audi.de 143.164.98.131
[+] PTR irfwweb02n10-8.audi.de 143.164.98.132
[+] PTR ihwc01.audi.de 143.164.98.139
[+] PTR ihwc02.audi.de 143.164.98.140
[+] PTR ihwc03.audi.de 143.164.98.141
[+] PTR ihwc04.audi.de 143.164.98.142
[+] PTR is0347.audi.de 143.164.98.249
[+] PTR mailgate.audi.de 143.164.98.252
[+] PTR is0394.audi.de 143.164.98.251
[+] PTR is0346.audi.de 143.164.98.250
[+] PTR mail.ve-carnect.audi-online.de 143.164.99.67
[+] PTR ve-carnect.audi-online.de 143.164.99.66
[+] PTR irwebn10.audi.de 143.164.99.130
[+] PTR irweba57.audi.de 143.164.99.129
[+] PTR inzurt02a57--hsa.audi.de 143.164.99.131
[+] PTR irfwweb01.audi.de 143.164.99.133
[+] PTR irwebn10-5.audi.de 143.164.99.132
[+] PTR irfwweb01a57-6.audi.de 143.164.99.135
[+] PTR irfwweb02n10-6.audi.de 143.164.99.136
[+] PTR irfwweb02.audi.de 143.164.99.134
[+] PTR vpn-test-1.audi.de 143.164.99.167
[+] PTR vpn-test-2.audi.de 143.164.99.169
[+] PTR inzurt02a57-ql-ge0-3-0.audi.de 143.164.99.217
[+] PTR irwebn10.audi.de 143.164.99.218
[+] PTR irviag.audi.de 143.164.99.225
[+] PTR irweba57.audi.de 143.164.99.226
[+] PTR irviag.audi.de 143.164.99.233
[+] PTR irwebn10.audi.de 143.164.99.234
[+] PTR inzurt02a57--hsp.audi.de 143.164.99.239
[+] PTR irwebn10.audi.de 143.164.99.242
[+] PTR iruunet.audi.de 143.164.99.241
[+] PTR iruunet.audi.de 143.164.99.249
[+] PTR irweba57.audi.de 143.164.99.250
[+] PTR pre-akamai-www.audi.com 143.164.100.160
[+] PTR pre-akamai-cms.audi.com 143.164.100.162
[+] PTR www.audi-mynet.de 143.164.100.179
[+] PTR ak-edit.audi.de 143.164.100.195
[+] PTR ak4-es.audi.de 143.164.100.203
[+] PTR ns.audi.de 143.164.100.253
[+] PTR ns2.audi.de 143.164.100.254
[+] PTR webprx1.audi.de 143.164.102.13
[+] PTR mailin3.audi.de 143.164.102.17
```

```
[+] PTR webprx2.audi.de 143.164.102.14
[+] PTR mailin4.audi.de 143.164.102.18
[+] PTR mailin7.audi.de 143.164.102.23
[+] PTR mailin8.audi.de 143.164.102.24
[+] PTR mailin5.audi.de 143.164.102.19
[+] PTR mailin6.audi.de 143.164.102.20
[+] PTR mailin11.audi.de 143.164.102.58
[+] PTR mailin10.audi.de 143.164.102.59
[+] PTR mailin12.audi.de 143.164.102.57
[+] PTR mailin14.audi.de 143.164.102.55
[+] PTR mailin13.audi.de 143.164.102.56
[+] PTR www.audi-partner.de 143.164.247.2
[+] PTR www.audi.hu 143.164.247.1
[+] PTR www.sommerkonzerte.de 143.164.247.3
[+] PTR shop.audi.de 143.164.247.5
[+] PTR www.audi-tt.com 143.164.247.4
[+] PTR www.audi.de 143.164.247.7
[+] PTR www.audi-tt.de 143.164.247.6
[+] PTR web10.audi.de 143.164.247.10
[+] PTR www.audi.com 143.164.247.8
[+] PTR web11.audi.de 143.164.247.11
[+] PTR extranet.audi.de 143.164.247.12
[+] PTR www.audi-marketing.com 143.164.247.9
[+] PTR aria.audi.de 143.164.247.13
[+] PTR web17.audi.de 143.164.247.17
[+] PTR www.audi-a2.com 143.164.247.14
[+] PTR web18.audi.de 143.164.247.18
[+] PTR web16.audi.de 143.164.247.16
[+] PTR www.audi-a4.com 143.164.247.21
[+] PTR web22.audi.de 143.164.247.22
[+] PTR web31.audi.de 143.164.247.31
[+] PTR web30.audi.de 143.164.247.30
[+] PTR web32.audi.de 143.164.247.32
[+] PTR www.audi-servicenet.de 143.164.247.53
[+] PTR www.audi-allroad-quattro.com 143.164.247.51
[+] PTR konfigurator.audi.de 143.164.247.54
[+] PTR wap.audi.de 143.164.247.52
[+] PTR www.do-not-open.com 143.164.247.57
[+] PTR gate5.audi.de 143.164.248.5
[+] PTR gate4.audi.de 143.164.248.4
[+] PTR gate2.audi.de 143.164.249.1
[+] PTR gate3.audi.de 143.164.249.2
[+] PTR gate15.audi.de 143.164.249.66
[+] PTR gate16.audi.de 143.164.249.67
[+] PTR gate1.audi.de 143.164.249.254
```



## 3.3. Nombres de dominios y subdominios encontrados

Los nombres de dominio de nivel superior (TLD) encontrados son los siguientes

```
└─$ dnsrecon -t tld -d audi
[*] tld: Performing TLD Brute force Enumeration against audi...
[*] The operation could take up to: 00:08:13
[+]      A audi.cymru 64.190.63.222
[+]      A audi.live 198.148.126.56
[+]      A site.my.box 34.232.152.68
[+]      A site.my.box 52.20.143.163
[+]      A site.my.box 3.221.134.22
[+]      A site.my.box 18.215.42.147
[+]      A audi.barcelona 31.214.178.54
[+]      A audi.krd 104.21.75.33
[+]      A audi.krd 172.67.210.154
[+]      AAAA audi.krd 2606:4700:3035::ac43:d29a
[+]      AAAA audi.krd 2606:4700:3030::6815:4b21
[+]      A audi.paris 185.43.62.20
[+]      A audi.yokohama 150.95.255.38
[+]      A audi.stream 213.155.69.214
[+]      AAAA audi.stream 2001:780:205:0:213:155:69:214
[+]      A audi.link 44.227.76.166
[+]      A audi.link 44.227.65.245
[+]      A audi.kaufen 192.166.192.19
[+]      A 77980.bodis.com 199.59.243.225
[+]      A audi.video 46.23.69.44
[+]      A audi.fashion 15.197.162.184
[+]      A audi.yoga 3.33.130.190
[+]      A audi.yoga 15.197.148.33
[+]      A audi.xyz 76.223.54.146
[+]      A audi.xyz 13.248.169.48
[+]      A audi.vegas 15.197.148.33
[+]      A audi.vegas 3.33.130.190
[+]      A audi.fun 98.124.224.17
[+]      A audi.ceo 45.87.158.7
[+]      A audi.music 127.0.53.53
[+]      A audi.tokyo 150.95.255.38
[+]      A audi.one 192.64.119.80
[+]      A audi.arab 127.0.53.53
```

```
[+] A audi.xn--ngbrx 127.0.53.53
[+] A audi.bar 91.189.114.22
[+] A audi.nyc 52.33.207.7
[+] A audi.nyc 44.230.85.241
[+] A audi.org 3.33.130.190
[+] A audi.org 15.197.148.33
[+] A audi.sexy 109.234.111.119
[+] A audi.jobs 143.164.101.227
[+] A audi.ovh 144.217.153.176
[+] A audi.global 3.64.163.50
[+] A audi.xn--kput3i 47.57.12.156
[+] A audi.swiss 37.153.81.16
[+] A audi.com 143.164.101.69
[+] A audi.wales 64.190.63.222
[+] A audi.xn--mxtqlm 127.0.53.53
[+] A audi.party 3.64.163.50
[+] A audi.haus 199.83.62.140
[+] A audi.motorcycles 3.64.163.50
[+] A audi.ruhr 217.160.0.61
[+] AAAA audi.ruhr 2001:8d8:100f:f000::290
[+] A audi.ing 64.190.63.222
[+] A audi.cyou 172.67.197.153
[+] A audi.cyou 104.21.36.169
[+] AAAA audi.cyou 2606:4700:3033::6815:24a9
[+] A audi.tel 195.253.75.107
[+] A audi.tech 76.223.54.146
[+] A audi.tech 13.248.169.48
[+] A audi.cat 216.185.152.151
[+] A audi.miami 3.33.130.190
[+] A audi.miami 15.197.148.33
[+] A audi.cam 162.144.4.132
[+] A audi.xn--vuq861b 45.120.243.27
[+] AAAA audi.xn--vuq861b 2402:7d80:fffc::27
[+] A audi.best 104.21.24.11
[+] A audi.best 172.67.215.72
[+] AAAA audi.best 2606:4700:3033::6815:180b
[+] AAAA audi.best 2606:4700:3037::ac43:d748
[+] A audi.asia 143.164.100.183
[+] A audi.click 217.160.0.171
[+] AAAA audi.click 2001:8d8:100f:f000::214
[+] A audi.melbourne 202.124.241.178
[+] A audi.monster 172.67.182.203
[+] A audi.monster 104.21.32.42
[+] AAAA audi.monster 2606:4700:3033::ac43:b6cb
[+] AAAA audi.monster 2606:4700:3030::6815:202a
```

```
[+]      A audi.moscow 194.58.112.165
[+]      AAAA audi.moscow 2a00:f940:4::152
[+]      A audi.alsace 143.164.101.227
[+]      A audi.dev 217.70.184.38
[+]      A audi.repair 109.234.111.119
[+]      A audi.ac 143.164.101.227
[+]      A audi.af 143.164.101.227
[+]      A audi.ag 143.164.101.227
[+]      A audi.ai 143.164.101.227
[+]      A audi.al 212.183.88.29
[+]      A audi.al 212.183.88.30
[+]      A audi.am 143.164.101.67
[+]      A audi.as 143.164.101.227
[+]      A audi.au 165.160.13.20
[+]      A audi.au 165.160.15.20
[+]      A audi.at 212.183.88.30
[+]      A audi.at 212.183.88.29
[+]      A audi.az 104.21.30.171
[+]      A audi.az 172.67.173.119
[+]      AAAA audi.az 2606:4700:3035::ac43:ad77
[+]      AAAA audi.az 2606:4700:3035::6815:1eab
[+]      A audi.ba 212.183.88.30
[+]      A audi.ba 212.183.88.29
[+]      A audi.bb 143.164.101.173
[+]      A audi.be 193.53.139.84
[+]      A audi.bg 212.183.88.29
[+]      A audi.bg 212.183.88.30
[+]      A audi.bi 143.164.101.227
[+]      A audi.bo 143.164.101.67
[+]      A audi.bs 143.164.101.227
[+]      A audi.by 143.164.101.67
[+]      A audi.ca 143.164.101.67
[+]      A audi.cc 3.33.152.147
[+]      A audi.cc 15.197.142.173
[+]      A audi.bz 143.164.101.227
[+]      A audi.cd 143.164.101.227
[+]      A audi.cg 143.164.101.227
[+]      A audi.cf 143.164.101.227
[+]      A audi.ch 143.164.101.67
[+]      A audi.ci 143.164.101.227
[+]      A audi.cl 212.183.88.29
[+]      A audi.cl 212.183.88.30
[+]      A audi.cm 143.164.101.227
[+]      A audi.co 212.183.88.29
[+]      A audi.co 212.183.88.30
```

---

```
[+] A audi.cu 143.164.101.227
[+] A audi.cw 184.28.224.43
[+] A audi.cx 143.164.101.227
[+] A audi.cz 212.183.88.30
[+] A audi.cz 212.183.88.29
[+] A audi.de 143.164.101.67
[+] A audi.dj 143.164.101.227
[+] A audi.dk 143.164.101.67
[+] A audi.dm 143.164.101.227
[+] A audi.ee 143.164.101.67
[+] A audi.es 143.164.101.67
[+] A audi.fi 143.164.101.67
[+] A audi.fm 143.164.101.227
[+] A audi.fr 143.164.101.67
[+] A audi.gd 143.164.101.227
[+] A audi.gf 143.164.101.67
[+] A audi.ge 91.212.213.32
[+] A audi.gg 143.164.101.227
[+] A audi.cn 123.56.6.133
[+] A audi.gp 143.164.101.67
[+] A audi.gr 143.164.101.67
[+] A audi.gs 143.164.101.227
[+] A audi.gy 143.164.101.227
[+] A audi.hn 143.164.101.67
[+] A audi.hr 212.183.88.30
[+] A audi.hr 212.183.88.29
[+] A audi.gm 143.164.101.227
[+] A audi.hu 195.228.75.127
[+] A audi.ie 143.164.101.67
[+] A audi.im 143.164.101.227
[+] A audi.in 143.164.101.67
[+] A audi.io 143.164.101.227
[+] A audi.is 143.164.101.67
[+] A audi.it 143.164.101.67
[+] A audi.ir 143.164.101.227
[+] A audi.je 143.164.101.227
[+] A audi.jo 143.164.101.227
[+] A audi.kg 143.164.101.227
[+] A audi.hm 143.164.101.227
[+] A audi.ki 143.164.101.227
[+] A audi.kn 143.164.101.227
[+] A audi.la 143.164.101.227
[+] A audi.ky 107.180.100.15
[+] A audi.lc 143.164.101.67
[+] A audi.kz 194.39.65.2
```

```
[+] AAAA audi.kz 2a00:5da0:1000::151
[+] A audi.lk 143.164.101.67
[+] A audi.lt 143.164.101.67
[+] A audi.lu 143.164.101.67
[+] A audi.jp 52.198.232.1
[+] A audi.ly 143.164.101.227
[+] A audi.lv 143.164.101.67
[+] A audi.ma 143.164.101.67
[+] A audi.md 143.164.101.67
[+] A audi.mg 143.164.101.227
[+] A audi.me 212.183.88.29
[+] A audi.me 212.183.88.30
[+] A audi.mk 212.183.88.30
[+] A audi.mk 212.183.88.29
[+] A audi.mn 143.164.101.227
[+] A audi.ml 143.164.101.227
[+] A audi.ms 143.164.101.227
[+] A audi.mq 143.164.101.227
[+] A audi.mu 143.164.101.227
[+] A audi.mp 143.164.101.227
[+] A audi.my 185.116.31.150
[+] A audi.mw 162.210.102.212
[+] A audi.mx 143.164.100.200
[+] A audi.nf 143.164.101.227
[+] A audi.no 143.164.101.67
[+] A audi.nl 143.164.101.67
[+] A audi.ng 143.164.101.227
[+] A audi.mv 143.164.101.227
[+] A audi.ph 143.164.101.67
[+] A audi.pk 143.164.101.67
[+] A audi.pl 143.164.101.67
[+] A audi.pm 143.164.101.227
[+] A audi.pn 143.164.101.227
[+] A audi.ps 143.164.101.227
[+] A audi.pt 212.183.88.30
[+] A audi.pt 212.183.88.29
[+] A audi.nr 143.164.101.227
[+] A audi.pw 143.164.101.227
[+] A audi.pr 143.164.101.227
[+] A audi.re 213.186.33.5
[+] A audi.rs 212.183.88.29
[+] A audi.rs 212.183.88.30
[+] A audi.ro 212.183.88.29
[+] A audi.ro 212.183.88.30
[+] A audi.ru 143.164.101.67
```

```
[+] A audi.sa 143.164.101.227
[+] A audi.sc 143.164.101.227
[+] A audi.rw 143.164.101.227
[+] A audi.sd 143.164.101.227
[+] A audi.si 212.183.88.30
[+] A audi.si 212.183.88.29
[+] A audi.se 143.164.101.67
[+] A audi.sh 143.164.101.227
[+] A audi.sk 212.183.88.30
[+] A audi.sk 212.183.88.29
[+] A audi.so 143.164.101.227
[+] A audi.sl 143.164.101.227
[+] A audi.sn 143.164.101.227
[+] A audi.sr 143.164.101.227
[+] A audi.td 143.164.101.227
[+] A audi.tf 143.164.101.227
[+] A audi.st 143.164.101.227
[+] A audi.tj 143.164.101.227
[+] A audi.tl 143.164.101.227
[+] A audi.tk 143.164.101.227
[+] A audi.tc 143.164.101.227
[+] A audi.to 143.164.101.227
[+] A audi.tn 143.164.101.173
[+] A audi.tm 143.164.101.227
[+] A audi.tg 143.164.101.227
[+] A audi.tt 143.164.101.67
[+] A audi.tv 143.164.101.227
[+] A audi.ug 143.164.101.227
[+] A audi.uk 3.33.139.32
[+] A audi.us 67.199.248.13
[+] A audi.vc 143.164.101.227
[+] A audi.uz 80.80.218.172
[+] A audi.tw 61.221.12.104
[+] A audi.vg 143.164.101.227
[+] A audi.vu 143.164.101.227
[+] A audi.ua 212.183.88.30
[+] A audi.ua 212.183.88.29
[+] A audi.vn 143.164.101.67
[+] A audi.xn--node 188.93.95.11
[+] A audi.fi.fit 3.64.163.50
[+] A audi.la.tips 13.248.169.48
[+] A audi.la.tips 76.223.54.146
[+] A 77980.bodis.com 199.59.243.225
[+] A audi.ls.mortgage 91.195.240.94
[+] A audi.my.catering 72.52.179.175
```

```
[+]      A audi.pr.health 3.64.163.50
[+]      A audi.us.center 3.64.163.50
[+]      A audi.vc.whoswho 82.196.14.243
[+] 265 Records Found
```

Se han identificado los siguientes subdominios:

```
└─$ fierce --domain audi.com
NS: ns2.audi.de. ns5.xc-ns.de.
SOA: ns2.audi.de. (143.164.100.254)
Zone: failure
Wildcard: failure
Found: access.audi.com. (199.5.50.33)
Nearby:
{'199.5.50.33': 'sip.audi.ca.',
'199.5.50.34': 'webconf.electrifyamerica.com.',
'199.5.50.35': 'av.vw.com.',
'199.5.50.36': 'access.gtb-procurement.com.',
'199.5.50.37': 'webconf.gtb-procurement.com.',
'199.5.50.38': 'av.volkswagen.ca.'}
Found: akamai.audi.com. (143.164.100.213)
Found: av.audi.com. (199.5.50.35)
Nearby:
{'199.5.50.39': 'access.audi.ca.'}
Found: blog.audi.com. (195.93.201.191)
Nearby:
{'195.93.201.193': 'secure.gil.kundenserver42.de.'}
Found: commerce.audi.com. (207.173.193.19)
Found: contact.audi.com. (161.71.33.242)
Nearby:
{'161.71.33.237': 'gx237.mta.exacttarget.com.',
'161.71.33.238': 'gx238.mta.exacttarget.com.',
'161.71.33.239': 'gx239.mta.exacttarget.com.',
'161.71.33.240': 'gx240.mta.exacttarget.com.',
'161.71.33.241': 'gx241.mta.exacttarget.com.',
'161.71.33.242': 'reply.s50.exacttarget.com.',
'161.71.33.243': 'manage.s50.exacttarget.com.',
'161.71.33.244': 'cloud.straps1-sfmctest.com.',
'161.71.33.245': 'gx245.mta.exacttarget.com.',
'161.71.33.246': 'mon-s50.monitor.marketingcloud.com.',
'161.71.33.247': 'user-content.s50.sfmcontent.com.'}
Found: crs.audi.com. (199.5.55.137)
Found: dc.audi.com. (63.140.62.27)
Nearby:
{'63.140.62.22': 'ip-63-140-62-22.data.adobedc.net.',
```

```
'63.140.62.23': 'ip-63-140-62-23.data.adobedc.net.',
'63.140.62.24': 'ip-63-140-62-24.data.adobedc.net.',
'63.140.62.25': 'ip-63-140-62-25.data.adobedc.net.',
'63.140.62.26': 'ip-63-140-62-26.data.adobedc.net.',
'63.140.62.27': 'ip-63-140-62-27.data.adobedc.net.',
'63.140.62.28': 'ip-63-140-62-28.data.adobedc.net.',
'63.140.62.29': 'ip-63-140-62-29.data.adobedc.net.',
'63.140.62.30': 'ip-63-140-62-30.data.adobedc.net.',
'63.140.62.31': 'ip-63-140-62-31.data.adobedc.net.',
'63.140.62.32': 'ip-63-140-62-32.data.adobedc.net.}'
Found: developer.audi.com. (121.36.157.125)
Nearby:
{'121.36.157.120': 'ecs-121-36-157-120.compute.hwclouds-dns.com.',
'121.36.157.121': 'ecs-121-36-157-121.compute.hwclouds-dns.com.',
'121.36.157.122': 'ecs-121-36-157-122.compute.hwclouds-dns.com.',
'121.36.157.123': 'ecs-121-36-157-123.compute.hwclouds-dns.com.',
'121.36.157.124': 'ecs-121-36-157-124.compute.hwclouds-dns.com.',
'121.36.157.125': 'ecs-121-36-157-125.compute.hwclouds-dns.com.',
'121.36.157.126': 'ecs-121-36-157-126.compute.hwclouds-dns.com.',
'121.36.157.127': 'ecs-121-36-157-127.compute.hwclouds-dns.com.',
'121.36.157.128': 'ecs-121-36-157-128.compute.hwclouds-dns.com.',
'121.36.157.129': 'ecs-121-36-157-129.compute.hwclouds-dns.com.',
'121.36.157.130': 'ecs-121-36-157-130.compute.hwclouds-dns.com.}'
Found: download.audi.com. (18.198.83.150)
Nearby:
{'18.198.83.145': 'ec2-18-198-83-145.eu-central-1.compute.amazonaws.com.',
'18.198.83.146': 'ec2-18-198-83-146.eu-central-1.compute.amazonaws.com.',
'18.198.83.147': 'ec2-18-198-83-147.eu-central-1.compute.amazonaws.com.',
'18.198.83.148': 'ec2-18-198-83-148.eu-central-1.compute.amazonaws.com.',
'18.198.83.149': 'ec2-18-198-83-149.eu-central-1.compute.amazonaws.com.',
'18.198.83.150': 'ec2-18-198-83-150.eu-central-1.compute.amazonaws.com.',
'18.198.83.151': 'ec2-18-198-83-151.eu-central-1.compute.amazonaws.com.',
'18.198.83.152': 'ec2-18-198-83-152.eu-central-1.compute.amazonaws.com.',
'18.198.83.153': 'ec2-18-198-83-153.eu-central-1.compute.amazonaws.com.',
'18.198.83.154': 'ec2-18-198-83-154.eu-central-1.compute.amazonaws.com.',
'18.198.83.155': 'ec2-18-198-83-155.eu-central-1.compute.amazonaws.com.}'
Found: ecommerce.audi.com. (199.5.47.123)
Nearby:
{'199.5.47.125': 'st_qa.vw.com.', '199.5.47.126': 'vwcourtsettlements.com.}'
Found: europe.audi.com. (192.229.202.3)
Found: extranet.audi.com. (199.5.55.142)
Found: feedback.audi.com. (81.169.188.180)
Nearby:
{'81.169.188.176': 'concept-rs.de.',
'81.169.188.177': 'h2928748.stratoserver.net.',
```



```
'81.169.188.179': 'h2809758.stratoserver.net.',
'81.169.188.181': 'vps000.niemann.com.de.',
'81.169.188.182': 'h3003773.stratoserver.net.',
'81.169.188.183': 'h2992689.stratoserver.net.',
'81.169.188.184': 'h2834229.stratoserver.net.',
'81.169.188.185': 'mail-lines.com.')}
Found: login.audi.com. (108.157.125.93)
Nearby:
{'108.157.125.88': 'server-108-157-125-88.mad53.r.cloudfront.net.',
'108.157.125.89': 'server-108-157-125-89.mad53.r.cloudfront.net.',
'108.157.125.90': 'server-108-157-125-90.mad53.r.cloudfront.net.',
'108.157.125.91': 'server-108-157-125-91.mad53.r.cloudfront.net.',
'108.157.125.92': 'server-108-157-125-92.mad53.r.cloudfront.net.',
'108.157.125.93': 'server-108-157-125-93.mad53.r.cloudfront.net.',
'108.157.125.94': 'server-108-157-125-94.mad53.r.cloudfront.net.',
'108.157.125.95': 'server-108-157-125-95.mad53.r.cloudfront.net.',
'108.157.125.96': 'server-108-157-125-96.mad53.r.cloudfront.net.',
'108.157.125.97': 'server-108-157-125-97.mad53.r.cloudfront.net.',
'108.157.125.98': 'server-108-157-125-98.mad53.r.cloudfront.net.')}
Found: mail.audi.com. (13.111.18.27)
Nearby:
{'13.111.18.22': 'orionims.s10.exacttarget.com.',
'13.111.18.23': 'orionsmtp.s10.exacttarget.com.',
'13.111.18.24': 'orionimsw.s10.exacttarget.com.',
'13.111.18.25': 'pages.s10.exacttarget.com.',
'13.111.18.26': 'ej26.mta.exacttarget.com.',
'13.111.18.27': 'ej27.mta.exacttarget.com.',
'13.111.18.28': 'ej28.mta.exacttarget.com.',
'13.111.18.29': 'ej29.exacttarget.com.',
'13.111.18.30': 'pub.s10.sfmctest.com.',
'13.111.18.31': 'sock.s10.exacttarget.com.',
'13.111.18.32': 'view.s10.exacttarget.com.')}
Found: marketplace.audi.com. (13.224.115.80)
Nearby:
{'13.224.115.75': 'server-13-224-115-75.mad50.r.cloudfront.net.',
'13.224.115.76': 'server-13-224-115-76.mad50.r.cloudfront.net.',
'13.224.115.77': 'server-13-224-115-77.mad50.r.cloudfront.net.',
'13.224.115.78': 'server-13-224-115-78.mad50.r.cloudfront.net.',
'13.224.115.79': 'server-13-224-115-79.mad50.r.cloudfront.net.',
'13.224.115.80': 'server-13-224-115-80.mad50.r.cloudfront.net.',
'13.224.115.81': 'server-13-224-115-81.mad50.r.cloudfront.net.',
'13.224.115.82': 'server-13-224-115-82.mad50.r.cloudfront.net.',
'13.224.115.83': 'server-13-224-115-83.mad50.r.cloudfront.net.',
'13.224.115.84': 'server-13-224-115-84.mad50.r.cloudfront.net.',
'13.224.115.85': 'server-13-224-115-85.mad50.r.cloudfront.net.'}
```

```

Found: media.audi.com. (96.16.88.157)
Nearby:
{'96.16.88.152': 'a96-16-88-152.deploy.static.akamaitechnologies.com.',
'96.16.88.153': 'a96-16-88-153.deploy.static.akamaitechnologies.com.',
'96.16.88.154': 'a96-16-88-154.deploy.static.akamaitechnologies.com.',
'96.16.88.155': 'a96-16-88-155.deploy.static.akamaitechnologies.com.',
'96.16.88.156': 'a96-16-88-156.deploy.static.akamaitechnologies.com.',
'96.16.88.157': 'a96-16-88-157.deploy.static.akamaitechnologies.com.',
'96.16.88.158': 'a96-16-88-158.deploy.static.akamaitechnologies.com.',
'96.16.88.159': 'a96-16-88-159.deploy.static.akamaitechnologies.com.',
'96.16.88.160': 'a96-16-88-160.deploy.static.akamaitechnologies.com.',
'96.16.88.161': 'a96-16-88-161.deploy.static.akamaitechnologies.com.',
'96.16.88.162': 'a96-16-88-162.deploy.static.akamaitechnologies.com.'}
Found: my.audi.com. (108.157.125.93)
Found: nokia.audi.com. (143.164.6.159)

```

## 3.4. Servidores de correo

Se han identificado los siguientes servidores de correo

```

(jose@kali)-[~]
└─$ host -t mx audi.com
audi.com mail is handled by 10 mg2.vw.com.
audi.com mail is handled by 10 mg10.vw.com.
audi.com mail is handled by 10 mg7.vw.com.
audi.com mail is handled by 10 mg9.vw.com.
audi.com mail is handled by 10 mg11.vw.com.
audi.com mail is handled by 10 mg1.vw.com.
audi.com mail is handled by 10 mg5.vw.com.
audi.com mail is handled by 10 mg12.vw.com.
audi.com mail is handled by 10 mg6.vw.com.
audi.com mail is handled by 10 mg8.vw.com.
audi.com mail is handled by 50 mg3.vw.com.
audi.com mail is handled by 10 mg4.vw.com.

```

Ahora procederemos a obtener la dirección IP de cada servidor.

```

(jose@kali)-[~]
└─$ host mg2.vw.com
Host mg2.vw.com not found: 3(NXDOMAIN)

(jose@kali)-[~]
└─$ host mg10.vw.com

```

```
mg10.vw.com has address 199.5.47.223

(jose@kali)-[~]
└─$ host mg7.vw.com
mg7.vw.com has address 199.5.47.203

(jose@kali)-[~]
└─$ host mg9.vw.com
mg9.vw.com has address 199.5.47.230

(jose@kali)-[~]
└─$ host mg11.vw.com
mg11.vw.com has address 199.5.47.226

(jose@kali)-[~]
└─$ host mg1.vw.com
Host mg1.vw.com not found: 3 (NXDOMAIN)

(jose@kali)-[~]
└─$ host mg5.vw.com
mg5.vw.com has address 199.5.47.161

(jose@kali)-[~]
└─$ host mg12.vw.com
mg12.vw.com has address 199.5.47.250

(jose@kali)-[~]
└─$ host mg6.vw.com
;; communications error to 100.100.1.1#53: timed out
mg6.vw.com has address 199.5.47.197

(jose@kali)-[~]
└─$ host mg8.vw.com
mg8.vw.com has address 199.5.47.204

(jose@kali)-[~]
└─$ host mg3.vw.com
Host mg3.vw.com not found: 3 (NXDOMAIN)

(jose@kali)-[~]
└─$ host mg4.vw.com
mg4.vw.com has address 199.5.47.158
```

## 3.5. Servidores de nombres

Se han encontrado dos servidores de nombres:

```
(jose@kali)-[~]  
$ host -t ns audi.com  
audi.com name server ns5.xc-ns.de.  
audi.com name server ns2.audi.de.
```

Podemos obtener la ip de estos nombres para profundizar mas sobre ellos

```
(jose@kali)-[~]  
$ host ns5.xc-ns.de  
ns5.xc-ns.de has address 194.50.187.172  
  
(jose@kali)-[~]  
$ host ns2.audi.de  
ns2.audi.de has address 143.164.100.254
```

Vamos a analizar mas detalladamente cada ip

```
$ whois 194.50.187.172  
% This is the RIPE Database query service.  
% The objects are in RPSL format.  
%  
% The RIPE Database is subject to Terms and Conditions.  
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions  
  
% Note: this output has been filtered.  
%       To receive output for a database update, use the "-B" flag.  
  
% Information related to '194.50.187.0 - 194.50.187.255'  
  
% Abuse contact for '194.50.187.0 - 194.50.187.255' is 'info@lapi.net'  
  
inetnum:        194.50.187.0 - 194.50.187.255  
netname:        CentralNic-Anycast-J  
descr:          CentralNic  
descr:          CentralNic Anycast-J IPv4 Allocation
```

```
country:      DE
org:          ORG-GA152-RIPE
admin-c:      CNO4-RIPE
tech-c:       CNO4-RIPE
status:       ASSIGNED PI
mnt-by:       RIPE-NCC-END-MNT
mnt-by:       ONEAPI-MNT
mnt-by:       CENTRALNIC-MNT
created:      2006-04-25T09:26:13Z
last-modified: 2020-12-07T09:27:53Z
source:       RIPE # Filtered

organisation: ORG-GA152-RIPE
org-name:     1api GmbH
country:      DE
org-type:     LIR
address:      Kaiserstraße 172-174
address:      66386
address:      St. Ingbert
address:      GERMANY
phone:        +4968949396760
fax-no:       +4968416984299
abuse-c:      AR14484-RIPE
mnt-ref:      RIPE-NCC-HM-MNT
mnt-ref:      ISPAPI-M
mnt-by:       RIPE-NCC-HM-MNT
mnt-by:       ISPAPI-M
admin-c:      CH3108-RIPE
tech-c:       CH3108-RIPE
created:      2008-01-29T12:34:34Z
last-modified: 2024-01-26T09:17:47Z
source:       RIPE # Filtered

role:         CentralNic Network Operations
address:      CentralNic Ltd
address:      4th Floor, Saddlers House
address:      44 Gutter Lane
address:      London
address:      EC2V 6BR
address:      United Kingdom
org:          ORG-CL213-RIPE
admin-c:      DNS53
admin-c:      CACH3
admin-c:      KA4521-RIPE
admin-c:      JH30387-RIPE
```

```
tech-c:      DNS53
nic-hdl:     CNO4-RIPE
mnt-by:      CENTRALNIC-MNT
created:     2013-04-08T09:10:27Z
last-modified: 2023-01-25T14:22:39Z
source:      RIPE # Filtered
```

```
% Information related to '194.50.187.0/24AS1921'
```

```
route:       194.50.187.0/24
origin:      AS1921
mnt-by:      CENTRALNIC-MNT
created:     2023-09-18T09:19:53Z
last-modified: 2023-09-18T09:19:53Z
source:      RIPE
```

```
% Information related to '194.50.187.0/24AS207021'
```

```
route:       194.50.187.0/24
origin:      AS207021
mnt-by:      CENTRALNIC-MNT
created:     2023-09-18T09:20:09Z
last-modified: 2023-09-18T09:20:09Z
source:      RIPE
```

```
% Information related to '194.50.187.0/24AS212390'
```

```
route:       194.50.187.0/24
origin:      AS212390
mnt-by:      CENTRALNIC-MNT
created:     2020-12-07T09:28:30Z
last-modified: 2020-12-07T09:28:30Z
source:      RIPE # Filtered
```

```
% This query was served by the RIPE Database Query Service version 1.111 (SHETLAND)
```

En este caso, podemos observar que la dirección 194.50.187.172 está asociada a la organización CentralNic, una plataforma de reventa de dominios. Esta dirección pertenece a 1api GmbH, un proveedor de servicios de Internet con sede en Homburg, Alemania. Es posible que esta dirección IP se utilice para servicios relacionados con la gestión de dominios y otros servicios en línea.

```
└─$ whois 143.164.100.254
```

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange:          143.163.0.0 - 143.164.255.255
CIDR:              143.163.0.0/16, 143.164.0.0/16
NetName:           RIPE-ERX-143-163-0-0
NetHandle:         NET-143-163-0-0-1
Parent:            NET143 (NET-143-0-0-0-0)
NetType:           Early Registrations, Transferred to RIPE NCC
OriginAS:
Organization:      RIPE Network Coordination Centre (RIPE)
RegDate:           2003-11-12
Updated:           2003-11-12
Comment:           These addresses have been further assigned to users in
Comment:           the RIPE NCC region. Contact information can be found in
Comment:           the RIPE database at http://www.ripe.net/whois
Ref:               https://rdap.arin.net/registry/ip/143.163.0.0

ResourceLink:      https://apps.db.ripe.net/search/query.html
ResourceLink:      whois.ripe.net

OrgName:           RIPE Network Coordination Centre
OrgId:             RIPE
Address:           P.O. Box 10096
City:              Amsterdam
StateProv:
PostalCode:        1001EB
Country:           NL
RegDate:
Updated:           2013-07-29
Ref:               https://rdap.arin.net/registry/entity/RIPE

ReferralServer:    whois://whois.ripe.net
ResourceLink:      https://apps.db.ripe.net/search/query.html
```

```
OrgAbuseHandle: ABUSE3850-ARIN
OrgAbuseName: Abuse Contact
OrgAbusePhone: +31205354444
OrgAbuseEmail: abuse@ripe.net
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE3850-ARIN

OrgTechHandle: RNO29-ARIN
OrgTechName: RIPE NCC Operations
OrgTechPhone: +31 20 535 4444
OrgTechEmail: hostmaster@ripe.net
OrgTechRef: https://rdap.arin.net/registry/entity/RNO29-ARIN

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

Found a referral to whois.ripe.net.

% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://apps.db.ripe.net/docs/HTML-Terms-And-Conditions

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to '143.164.0.0 - 143.164.255.255'

% No abuse contact registered for 143.164.0.0 - 143.164.255.255

inetnum: 143.164.0.0 - 143.164.255.255
netname: NET-AUDI
descr: Audi AG, Ingolstadt
country: DE
admin-c: AD1626-RIPE
```



```
tech-c:      AD1626-RIPE
status:      LEGACY
mnt-by:      AS12331-MNT
created:     2002-01-02T11:06:54Z
last-modified: 2019-12-04T13:10:29Z
source:      RIPE

role:        Audi Domainservice
address:     Audi AG
address:     D-85045 Ingolstadt
address:     Germany
admin-c:     RZ3093-RIPE
tech-c:      MR2740-RIPE
tech-c:      CS17416-RIPE
nic-hdl:     AD1626-RIPE
mnt-by:      AS12331-MNT
created:     2003-08-11T11:33:12Z
last-modified: 2023-02-22T11:57:47Z
source:      RIPE # Filtered

% Information related to '143.164.0.0/16AS12331'

route:       143.164.0.0/16
descr:       AUDI
origin:      AS12331
mnt-by:      AS12331-MNT
created:     2002-01-02T13:01:38Z
last-modified: 2002-01-02T13:01:38Z
source:      RIPE

% This query was served by the RIPE Database Query Service version 1.111 (SHETLAND)
```

La dirección 143.164.100.254 efectivamente corresponde a la organización de Audi. A simple vista, podemos notar que esta dirección IP se encuentra dentro del rango de direcciones IP que obtuvimos previamente utilizando DNSRecon para los TLD asociados con Audi

## 4. Reconocimiento Web

Podemos comenzar realizando un escaneo de los puertos abiertos en la dirección IP de Audi.com, que en este caso es 143.164.101.69.

```

➔ sudo nmap -sS -sV -sC -A 143.164.101.69
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 13:37 EDT
Nmap scan report for 143.164.101.69
Host is up (0.0021s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  tcpwrapped
|_ http-title: 403 Forbidden
443/tcp   open  tcpwrapped
|_ http-title: 403 Forbidden
|_ ssl-date: TLS randomness does not represent time
|_ ssl-cert: Subject: commonName=audi.de/organizationName=Audi AG/countryName=DE
|_ Subject Alternative Name: DNS:audi.de, DNS:audi.am, DNS:audi.bb, DNS:fr.audi.be, DNS:nl.audi.be, DNS:audi.bo, DNS:audi.ca, DNS:audi.ch, DNS:audi.co.id, DNS:
audi.co.jp, DNS:audi.co.kr, DNS:audi.co.nz, DNS:audi.co.th, DNS:audi.co.uk, DNS:audi.co.za, DNS:audi.com, DNS:audi.com.au, DNS:audi.com.bd, DNS:audi.com.br,
DNS:audi.com.cy, DNS:audi.com.do, DNS:audi.com.ec, DNS:audi.com.gt, DNS:audi.com.ht, DNS:audi.com.kh, DNS:audi.com.mt, DNS:audi.com.mx, DNS:audi.com.my, DNS:
audi.com.pa, DNS:audi.com.pe, DNS:audi.com.pk, DNS:audi.com.py, DNS:audi.com.sg, DNS:audi.com.sv, DNS:audi.com.tr, DNS:audi.com.tt, DNS:audi.com.tw, DNS:audi.
i.com.uy, DNS:audi.com.ve, DNS:audi.dk, DNS:audi.ee, DNS:audi.es, DNS:audi.fi, DNS:audi.fr, DNS:audi.gf, DNS:audi.gp, DNS:audi.hn, DNS:audi.ie,
DNS:audi.in, DNS:audi.it, DNS:audi.lc, DNS:audi.lk, DNS:audi.lt, DNS:audi.lu, DNS:audi.lv, DNS:audi.md, DNS:audi.mu, DNS:audi.nl, DNS:audi.no, DNS:audi.ph, D
NS:audi.pl, DNS:audi.se, DNS:audi.tt, DNS:audi.vn, DNS:audi-abudhabi.com, DNS:audi-bahrain.com, DNS:audi-brunei.com, DNS:audi-brussels.be, DNS:audicanarias.es
, DNS:audi-caymanislands.com, DNS:audi-curacao.com, DNS:audi-dubai.com, DNS:audi-eg.com, DNS:audi-jamaica.com, DNS:audi-jordan.com, DNS:audi-kuwait.com, DNS:au
dilatinomerica.com, DNS:audi-lebanon.com, DNS:audi-me.com, DNS:audi-oman.com, DNS:audi-qatar.com, DNS:audi-saudiarabia.com, DNS:denkwerkstatt.audi, DNS:audi
usa.com, DNS:a2d2.audi, DNS:audi-environmental-foundation.com, DNS:audi-umweltstiftung.de, DNS:progress.audi, DNS:audi-planung.de, DNS:audi-planung.de, DNS:
sommerkonzerte.de, DNS:audi.businessinnovation.de, DNS:audi.businessinnovation.com, DNS:audi.interaction.com, DNS:partneranbindung.audi, DNS:nic.audi
|_ Not valid before: 2024-03-13T00:00:00
|_ Not valid after: 2025-03-17T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.63 ms 143.164.101.69

```

**Puertos Abiertos:** El escaneo detecta que los puertos 80/tcp y 443/tcp están abiertos en el host. Ambos puertos están etiquetados como "tcpwrapped", lo que sugiere que pueden estar protegidos o filtrados por un firewall o algún otro mecanismo de seguridad.

**Servicios:** No se revela ningún servicio específico que se esté ejecutando en los puertos abiertos, aparte de la indicación de que ambos están "tcpwrapped". El título de las páginas web en ambos puertos indica un mensaje "403 Forbidden", lo que sugiere que el acceso está prohibido en estos puertos.

**Certificado SSL:** Se muestra información del certificado SSL en el puerto 443, que parece pertenecer a Audi AG. La lista de Subject Alternative Name en el certificado muestra una amplia gama de dominios asociados con la marca Audi.

**Fechas de Validez del Certificado:** El certificado SSL es válido desde el 13 de marzo de 2024 hasta el 17 de marzo de 2025.

Para determinar qué CMS está utilizando, consulté [WhatCMS.org](https://whatcms.org/), que indica que Audi.com está utilizando Adobe Experience Manager (AEM). AEM es un sistema líder de gestión de contenidos empresariales de Adobe que ofrece una amplia gama de posibilidades de diseño para sitios web corporativos con requisitos complejos.

## What CMS Is This Site Using?

Currently detecting 1540 website powering technologies

✓ Success

JSON

[www.audi.com/en.html](https://www.audi.com/en.html) uses

Category	Software	Version
Other CMS, CMS	<a href="#">Adobe Experience Manager</a>	
Programming Language	<a href="#">Java</a>	
CDN	<a href="#">Azure CDN</a>	

## 4.1. Reconocimiento manual del código

Podemos descargar el código fuente de la página web utilizando herramientas como wget para su análisis local. Alternativamente, podemos emplear otras herramientas específicas o simplemente utilizar la función del navegador que nos permite ver el código fuente con solo presionar Ctrl + U.

```
wget \  
  --recursive \  
  --no-clobber \  
  --page-requisites \  
  --html-extension \  
  --convert-links \  
  --adjust-extension \  
  --output-document=
```

```
--convert-links \  
--restrict-file-names=windows \  
--domains website.org \  
--no-parent \  
https://www.audi.com/en.html
```

```
(kali@kali)-[~]  
$ wget \  
  --recursive \  
  --no-clobber \  
  --page-requisites \  
  --html-extension \  
  --convert-links \  
  --restrict-file-names=windows \  
  --domains website.org \  
  --no-parent \  
  https://www.audi.com/en.html  
Ambos --no-clobber y --convert-links fueron especificados, sólo se usará --convert-links.  
--2024-05-11 12:25:09--  https://www.audi.com/en.html  
Resolviendo www.audi.com (www.audi.com)... 192.229.202.3  
Conectando con www.audi.com (www.audi.com)[192.229.202.3]:443... conectado.  
Petición HTTP enviada, esperando respuesta... 200 OK  
Longitud: 272858 (266K) [text/html]  
Grabando a: «www.audi.com/en.html»  
  
www.audi.com/en.html      100%[=====] 266,46K  979KB/s  en 0,3s  
  
2024-05-11 12:25:45 (979 KB/s) - «www.audi.com/en.html» guardado [272858/272858]  
  
ACABADO --2024-05-11 12:25:46--  
Tiempo total de reloj: 36s  
Descargados: 1 ficheros, 266K en 0,3s (979 KB/s)  
Convirtiendo enlaces en www.audi.com/en.html... 237.  
5-232  
Enlaces convertidos en 1 ficheros en 0,009 segundos.  
  
(kali@kali)-[~]
```

Al examinar el código fuente, podemos identificar la presencia de comentarios. En ocasiones, los desarrolladores incluyen comentarios que pueden proporcionarnos información valiosa y útil para nuestro análisis.

```
34  
35 <!-- config refresh on 1714612388045 -->  
36  
37 <meta property="og:title" content="Audi.com the international Audi website | audi.com"/>  
38 <meta name="twitter:title" content="Audi.com the international Audi website | audi.com"/>  
39  
40 <meta property="og:description" content="Discover Audi as a brand, company and employer on c  
41 <meta name="twitter:description" content="Discover Audi as a brand, company and employer on  
42  
43 <meta property="og:type" content="website"/>  
44 <meta name="twitter:card" content="summary"/>  
45 <meta property="og:url" content="https://www.audi.com/en.html"/>
```

Parece ser una nota para los desarrolladores o administradores del sitio web. El texto "**<!-- config refresh on 1714612388045 -->**" indica que puede estar relacionado con una

actualización de la configuración del sitio. Es posible que este comentario esté vinculado a alguna tarea de mantenimiento o actualización técnica del sitio web de Audi.

```
137
138 </head>
139 <body>
140   <div class="gbp-upnavigation" id="js-gbp-upnavigation">
141     <svg class="gbp-icon gbp-icon-arrow-down" width="48" height="48">
142       <use xlink:href="#arrow-down" width="100%" height="100%" fill="currentColor"></use>
143     </svg>
144   </div -->
145   <div id="js-page" class="gbp-page ">
146     <div id="gbp-svg">
147       <svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink">
148         <symbol id="arrow-down" viewBox="0 0 48 48">
149           <path d="M15.5 19.5L24.5 28.5 33.5 19.5" stroke="currentColor" stroke-width="1" fill="none" fill-rule="evenodd"></path>
150         </symbol>
```

Este bloque de código parece estar diseñado para mostrar una flecha hacia abajo como parte de la navegación en la página web.

Al revisar las extensiones de archivos, notamos que la página utiliza Swiper 4.3.3, una biblioteca de JavaScript para crear interfaces de usuario tipo 'swiper'. Esto permite deslizar contenido horizontal o verticalmente en dispositivos táctiles o de escritorio."

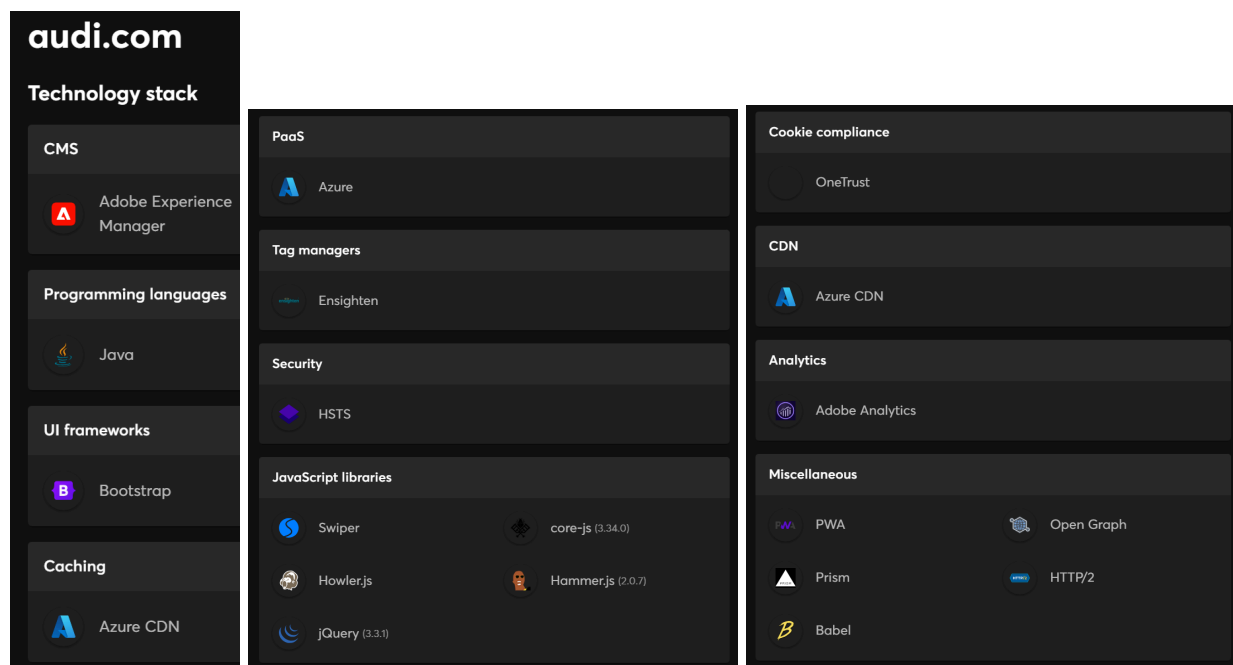
```
<script src="/etc/designs/gbp2/js/gbp2.ACSHASHafeed7b1e9eed6da50f6af605747fe29.js"></script>
```

```
/**
 * Swiper 4.3.3
 * Most modern mobile touch slider and framework with hardware accelerated transitions
 * http://www.idangero.us/swiper/
 *
 * Copyright 2014-2018 Vladimir Kharlampidi
 *
 * Released under the MIT License
 *
 * Released on: June 5, 2018
 */
```

Al investigar un poco, parece que no se está utilizando la última versión de Swiper, sino la 4.3.3, la cual puede verse afectada por [prototype pollution](#). una vulnerabilidad en JavaScript donde se

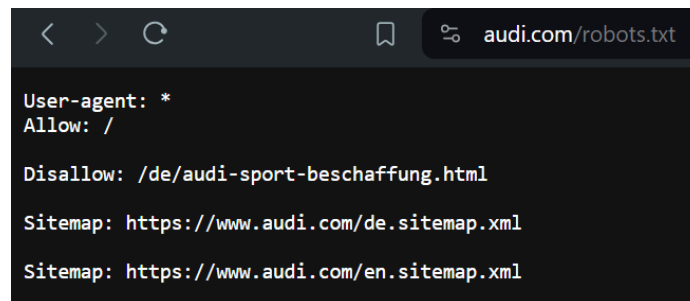
puede modificar el prototipo de un objeto de manera insegura, lo que puede conducir a comportamientos inesperados o incluso a ejecución de código malicioso.

Aparte del análisis del código fuente de la página implica también el uso de otras herramientas, como Wappalyzer. Simplemente proporcionando el dominio de audi.com, esta herramienta nos dará una lista de todas las tecnologías que utiliza la página.



## 4.2. Hacking con buscadores

Podemos verificar la disponibilidad del archivo robots.txt, el cual es utilizado por los sitios web para interactuar con los rastreadores web, también conocidos como 'bots' o 'spiders'. Estos programas son empleados por los motores de búsqueda para indexar y recopilar información sobre el contenido de un sitio web.



```
< > ↻ audi.com/robots.txt

User-agent: *
Allow: /

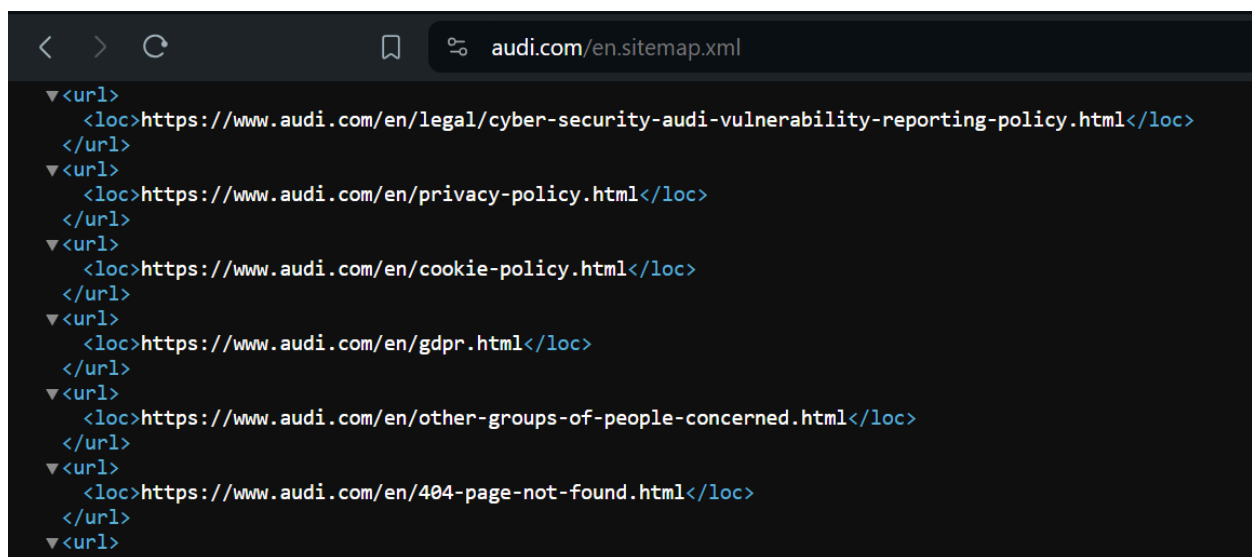
Disallow: /de/audi-sport-beschaffung.html

Sitemap: https://www.audi.com/de.sitemap.xml
Sitemap: https://www.audi.com/en.sitemap.xml
```

**Disallow: /de/audi-sport-beschaffung.html:** Esta línea indica que se prohíbe el acceso a una página específica del sitio web. El URL "/de/audi-sport-beschaffung.html" está marcado como no accesible para los rastreadores web.

**Sitemap: https://www.audi.com/de.sitemap.xml:** Esta línea especifica la ubicación del mapa del sitio XML para la versión en alemán (de) del sitio web. El mapa del sitio XML proporciona una lista de URLs que el propietario del sitio considera importantes y desea que los motores de búsqueda indexen.

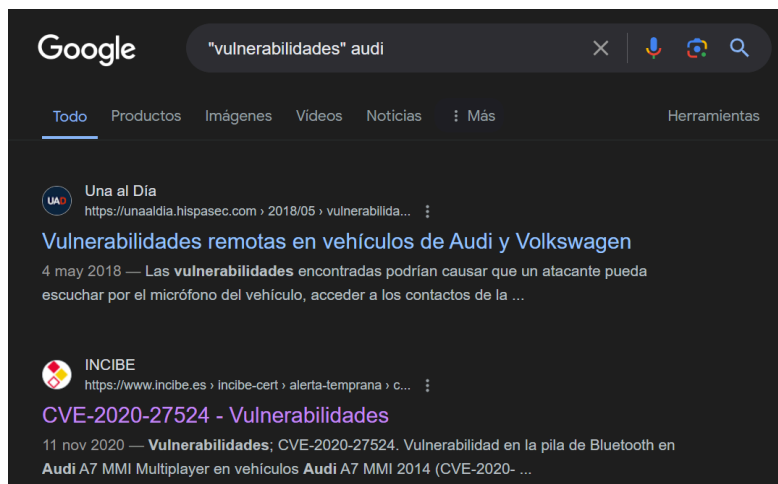
**Sitemap: https://www.audi.com/en.sitemap.xml:** Similar a la línea anterior, esta especifica la ubicación del mapa del sitio XML para la versión en inglés (en) del sitio web.



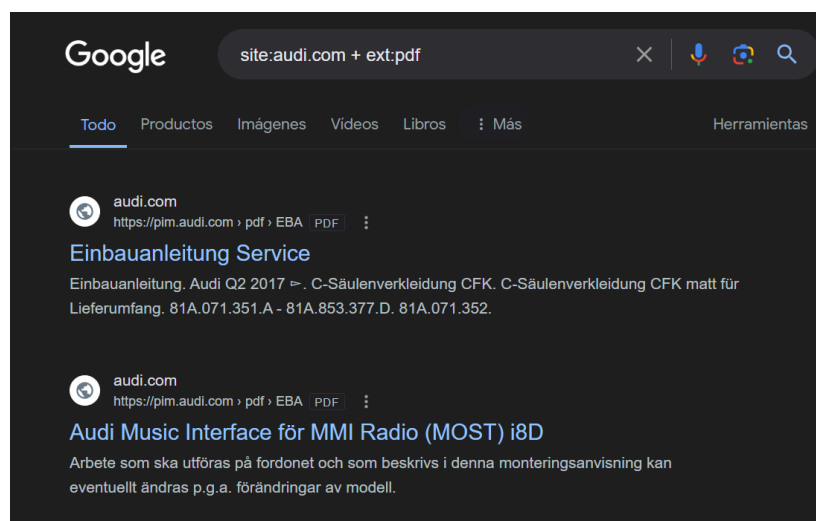
```
< > ↻ audi.com/en.sitemap.xml

▼<url>
  <loc>https://www.audi.com/en/legal/cyber-security-audi-vulnerability-reporting-policy.html</loc>
</url>
▼<url>
  <loc>https://www.audi.com/en/privacy-policy.html</loc>
</url>
▼<url>
  <loc>https://www.audi.com/en/cookie-policy.html</loc>
</url>
▼<url>
  <loc>https://www.audi.com/en/gdpr.html</loc>
</url>
▼<url>
  <loc>https://www.audi.com/en/other-groups-of-people-concerned.html</loc>
</url>
▼<url>
  <loc>https://www.audi.com/en/404-page-not-found.html</loc>
</url>
▼<url>
  <loc>https://www.audi.com/en/contact.html</loc>
```

Podemos realizar búsquedas avanzadas utilizando operadores, como colocar la palabra clave que deseamos buscar entre comillas. Esto nos ayudará a encontrar resultados específicos que contengan la frase exacta que estamos buscando, en lugar de resultados que contengan palabras individuales de forma dispersa.

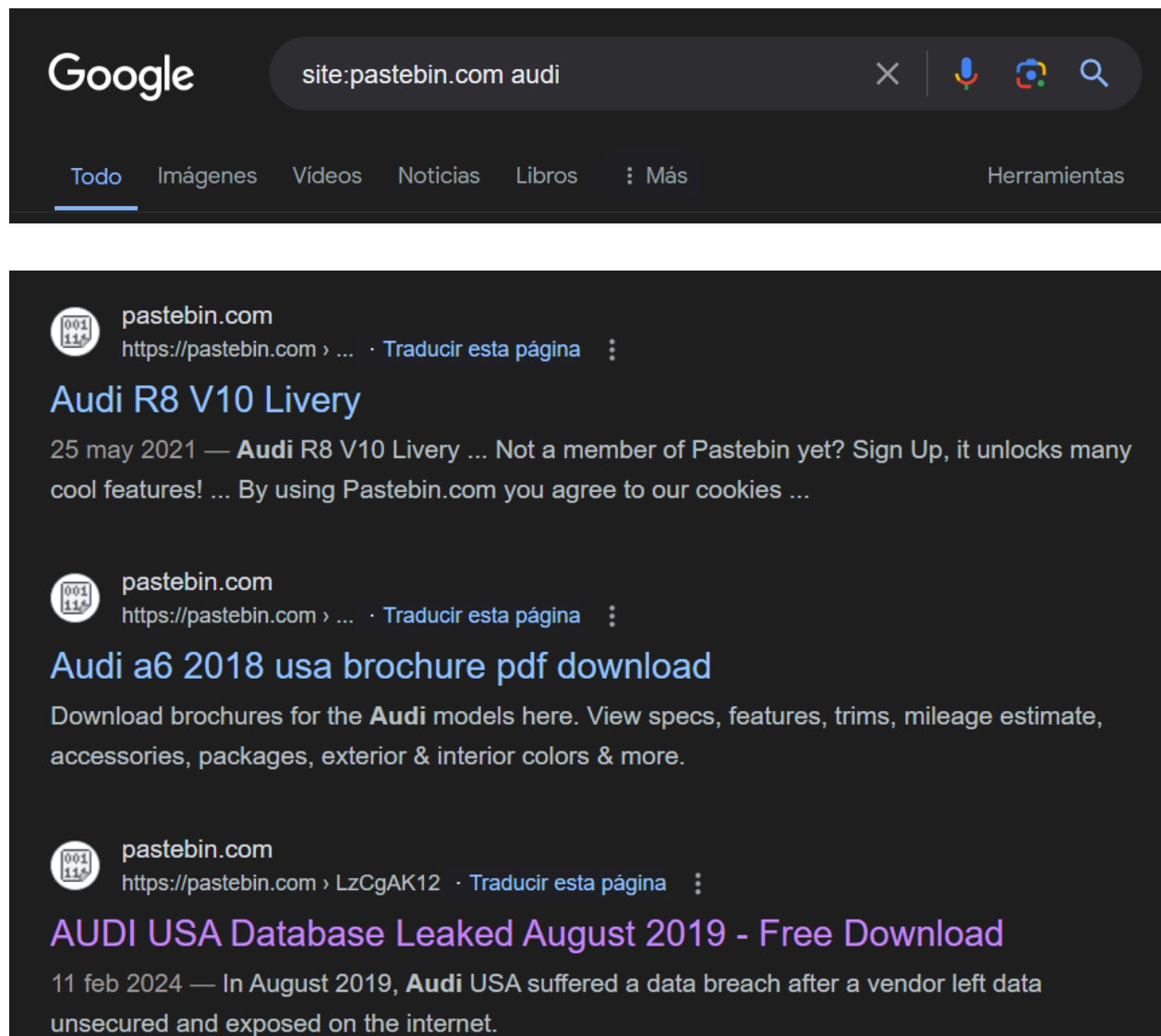


Podemos usar el operador "site" para especificar el dominio y "ext" para especificar la extensión de los archivos que estamos buscando. En este caso, estamos buscando archivos PDF del dominio de Audi.





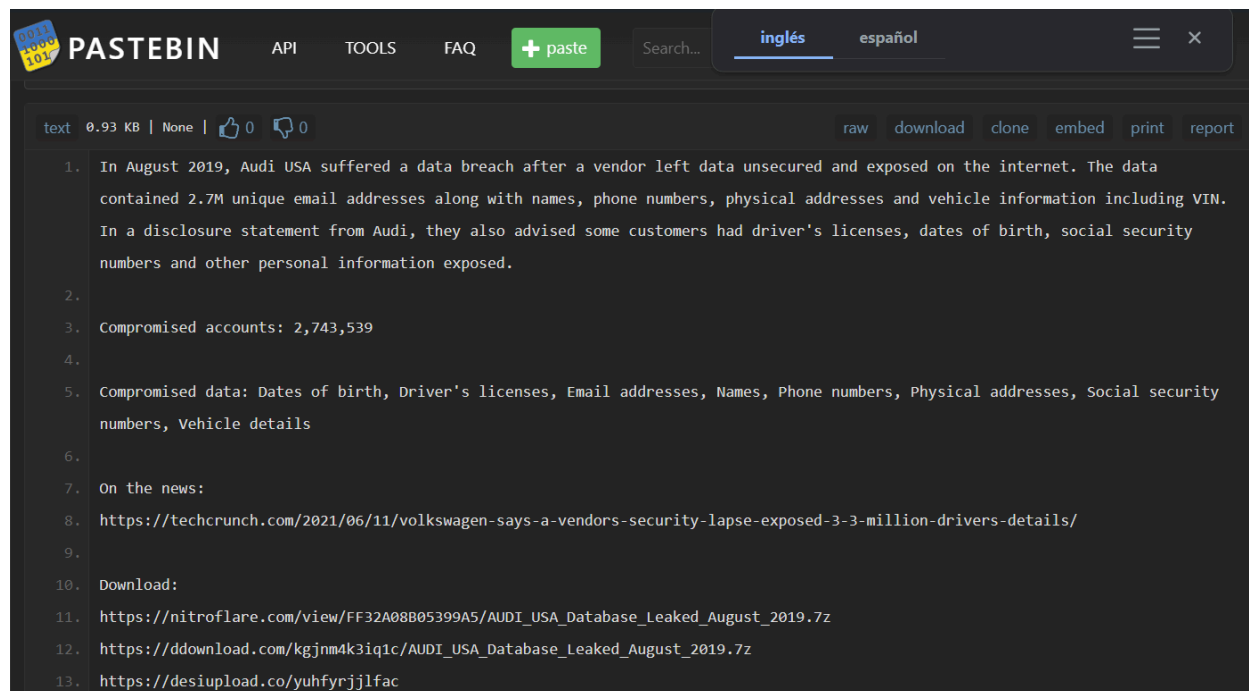
Pastebin se destaca como un sitio web donde muchos programadores comparten fragmentos de código fuente. Sin embargo, hasta hace algunos años, también era ampliamente utilizado para compartir cuentas crackeadas de diversas plataformas como Netflix, Spotify, HBO, entre otras, así como combos, que son listas de correos electrónicos y contraseñas segmentadas por país o plataforma.



The screenshot shows a Google search interface with the query 'site:pastebin.com audi'. Below the search bar, there are three search results from pastebin.com:

- Audi R8 V10 Livery**  
25 may 2021 — Audi R8 V10 Livery ... Not a member of Pastebin yet? Sign Up, it unlocks many cool features! ... By using Pastebin.com you agree to our cookies ...
- Audi a6 2018 usa brochure pdf download**  
Download brochures for the Audi models here. View specs, features, trims, mileage estimate, accessories, packages, exterior & interior colors & more.
- AUDI USA Database Leaked August 2019 - Free Download**  
11 feb 2024 — In August 2019, Audi USA suffered a data breach after a vendor left data unsecured and exposed on the internet.

Podemos descubrir que en 2019 se produjo una filtración de datos en Estados Unidos.



## 4.3. Análisis de ficheros

Podemos utilizar herramientas como Metagoofil para obtener diversos archivos de un dominio

```
(kali㉿kali)-[~/audi]
└─$ metagoofil -d audi.com -t pdf -l 100 -n 25 -o audi.psf -f audipsf.html
[*] Searching for 100 .pdf files and waiting 30.0 seconds between searches
[*] Results: 100 .pdf files found
https://pim.audi.com/pdf/EBA/EBA_8V0051960_sv_140528.pdf
https://pim.audi.com/pdf/EBA/EBA_8X3060306ASX7W_it_120426.pdf
https://pim.audi.com/pdf/EBA/EBA_4G0092157_en_130626.pdf
https://pim.audi.com/pdf/EBA/EBA_8W6071609_9AX_de_170828.PDF
https://pim.audi.com/pdf/EBA/EBA_8V0054690B_sv_120926.pdf
https://pim.audi.com/pdf/EBA/EBA_8W8052400_de_180316.pdf
https://pim.audi.com/pdf/EBA/EBA_8X3060306ARX7W_sv_120426.pdf
https://pim.audi.com/pdf/EBA/EBA_8U0071151_en_110926.pdf
https://pim.audi.com/pdf/EBA/EBA_8V0054960D_de_190315.pdf
https://pim.audi.com/pdf/EBA/EBA_4G0063511C_es_190404.pdf
https://pim.audi.com/pdf/EBA/EBA_4K2064205_en_170926.pdf
https://pim.audi.com/pdf/EBA/EBA_8V0071620A_9AX_pt_120719.pdf
https://pim.audi.com/pdf/EBA/EBA_8V0054690J_en_200303.pdf
```

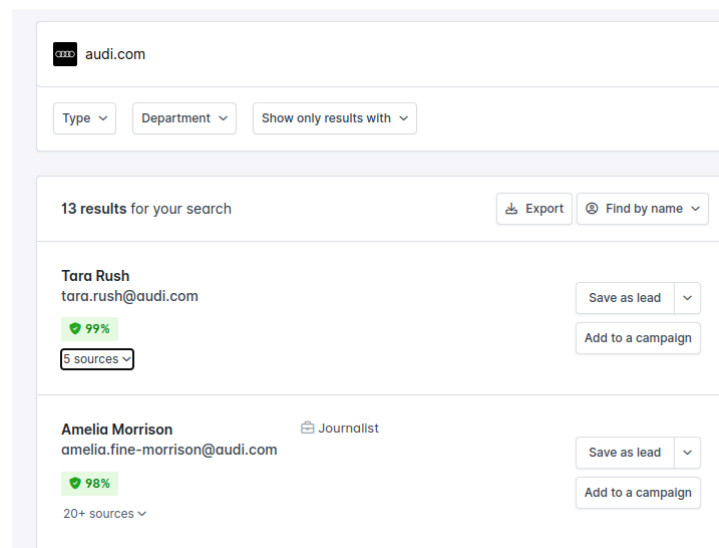
Podemos examinar los metadatos de los archivos que hemos obtenido con ExifTool para conocer detalles como el sistema desde el cual se creó el archivo y la fecha en que fue creado.

```
(kali@kali)-[/media/sf_Carpeta-Compartida/audi]
$ exiftool EBA_4G0063511C_es_190404.pdf
ExifTool Version Number      : 12.76
File Name                    : EBA_4G0063511C_es_190404.pdf
Directory                    : .
File Size                    : 2.8 MB
File Modification Date/Time   : 2024:05:12 11:03:30-04:00
File Access Date/Time        : 2024:05:12 12:04:05-04:00
File Inode Change Date/Time   : 2024:05:12 11:04:33-04:00
File Permissions              : -rwxrwx---
File Type                    : PDF
File Type Extension          : pdf
MIME Type                    : application/pdf
PDF Version                  : 1.6
Linearized                   : Yes
Create Date                  : 2019:04:02 11:39:15+02:00
Creator                      : AH XSL Formatter V6.4 MR5 for Windows (x64) : 6.4.7.29948 (2017/07/31 11:23JST)
Modify Date                  : 2019:04:04 07:47:59+02:00
Title                        :
XMP Toolkit                  : Adobe XMP Core 5.6-c015 84.159810, 2016/09/10-02:41:30
Metadata Date                : 2019:04:04 07:47:59+02:00
Creator Tool                 : AH XSL Formatter V6.4 MR5 for Windows (x64) : 6.4.7.29948 (2017/07/31 11:23JST)
Format                      : application/pdf
Document ID                  : uuid:e85a5d0-9cce-4f77-a3cb-84e66e60c97b
Instance ID                  : uuid:b367d4f4-5761-4507-af67-32acbbe8ca9d
Producer                     : Antenna House PDF Output Library 6.4.1077 (Windows (x64))
Page Count                   : 34
```

## 5. Información personal y leaks


### 5.1. Empleados

Para obtener correos electrónicos de los empleados, podemos utilizar herramientas como Hunter.io



- 
- Daniel Weissland,
    - Puesto: Jefe de Audi Norteamérica
  - Amelia Fine-Morrison,
    - Tel: +1.703.364.7678,
    - Mobile: +1.571.208.5426,
    - Email: [amelia.fine-morrison@audi.com](mailto:amelia.fine-morrison@audi.com)
    - Puesto: Gerente de Comunicaciones de Producto en Audi en America
  - Amanda Koons,
    - Tel: +1-703-364-7442,
    - Mobile: +1-571-524-8586,
    - EMail: [amanda.koons@audi.com](mailto:amanda.koons@audi.com)
    - Puesto: Gerente Senior, Comunicaciones, Redes Sociales e Integración de Socios
  - Mark Dahncke,
    - Tel: +1 703 364 7414 7423,
    - Mobile: +1 703 248229 6222549 3703,
    - EMail: [mark.dahncke@audi.com](mailto:mark.dahncke@audi.com)
    - Puesto: Gerente de Marketing Minorista de Audi America
  - Jeff Kuhlman,
    - Tel: +1 703 364 7414 7423
    - Mobile: +1 703 248229 6222549 3703,
    - EMail: [jeff.kuhlman@audi.com](mailto:jeff.kuhlman@audi.com)
  - Tara Rush,
    - Email: [tara.rush@audi.com](mailto:tara.rush@audi.com)
    - Puesto: Director Marketing de Audi America
  - Miranda Harper,
    - Email: [miranda.harper@audi.com](mailto:miranda.harper@audi.com)
    - Tel: +1 646 603 7732
    - Puesto: Ex Director Communications de Audi America

Podemos buscar en herramientas como [Have I Been Pwned](#) si estos correos han sido comprometidos. En caso afirmativo, podemos comenzar buscando el correo de Amelia Fine-Morrison, que, según nuestras observaciones, ha sido comprometido por tres empresas.




**Apollo:** In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher Vinny Troia who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including places of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. [The Apollo website has a contact form](#) for those looking to get in touch with the organisation.

**Compromised data:** Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles

NETPROSPEX

**NetProspex (spam list):** In 2016, a list of over 33 million individuals in corporate America sourced from Dun & Bradstreet's NetProspex service was leaked online. D&B believe the targeted marketing data was lost by a customer who purchased it from them. It contained extensive personal and corporate information including names, email addresses, job titles and general information about the employer.

**Compromised data:** Email addresses, Employers, Job titles, Names, Phone numbers, Physical addresses



**Public Business Data:** In approximately August 2021, hundreds of gigabytes of business data collated from public sources was obtained and later published to a popular hacking forum. Sourced from a customer of Bureau van Dijk's (BvD) "Orbis" product, the corpus of data released contained hundreds of millions of lines about corporations and individuals, including personal information such as names and dates of birth. The data also included 28M unique email addresses along with physical addresses (presumably corporate locations), phone numbers and job titles. There was no unauthorised access to BvD's systems, nor did the incident expose any of their or parent company's Moody's clients.

Según lo que he podido observar, todos los correos, excepto el de Tara Rush, están comprometidos.

---

## 5.2. Contactos encontrados

Estos son los miembros del Consejo de Dirección de Producción y Logística de [AUDI AG](#)

- Jürgen Rittersberger
- Javier Ros Hernández
- Renate Wachenauer
- Gerd Walker
- Hildegarda Wortmann

También podemos encontrar el [personal de prensa](#) de todas las regiones en la web

## 6. Conclusiones

Lo más relevante que he encontrado es que la biblioteca Swiper está desactualizada, lo que podría ser un riesgo. Sería útil investigar más sobre el ataque de Prototype Pollution para determinar si es posible llevar a cabo un ataque. Además, deberíamos examinar otras tecnologías en busca de posibles vulnerabilidades que podrían ser explotadas para acceder a los servidores. También podríamos utilizar los correos electrónicos encontrados para intentar realizar un ataque de phishing.