

Broken access control not indexed directory

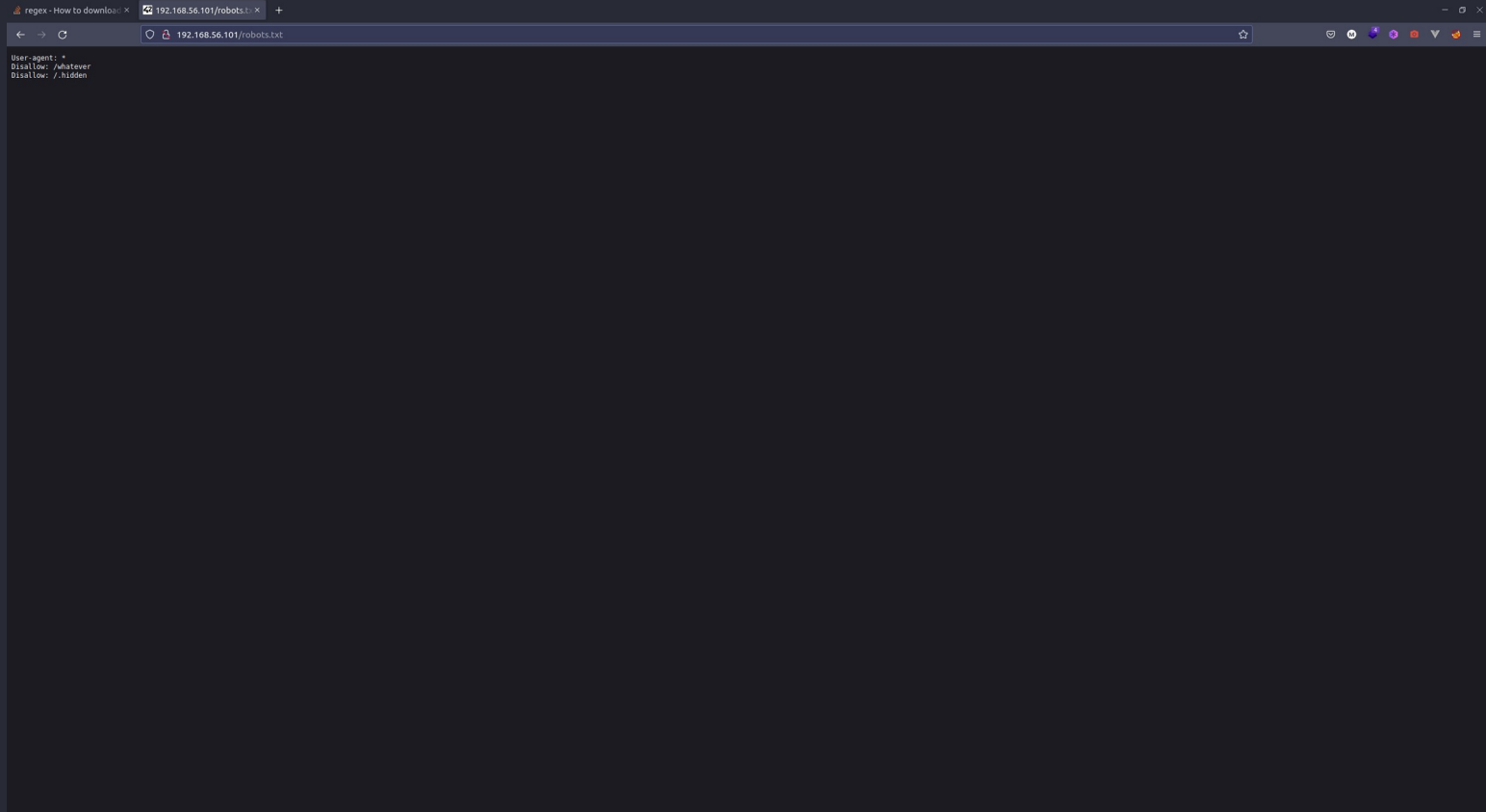
Moving up from the fifth position, 94% of applications were tested for some form of broken access control with the average incidence rate of 3.81%, and has the most occurrences in the contributed dataset with over 318k. Notable Common Weakness Enumerations (CWEs) included are CWE-200: Exposure of Sensitive Information to an Unauthorized Actor, CWE-201: Insertion of Sensitive Information Into Sent Data, and CWE-352: Cross-Site Request Forgery.

Access control enforces policy such that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.

In this context we talk about an hidden directory

Walk through

Step 1 : try to access the robots.txt file we saw 2 not indexed directories



Step 2 : Try to access to the .hidden directory, they have a lot of directories/files, so download with the command 'wget -r --no-parent -e robots=off http://192.168.56.101/.hidden/'

regex - How to download x index of /.hidden/ x +

← → ↻ 192.168.56.101/.hidden/ ☆

Index of /.hidden/

..	29-Jun-2021 18:15	-
amchevoondpcrl0o0uzivpjd/	29-Jun-2021 18:15	-
bmupenskybcbmcyvjalshd/	29-Jun-2021 18:15	-
cecoj1dd8ibvuyd0z19dth/	29-Jun-2021 18:15	-
doxelttrvbeenh1hrkqfzsg/	29-Jun-2021 18:15	-
esjmmehatmeph1uayvfrmyhr/	29-Jun-2021 18:15	-
ffebekonzbiqbauhhbfzrrg/	29-Jun-2021 18:15	-
ghubrvogocass1jbn1htcsyfr/	29-Jun-2021 18:15	-
hw4yephtcotend0uayv1f0m/	29-Jun-2021 18:15	-
jsufscgmpactarj1fjnnenkuz/	29-Jun-2021 18:15	-
j1f0ebdhu1ex1sawp0rubbzr/	29-Jun-2021 18:15	-
qulb0x1anvzrc0cz0v1bui1mz/	29-Jun-2021 18:15	-
ldk1ms0yvdlhtq11j0ad0uz/	29-Jun-2021 18:15	-
mrucag0pc0w6j10mpeyztah/	29-Jun-2021 18:15	-
ntvrb1k1nd0ajevzr1ebwaxr/	29-Jun-2021 18:15	-
oast0dm0emdz0c1100p1ay/	29-Jun-2021 18:15	-
q01q0ia0kcm0f0t0mcf0u0g/	29-Jun-2021 18:15	-
q0c0t0f0110k0y0h10m0h0c/	29-Jun-2021 18:15	-
r1n0yducc00k0c110nd1k1f0vz/	29-Jun-2021 18:15	-
sd0f0t0v1r1100ct0m0v11c/	29-Jun-2021 18:15	-
trv0c0m010010000010v0m0/	29-Jun-2021 18:15	-
urh0hrm0u0ab0d0m00k1sk0v0/	29-Jun-2021 18:15	-
v10h00100000000000000000/	29-Jun-2021 18:15	-
wh0cc10k0y0h10v0c0v0k0sf0/	29-Jun-2021 18:15	-
x00rcv110m0k1r1rm0h0v10h/	29-Jun-2021 18:15	-
y10m10p010k0v11v10h0000/	29-Jun-2021 18:15	-
zz1r1v10u0g100t0x0t0z0d011/	29-Jun-2021 18:15	-
README	29-Jun-2021 18:15	34

Step 3 : Get the value of all the files with the command : `cat */**/* > flag`

```
Terminal
1 Demande à ton voisin de gauche
2 Non ce n'est toujours pas bon ...
3 Demande à ton voisin du dessous
4 Demande à ton voisin du dessus
5 Demande à ton voisin de gauche
6 Toujours pas tu vas craquer non ?
7 Demande à ton voisin du dessous
8 Demande à ton voisin du dessus
9 Toujours pas tu vas craquer non ?
10 Toujours pas tu vas craquer non ?
11 Non ce n'est toujours pas bon ...
12 Demande à ton voisin de droite
13 Tu veux de l'aide ? Mot aussi !
14 Non ce n'est toujours pas bon ...
15 Demande à ton voisin du dessous
16 Demande à ton voisin de droite
17 Demande à ton voisin de gauche
18 Toujours pas tu vas craquer non ?
19 Toujours pas tu vas craquer non ?
20 Demande à ton voisin de gauche
21 Toujours pas tu vas craquer non ?
22 Tu veux de l'aide ? Mot aussi !
23 Non ce n'est toujours pas bon ...
24 Demande à ton voisin de droite
25 Toujours pas tu vas craquer non ?
26 Demande à ton voisin du dessous
27 Demande à ton voisin de droite
28 Demande à ton voisin de droite
29 Tu veux de l'aide ? Mot aussi !
30 Demande à ton voisin du dessous
31 Toujours pas tu vas craquer non ?
32 Tu veux de l'aide ? Mot aussi !
33 Demande à ton voisin du dessous
34 Demande à ton voisin de droite
35 Demande à ton voisin de gauche
36 Non ce n'est toujours pas bon ...
37 Demande à ton voisin de gauche
38 Tu veux de l'aide ? Mot aussi !
39 Tu veux de l'aide ? Mot aussi !
40 Demande à ton voisin de gauche
41 Non ce n'est toujours pas bon ...
42 Demande à ton voisin de droite
43 Demande à ton voisin de gauche
44 Demande à ton voisin du dessous
45 Demande à ton voisin de gauche
46 Demande à ton voisin du dessous
47 Tu veux de l'aide ? Mot aussi !
48 Demande à ton voisin de gauche
49 Non ce n'est toujours pas bon ...
50 Demande à ton voisin de gauche
51 Demande à ton voisin de droite
52 Non ce n'est toujours pas bon ...
53 Tu veux de l'aide ? Mot aussi !
54 Toujours pas tu vas craquer non ?
55 Toujours pas tu vas craquer non ?
56 Non ce n'est toujours pas bon ...
57 Demande à ton voisin de gauche
58 Demande à ton voisin du dessous
59 Demande à ton voisin de gauche
60 Demande à ton voisin de gauche
61 Demande à ton voisin du dessous
62 Demande à ton voisin de gauche
63 Tu veux de l'aide ? Mot aussi !
64 Tu veux de l'aide ? Mot aussi !
65 Demande à ton voisin du dessous
66 Non ce n'est toujours pas bon ...
67 Demande à ton voisin de gauche
68 Demande à ton voisin du dessous
69 Non ce n'est toujours pas bon ...
70 Demande à ton voisin du dessous
71 Demande à ton voisin du dessous
72 Demande à ton voisin du dessous

logs
0 nvim 1 zsh
1.41 2.51 2.01 GPU RAM 4GB/15GB
```

Step 4 : search for the flag keyword in vim or with cat file | grep flag for example and get the flag !

```
15057 Demande à ton voisin de gauche
15058 Demande à ton voisin du dessous
15059 Tu veux de l'aide ? Moi aussi !
15060 Demande à ton voisin de gauche
15061 Toujours pas tu vas craquer non ?
15062 Demande à ton voisin du dessus
15063 Demande à ton voisin du dessous
15064 Demande à ton voisin de droite
15065 Demande à ton voisin du dessous
15066 Demande à ton voisin du dessous
15067 Demande à ton voisin du dessous
15068 Tu veux de l'aide ? Moi aussi !
15069 Demande à ton voisin du dessous
15070 Demande à ton voisin du dessous
15071 Demande à ton voisin de droite
15072 Non ce n'est toujours pas bon ...
15073 Tu veux de l'aide ? Moi aussi !
15074 Toujours pas tu vas craquer non ?
15075 Demande à ton voisin du dessous
15076 Demande à ton voisin du dessous
15077 Demande à ton voisin du dessous
15078 Demande à ton voisin de gauche
15079 Demande à ton voisin du dessous
15080 Demande à ton voisin de droite
15081 Demande à ton voisin du dessous
15082 Demande à ton voisin de gauche
15083 Demande à ton voisin de gauche
15084 Non ce n'est toujours pas bon ...
15085 Demande à ton voisin du dessous
15086 Demande à ton voisin du dessous
15087 Toujours pas tu vas craquer non ?
15088 Demande à ton voisin du dessous
15089 Non ce n'est toujours pas bon ...
15090 Demande à ton voisin du dessous
15091 Non ce n'est toujours pas bon ...
15092 Hey, here is your flag : d5ee3ac36cf80dce44a896f961c1831a05526ec215693c8f2c39543497d4466
15093 Toujours pas tu vas craquer non ?
15094 Tu veux de l'aide ? Moi aussi !
15095 Toujours pas tu vas craquer non ?
15096 Demande à ton voisin du dessous
15097 Non ce n'est toujours pas bon ...
15098 Demande à ton voisin de gauche
15099 Tu veux de l'aide ? Moi aussi !
15100 Demande à ton voisin du dessous
15101 Demande à ton voisin du dessous
15102 Non ce n'est toujours pas bon ...
15103 Demande à ton voisin du dessous
15104 Demande à ton voisin du dessous
15105 Demande à ton voisin de gauche
15106 Demande à ton voisin de gauche
15107 Demande à ton voisin du dessous
15108 Non ce n'est toujours pas bon ...
15109 Non ce n'est toujours pas bon ...
15110 Demande à ton voisin du dessous
15111 Demande à ton voisin du dessous
15112 Demande à ton voisin de gauche
15113 Toujours pas tu vas craquer non ?
15114 Demande à ton voisin du dessous
15115 Tu veux de l'aide ? Moi aussi !
15116 Demande à ton voisin de droite
15117 Demande à ton voisin du dessous
15118 Demande à ton voisin du dessous
15119 Demande à ton voisin de droite
15120 Toujours pas tu vas craquer non ?
15121 Demande à ton voisin de droite
15122 Demande à ton voisin du dessous
15123 Tu veux de l'aide ? Moi aussi !
15124 Demande à ton voisin de droite
15125 Non ce n'est toujours pas bon ...
15126 Non ce n'est toujours pas bon ...
15127 Demande à ton voisin de droite
15128 Toujours pas tu vas craquer non ?
```

logs
//flag
0 nvim 1 zsh

15092,19 86%

1.17 2.41 1.99 GPU RAM 4GB/15GB

How to fix

- Disable directory listing in the webserver config
- Block access to the unindexed directories