# Using SPI Fuzz r

2007.0 .29

1.

"Fuzzing"

submit . BOF

tester entry point

.

# 2. HTTP Fuzzing

HTTP request reading section(request method, Uniform Resource Identifier, version, headers, cookies, post data) .

- method

Method request-URI

GET, POST

- Request-URI

Request-URI 가 resource

Resource path, file, file extension .

parameter=value & .

Fuzzing section 8가

SECTION	Example
Resource Path	/ <b>Folder</b> /file.html
Resource File	/Folder/ <b>file</b> .html
Resource File extension	/Folder/file. <b>html</b>
Resource and query delimiter	/Folder/file.html?parameter=value
Parameter name	/Folder/file.html? <b>parameter</b> =value
Parameter name value assignment	/Folder/file.html?parameter=value
Parameter value	/Folder/file.html?parameter= <b>value</b>
Parameter separator	/Folder/file.html?parameter=value&

```
- protocol version
```

HTTP 0.9,1.0,1.1 "HTTP/version" "/"

- Header Fields

Header

가 . Host User-Agent

Header name: value 가

- Cookies

Cookie: name=value;name=value

- Post Data(Entity Body)

URI qurey 가 POST method Post data Content-Length

# 3. SPI Fuzzer

1) Basic Example

SPI Fuzzer

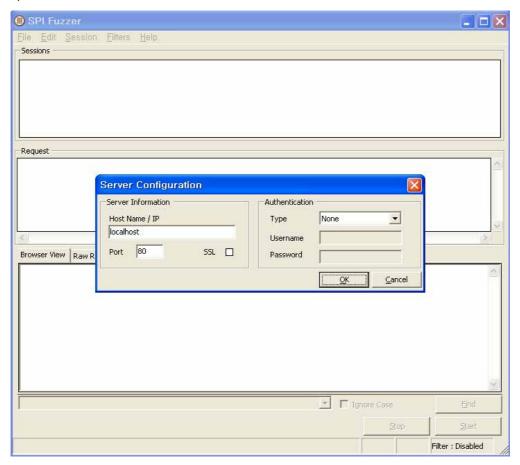
asp . .

```
If (Request.QueryString("id") >= "1") And (Request.QueryString("id") <= "10") Then
        strContent = " it's true
        Else
        strContent = " it's false"
        End If
        If Request.QueryString("id") = "39" Then
        strContent = " it's true"
        End if
12 *>
14 <html>
15 <head>
16 <title>basic example</title>
17 </head>
18 <body>
19 
20
      >
        the value : 
<%=strContent%>
   </body>
   </html>
```

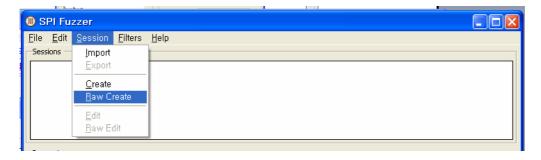
id 1~10 it's true

false . id 39 true

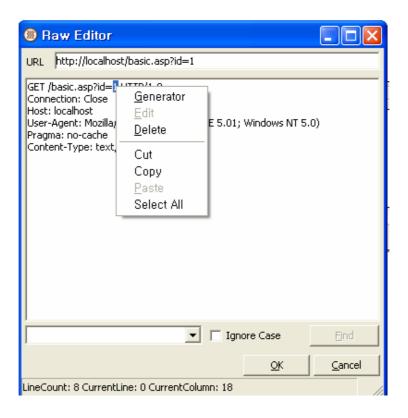
spi fuzzer .



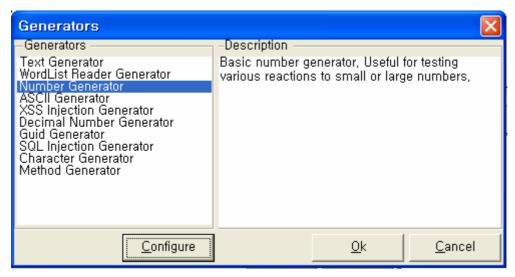
ip .



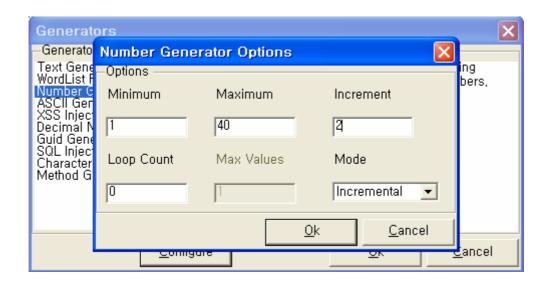
RAW create editor



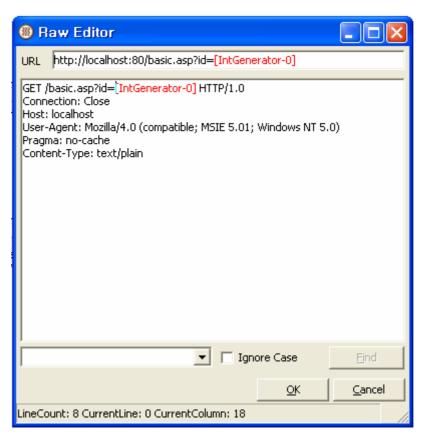
url



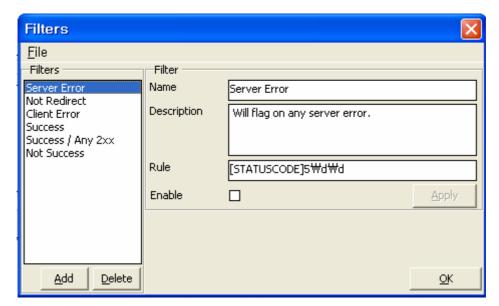
가 . Configure



1 40 2 가

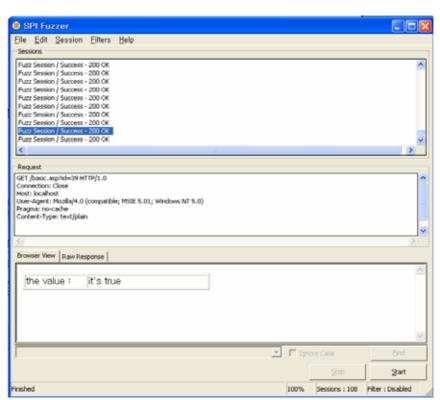


[IntGenerator-0]



filter

#### start



### 2) Testing For BOF

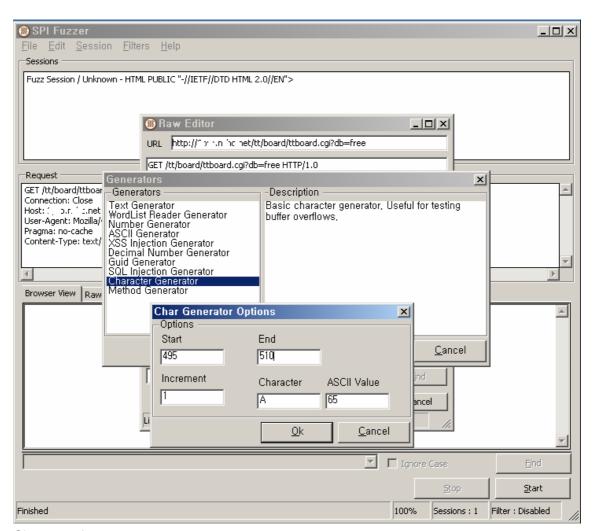
BOF가 500 server error 502 Gateway error

BOF 가 가

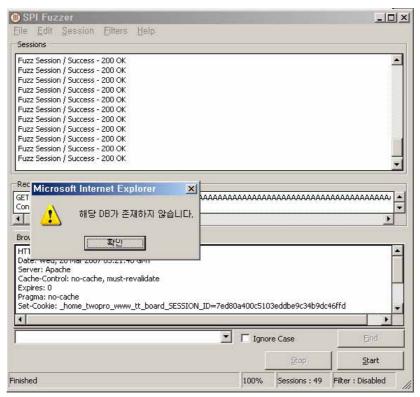
generators

# http://xxxxxxxxxxx/tt/board/ttboard.cgi?db=free

URL DB (free) test



Character A 495 510



200 OK 가 A가 503 504

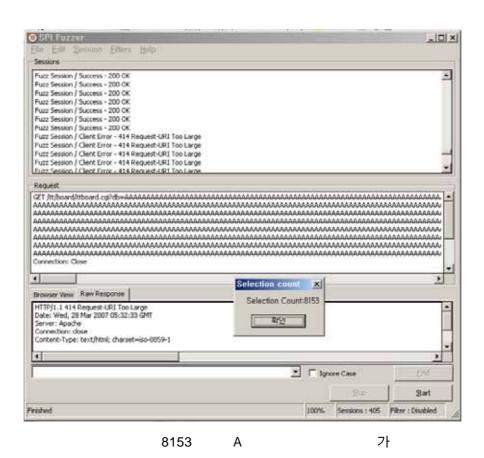
Finished

SPI Fuzzer <u>File Edit Session Filters Help</u> -Sessions Fuzz Session / Success - 200 OK Fuzz Session / Success - 200 OK • Fuzz Session / Success - 200 OK Fuzz Session / Succes Microsoft Internet Explorer X Request file\_exists(): File name is too long or invalid, GET /tt/board/ttboard Connection: Close "확인" 1 Browser View Raw Response HTTP/1.1 200 OK Date: Wed, 28 Mar 2007 05:21:48 GMT Server: Apache Cache-Control: no-cache, must-revalidate Expires: 0 Pragma: no-cache Set-Cookie: \_home\_twopro\_www\_tt\_board\_SESSION\_ID=eba4918b83762a32b2619479c43813a8 ▼ ☐ Ignore Case

Start

Filter : Disabled

100% Sessions : 49



HTTP

**BOF** 

id

Set-Cookie:

\_home\_xxxxxx\_www\_tt\_board\_SESSION\_ID=740d433bc3bc24d849c7e8997a4bd6ee

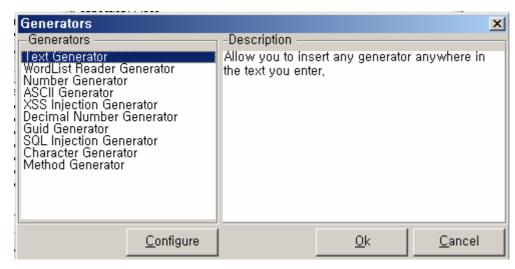
ID

가

generators 가

.. T T

# generators



Text generator : 가

WordList Reader Generator: wordlist

Number generator : 가 . 가

ASCII generator : ASCII

GET /Fuzzing/SimpleValidation.aspx?id=2a HTTP/1.0 GET /Fuzzing/SimpleValidation.aspx?id=2{ HTTP/1.0

GET /Fuzzing/SimpleValidation.aspx?id=2@ HTTP/1.0

GET /Fuzzing/Simple Validation.aspx?id=2! HTTP/1.0

GET /Fuzzing/SimpleValidation.aspx?id=2, HTTP/1.0

XSS injection Generator: XSS

**Decimal Number Generator:** 

Guid Generator: "a5ef51cc-3555-43fb-a911-577026407d0b"

**SQL** injection Generator : SQL injection

가 가

**HTTP** 

....

2007.0 .28