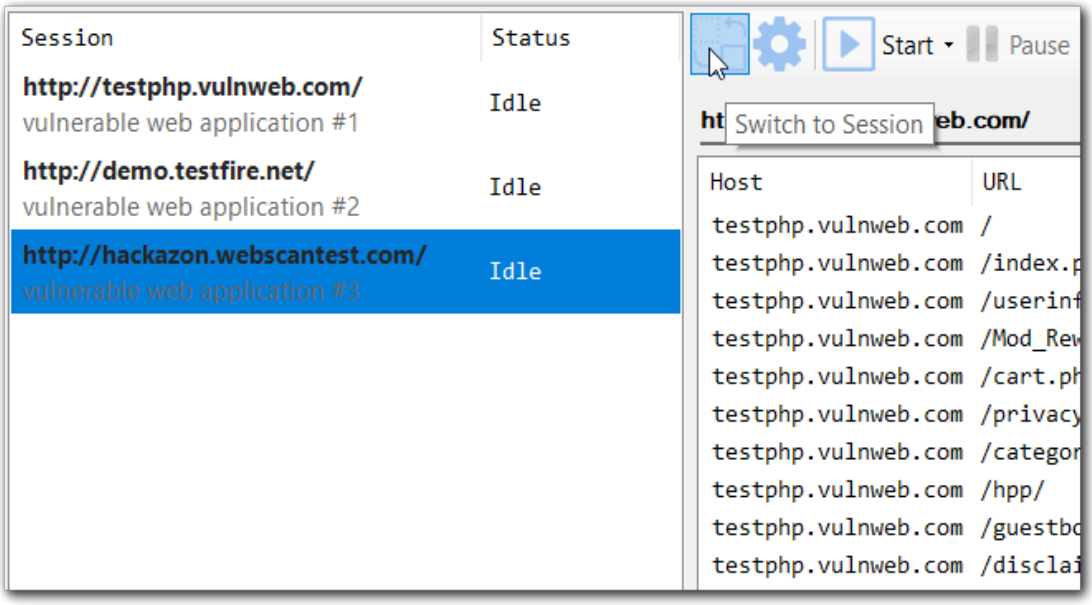
Version 1.0

Beagle Technical Document

DOC VERSION 1.1
11.04.2018

BEAGLE

Multi-Scan Session



Unlike the other web application security scanners, Beagle can manage more than one scan session at the same time in one instance of the application.

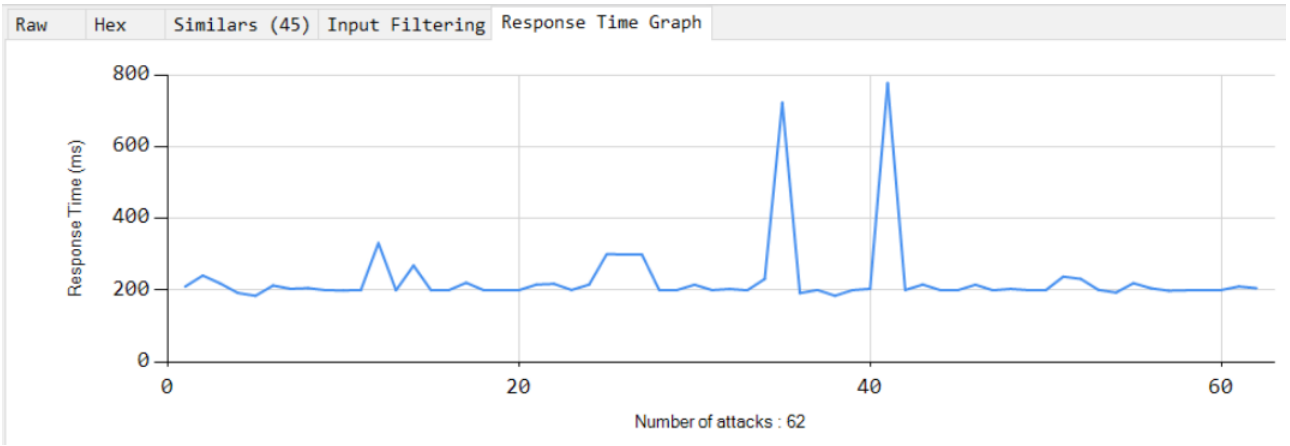
Switching between sessions is just one click away.

Intuitive Sitemap

Host	Path	Method	Avg Response Time	#Params	Attack Duration	
testphp.vulnweb.com	/pictures/wp-config.bak	GET	110 ms	0	00:00:03	
testphp.vulnweb.com	/cart.php	POST	178 ms	P2	00:00:35	
testphp.vulnweb.com	/comment.php	GET	91 ms	0	00:00:02	
testphp.vulnweb.com	/medias/	GET	122 ms	0	00:00:12	
testphp.vulnweb.com	/medias/img/	GET	128 ms	0	00:00:14	
testphp.vulnweb.com	/sendcommand.php	POST	317 ms	P2	00:00:33	
testphp.vulnweb.com	/sendcommand.php	GET	117 ms	0	00:00:03	
testphp.vulnweb.com	/AJAX/artists.php	GET	96 ms	0	00:00:02	
testphp.vulnweb.com	/AJAX/infoartist.php?id=1	GET	142 ms	G1	00:00:02	
testphp.vulnweb.com	/AJAX/categories.php	GET	124 ms	0	00:00:03	
testphp.vulnweb.com	/AJAX/infocateg.php?id=1	GET	146 ms	G1	00:00:02	
testphp.vulnweb.com	/AJAX/titles.php	GET	117 ms	0	00:00:03	
testphp.vulnweb.com	/AJAX/infotitle.php	POST	252 ms	P1	00:00:18	

Each of the crawled pages gets added into the sitemap and it is easy to track down the attack progress. Sitemap gives you the most important details about pages throughout the crawling & attacking. You can see;

- HTTP method (GET | POST | PUT | DELETE etc.)
- Total number of parameters to attack
- **Average response time** which changes during attacking. This will give you a clue about there might be a problem with loading page under heavy load.
- Attack duration
- If there is an **issue found** for the page.

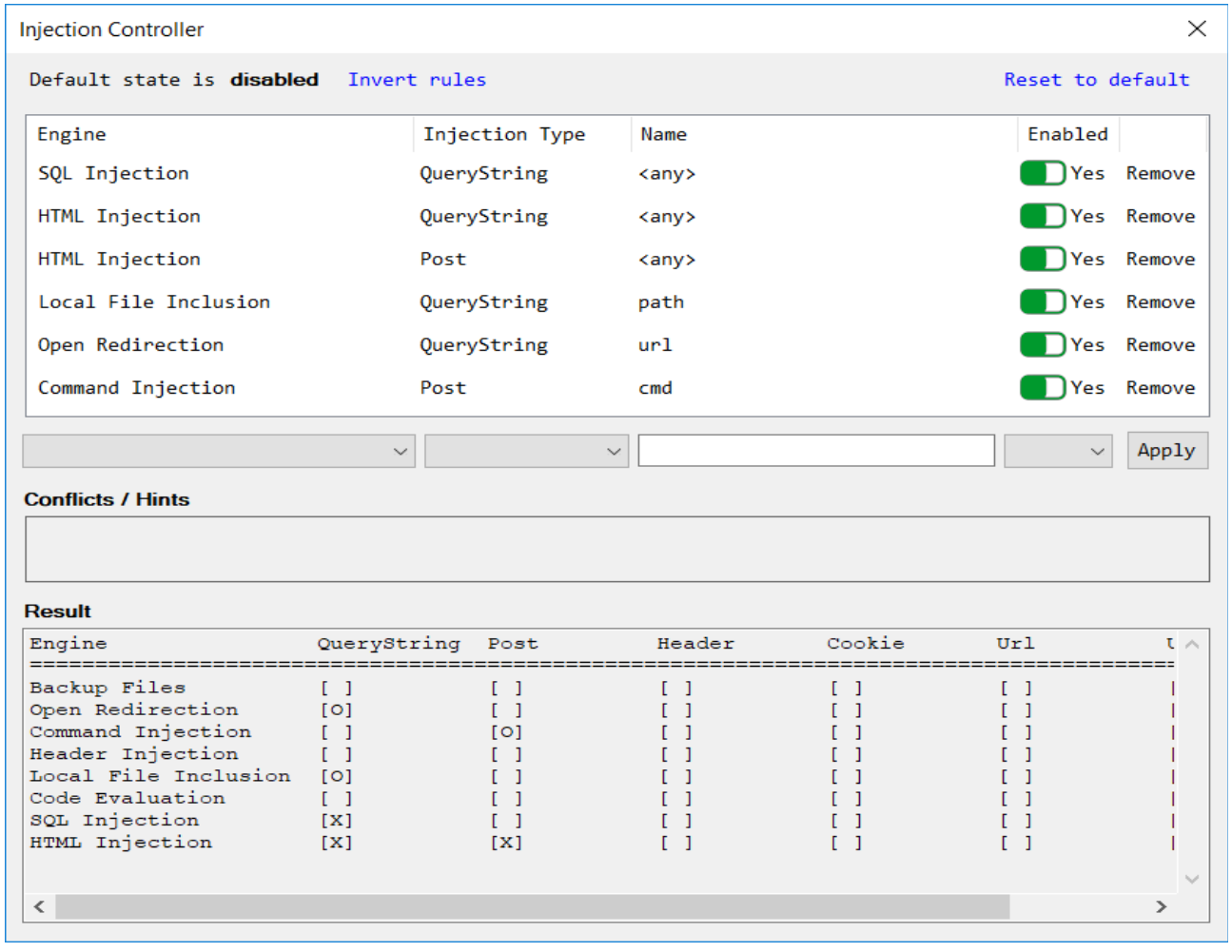


Injection Configuration

Sometimes you will need to restrict the scan. For example you only need to;

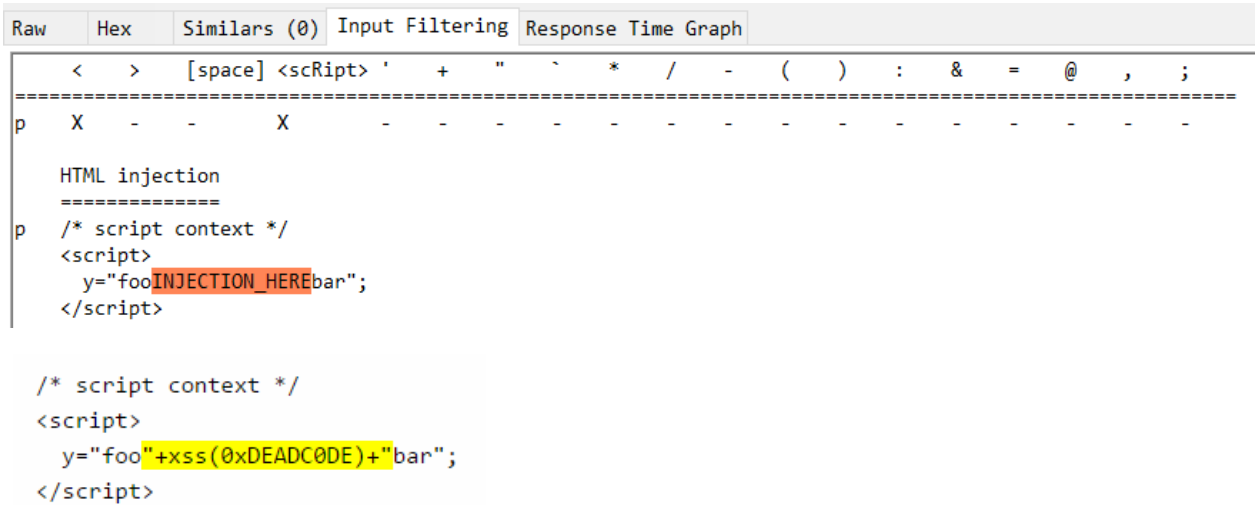
1- Detect specific type(s) of vulnerability (e.g, SQL injection)
2- Attack only an injection point (e.g, POST parameters)
3- Filter parameter names

Beagle can restrict scans based on 3 combinations above.



Context-Aware Analyze

When a user controllable input is reflected without being encoded in HTML, it might lead to a security issue in a certain level.
Beagle detects these types of vulnerabilities by analyzing context not brute-force attacks. In first step, it identifies the context by analyzing the reflection and then generates a payload based on this context without breaking the javascript context.



Exploitation

Boolean SQL Injection

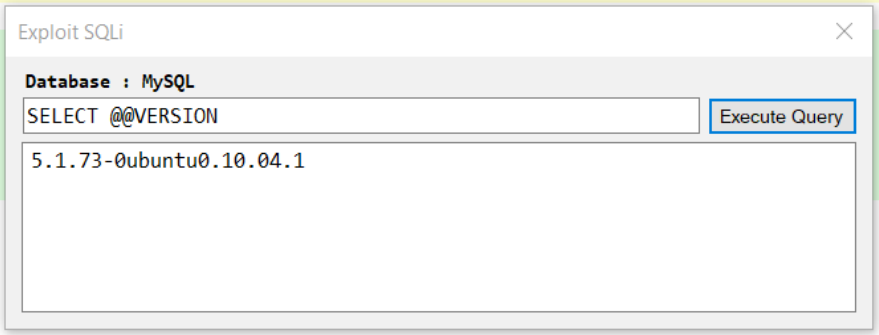
Url: http://testphp.vulnweb.com/artists.php?artist=1

Injection Point: artist

Type: QueryString

Payload: 1 AND 1=1

Exploit



Request

```
GET /artists.php?artist=1%20AND%201%3d1 HTTP/1.1
```

Command Injection

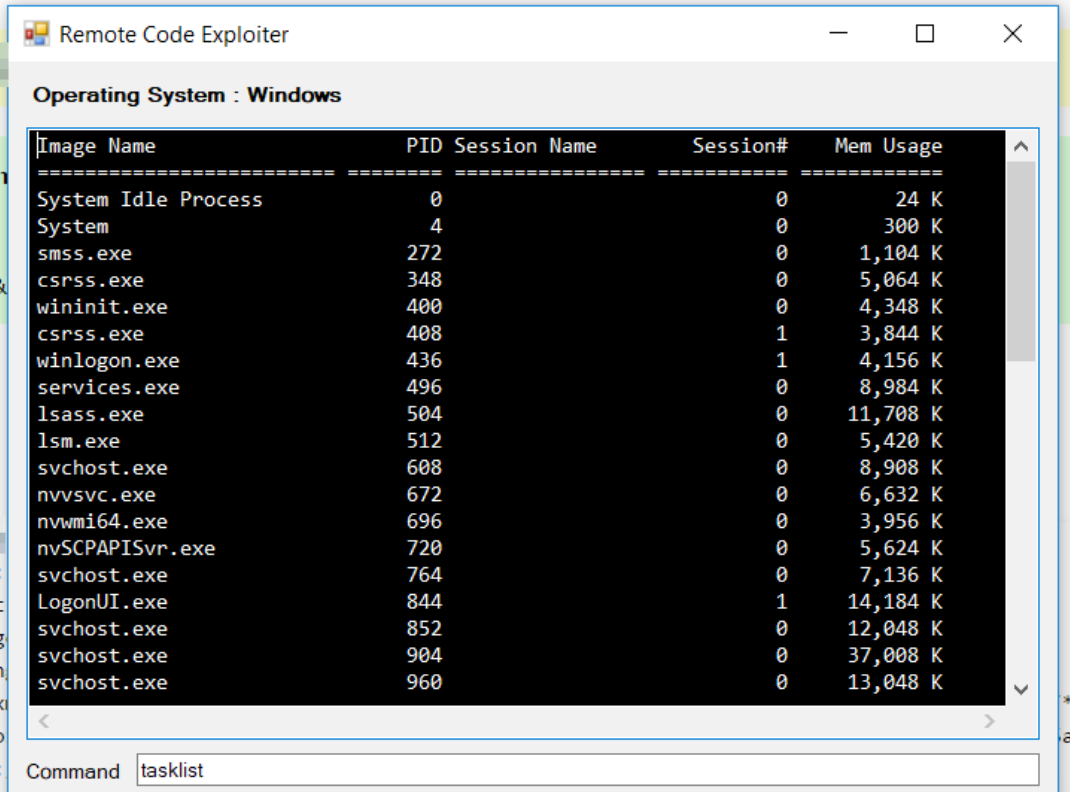
Url:

Injection Poin

Type: Post

Payload: -1&&

Exploit



Request

```
POST
Cache-Control:
Accept-Charset
Accept-Languag
Accept-Encodin
Accept: text/x
User-Agent: Mo
Referer: http:
```

Scripting

This feature is only available in Professional Edition

Beagle scripting engine allows you to generate payloads on the fly while performing manual assessments. Its integrated tools, internal data sources and 30+ commands make payload generation easier to carry out in HTTP requests.

You can work with as much different data sources as possible and combine them.