

الفصل التاسع عشر

ثغرات ال HTTP Headers

المؤلف

د.م/ أحمد هاشم الفقي

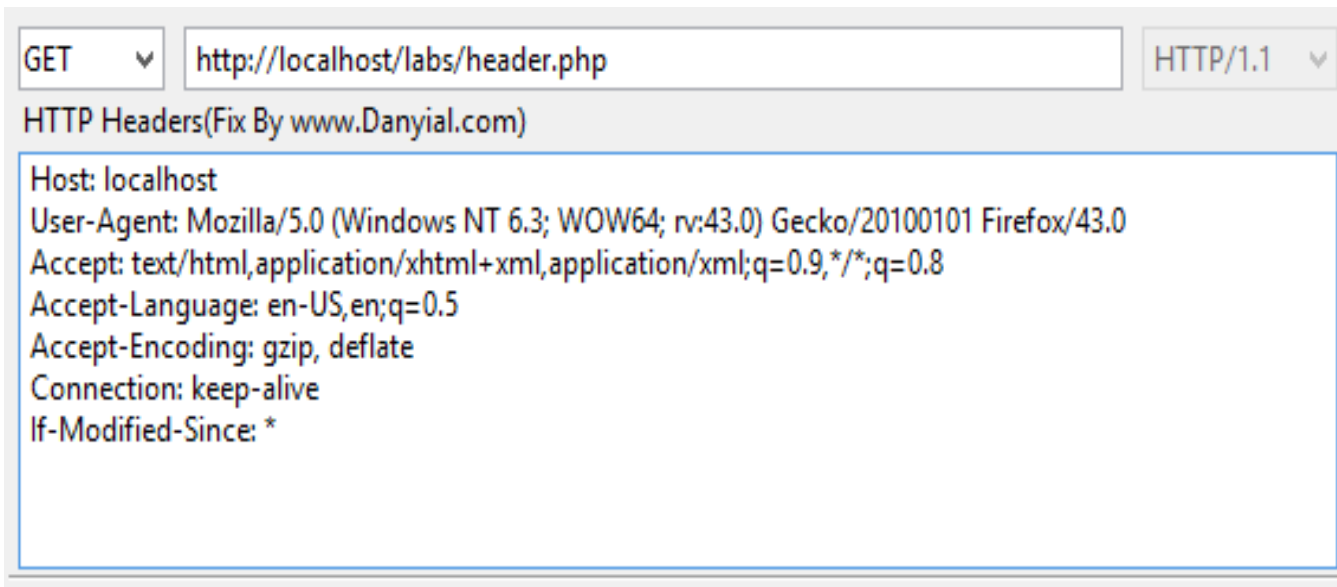
استشاري أمن المعلومات و التحول الرقمي

Ahmed.Hashem.ElFiky@outlook.com

ثغرات ال HTTP Headers

- الكثير من مختبري الاختراق اليدوي يعتمدون على HTTP header في ارسال واستقبال الطلبات لفهم ما يجري في الطلب والرد على الطلب من السيرفر .
- اليوم سنشرح اهم العناصر الموجودة في الطلب وفي الرد والتي ستساعدك في فهم واكتشاف الثغرات المتعلقة بتطبيقات الويب كما يمكن ان تكون نوع من ال Input القابلة للاختراق .

- لنحل طلب عادي الى localhost



ثغرات ال HTTP Headers (تكملة...)

• ال HOST

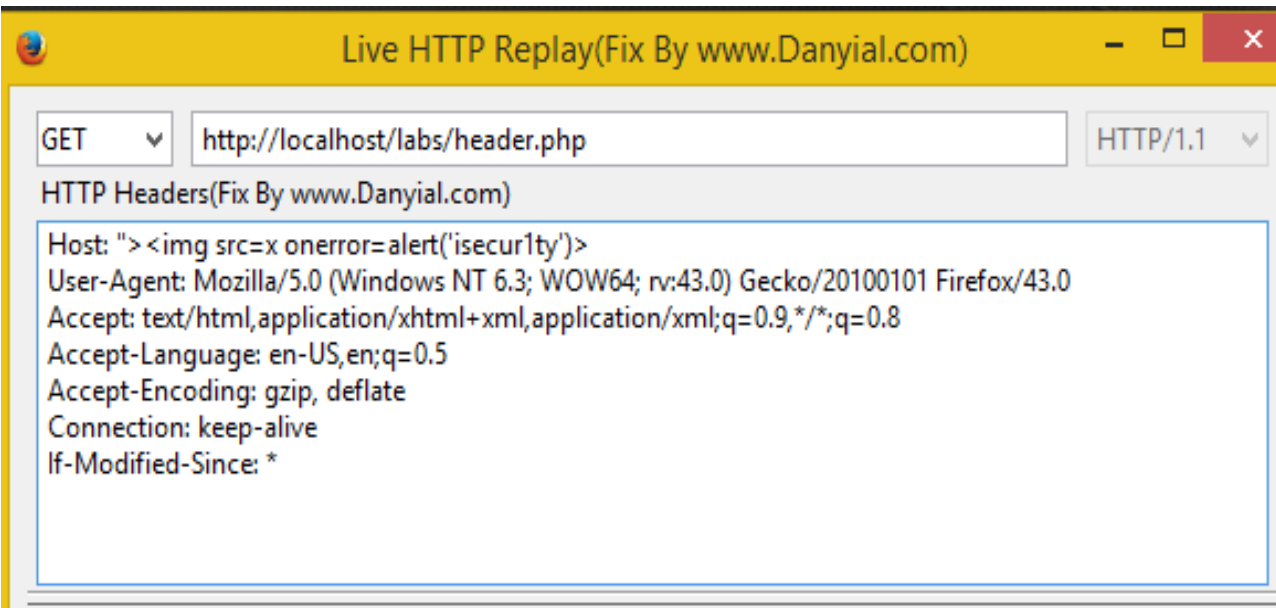
• في أكثر الأحيان يستخدم المبرمجون هذا العنصر في الصفحة لكي يستدعوا الروابط بدون تكرار اسم الموقع في البرمجة عن طريق معرفته من ال HOST حيث يوجد هنا سؤال : من أين عرف السيرفر ما هو الرابط المطلوب ؟

• الجواب : في الطلب الاصيل حين تذهب الى الموقع سوف يقوم المتصفح باضافة اسم الموقع الى الطلب في HOST

• الآن نقوم بعمل اختبار اختراق لثغرة XSS

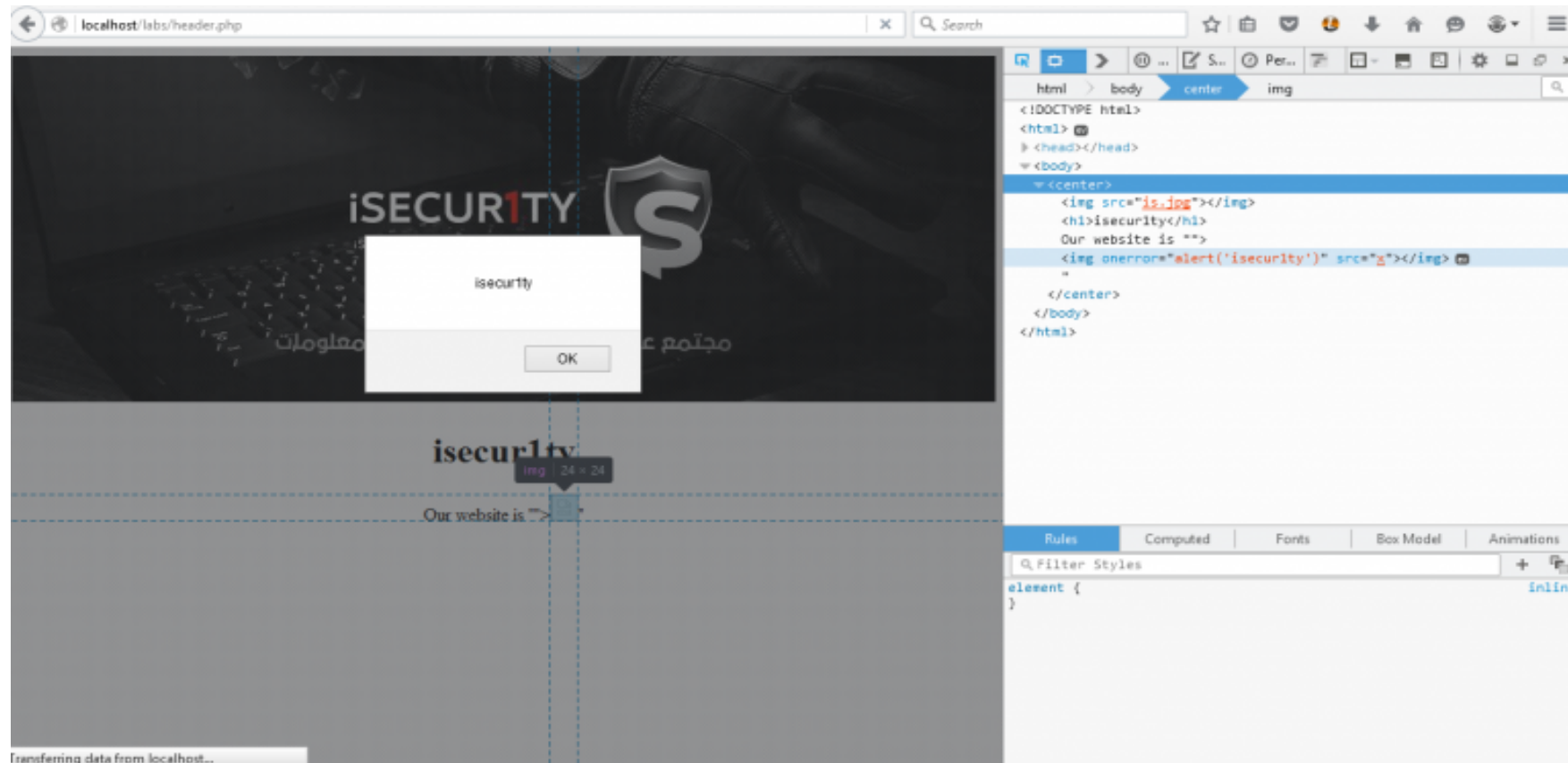
• لو نغير الطلب عن طريق اداة

live HTTP header كالتالي :



ثغرات ال HTTP Headers (تكملة...)

- سوف يقوم السيرفر بقراءة ال HOST وسوف يظهره بالصفحة وتحصل على ثغرة XSS




ثغرات ال HTTP Headers (تكملة...)

• REFERER

- الريفيرر هو مهم جداً في البرمجيات والكثير من المبرمجين يعتمدون عليه في العودة للصفحات السابقة او معرفة الصفحة التي أتى منها الزائر لغرض التحليل والاحصاء ، كمثال :
- لو دخلت لهذه الصفحة عن طريق Google، سيكون الطلب والصفحة كالآتي :

ثغرات ال HTTP Headers (تكملة...)

localhost/labs/header.php



isecur1ty

you can back to previous page from [here](http://www.google.com)

```
<!DOCTYPE html>
<html>
  <head></head>
  <body>
    <center>
      </img>
      <h1>isecur1ty</h1>
      you can back to previous page from here
      <a href="http://www.google.com">here</a>
    </center>
  </body>
</html>
```

Live HTTP Replay(Fix By www.Danyial.com)

GET http://localhost/labs/header.php HTTP/1.1

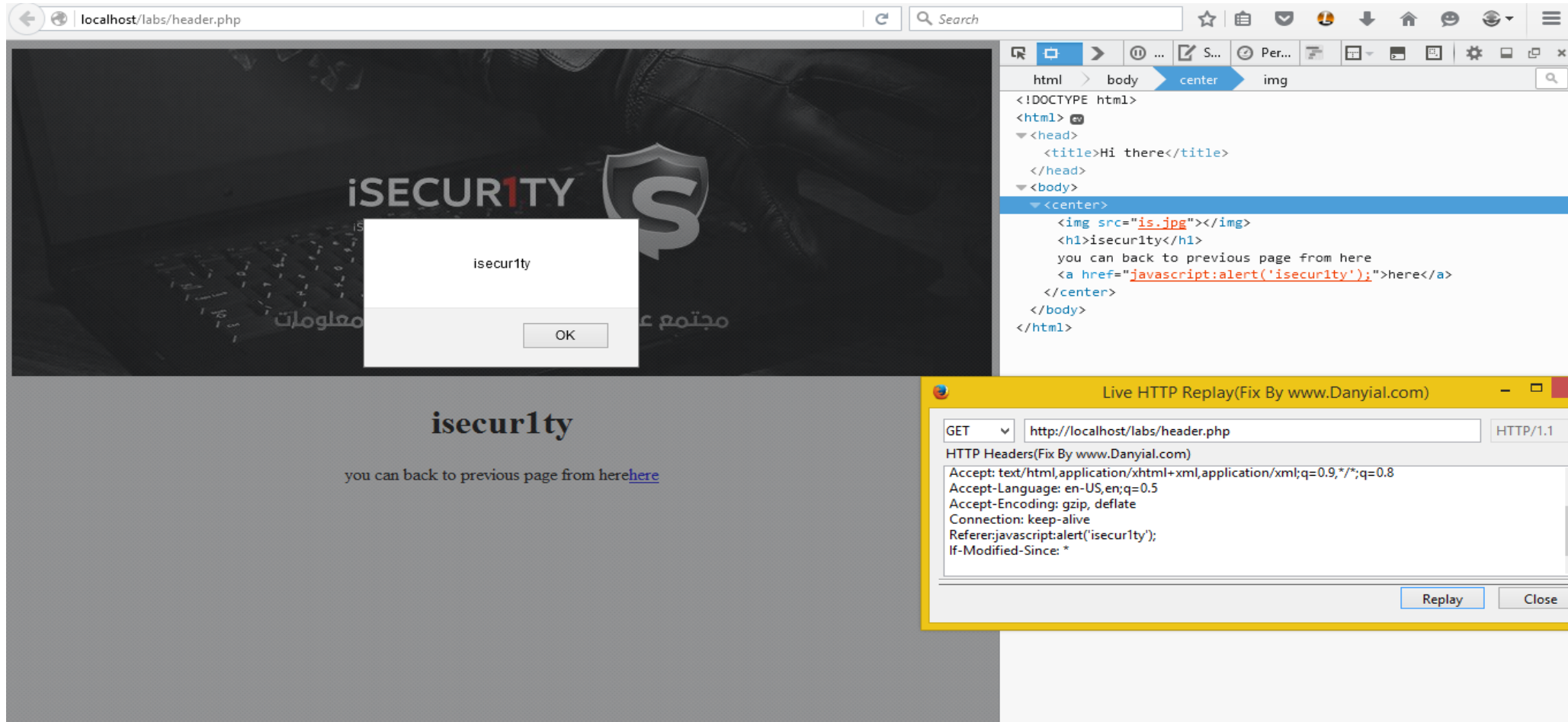
HTTP Headers(Fix By www.Danyial.com)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: <http://www.google.com>
If-Modified-Since: *

Replay Close

ثغرات ال HTTP Headers (تكملة...)

- لو غيرنا قيمة ال REFERER الى javascript:alert('isecur1ty'); سوف يتم اظهار الرابط كجافا سكربت ويتم تطبيقه بمجرد الضغط على الرابط



تم بحمد الله انتهاء الفصل التاسع عشر