الفصل الحادى عشر
ثغرة ال Click Jacking

المؤلف
د.م/ أحمد هاشم الفقي
استشارى أمن المعلومات و التحول الرقمي
Ahmed.Hashem.ElFiky@outlook.com

ثغرة ال Click Jacking

- تعرف الثغرة بمُصطلح متداول وهو" سرق الضغطات " هو هجوم يقوم به المهاجم باخفاء صفحة من موقع معين في صفحة اخرى وهمية حيث يريد ان يقوم الضحية بالضغط في مكان ما في الصفحة ليقوم بتنشيط فعالية او الموافقة على طلبات من الموقع للدخول الى موارد او غيرها ك OAuth مثلاً .
- لو فرضنا على سبيل المثال (example.isecur1ty.org) هو موقع عادي كل ما نحتاج اليه لكشف الثغرة هو الدخول للصفحة المطلوبة . بطلب GET
- الان نراجع الرد من السيرفر :

ثغرة ال Click Jacking (تكمله...)

```
Get:http://example.isecur1ty.org/ouath.page
```

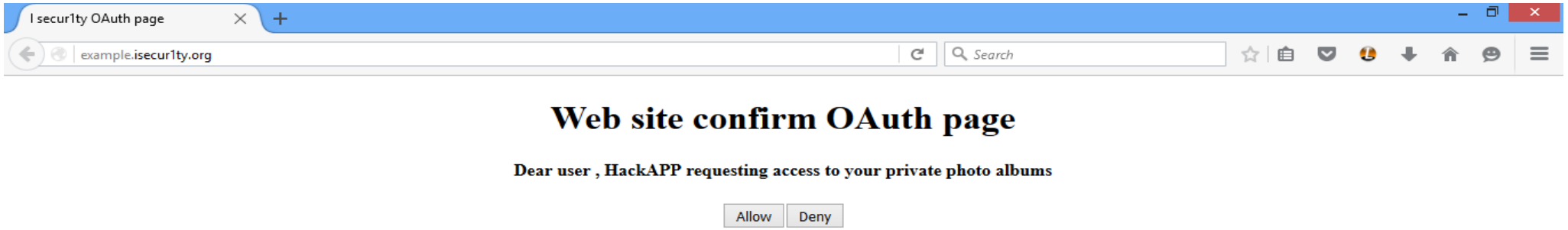
```
Host: example.isecur1ty.org
User-Agent: Mozilla/5.0 (Windows NT 6.2; WOW64; rv:44.0) Gecko/20100101 Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
If-Modified-Since: *<span style="color: #ffffff;">x
sdasd

</span>
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 11 Feb 2016 11:45:34 GMT
Content-Length: 1221
```

ثغرة ال Click Jacking (تكمله...)

- لا يوجد في هذه ال X-Frame-Options ولا يوجد قيمة له لذلك سيعرض المتصفح هذه الصفحة من اي frame أو Iframe او object في صفحة اخرى في موقع اخر .
- ممكن ان يكون الموقع مصاب بثغرة Clickjacking ناتي الان لنفحص الصفحة
- لو فرضاً ان example.isecur1ty.org موقع حفظ الصور و لديك صور مخفية وهناك خاصية يمكن من خلالها ان تسمح للتطبيقات بالدخول للصور المخفية بموافقتك .

ثغرة ال Click Jacking (تكمله...)

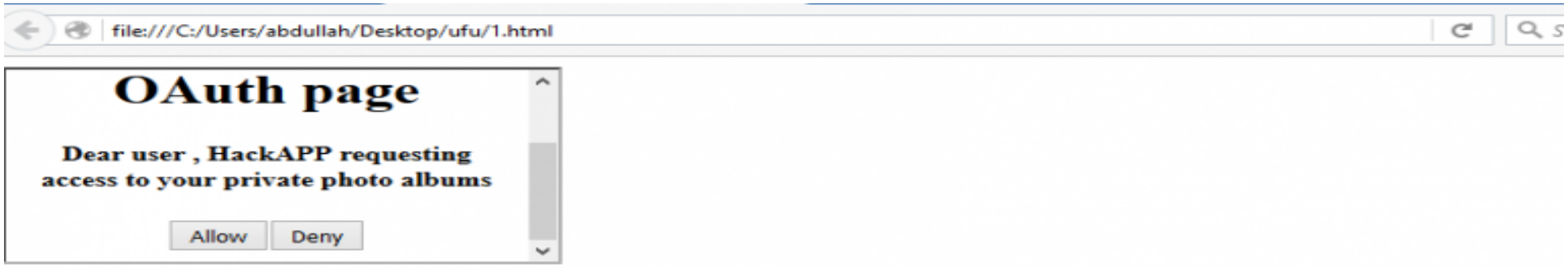


ثغرة ال Click Jacking (تكمله...)

- الان لنجرب الثغرة ونقوم بعمل صفحة html تحتوي على iframe في جهازنا وال iframe يؤدي الى example.isecur1ty.org/oauth.page

```
<"iframe src="http://example.isecur1ty.org/oauth.page?id=123&app=hackerapp>
```

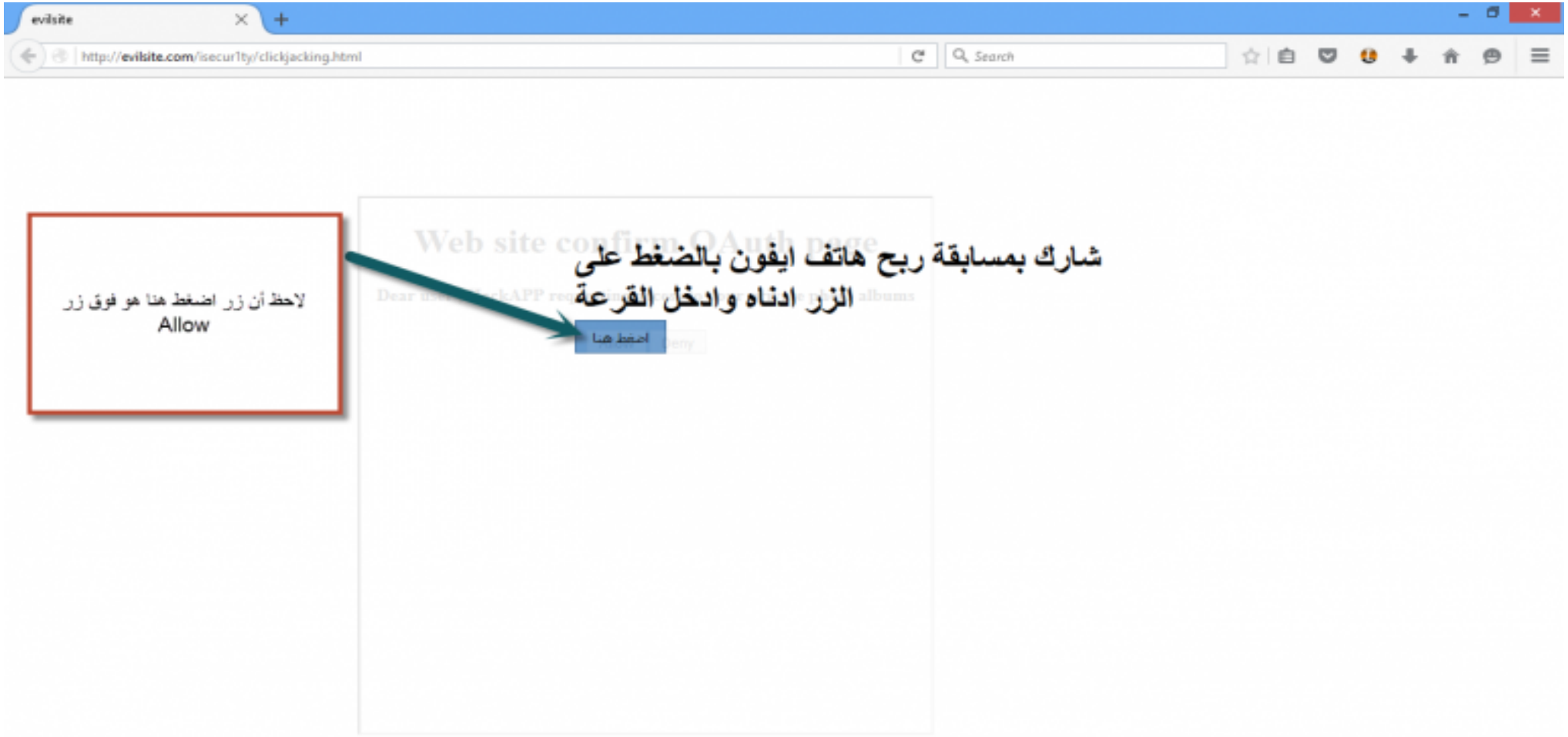
ثغرة ال Click Jacking (تكمله...)



ثغرة ال Click Jacking (تكمله...)

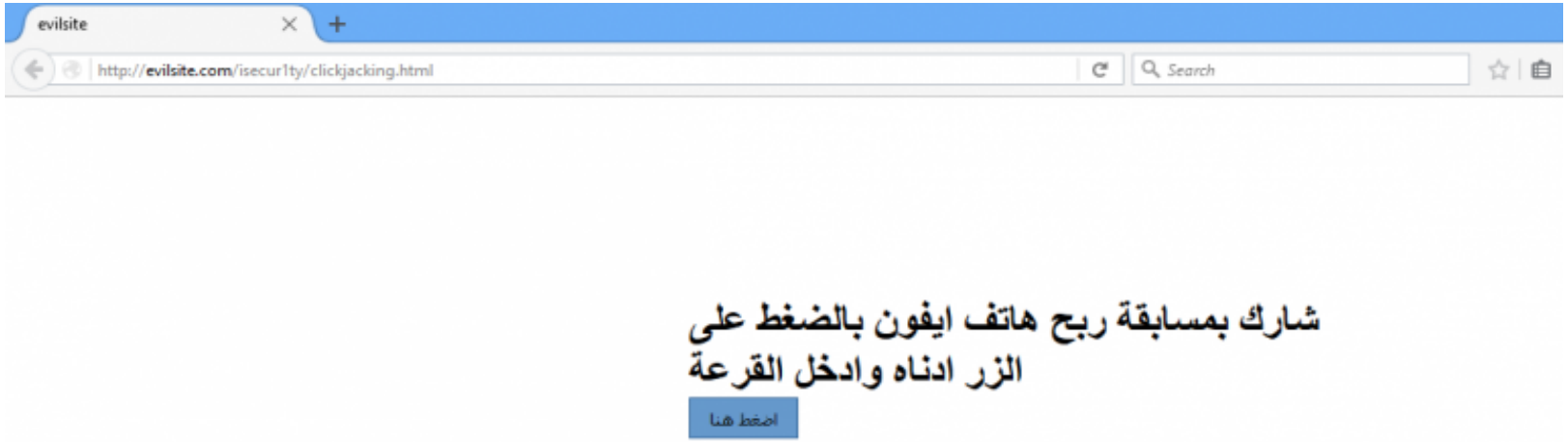
- تم الحصول على الصفحة في ال iframe في صفحة اخرى وبذلك فان الموقع مصاب بثغرة clickjacking في هذه الصفحة .
- الان سيتم اخفاء الايفريم ببعض خدع CSS سيتم اخفاء الايفريم في صفحة اخرى غير تابعة للموقع نفسه .

ثغرة ال Click Jacking (تكمله...)



ثغرة ال Click Jacking (تكمله...)

- الان ان صنعت هذه الصفحة كمثال بسيط وضعت مسابقة خدعة ووضعت زر اضغط هنا لكي اسرق ضغطة ويضغط فوق زر allow للسماح بتطبيق الهكر الخاص بي بسرقة الصور الخاصة به .
- الان ساخفي الايفريم تماماً



ثغرة ال Click Jacking (تكمله...)

- الان سيكون من السهل خداع الضحية وبمجرد ان يضغط على زر اضغط الان الذي هو معطل اصلا فهو يقوم بضغط زر allow في موقع example.isecur1ty.org بدون علمه ويسمح لتطبيقي الخبيث بالحصول على الصور .
- الحماية من الثغرة :
- يوجد العديد من الطرق لاصلح وتفادي الثغرة منها :
  - وضع X-Frame-Options في السيرفر لكل الصفحات او للصفحات المهمة .
  - برمجة جافا سكربت في الصفحات يقوم بمراجعة الصفحات في حالة عدم امكانية التحكم بالسيرفر او الصفحة .

ثغرة ال Click Jacking (تكمله...)

- بعض المعلومات حول X-Frame-Options
- يوجد قيم لهذا ال Header منها
  - DENY يمنع ان يتم استدعاء هذه الصفحة في Iframe
  - SAMEORIGIN يمكن استدعاء هذه الصفحة في نفس الموقع " فقط "عن طريق ايفريم (ينصح به) .
  - ALLOW-FROM uri السماح لرابط او موقع معين باستخدام الايفريم لربط هذه الصفحة.
- أصلاح عام للسيرفرات
- سيرفر اباتشي Apache
- يمكنك اضافة السطر التالي الى httpd.conf

```
1 Header always append X-Frame-Options SAMEORIGIN
```

ثغرة ال Click Jacking (تكمله...)

- سيرفر nginx
- في ملف nginx.conf اضفط السطر التالي في خانة السيرفر

```
1 add_header X-Frame-Options "SAMEORIGIN";<span style="color: #ffffff;">x
2 </span>
```

```
server {
    listen       80;
    server_name  localhost;
    server_tokens off;
    add_header X-Frame-Options "SAMEORIGIN";
```

ثغرة ال Click Jacking (تكمله...)

- سيرفر IIS
- في ملف Web.config اضف النص التالي

```
<system.webServer>

<httpProtocol>
<customHeaders>
<add name="X-Frame-Options" value="SAMEORIGIN" /   >
<customHeaders/>
<httpProtocol/>

<system.webServer/>
```

تم بحمد الله انتهاء الفصل الحادى عشر