

# JavaScript Static Analysis (Arabic)

بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله وبركاته

الكاتب:

عبدالرحمن عبدالله

تويتر:

[@Infosec 90](#)

الفئة المستهدفة :

مطور المواقع

مختبر اختراق

صائد مكافآت

مستوى الصعوبة

من متوسط الى متقدم

(سيتم ذكر سيناريو متوسط ومتقدم بحيث يمكن اكتشاف الثغرات عن طريق محرر نصوص او بشكل يدوي)

متطلبات الشرح:

PhpStrom تثبيت محرر نصوص برمجي بالشرح تم استخدام

(يمكن للطلاب او الخريجين اخذ نسخة مجانية باستخدام ايميل الجامعة)

نظام لينكس او يمكن استخدام النسخة المصغرة على ويندوز

يفضل المعرفة مسبقا في قراءة اكواد الجافا سكريبت

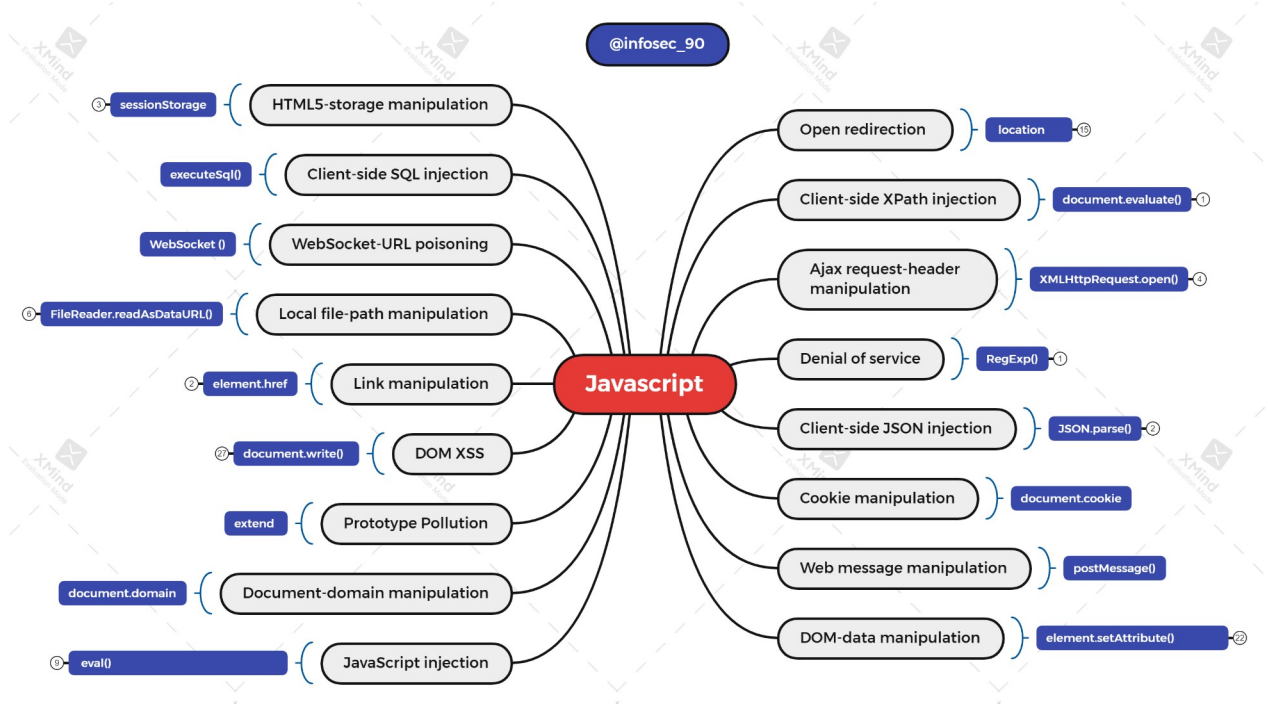
يفضل معرفة في التعامل مع التيرمنال

متوقع مخرجات المقالة:

جمع ملفات الجافا سكريبت من الهدف

اكتشاف عدة ثغرات في ملفات الجافا سكريبت

الحصول على اول CVE لك



<https://github.com/Ph33rr/attack/tree/main/Javascript>

عندما نتحدث عن سيناريو فحص blackbox عملية recon هي الاساس اذا كانت اعني نتائج افضل. والنتيجة ثغرات اكثر وسرعة في الاكتشاف في هذه المقالة لجمع ملفات الجافا سكريبت نستخدم recon ثم عمل تحليل للملفات وعمل اختبار اختراق بعدة طرق حيث تحدثت سابقا في مقالة عن webstroage بناءا على تجربة المستخدم وايضا تحدثت عن ماهي ملفات الجافا سكريبت ووظيفتها واهميتها بحيث اذا كنت لاتعلم ما هي يمكنك الرجوع للمقدمة الموجودة في المقالة والتي تشرح ماهي ملفات الجافا سكريبت بتفصيل اكثر حيث لن يتم اعادة تعريفها هنا وأيضا تجدون لاب لتجربة الثغرة وفهمها مع شرح امثلة حقيقية منها رواتر هواوي حيث كانت الإصابة بعدة إصدارات وتم إصلاحها

<https://github.com/Ph33rr/webstorage>

قبل البدء في عملية التحليل لملفات الجافا سكربت علينا ان نتعلم بعض الأساسيات  
نسرد لكم قصة قصيرة في احدى الأيام قرر صديق لنا السفر لحدى الدول كسائح  
لتمضية بعض الوقت كفترة نقاهة في يوم الثلاثاء استلم صديقنا ايميل  
من قبل احدى مواقع الحجوزات في الفنادق و يفيد الايميل  
بوجود خصم 50% على جميع الفنادق في حال تم الحجز خلال 24 ساعة  
فقرر صديقنا الحجز عن طريق هذا الموقع لاستغلال الخصم والاستفادة منه  
ولكن حدثت مشكلة اثناء الحجز

؟ بدون بطاقة؟

كيف ترغب بالدفع؟

CVC رمز



يمكنك أن تجد رمز CVC في الجزء الخلفي من بطاقة الائتمان الخاصة بك. إنها الأرقام الثلاثة الأخيرة المطبوعة على شريط التوقيع.

\* اسم حامل البطاقة

Abdullah Abdulrahman

\* نوع البطاقة

MasterCard

\* رقم بطاقة الائتمان / الخصم

\* تاريخ انتهاء الصلاحية

برجى إدخال تاريخ انتهاء صلاحية صالح خلال تواريخ حرك

X 2018 / 01

\* رمز CVC

454

✓ أضف بطاقة الائتمان هذه لحسابك للحصول على حجز أسرع

بطاقة الائتمان انتهت صلاحياتها حاول صديقنا الاتصال بالبنك

لمحاولة الاستفادة من العرض كان رد البنك سيتم ارسال بطاقة جديدة بعد 15 يوم عمل  
عندها سيكون العرض منتهي فكر وفكر صديقنا المبرمج هل يوجد حل خصوصا ان الموقع  
لايحتاج الى خصم المبلغ بالوقت الحالي فقط يحتاج الى بطاقة انتمان لسوء حظ هذا الموقع  
ان صديقنا لديه خلفية في البرمجة صديقنا يرغب في هذا العرض بشدة  
وبعد بحث مطول بطريقة مختصرة في الموقع باستخدام أدوات المطور في المتصفح  
توصل صديقنا للتالي:

```

> FormData
< f FormData() { [native code] }

> TargetDate
< "12/31/2020 5:00 AM"

> booking_extra
< {pageview_id: "2625740834810018", b_aid: "397594", b_stid: "397594", b_lang_for_url: "ar", b_gtt: "a
  b_action: "book"
  b_aid: "397594"
  b_bp_blocks: [""]
  b_bp_checkin: "2020-08-26"
  b_bp_checkout: "2020-09-23"
  b_bp_hid: "1920592"
  b_bp_stage: "3"
  b_ch: "d"
  b_gtt: "a
  b_lang_for_url: "ar"
  b_site_type_id: "1"
  b_stid: "397594"
  pageview_id: "2625740834810018"
  [[Prototype]]: Object

> dthen
< Thu Dec 31 2020 05:00:00 GMT+0300 (Arabian Standard Time)

> performance
< Performance {timeOrigin: 1609375000.7, onresourcetimingbufferfull: null, eventCounts: EventCount
  s, timing: PerformanceTiming, navigation: PerformanceNavigation, ...}
  eventCounts: EventCounts {size: 36}
  memory: MemoryInfo {totalJSHeapSize: 22672249, usedJSHeapSize: 20448089, jsHeapSizeLimit: 217
  navigation: PerformanceNavigation {type: 0, redirectCount: 0}
  onresourcetimingbufferfull: null
  timeOrigin: 1609375000.7
  timing: PerformanceTiming {navigationStart: 1609375000.7, unloadEventStart: 1609375000.7, unloa...
  [[Prototype]]: Performance

```

صديقنا بدا في البحث في عدة متغيرات بعضها تستخدم تاريخ كنص وبعضها تستخدم timestamp بعد تعديلها تم قبول بطاقة صديقنا

اسم حامل البطاقة \*

Abdullah Abdulrahman

نوع البطاقة \*

MasterCard

رقم بطاقة الائتمان / الخصم \*

تاريخ انتهاء الصلاحية \*

2018 / 01

رمز CVC \*

454

أضف بطاقة الائتمان هذه لحسابك للحصول على حجز أسرع ☒



"East Side Studio طريق عن Booki  
ng.com" <[REDACTED]  
[REDACTED]@booking.c  
om>



يتحمل مزود مكان الإقامة مسؤولية محتوى هذه الرسالة بالكامل. رسالة عبر  
Booking.com.

Dear ABDULRAHMAN,

Thanks for booking East Side Studio. We are looking forward to  
welcoming you in [REDACTED]!

Once you have arrived at the airport or are 30 minutes away from  
[REDACTED], can you please give me a call at this number

+316 21216951. If you want to check in always call 30 minutes ahead

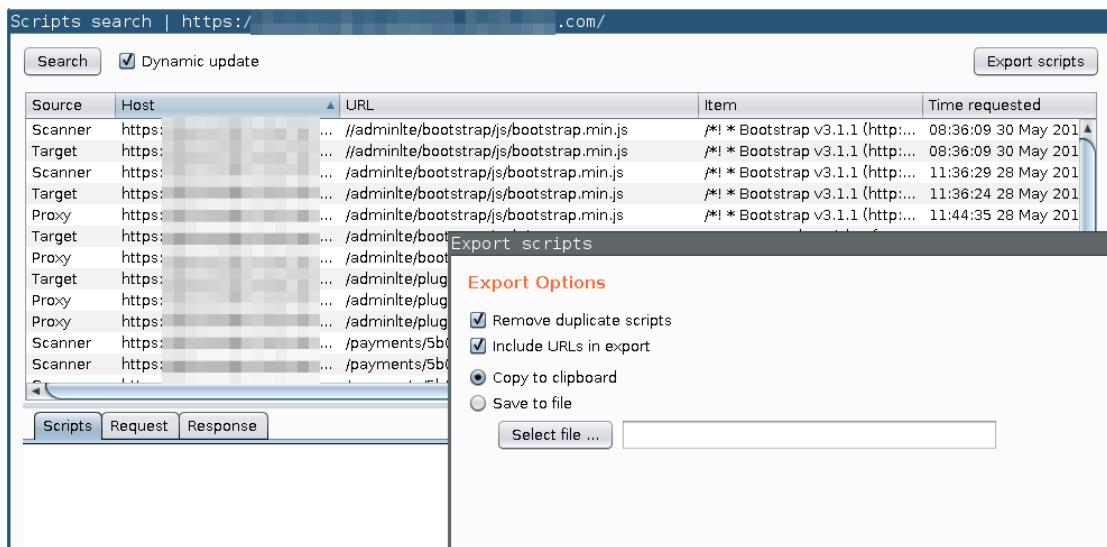
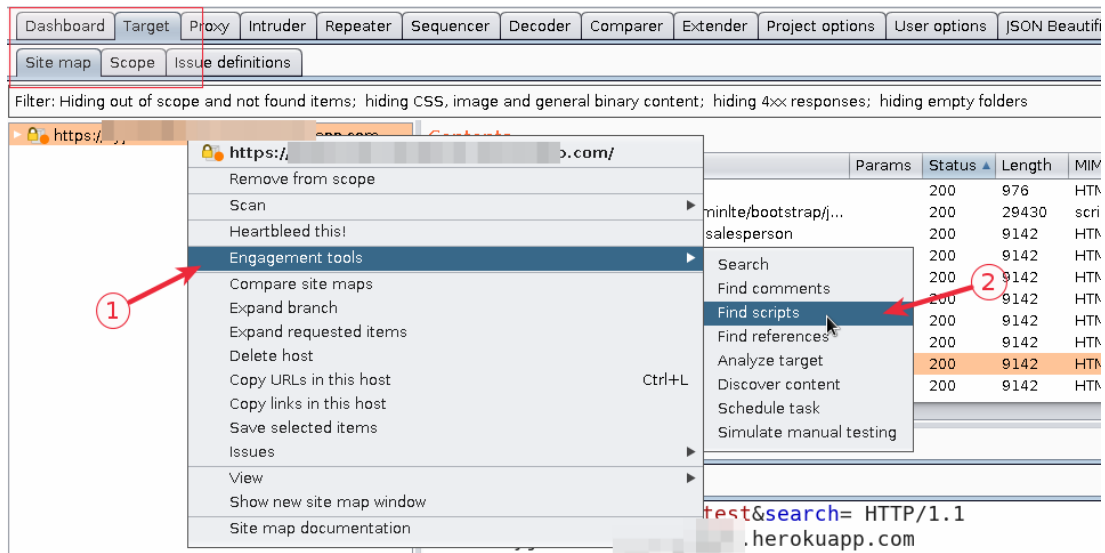
وبعدها عاش صديقنا في سعادة غامرة شكرا جافا سكرت

لنذهب الى الجزء العملي ولا يتضمن قصص خيالية

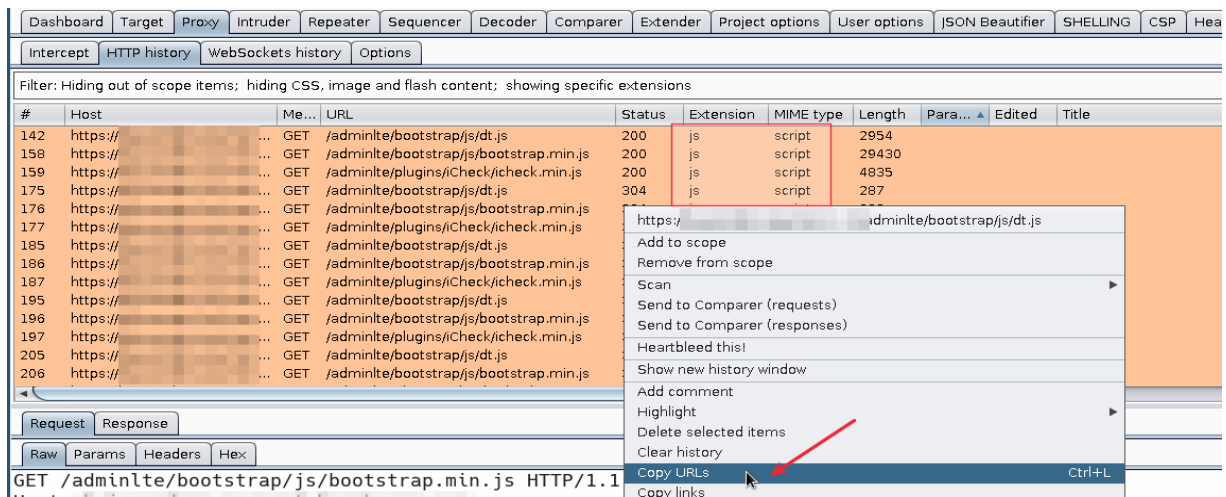
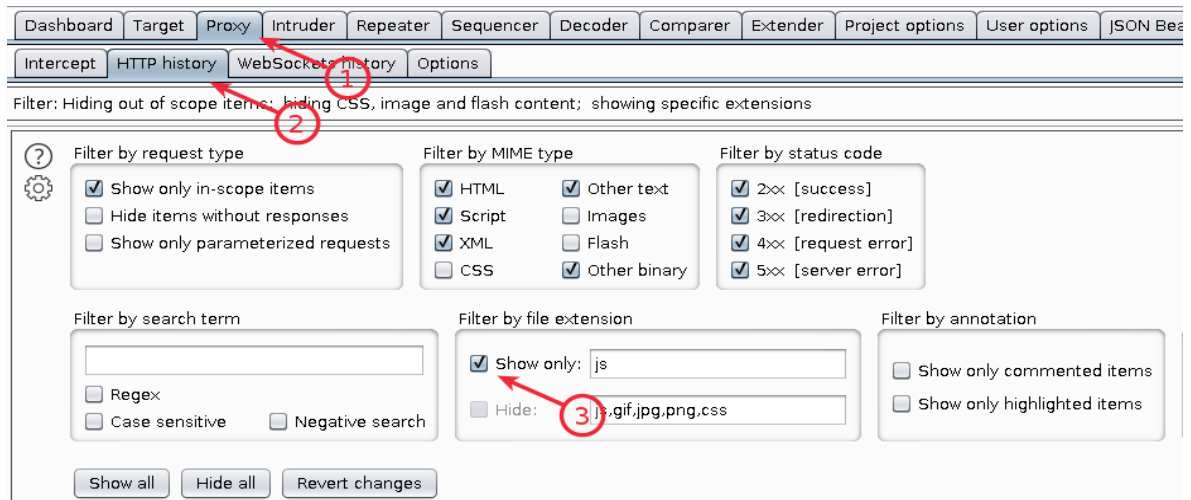
## جمع ملفات الجافا سكريبت

توجد عدة طرق في جمع ملفات الجافا سكريبت من موقع محدد او مجموعة مواقع ولكل شخص  
**Methodology** خاصة به نذكر منها التالي :

### استخدام burpsuite لحفظ ملفات الجافا سكريبت بجهازك



هذه فقط متواجدة في النسخة المدفوعة لكن للنسخة المجانية نتبع الطريقة التالية لنسخ الروابط



والان نحفظ روابط ملفات الجافا سكريبت في ملف txt مثال:

targetJS.txt



بعد حفظ الروابط في ملف txt

نكتب Loop لتحميل ملفات الجافا سكريبت في جهازنا

for i in \$(cat targetJS.txt);do wget \$i;done

```
https://github.githubassets.com/assets/chunk-profile-860a1228.js
https://github.githubassets.com/assets/chunk-readme-toc-element-5bf0869b.js
https://github.githubassets.com/assets/chunk-ref-selector-fd78f451.js
https://github.githubassets.com/assets/chunk-responsive-underlinenav-0ff33106.js
https://github.githubassets.com/assets/chunk-runner-groups-496cb7e9.js
https://github.githubassets.com/assets/chunk-series-table-49574ad0.js
https://github.githubassets.com/assets/chunk-severity-calculator-element-b64efa7a.js
https://github.githubassets.com/assets/chunk-sortable-behavior-8fb3dbd4.js
https://github.githubassets.com/assets/chunk-three.module-9ca6b751.js
https://github.githubassets.com/assets/chunk-toast-58af155f.js
https://github.githubassets.com/assets/chunk-tweetsodium-d6f499bf.js
https://github.githubassets.com/assets/chunk-unveil-7ef70e39.js
https://github.githubassets.com/assets/chunk-user-status-submit-50e14d5b.js
https://github.githubassets.com/assets/chunk-webgl-warp-70abbff9.js
```

```
(kali@kali)-[~/Desktop]
$ cat FileJs.txt|cut -d = -f 9|cut -d \" -f 2 > targetJS.txt
```

```
(kali@kali)-[~/Desktop]
$ for i in $(cat targetJS.txt);do wget $i;done
```

```
(14.9 MB/s) - 'chunk-unveil-7ef70e39.js' saved [682/682]
https://github.githubassets.com/assets/chunk-user-status-submit-50e14d5b.js
Resolving github.githubassets.com (github.githubassets.com)... 185.199.110.154, 185.199.111.154,
Connecting to github.githubassets.com (github.githubassets.com)|185.199.110.154|:443... connecte
HTTP request sent, awaiting response... 200 OK
Length: 8038 (7.8K) [application/javascript]
Saving to: 'chunk-user-status-submit-50e14d5b.js' integrity="sha512-
chunk-user-status-submit-50e14d5b.js 100%[=====]
(792 KB/s) - 'chunk-user-status-submit-50e14d5b.js' saved [8038/8038]
https://github.githubassets.com/assets/chunk-webgl-warp-70abbff9.js
Resolving github.githubassets.com (github.githubassets.com)... 185.199.110.154, 185.199.108.154,
Connecting to github.githubassets.com (github.githubassets.com)|185.199.110.154|:443... connecte
HTTP request sent, awaiting response... 200 OK
Length: 7409 (7.2K) [application/javascript]
Saving to: 'chunk-webgl-warp-70abbff9.js' integrity="sha512-
chunk-webgl-warp-70abbff9.js 100%[=====]
(1.27 MB/s) - 'chunk-webgl-warp-70abbff9.js' saved [7409/7409]
(kali@kali)-[~/Desktop]
$
```

الان تم حفظ الملفات المراد فحصها في الجهاز

سيناريو اخر نستخدم اداعة JS\_Scrapper

برمجة الاخ مشعل @Mesh3l\_911

: لتنزيل الاداعة

[https://github.com/Mesh3l911/JS\\_Scrapper](https://github.com/Mesh3l911/JS_Scrapper)

```
JS for https://medium.com/ :  
https://cdn-client.medium.com/lite/static/js/manifest.9a8ac41b.js  
https://cdn-client.medium.com/lite/static/js/9115.1a9358c4.js  
https://cdn-client.medium.com/lite/static/js/main.444bb8d9.js  
https://cdn-client.medium.com/lite/static/js/5573.159bf40f.chunk.js  
https://cdn-client.medium.com/lite/static/js/instrumentation.79ae5839.chunk.js  
https://cdn-client.medium.com/lite/static/js/reporting.6471519f.chunk.js  
https://cdn-client.medium.com/lite/static/js/2499.851d7502.chunk.js  
https://cdn-client.medium.com/lite/static/js/192.961ccdd2.chunk.js  
https://cdn-client.medium.com/lite/static/js/1645.857c77e3.chunk.js  
https://cdn-client.medium.com/lite/static/js/8940.b1644406.chunk.js  
https://cdn-client.medium.com/lite/static/js/1801.e27003de.chunk.js  
https://cdn-client.medium.com/lite/static/js/7883.1f12fa26.chunk.js  
https://cdn-client.medium.com/lite/static/js/2018.cda2d533.chunk.js  
https://cdn-client.medium.com/lite/static/js/2264.1681143f.chunk.js  
https://cdn-client.medium.com/lite/static/js/1478.b1452ac2.chunk.js  
https://cdn-client.medium.com/lite/static/js/3955.f6285986.chunk.js  
https://cdn-client.medium.com/lite/static/js/1373.2fa5a199.chunk.js  
https://cdn-client.medium.com/lite/static/js/Homepage.1d77d301.chunk.js  
$ for i in $(cat targetJS.txt);do wget $i;done
```

الان نحفظ الروابط في ملف txt ثم ننفذ Loop مثل المره السابقة

لحفظ ملفات الجافا سكربت في الجهاز

طرق اخرى

استخدام اداة Linkfinder

<https://github.com/GerbenJavado/LinkFinder>

وطريقة اخرى تستخدم Archive

[https://web.archive.org/cdx/search/cdx?](https://web.archive.org/cdx/search/cdx?url=google.com&matchType=domain&fl=original&collapse=urlkey&output=text&filter=statuscode:200)

[url=google.com&matchType=domain&fl=original&collapse=urlkey&output=text&filter=statuscode:200](https://web.archive.org/cdx/search/cdx?url=google.com&matchType=domain&fl=original&collapse=urlkey&output=text&filter=statuscode:200)

وتنفيذ نفس Loop لتنزيل ملفات الجافا سكربت ولاتنسى استخدام الامر grep لفلتر النتائج JS

خارج الموضوع هدية

تغيير statuscode في الرابط من الرقم 200 الى الرقم 403 ثم استخدام Loop على كل الروابط وعند وجود رابط الرد 200 يكون تخطيت 403 وحصلت على ثغرة بشكل سريع سيتم شرحها في تغريدة

توجد ايضا عدة طرق اخرى وادوات لم يتم ذكرها يجب عليك بناء Methodology خاصة بك

في جمع ملفات الجافا سكربت

بعد الانتهاء من جمع الملفات تنتقل للخطوة التالية التحليل والبحث:

بعد ما تم حفظ الملفات في مجلد الان نستخدم التيرمنال للبحث عن بعض الدوائل الموجودة في الملفات السيناريو سيكون كالتالي البحث عن Domxss واكثر دالة مصابة هي innerHTML موضحة في الخريطة الذهنية بعد معرفة الدالة نعيد كتابتها بحيث يمكن تتبعها بسهولة وإذا كانت تحتوي على regex نتخطاها او نتعلم كيفية عملها بطريقة اسرع واسهل نبدا في البحث بالطريقة التقليدية حيث تم حفظ الملفات في مجلد باسم test

```
kali@kali: ~/D
File Actions Edit View Help

(kali@kali)~[~/Desktop]
$ grep "innerHTML" -r test
test/ie7.js: var html = el.innerHTML;
test/ie7.js: el.innerHTML = '<span style="font-family: \'cycle2-icons
test/jquery.templ.min.js:(function(a){var r=a.fn.domManip,d="_tmplitem",q=/^[^<]*
i){var c={data:i||(d?d.data:{}),_wrap:d?d._wrap:null,tmpl:null,parent:d||null,no
){c.tmpl=g;c._cnt=c._cnt||c.tmpl(a,c);c.key++;h;(l.length?f:b)[h]=c}return c}a
replaceAll:"replaceWith"},function(f,d){a.fn[f]=function(n){var g=[],i=a(n),k,h,
ength===1&&i.length===1){i[d](this[0]);g=this}else{for(h=0,m=i.length;h<m;h++){d
s.pushStack(g,f,i.selector)}l=e;e=null;a.tmpl.complete(l);return g}});a.fn.exten
Item(this[0])},template:function(b){return a.template(b,this[0])},domManip:func
i<g&&(h=a.data(d[i++], "tmplItem")));if(g>1)f[0]=[a.makeArray(d)];if(h&&c)f[2]=f
0;!e&&a.tmpl.complete(b);return this}});a.extend({tmpl:function(d,h,e,c){var j,k
c.nodes=[];c.wrapped&&n(c,c.wrapped);return a(i(c,null,c.tmpl(a,c)))}if(!d)retur
)?a.map(h,function(a){return a?g(e,c,d,a):null}):[g(e,c,d,h)];return k?a(i(c,nul
(c=a.data(b, "tmplItem"))&&(b=b.parentNode));return c||p},template:function(c,b){
.data(b, "tmpl")||a.data(b, "tmpl", o(b.innerHTML));return typeof c=="string"?a.t
te(null,q.test(c)?c:a(c)):null},encode:function(a){return ("<").split("<").join(
extend(a.tmpl,{tag:{tmpl:{_default:{$2:"null"},open:"if($notnull_1){_=_concat($
e:"call=$item.calls();_=_concat($item.wrap(call,_));"},each:{_default:{$2:
}}},"if":{open:"if(($notnull_1) && $1a){",close:""},"else":{_default:{$1:"true"
:{$_default:{$1:"$data"},open:"if($notnull_1){_.push($encode($1a));"}},"!":{open
Array(b.childNodes):b.nodeType===1?[b]:[];d.call(f,b);m(e);c++}});function i(e,g
[\s>])(?![^\>]*_tmplitem)([^\>]*)/g,"$1 "+d+"'"+e.key+"' "$2'):a(i(a,e,a._cnt))}:
/,function(f,c,e,d){b=a(e).get();m(b);if(c)b=j(c).concat(b);if(d)b=b.concat(j(d)
urn a.makeArray(b.childNodes)}function o(b){return new Function("jQuery","$item"
```

لم نجد شيء مهم او يمكن تتبعه بسهولة نبحث عن دالة أخرى document.location



```
(kali㉿kali)-[~/Desktop]
$ grep "document.location" -r test
test/redirect1.txt:if(isValidUrl(document.location.hash.slice(1))) {
test/redirect1.txt:    document.location = document.location.hash.slice(1);
test/tinyMCE.min.js:!function(){"use strict";var o=function(){for(var e=[],t=0;t<arguments.length;t++)e[t]=arguments[t];return n(r.apply(null,e))}}
on d(r){for(var o=[],e=1;e<arguments.length;e++)o[e-1]=arguments[e];return function
t(e);return r.apply(null,n)}}var e,t,n,r,i,a,u,s,c,l,f,m,g,p,h,v,b,y=function(n){re
return!n.apply(null,e)}};C=j(!1),x=j(!0),w=C,N=x,E=function(){return S},S=(r={fold:
n e},getOrThunk:t=function(e){return e()},getOrDie:function(e){throw new Error(e|| "
Undefined:function(){return undefined},or:n,orThunk:t,map:E,ap:E,each:function(){},
isNone()},equals_:e,toArray:function(){return[]},toString:j("none()")},Object.freez
(){return o},r=function(e){return e(n)},o={fold:function(e,t){return t(n)},is:funct
OrNull:e,getOrUndefined:e,or:t,orThunk:t,map:function(e){return k(e(n))},ap:functio
bind:r,flatten:e,exists:r,forall:r,filter:function(e){return e(n)?o:S},equals:funct
return t(n,e)}},toArray:function(){return[n]},toString:function(){return"some("+n+"
fined?S:k(e)}},T=function(t){return function(e){return function(e){if(null===e)retu
e)?"array":"object"}===t&&String.prototype.isPrototypeOf(e)?"string":t}(e)===t}},R=T
tion"),L=T("number"),I=(i=Array.prototype.indexOf)===undefined?function(e,t){return
},$=function(e,t){for(var n=e.length,r=new Array(n),o=0;o<n;o++){var i=e[o];r[o]=t(
)},W=function(e,t){for(var n=[],r=[],o=0,i=e.length;o<i;o++){var a=e[o];(t(a,o,e)?n
ngth;r<o;r++){var i=e[r];t(i,r,e)&&n.push(i)}return n},U=function(e,t,n){return F(e
{var o=e[n];if(t(o,n,e))return A.some(o)}return A.none()),K=function(e,t){for(var n
unction(e,t){for(var n=0,r=e.length;n<r;++n)if(e[n]===t)return n;return-1},Y=Array.
gth;n<r;++n)if(!Array.prototype.isPrototypeOf(e[n]))throw new Error("Arr.flatten i
,J=function(e,t){for(var n=0,r=e.length;n<r;++n)if(!0===t(e[n],n,e))return!1;return
M(t,e)}},ee=function(e){return 0===e.length?A.none():A.some(e[0])},te=function(e){
//var keyNav;
```

```
",t<r?Math.floor((r-t)/2):0);
test/mctabs.js: var pos, url = document.location.href;
```

```
(kali㉿kali)-[~/Desktop]
```

وجدنا شيء يستحق التتبع في ملف mctabs.js

```
mctabs.js
File Edit Search Options Help
if (!avoidFocus) {
    tabElm.focus();
}

// Show selected panel
t.showPanel(panelElm);
}
};

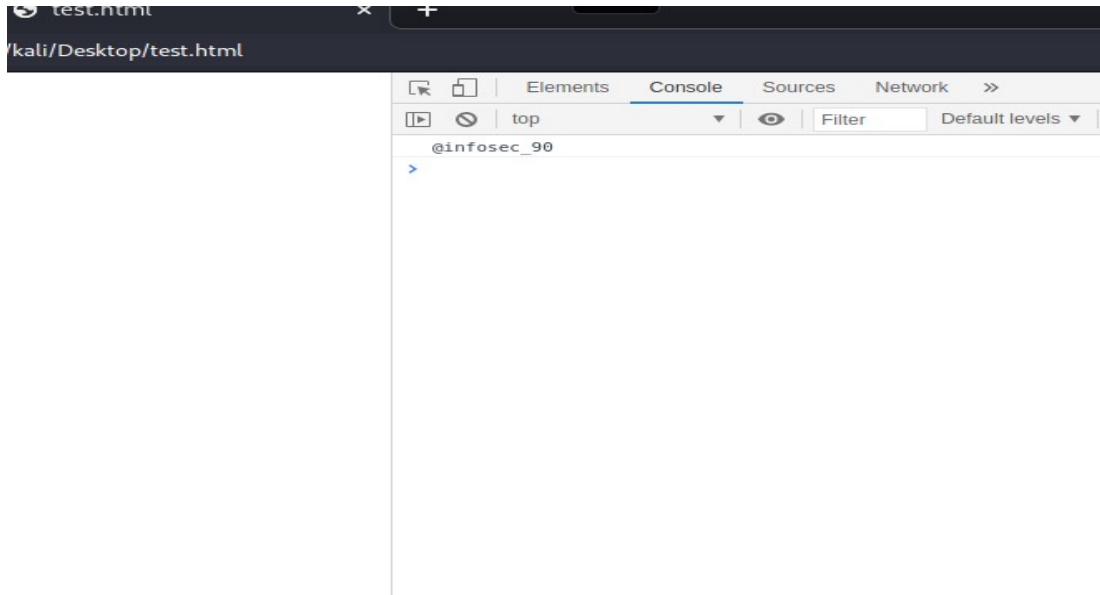
MCTabs.prototype.getAnchor = function() {
    var pos, url = document.location.href;

    if ((pos = url.lastIndexOf('#')) != -1)
        return url.substring(pos + 1);

    return "";
};

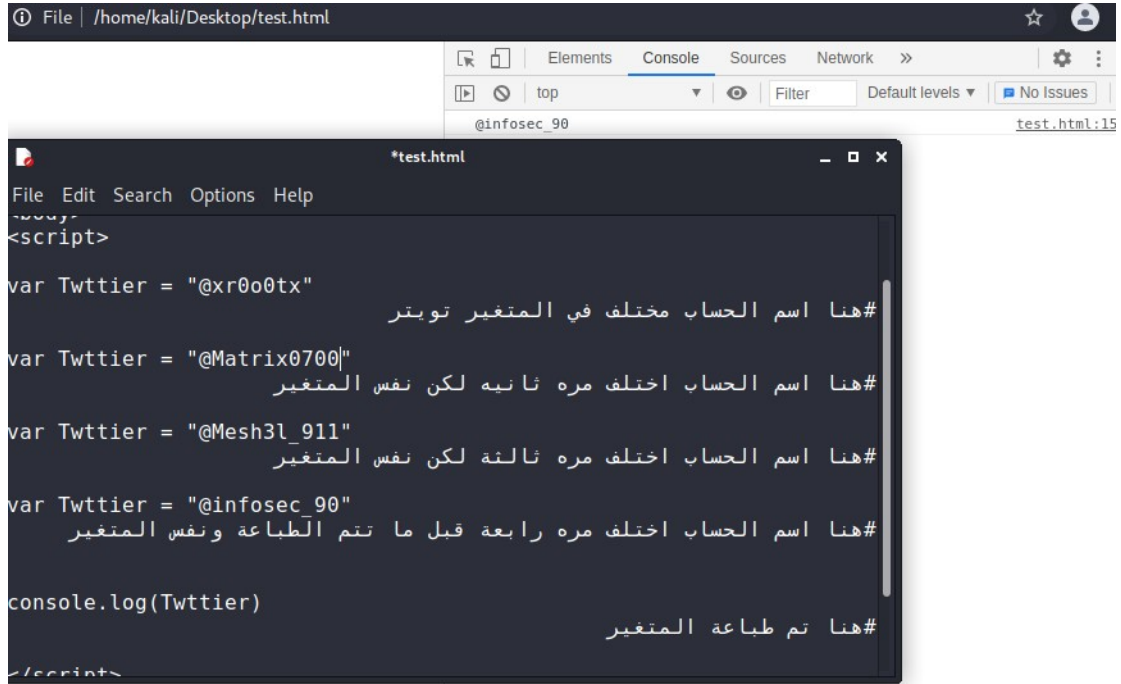
//Global instance
var mcTabs = new MCTabs();
```

وجدنا فنكشن الان نحتاج نعدل على الفنكشن لاختبارها وتتبعها وهذه من اهم الخطوات  
فهمك لهذه **Methodology** تختصر الوقت لك خصوصا عند محاولة تتبع دالة معينة او متغير  
في تطبيق فيه الالف الاسطر اذا لم تستطيع فهمها من المره الأولى لابس يمكنك السؤال او إعادة قراءتها  
الطريقة جدا بسيطة وهيا عند محاولة تتبع دالة معينة او متغير نستخدم **print**  
الان بشرح **Methodology** بطريقة مبسطة على جافا سكربت قبل تعديل الفنكشن طبعا وتعمل على كل اللغات  
لنفرض دخلنا على موقع وفيه ملف جافا سكربت يطبع اسم حساب في المتصفح كيف نتتبع المتغير



اول خطوة هيا عرض مصدر الصفحة وتتبع كود الجافا سكربت ضروري نتتبع الكود قبل الطباعة هل تم تنفيذ اكواد  
برمجية قبل طباعة النتيجة النهائية وهيا اسم الحساب **@infosec\_90**

بعد عرض المصدر وجدنا ان قبل طباعة الحساب تم تغيير الحساب اكثر من مره



المبرمج قبل طباعة النتيجة النهائية المتغير اختلف اكثر من 3 مرات وظهرت لنا النتيجة الأخيرة كان بالاول الاسم

mesh3l\_911 ثم اختلف الى matrix0700 ثم اختلف الى xr0o0tx

وقبل الطباعة اصبح infosec\_90

هذه الاختلافات في المتغير او الدالة لم تظهر لنا في البداية عند زيارة الموقع

فقط ظهر لنا اسم واحد وهو اسم infosec\_90

في الكود المبرمج استخدم المتغير اكثر من مرة بطريقة مختلفة فيه كم شخص يقول كود الجافا سكربت جدا واضح وتتبعه سهل كلامك لكن اذا كان فيه اكثر من 10 الالف سطر واكثر من 50 ملف جافا سكربت كيف تتبع الدالة

ببساطة نستخدم الMethodology الprint

الا هيا في كل مره لتتبع المتغير في جافا سكربت او اي لغة برمجية نستخدم print بين الاسطر

لنتبع المتغير او الدالة الان نحاول نتتبع المتغير باستخدام امر الطباعة في جافا سكربت وهو

console.log

عدلنا الكود بحيث في كل مره المتغير يتغير يتم طباعته لنا لمعرفة اين وصل المتغير وماهي قيمته في كل مره  
تفيد اكثر في حالة كان عدد الاسطر يتجاوز 10 الالف او عدد كبير ونختصر الوقت بهذا الطريقة

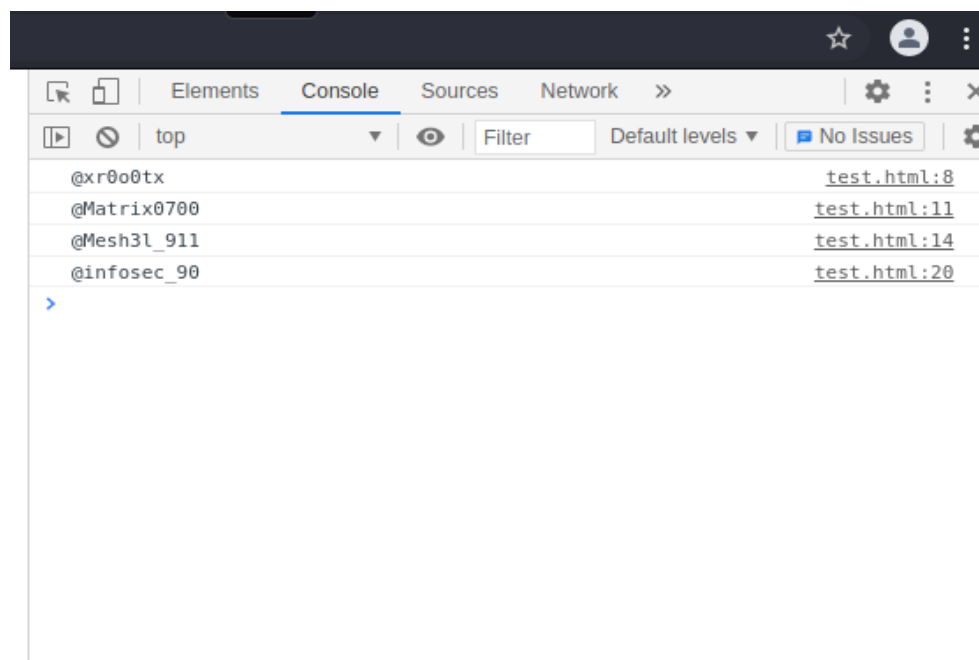
```
File Edit Search Options Help
<script>
var Twttier = "@xr0o0tx"
console.log(Twttier)

var Twttier = "@Matrix0700"
console.log(Twttier)

var Twttier = "@Mesh3l_911"
console.log(Twttier)

var Twttier = "@infosec_90"
console.log(Twttier)
</script>
```

### النتيجة النهائية لمتغير Twitter



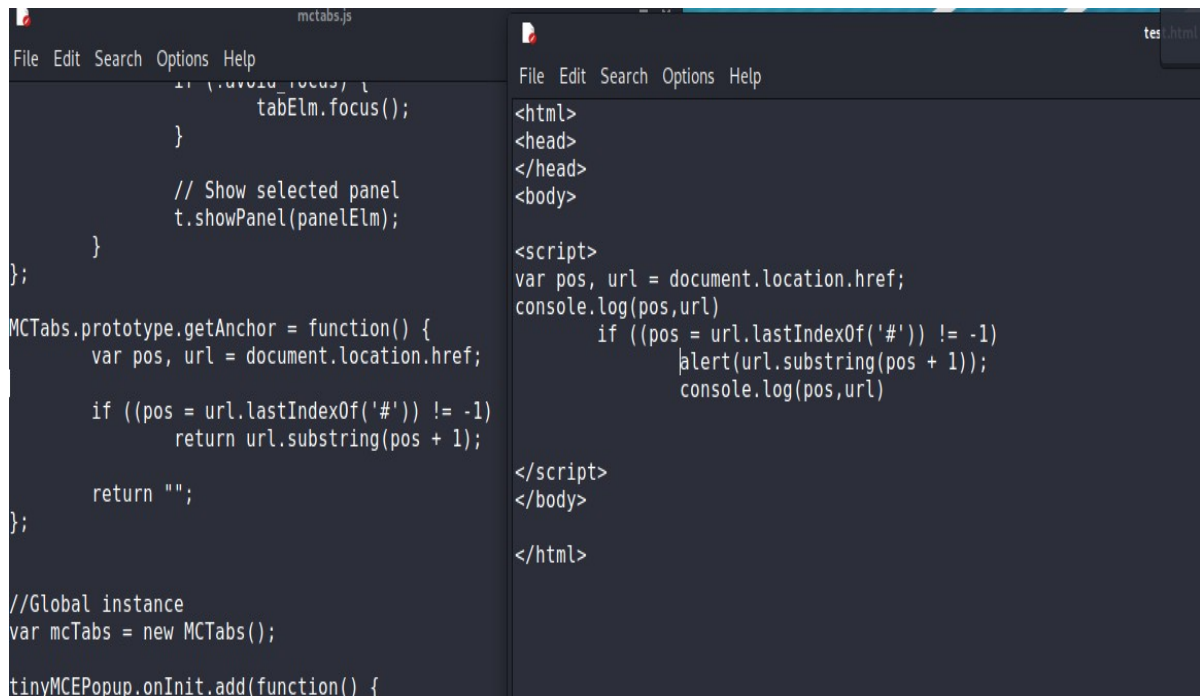


بهذا الطريقة نقدر نتتبع متغير والمراحل الا مختلف فيها وهل يمكن استغلاله او لا هذا Methodology تختصر وقت كثير في تتبع المتغيرات نرجع الان للفنكشن الا تم ايجادها ونعدل الفنكشن اول شي نستخرجها ونعيد كتابتها

شرح بسيط لها

```
MCTabs.prototype.getAnchor = function() {  
    |  
    var pos, url = document.location.href;  
    # pos + url يتم تخزين فيه العنوان  
  
    if ((pos = url.lastIndexOf('#')) != -1)  
        # هنا شرط ان يكون في العنوان علامة # ليتم تخزينها  
  
    return url.substring(pos + 1);  
    # هنا يتم تخزين اي نص او عنوان بعد علامة # الموجودة في الرابط  
  
    return "";  
};
```

الان نستخرجها ونعيد كتابتها



```
mctabs.js  
File Edit Search Options Help  
1. (function() {  
    tabElm.focus();  
    }  
  
    // Show selected panel  
    t.showPanel(panelElm);  
    }  
};  
  
MCTabs.prototype.getAnchor = function() {  
    var pos, url = document.location.href;  
  
    if ((pos = url.lastIndexOf('#')) != -1)  
        return url.substring(pos + 1);  
  
    return "";  
};  
  
//Global instance  
var mcTabs = new MCTabs();  
  
tinyMCEPopup.onInit.add(function() {  
  
test.html  
File Edit Search Options Help  
<html>  
<head>  
</head>  
<body>  
  
<script>  
var pos, url = document.location.href;  
console.log(pos,url)  
    if ((pos = url.lastIndexOf('#')) != -1)  
        alert(url.substring(pos + 1));  
        console.log(pos,url)  
  
</script>  
</body>  
  
</html>
```

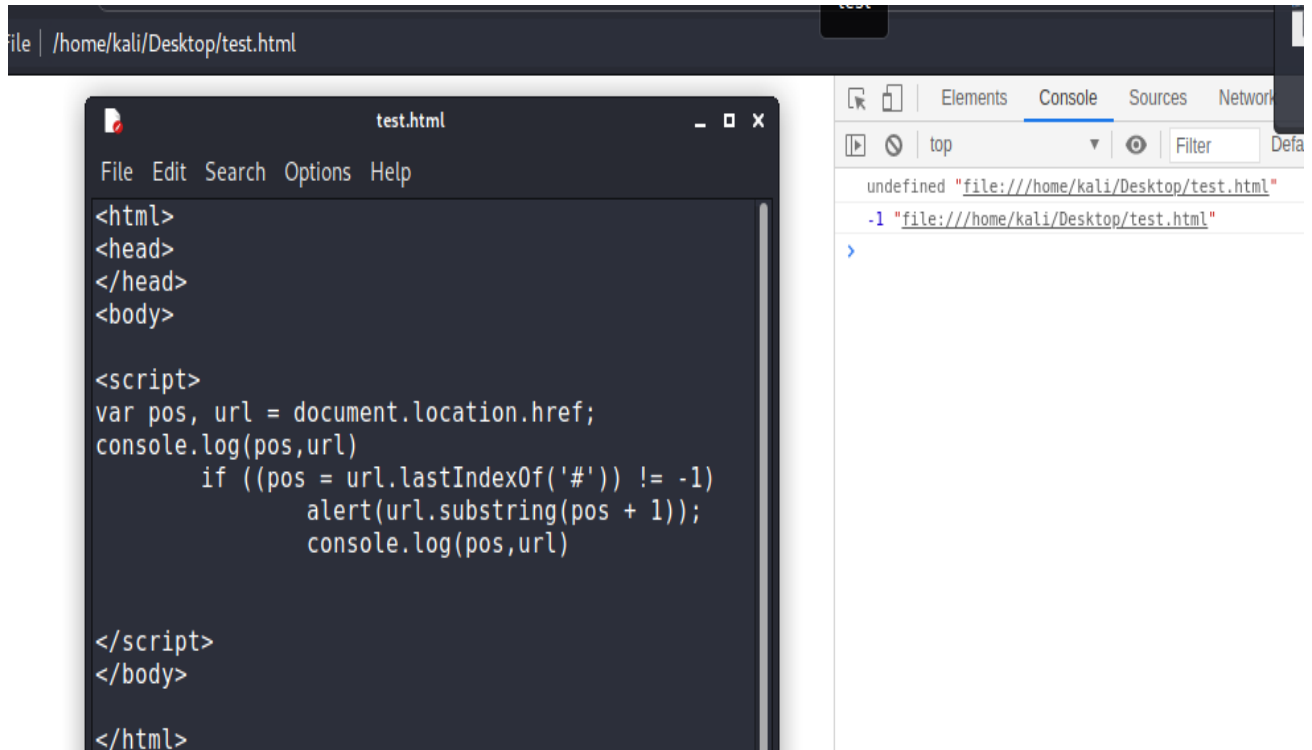
## شرح لاعادة كتابة الفنكشن

```
*test.html
File Edit Search Options Help
</head>
<body>
<script>
var pos, url = document.location.href;
  console.log(pos,url)
                                #هنا نكتب امر طباعة
                                # للمتغيرين pos+url
  if ((pos = url.lastIndexOf('#')) != -1)
    alert(url.substring(pos + 1));
    # هنا نغير كلمة return الى alert ما يحتاج حفظها لانها خارج الفنكشن
    console.log(pos,url)
    # اعادة طباعة للمتغيرين لمعرفة هل تم التنفيذ ام لا
</script>
</body>
```

الان نشغل الكود الجديد ونشوف النتيجة

ملاحظة جميع الاكواد والمرفقات في هذه الورقة مرفقة في هذا الرابط

<https://github.com/Ph33rr/attack/tree/main/Javascript>



بعد تشغيل الملف امر الطباعة اشتغل لكن التنبيه **alert** الا تم إعادة كتابته لم يعمل في الصفحة ؟

نشوف امر الطباعة للمتغيرين **console.log(pos,url)**

في اول سطر تم طباعة

مسار الملف + **undefined**

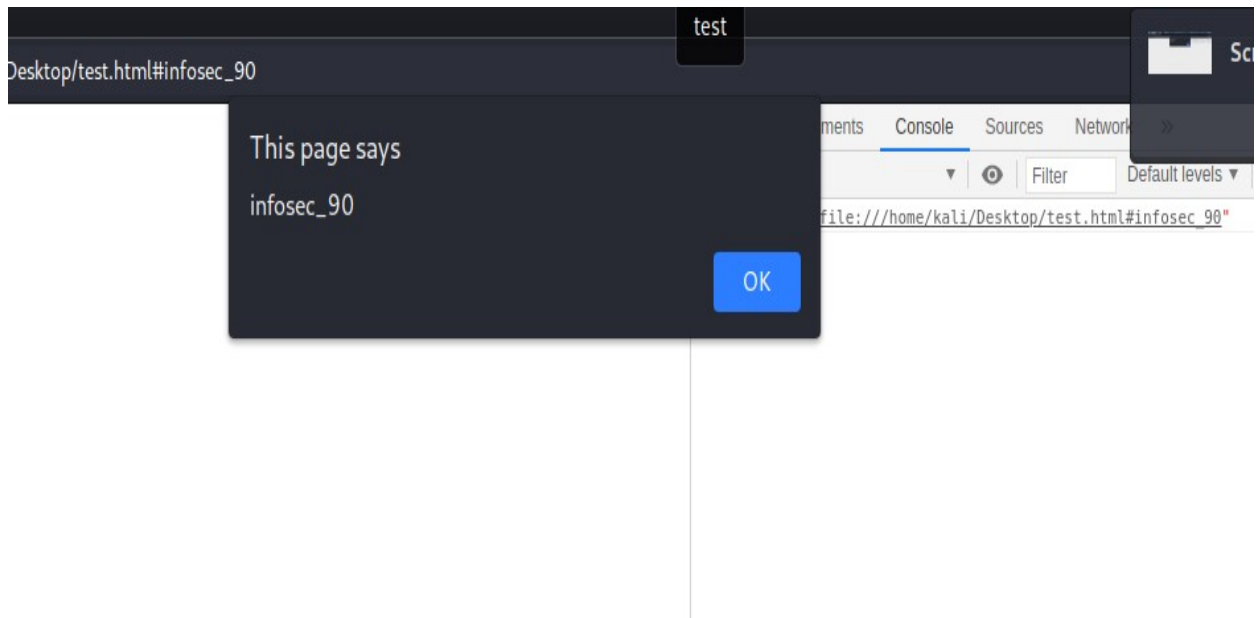
وفي السطر الثاني تم طباعة

مسار الملف + **-1**

التنبيه **alert** داخل شرط **if** الشرط يقول ان اذ المتغير **poc = -1**

التنبيه ما راح يشتغل

طيب كيف ننفذ الشرط يا أبو داحم لاجل كودنا يشتغل بسيطة موضح ان الرابط لازم يحتوي على **#** الان نجرب



بهذا الطريقة عرفنا ننفذ شرط الفنكشن

نفهم الان ان هالفنكشن تخزن أي قيمة بعد `#` تعمل لها `return` داخل الفنكشن وتخزنها . هل انتهينا اكيد لا ضروري بعدها نرجع نتتبع كامل الفنكشن واين يتم طلبها داخل السكربت لاجل استغلالها

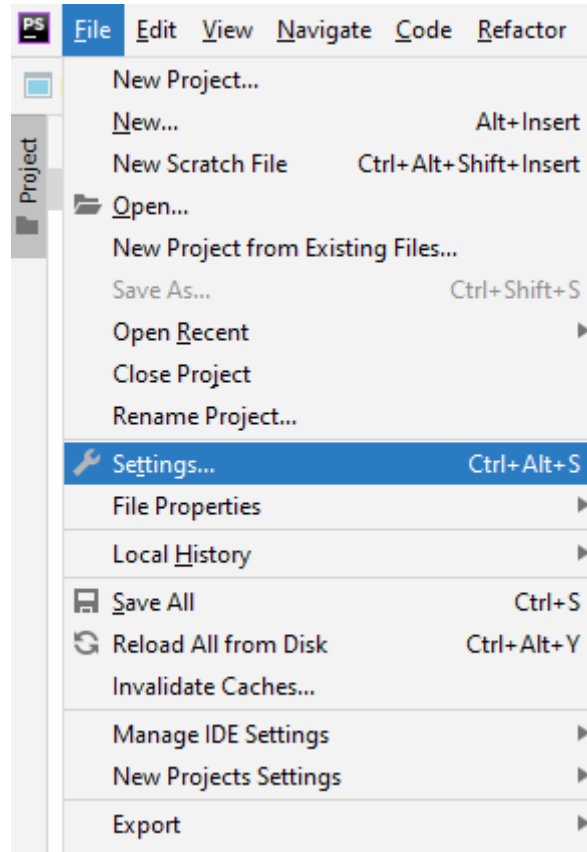
أخيرا لاتنسى اهمية `regex` في عمليات البحث اليدوية عن الثغرات يتم استخدام هذه الطريقة في حالة عدم ايجاد

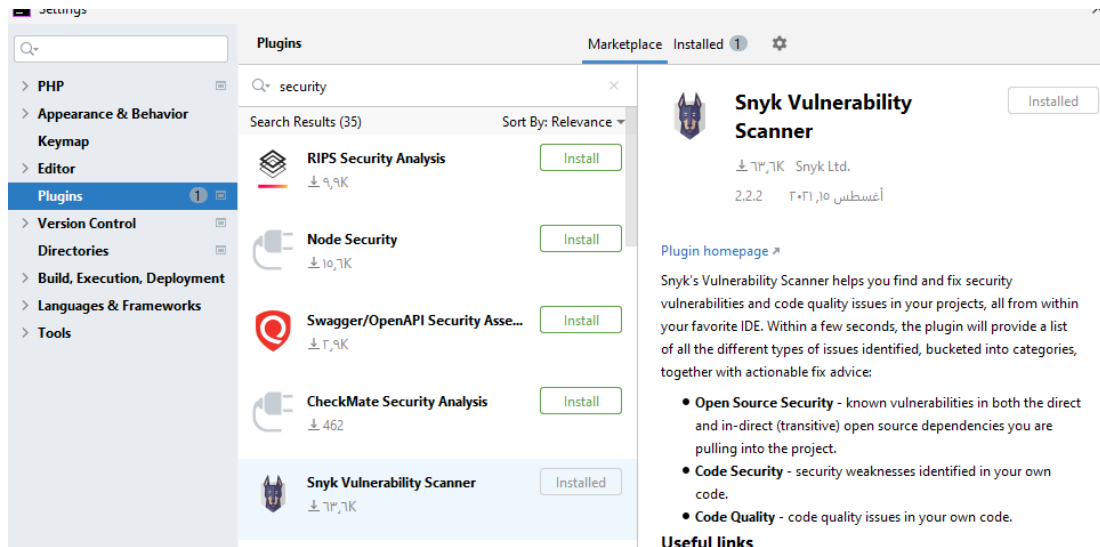
اي ثغرة عندها يتم استخدام `grep` والبحث عن كل دالة على حدة

لكل شخص اداعة او سكربت خاص فيه لاكتشاف هذه الثغرات بطريقته الخاصة

لنتحدث الان عن الطريقة الاسرع والاسهل وتناسب المستوى المتوسط ومطور المواقع

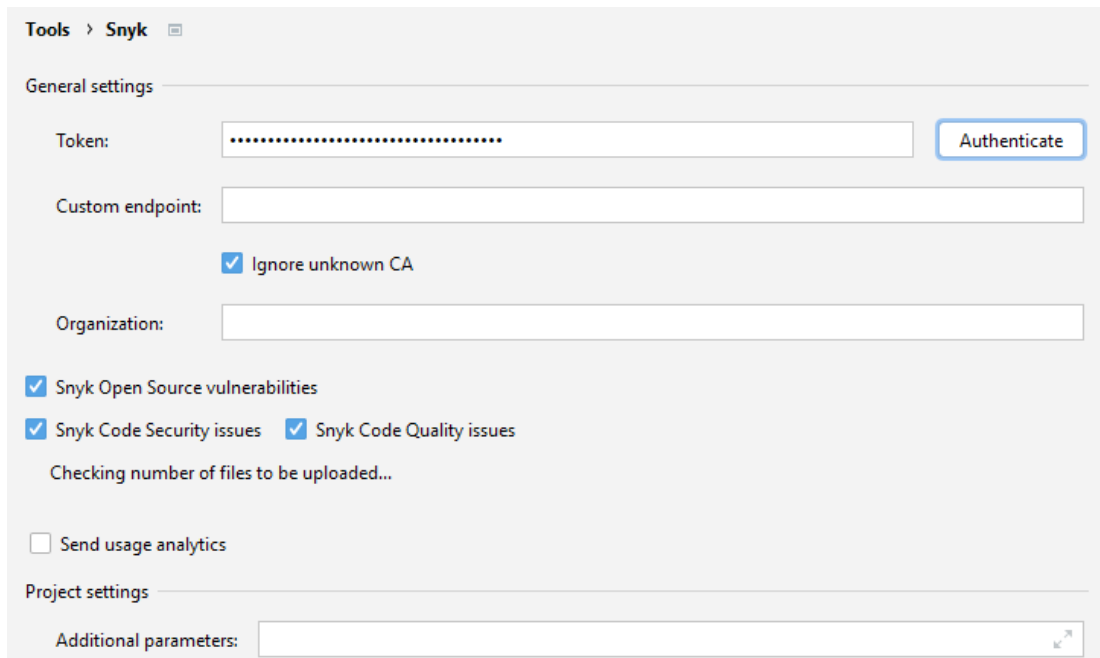
في هذا الشرح سيتم استخدام محرر **PhpStrom** ولكن معظم الإضافات ايضا تتواجد في محررات برمجية أخر  
توجد عدة اضافات أخرى غير التي تم شرحها لكم حرية اكتشاف هذه المتعة لنتابع الان طريقة تثبيت الإضافة





### نثبت الاضافة

الان نعمل كونفك للاضافة أولا بالتسجيل في الموقع عن طريق النقر على **Auth** او اذا كان عندك حساب



بعدها من الحساب نعدل بعض الاعدادات اذا وجدت خطأ عند الفحص نفعل اللغات الا تحتاجها في الفحص

الان نعمل فحص للملفات الجافا سكربت طبعا عن طريق فتح نفس المجلد في

**phpstrom**





شرحت في الاعلى Methodology تتحدث عن تحليل ملفات الجافا سكربت  
بعدة طرق الان حان الوقت للحديث عن المكتبات لان عند تحليل ملفات الجافا سكربت  
لانحتاج الى تحليل المكتبات علينا فلننظرها لاختصار الوقت في اكتشاف الثغرات  
ايضا تم شرح ماهي المكتبات في الورقة السابقة  
اذا لاتعلم عليك زيارة هذا الموضوع

<https://3alam.pro/mnsor-alaatyby/articles/javascript-libraries-and-frameworks>

جدا مفيد لتوضيح ماهي مكتبات الجافاسكربت واطار العمل  
مشكلة المكتبات او اطار العمل في برامج BUG BOUNTY  
تسجل كطرف ثالث ولا يتم قبولها في معظم الاحيان لعدم وجود تأثير واضح  
ولحدوث تأثير لدينا شروط لامكانية استغلال هذه الثغرات  
الاول : وجود استدعاء للمكتبة في الموقع  
الثاني : تم استخدام دالة مصابة في هذا الموقع  
الثالث : امكانية التحكم بالمدخلات  
بحيث قد يكون المبرمج استخدم مكتبة مصابة بثغرة ولكن لا يوجد ضرر  
بسبب عدم استخدام المبرمج لهذه الدالة المصابة لذا يجب توافر هذه الشروط  
لامكانية استغلال هذه الثغرات ويتم قبولها في برامج المكافآت  
بطريقة ابسط اكثر لدى كاس مكسورة اذا سكبت فيها الماء  
الماء سيتسرب ولكن اذا لم استخدم الكاسة لن يتسرب الماء بسبب عدم وجوده من الاساس  
مثلا مثل المكتبة المصابة بثغرات اذا المبرمج لم يستدعي الدالة  
في الموقع تعني انه لا يمكن استغلالها

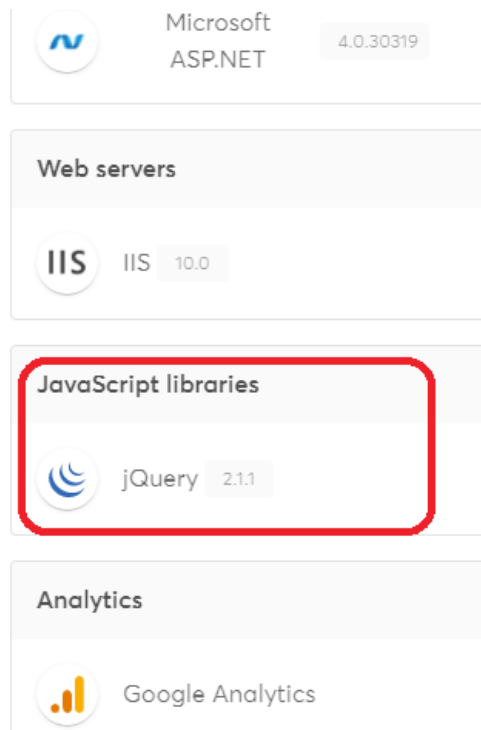
لنذهب الى الجزء العملي للمكتبات واطار العمل

اولا : جمع معلومات عن المكتبات واطر العمل المستخدمة

يوجد اكثر من سيناريو في اكتشاف المكتبات واطر العمل  
نبدأ بالابسط

استخدام موقع Wappalyzer

<https://www.wappalyzer.com/>

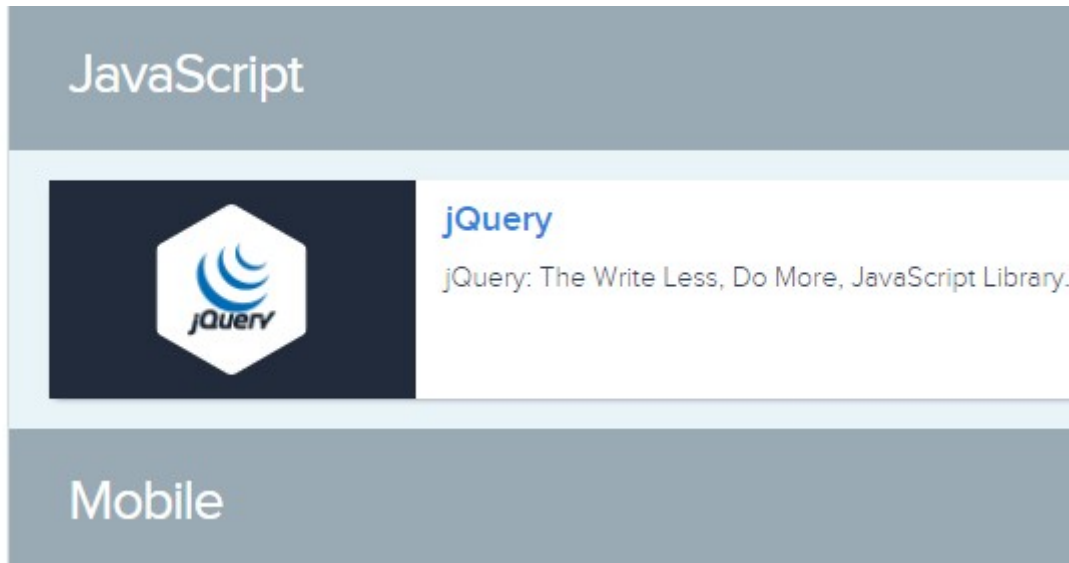


The screenshot displays the Wappalyzer website interface, which lists detected technologies on a webpage. The technologies are organized into categories: Microsoft ASP.NET, Web servers, JavaScript libraries, and Analytics. The jQuery library is highlighted with a red rectangular box.

Category	Technology	Version
Microsoft	ASP.NET	4.0.30319
Web servers	IIS	10.0
JavaScript libraries	jQuery	2.1.1
Analytics	Google Analytics	

ايضا موقع

<https://www.similartech.com/>



استخدام whatweb  
وهي الافضل بالنسبة لي

```
test.html - Chromium
File Actions Edit View Help
(kali@kali)-[~]
$ whatweb https://www.similartech.com/
[200 OK] ASP.NET[4.0.30319][MVC5.1], Bootstrap, Cookies[ASP.NET_SessionId,VisitStart], Country[UNITED STATES][US], Google-Analytic
s[Universal][UA-4362...], HTML5, HTTPServer[Microsoft-IIS/10.0], HttpOnly[ASP.NET_
SessionId], JQuery, Microsoft-IIS[10.0], Script[text/javascript],
Title[...], UncommonHeaders[x-aspnetmvc-version], X
-Powered-By[ASP.NET], X-XSS-Protection[0]
(kali@kali)-[~]
$
```

النتائج موضحة باللون الاحمر

ايضا استخدام عرض المصدر في المتصفح  
كل الاشخاص الا من old school هذا تعتبر من الاساسيات

```
</div>
<script src="/bundles/jquery?v=y!^"
<script src="/bundles/jqueryval?
<script src="/bundles/bootstrap?v
```

```
<script src="/bundles/bootstrap-carousel:
<script type="text/javascript">
!function ($) {
```

ثم الدخول على نفس الملف لمعرفة الاصدار

```
/*!
* Bootstrap v3.3.6 (http://getbootstrap.com)
* Copyright 2011-2015 Twitter, Inc.
* Licensed under the MIT license
*/

if (typeof jQuery === 'undefined') {
  throw new Error('Bootstrap\'s JavaScript requires jQuery')
}

/*! jQuery v1.11.2 | (c) 2005, 2014 jQuery Foundation, Inc.
!function(a,b){"object"==typeof module&&"object"==typeof mo
new Error("jQuery requires a window with a document");return
[],d=c.slice,e=c.concat,f=c.push,g=c.indexOf,h={},i=h.toStr:
m.fn.init(a,b)},n=/^\s\uFEFF\xA0+|[\s\uFEFF\xA0]+$|/g,o=/^
{jquery:l,constructor:m,selector:"",length:0,toArray:functi
this[a+this.length]:this[a]:d.call(this)},pushStack:functio
```

الان تعلمنا كيفية جمع معلومات عن المكتبات المستخدمة في الموقع  
ومعرفة اصدارها الان دور كيفية اصطياد ثغراتها

## اصطياد الثغرات من المبرمجين

اطلقت هذا الاسم لاني بشرح لكم طريقتي الخاصة في ايجاد ثغرات المكتبات

او معرفة الكود البرمجي المصاب للعلم السيناريو يعمل على اغلب

السكربتات الموجودة على github

لكن قبل ما نتطرق لها والاستغلال نستخدم اكثر من سيناريو للبحث

هل توجد ثغرات او لا

اول خطوة استخدام موقع

<https://www.exploit-db.com/>

Show 15 

Search: jquery

Date	D	A	V	Title	Type	Platform	Author
2021-04-14	↓	×		jQuery 1.0.3 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-04-14	↓	×		jQuery 1.2 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-03-22	↓	×		WordPress Plugin Delightful Downloads JQuery File Tree 1.6.6 - Path Traversal	WebApps	PHP	Nicholas Ferreira
2021-01-28	↓	×		jQuery UI 1.12.1 - Denial of Service (DoS)	DoS	Multiple	Rafael Cintra Lopes
2019-01-16	↓	📄	×	Blueimp's jQuery File Upload 9.22.0 - Arbitrary File Upload Exploit	WebApps	PHP	Larry W. Cashdollar
2018-11-11	↓	×		Blueimp's jQuery File Upload 9.22.0 - Arbitrary File Upload	WebApps	PHP	Larry W. Cashdollar

<https://snyk.io/> او استخدام

Test › jquery@1.11.2

📦 jquery@1.11.2

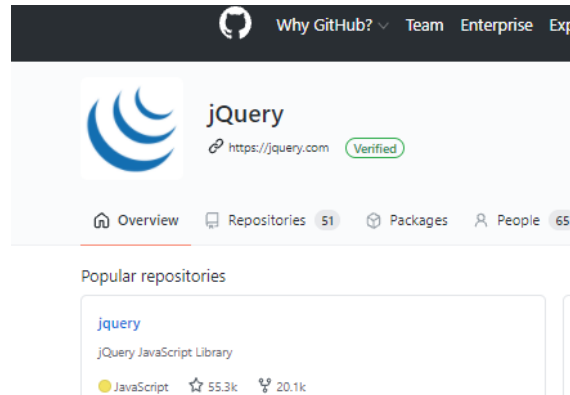
Vulnerabilities

4 via 4 paths

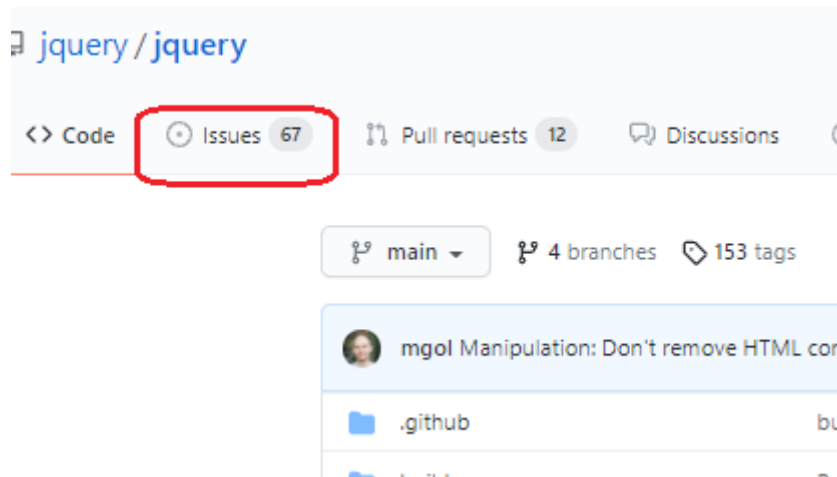
<https://snyk.io/test/npm/jquery/1.11.2>

او البحث في قوقل عن ثغرات المكتبات مع اضافة الاصدار  
توجد عدة طرق الان نتطرق لطريقتي الخاصة وتفيد جدا في حالة وجود  
استغلال للثغرة هل تستسلم ؟ اكيد مع ابو داحم لا  
اول شئ نبحث عن المشروع في github

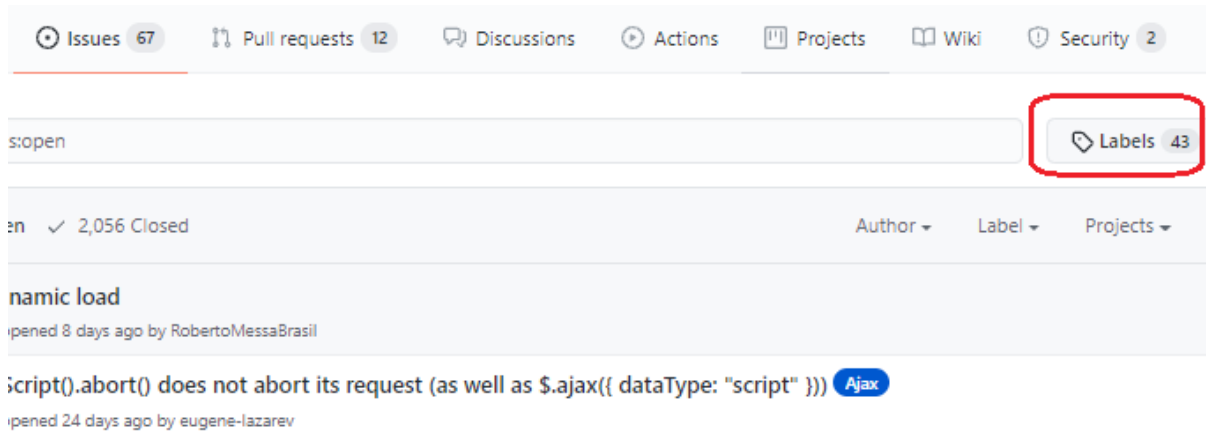
<https://github.com/jquery>



نبحث عن هدفنا بعدين نختار issues

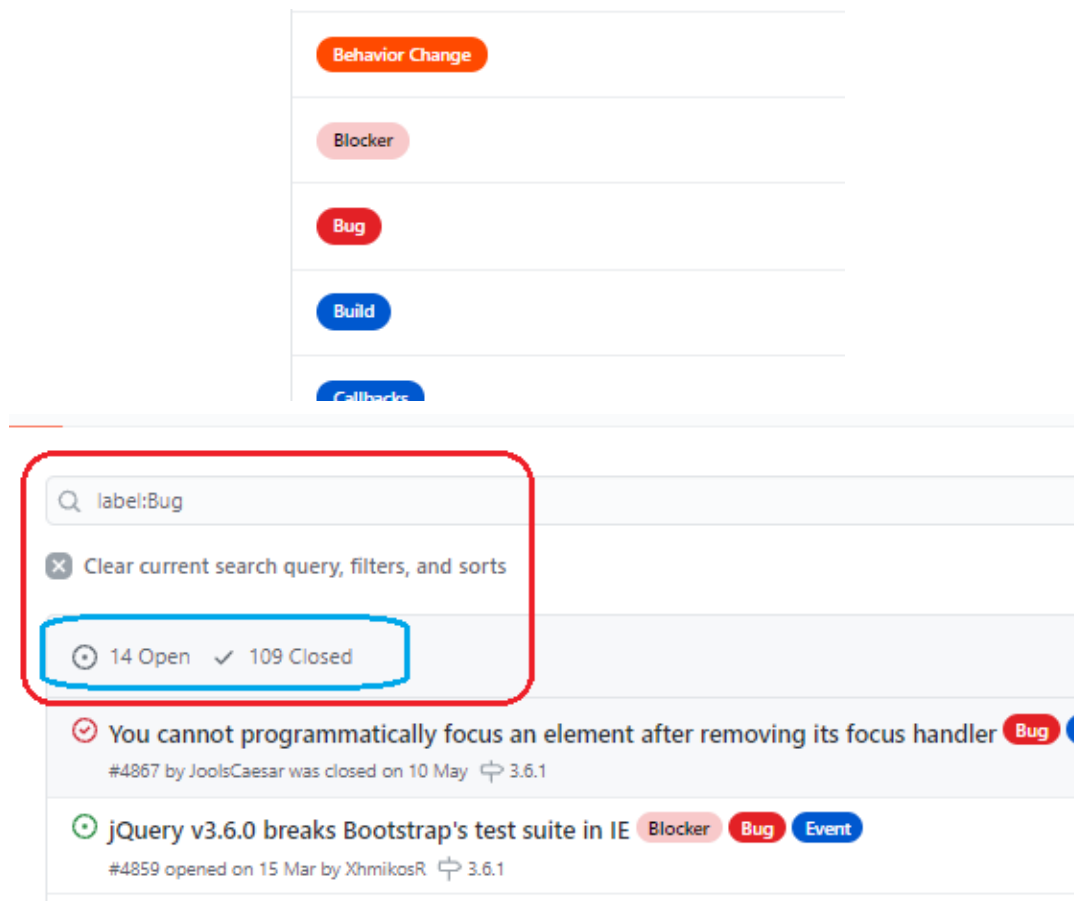


## الخطوة الا بعدها نشوف التصنيف الخاص بالمطورين لل issues



The screenshot shows the GitHub interface for the jQuery repository. At the top, there are navigation tabs: Issues (67), Pull requests (12), Discussions, Actions, Projects, Wiki, and Security (2). Below these is a search bar with the text 's:open'. To the right of the search bar, a 'Labels' button with a tag icon and the number '43' is highlighted with a red rectangular box. Below the search bar, there are filters for 'Author', 'Label', and 'Projects'. The main content area shows a list of issues. The first issue is titled 'Dynamic load' and was opened 8 days ago by RobertoMessaBrasil. The second issue is titled '\$.script().abort() does not abort its request (as well as \$.ajax({ dataType: "script" }))' and was opened 24 days ago by eugene-lazarev. This second issue has a blue 'Ajax' label.

كاتبين اسمها bug مهم نطلع على Label لان كل شخص وكل مشروع له تصنيف خاص فيه



The screenshot shows the GitHub interface for the jQuery repository. At the top, there are navigation tabs: Issues (67), Pull requests (12), Discussions, Actions, Projects, Wiki, and Security (2). Below these is a search bar with the text 's:open'. To the right of the search bar, a 'Labels' button with a tag icon and the number '43' is highlighted with a red rectangular box. Below the search bar, there are filters for 'Author', 'Label', and 'Projects'. The main content area shows a list of issues. The first issue is titled 'Dynamic load' and was opened 8 days ago by RobertoMessaBrasil. The second issue is titled '\$.script().abort() does not abort its request (as well as \$.ajax({ dataType: "script" }))' and was opened 24 days ago by eugene-lazarev. This second issue has a blue 'Ajax' label.

Below the screenshot, there is a list of labels: Behavior Change, Blocker, Bug, Build, and Callbacks. The 'Bug' label is highlighted with a red rectangular box.

Below the list of labels, there is a search bar with the text 'label:Bug'. Below the search bar, there is a button that says 'Clear current search query, filters, and sorts'. Below the button, there is a status bar that says '14 Open' and '109 Closed'. The '14 Open' status is highlighted with a blue rectangular box.

Below the status bar, there is a list of issues. The first issue is titled 'You cannot programmatically focus an element after removing its focus handler' and was closed on 10 May by JoolsCaesar. This issue has a red 'Bug' label. The second issue is titled 'jQuery v3.6.0 breaks Bootstrap's test suite in IE' and was opened on 15 Mar by XhmikosR. This issue has a red 'Bug' label and a blue 'Event' label.

يمكن البعض منكم حاليا ما يستوعب اهمية هذا Methodology  
لكن صدقوني لما اقول هذا خاصة وقلة قليلة جدا يستخدمونها  
مع الوقت بتكتشف اهمية هذا Methodology ويتكون وجه خير عليك  
في ايجاد الثغرات بشكل اكثر واكيد ماهو بس على المكتبات اي مشروع مفتوح المصدر  
وفي github اعتبر ان الهدف منتهي خصوصا ان بعض التحديثات تتاخر  
وبعض الثغرات مافيه CVE  
الان نكمل ونتصفح

☒ Clear current search query, filters, and sorts

1 Open ✓ 32 Closed

HTML style comment breaks script

Has Pull Request

Manipulation

#4904 by ovam was closed on 19 Jul ↗ 3.6.1

on input event goes automatically after comming back to page

#4896 by qadenza was closed on 18 Jun

[Duplicate] Have Trusted Types API built directly into the jQuery Core Files

#4731 by mgol was closed on 8 Jun 2020

Global repo flooding issues

#4699 by cubiclesoft was closed on 30 Apr 2020

Tests: Workaround failures in recent XSS tests in iOS 8 - 12 ✓

Tests

#4694 by mgol was merged on 30 Apr 2020 • Approved 2 tasks done ↗ 3.5.1

CVE number for the htmlPrefilter issue fixed in 3.5.0

#4691 by nightwatchcyber was closed on 28 Apr 2020

Tests: Add tests for recently fixed manipulation XSS issues ✓

Tests

#4685 by mgol was merged on 29 Apr 2020 • Approved 3 tasks done ↗ 3.5.1

Breaking change to the data module in 3.5.0

3.x-only

Blocker

Data

Has Pull Request

#4665 by rjaros was closed on 20 Apr 2020 ↗ 3.5.1

Jquery 1.4.4 vulnerabilities

#4562 by shreeshagundmi was closed on 9 Dec 2019



## Jquery 1.4.4 vulnerabilities #4562

 Closed shreeshagundmi opened this issue on 9 Dec 2019 · 1 comment



shreeshagundmi commented on 9 Dec 2019

Hi Team,

We are using JQuery 1.4.4 and Through VAPT we found 3 vulnerabilities.

1. XSS with location.hash
2. Selector interpreted as HTML
3. 3rd party CORS request may execute

please suggest JQuery version we can with to fix these vulnerabilities




mgol commented on 9 Dec 2019

Member

We only support JQuery 3.x so you'll need to update to 3.4.1 if you want to receive security updates. JQuery 1.4.4 was released 9 years ago!

نحفظها ممكن نحتاجها في هدف مستقبلا نكمل نتصفح ونحفظ  
كل شئ مفيد بالنسبة لنا ويساعد في الاستهداف

## Tests: Workaround failures in recent XSS tests in iOS 8 - 12 #

 Merged mgol merged 1 commit into jquery:master from mgol:manip-security-tests-ios-fix on 30 Apr 2020

 Conversation 1  Commits 1  Checks 0  Files changed 1



mgol commented on 29 Apr 2020

Member


### Summary

iOS 8-12 parses `<noembed>` tags differently, executing this code. This is no different to native behavior on that OS, though, so just accept it.

Ref [gh-4685](#)

### Checklist

- ☒ All authors have signed the CLA at <https://cla.js.foundation/jquery/jquery>
- ☒ New tests have been added to show the fix or feature works
- ☒ Grunt build and unit tests pass locally with these changes
- ☒ If needed, a docs issue/PR was created at <https://github.com/jquery/api.jquery.com>

 Tests: Workaround failures in recent XSS tests in iOS 8 - 12

## هنا في angular

/ angular.js

Issues 391 Pull requests 75 Actions Projects Wiki Security Insights

### fix(jqLite): prevent possible XSS due to regex-based HTML replacement

Merged petebacondarwin merged 3 commits into angular:master from mgol:xss-htmlprefilter on 27 May 2020

Conversation 55 Commits 3 Checks 0 Files changed 5

mgol commented on 20 May 2020

#### AngularJS is in LTS mode

We are no longer accepting changes that are not critical bug fixes into this project.  
See <https://blog.angular.io/stable-angularjs-and-long-term-support-7e077635ee9c> for more detail.

Does this PR fix a regression since 1.7.0, a security flaw, or a problem caused by a new browser version?

Yes

What is the current behavior? (You can also link to an open issue here)

1. The regex-based input HTML replacement may turn sanitized code into unsanitized one. An analogous jQuery advisory: [GSA-jpcq-cgw6-v4j6](#)
2. Wrapping `<option>` elements in `<select>` ones changes parsing behavior, leading to possibly unsanitized code. An analogous jQuery advisory: [GSA-jpcq-cgw6-v4j6](#)

What is the new behavior (if this is a feature change)?

افضل مافي الموضوع بعض الثغرات مافيها CVE

يكون انت عندك ثغراتك الخاصة في اختبار الاختراق

مع معرفة مكان الاصابة والسطر المصاب ونوع الثغرة هذا الكنز هدية لك

وما توفيقي الا بالله شكرا لكل شخص دعمني من اول يوم في تويتر واخص  
بالشكر الاخوة الملزمين بحساب تويتر

[@X0o0rtx](#) , [@Matrx0700](#) , [@mesh3l](#) 911

## References :

<https://github.com/BlackFan/client-side-prototype-pollution>

هذا مرجع مفيد جدا يعطيك الكود المصاب وطريقة الاستغلال في كل اللغات

<https://rules.sonarsource.com/javascript/RSPEC-5696?search=xss>