black hat
ASIA 2014

Ultimate DOM Based XSS Detection Scanner On Cloud

Nera W. C. Liu & Albert Yu

Paranoids

Yahoo

Agenda

- DOM XSS
- Our solution
- DEMO!

Who are we

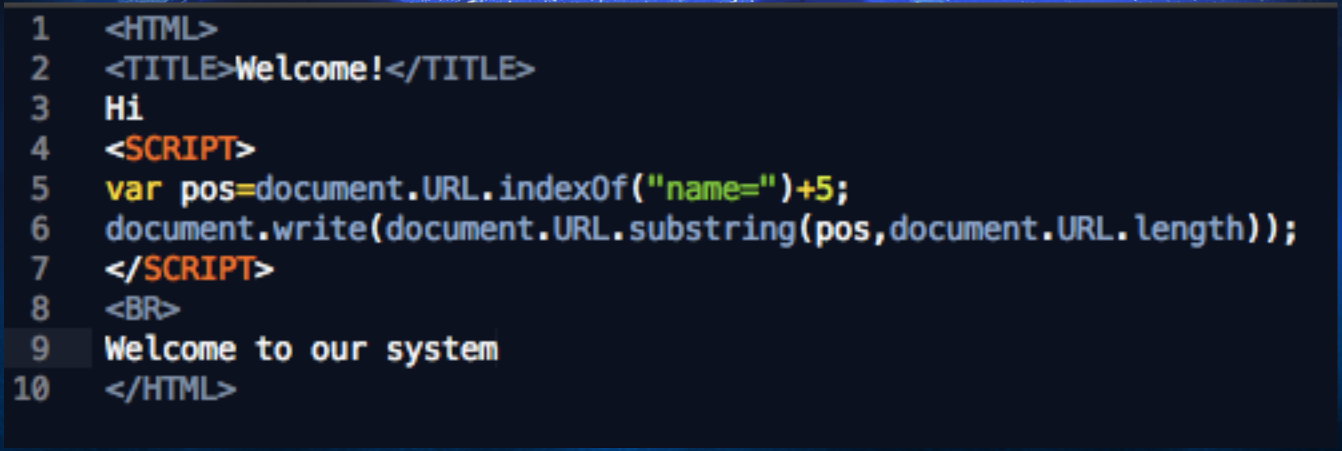
What people think we are?

What we think we are?

What we actually are?

DO[r]M XSS

“XSS of the 3rd Kind”



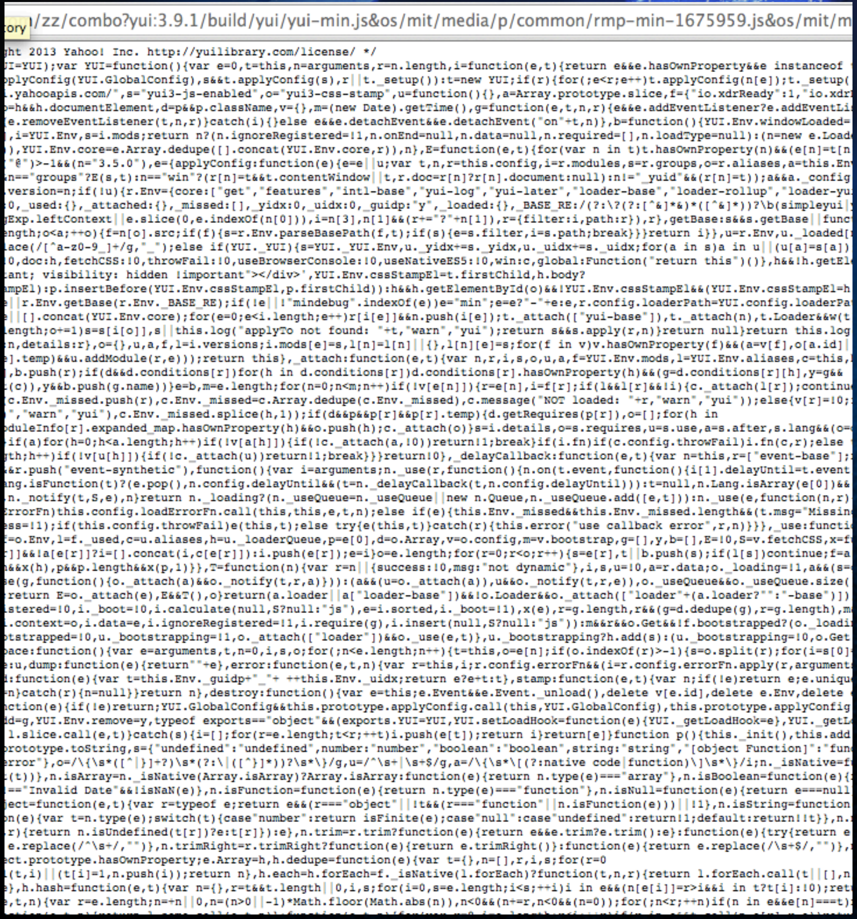
```
<HTML>
<TITLE>Welcome!</TITLE>
Hi
<SCRIPT>
var pos=document.URL.indexOf("name=")+5;
document.write(document.URL.substring(pos,document.URL.length));
</SCRIPT>
<BR>
Welcome to our system
</HTML>
```

- Does not rely on flaws in application containers
- Easier target for attacker
- Harder for defender to detect

See “DOM Based Cross Site Scripting or XSS of the Third Kind”. Amit Klein. 2005. http://www.webappsec.org/projects/articles/071105.shtml http://www.vulnerable.site/welcome.html#foo<script

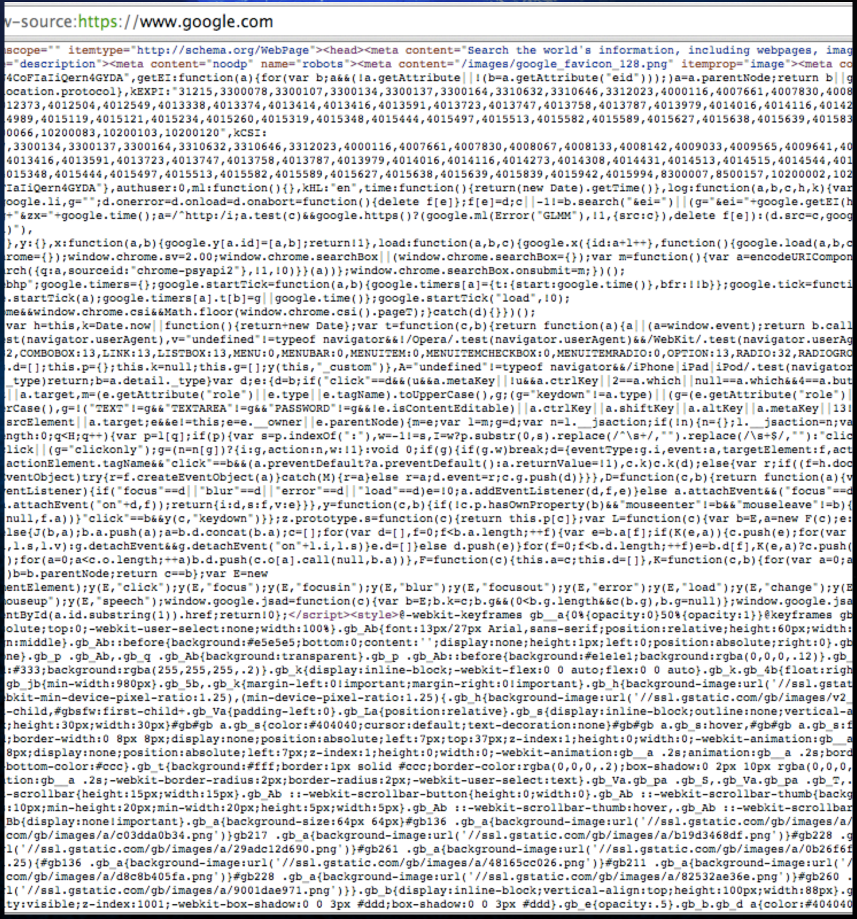
Static Analysis

⌥⌘U



ory /zz/combo?yui:3.9.1/build/yui/yui-min.js&os/mit/media/p/common/rmp-min-1675959.js&os/mit/m

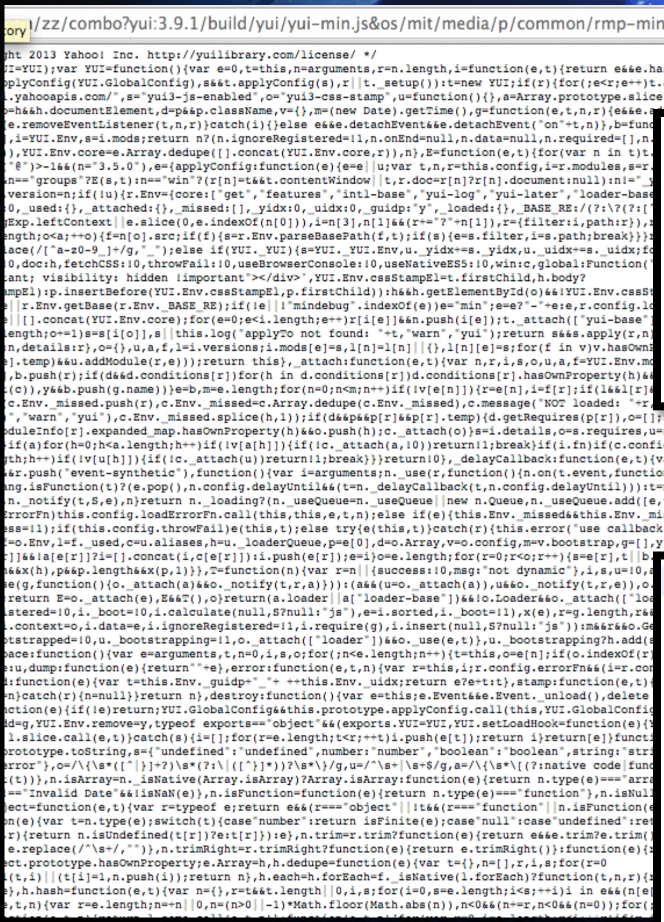
```
ght 2013 Yahoo! Inc. http://yuilibrary.com/license/ */
JI=YUI);var YUI=function(){var e=0,t=this,n=arguments,r=n.length,i=function(e,t){return e&&e.hasOwnProperty&&e instanceof
pplyConfig(YUI.GlobalConfig),s&&t.applyConfig(s),r||t._setup()):t=new YUI;if(r){for(;e<r;e++)t.applyConfig(n[e]);t._setup(
.yahooapis.com/",s="yui3-js-enabled",o="yui3-css-stamp",u=function(){},a=Array.prototype.slice,f={"io.xdrReady":1,"io.xdr
=h&&h.documentElement,d=p&&p.className,v={},m=(new Date).getTime(),g=function(e,t,n,r){e&&e.addEventListener?e.addEventLi
e.removeEventListener(t,n,r)}catch(i){}else e&&e.detachEvent&&e.detachEvent("on"+t,n)},b=function(){YUI.Env.windowLoaded=
,i=YUI.Env,s=i.mods;return n?(n.ignoreRegistered=!1,n.onEnd=null,n.data=null,n.required=[],n.loadType=null):(n=new e.Loade
),YUI.Env.core=e.Array.dedupe([].concat(YUI.Env.core,r)),n},E=function(e,t){for(var n in t)t.hasOwnProperty(n)&&(e[n]=t[n
"@")>-1&&(n="3.5.0"),e={applyConfig:function(e){e=e||u;var t,n,r=this.config,i=r.modules,s=r.groups,o=r.aliases,a=this.Env
n=="groups"?E(s,t):n=="win"?(r[n]=t&&t.contentWindow||t,r.doc=r[n]?r[n].document:null):n!="_yuid"&&(r[n]=t));a&&a._config
.version=n;if(!u){r.Env={core:["get","features","intl-base","yui-log","yui-later","loader-base","loader-rollup","loader-yu
0,_used:{},_attached:{},_missed:[],_yidx:0,_uidx:0,_guidp:"y",_loaded:{},_BASE_RE:/(?:\?(?:[^&]*&)*([^&]*))?\b(simpleyui|
gExp.leftContext||e.slice(0,e.indexOf(n[0])),i=n[3],n[1]&&(r+="?"+n[1]),r={filter:i,path:r}),r},getBase:s&&s.getBase||func
ength;o<a;++o){f=n[o].src;if(f){s=r.Env.parseBasePath(f,t);if(s){e=s.filter,i=s.path;break}}}return i}},u=r.Env,u._loaded[
ace(/[^a-z0-9_]+/g,"_");else if(YUI._YUI){s=YUI._YUI.Env,u._yidx+=s._yidx,u._uidx+=s._uidx;for(a in s)a in u||(u[a]=s[a])
0,doc:h,fetchCSS:!0,throwFail:!0,useBrowserConsole:!0,useNativeES5:!0,win:c,global:Function("return this")()},h&&!h.getEl
ant; visibility: hidden !important"></div>',YUI.Env.cssStampEl=t.firstChild,h.body?
mpEl):p.insertBefore(YUI.Env.cssStampEl,p.firstChild)):h&&h.getElementById(o)&&!YUI.Env.cssStampEl&&(YUI.Env.cssStampEl=h
e||r.Env.getBase(r.Env._BASE_RE);if(!e||!"mindebug".indexOf(e))e="min";e=e?"-"+e:e,r.config.loaderPath=YUI.config.loaderPa
e||[].concat(YUI.Env.core);for(e=0;e<i.length;e++)r[i[e]]&&n.push(i[e]);t._attach(["yui-base"]),t._attach(n),t.Loader&&w(t
ength;o+=1)s=s[i[o]],s||this.log("applyTo not found: "+t,"warn","yui");return s&&s.apply(r,n)}return null}return this.log
n,details:r},o={},u,a,f,l=i.versions;i.mods[e]=s,l[n]=l[n]||{},l[n][e]=s;for(f in v)v.hasOwnProperty(f)&&(a=v[f],o[a.id]|
].temp)&&u.addModule(r,e)));return this},_attach:function(e,t){var n,r,i,s,o,u,a,f=YUI.Env.mods,l=YUI.Env.aliases,c=this,
,b.push(r);if(d&&d.conditions[r])for(h in d.conditions[r])d.conditions[r].hasOwnProperty(h)&&(g=d.conditions[r][h],y=g&&
(c)),y&&b.push(g.name))}e=b,m=e.length;for(n=0;n<m;n++)if(!v[e[n]]){r=e[n],i=f[r];if(l&&l[r]&&!i){c._attach(l[r]);continu
(c.Env._missed.push(r),c.Env._missed=c.Array.dedupe(c.Env._missed),c.message("NOT loaded: "+r,"warn","yui"));else{v[r]=!0;
","warn","yui"),c.Env._missed.splice(h,1));if(d&&p&&p[r]&&p[r].temp){d.getRequires(p[r]),o=[];for(h in
duleInfo[r].expanded_map.hasOwnProperty(h)&&o.push(h);c._attach(o)}s=i.details,o=s.requires,u=s.use,a=s.after,s.lang&&(o=
if(a)for(h=0;h<a.length;h++)if(!v[a[h]]){if(!c._attach(a,!0))return!1;break}if(i.fn)if(c.config.throwFail)i.fn(c,r);else
th;h++)if(!v[u[h]]){if(!c._attach(u))return!1;break}}}return!0},_delayCallback:function(e,t){var n=this,r=["event-base"];
&r.push("event-synthetic"),function(){var i=arguments;n._use(r,function(){n.on(t.event,function(){i[1].delayUntil=t.event
ng.isFunction(t)?(e.pop(),n.config.delayUntil&&(t=n._delayCallback(t,n.config.delayUntil))):t=null,n.Lang.isArray(e[0])&&
n._notify(t,S,e),n}return n._loading?(n._useQueue=n._useQueue||new n.Queue,n._useQueue.add([e,t])):n._use(e,function(n,r)
rrorFn)this.config.loadErrorFn.call(this,this,e,t,n);else if(e){this.Env._missed&&this.Env._missed.length&&(t.msg="Missin
ss=!1);if(this.config.throwFail)e(this,t);else try{e(this,t)}catch(r){this.error("use callback error",r,n)}}},_use:functi
=o.Env,l=f._used,c=u.aliases,h=u._loaderQueue,p=e[0],d=o.Array,v=o.config,m=v.bootstrap,g=[],y,b=[],E=!0,S=v.fetchCSS,x=f
]]&&!a[e[r]]?i=[].concat(i,c[e[r]]):i.push(e[r]);e=i}o=e.length;for(r=0;r<o;r++){s=e[r],t||b.push(s);if(l[s])continue;f=a
&&x(h),p&&p.length&&x(p,1)}},T=function(n){var r=n||{success:!0,msg:"not dynamic"},i,s,u=!0,a=r.data;o._loading=!1,a&&(s=
e(g,function(){o._attach(a)&&o._notify(t,r,a)})):(a&&(u=o._attach(a)),u&&o._notify(t,r,e)),o._useQueue&&o._useQueue.size(
return E=o._attach(e),E&&T(),o}return(a.loader||a["loader-base"])&&!o.Loader&&o._attach(["loader"+(a.loader?"":"-base")])
stered=!0,i._boot=!0,i.calculate(null,S?null:"js"),e=i.sorted,i._boot=!1),x(e),r=g.length,r&&(g=d.dedupe(g),r=g.length),m
.context=o,i.data=e,i.ignoreRegistered=!1,i.require(g),i.insert(null,S?null:"js")):m&&r&&o.Get&&!f.bootstrapped?(o._loadi
tstrapped=!0,u._bootstrapping=!1,o._attach(["loader"])&&o._use(e,t)},u._bootstrapping?h.add(s):(u._bootstrapping=!0,o.Get
ace:function(){var e=arguments,t,n=0,i,s,o;for(;n<e.length;n++){t=this,o=e[n];if(o.indexOf(r)>-1){s=o.split(r);for(i=s[0]
:u,dump:function(e){return""+e},error:function(e,t,n){var r=this,i;r.config.errorFn&&(i=r.config.errorFn.apply(r,argument
:function(e){var t=this.Env._guidp+"_"+ ++this.Env._uidx;return e?e+t:t},stamp:function(e,t){var n;if(!e)return e;e.uniqu
n}catch(r){n=null}}return n},destroy:function(){var e=this;e.Event&&e.Event._unload(),delete v[e.id],delete e.Env,delete
ction(e){if(!e)return;YUI.GlobalConfig&&this.prototype.applyConfig.call(this,YUI.GlobalConfig),this.prototype.applyConfig
d=g,YUI.Env.remove=y,typeof exports=="object"&&(exports.YUI=YUI,YUI.setLoadHook=function(e){YUI._getLoadHook=e},YUI._getL
 l.slice.call(e,t)}catch(s){i=[];for(r=e.length;t<r;++t)i.push(e[t]);return i}return[e]}function p(){this._init(),this.add
rototype.toString,s={"undefined":"undefined",number:"number","boolean":"boolean",string:"string","[object Function]":"func
rror"},o=/\{\s*([^|}]+?)\s*(?:\|([^}]*))?\s*\}/g,u=/^\s+|\s+$/g,a=/\{\s*\[(?:native code|function)\]\s*\}/i;n._isNative=f
(t))},n.isArray=n._isNative(Array.isArray)?Array.isArray:function(e){return n.type(e)==="array"},n.isBoolean=function(e){
=="Invalid Date"&&!isNaN(e)},n.isFunction=function(e){return n.type(e)==="function"},n.isNull=function(e){return e===null
ect=function(e,t){var r=typeof e;return e&&(r==="object"||!t&&(r==="function"||n.isFunction(e)))||!1},n.isString=function
n(e){var t=n.type(e);switch(t){case"number":return isFinite(e);case"null":case"undefined":return!1;default:return!!t}},n.
r){return n.isUndefined(t[r])?e:t[r]}):e},n.trim=r.trim?function(e){return e&&e.trim?e.trim():e}:function(e){try{return e
 e.replace(/^\s+/,"")},n.trimRight=r.trimRight?function(e){return e.trimRight()}:function(e){return e.replace(/\s+$/,"")},
ct.prototype.hasOwnProperty;e.Array=h,h.dedupe=function(e){var t={},n=[],r,i,s;for(r=0
(t,i)||(t[i]=1,n.push(i));return n},h.each=h.forEach=f._isNative(l.forEach)?function(t,n,r){return l.forEach.call(t||[],n
},h.hash=function(e,t){var n={},r=t&&t.length||0,i,s;for(i=0,s=e.length;i<s;++i)i in e&&(n[e[i]]=r>i&&i in t?t[i]:!0);ret
,t,n){var r=e.length;n=+n||0,n=(n>0||-1)*Math.floor(Math.abs(n)),n<0&&(n+=r,n<0&&(n=0));for(;n<r;++n)if(n in e&&e[n]===t)
```



v-source:https://www.google.com

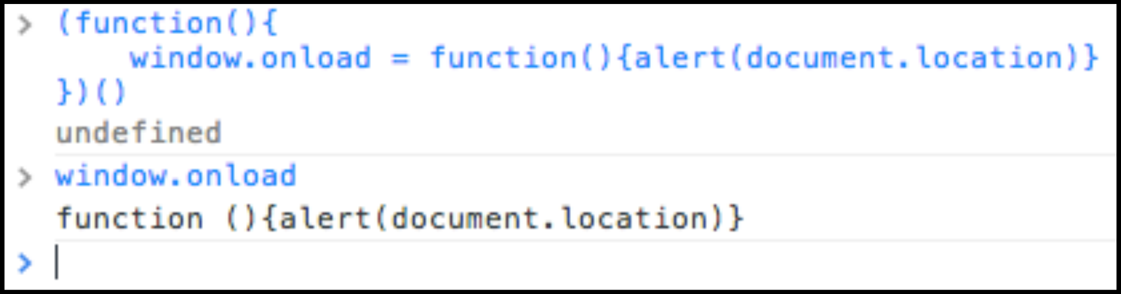
```
scope="" itemtype="http://schema.org/WebPage"><head><meta content="Search the world's information, including webpages, imag
="description"><meta content="noodp" name="robots"><meta content="/images/google_favicon_128.png" itemprop="image"><meta co
4CoFIaIiQern4GYDA",getEI:function(a){for(var b;a&&(!a.getAttribute||!(b=a.getAttribute("eid")));)a=a.parentNode;return b||g
ocation.protocol},kEXPI:"31215,3300078,3300107,3300134,3300137,3300164,3310632,3310646,3312023,4000116,4007661,4007830,4008
12373,4012504,4012549,4013338,4013374,4013414,4013416,4013591,4013723,4013747,4013758,4013787,4013979,4014016,4014116,40142
4989,4015119,4015121,4015234,4015260,4015319,4015348,4015444,4015497,4015513,4015582,4015589,4015627,4015638,4015639,401583
0066,10200083,10200103,10200120",kCSI:
,3300134,3300137,3300164,3310632,3310646,3312023,4000116,4007661,4007830,4008067,4008133,4008142,4009033,4009565,4009641,40
4013416,4013591,4013723,4013747,4013758,4013787,4013979,4014016,4014116,4014273,4014308,4014431,4014513,4014515,4014544,401
015348,4015444,4015497,4015513,4015582,4015589,4015627,4015638,4015639,4015839,4015942,4015994,8300007,8500157,10200002,102
IaIiQern4GYDA"},authuser:0,ml:function(){},kHL:"en",time:function(){return(new Date).getTime()},log:function(a,b,c,h,k){var
oogle.li,g="";d.onerror=d.onload=d.onabort=function(){delete f[e]};f[e]=d;c||-1!=b.search("&ei=")||(g="&ei="+google.getEI(h
+"&zx="+google.time();a=/^http:/i;a.test(c)&&google.https()?(google.ml(Error("GLMM"),!1,{src:c}),delete f[e]):(d.src=c,goog
)"),
},y:{},x:function(a,b){google.y[a.id]=[a,b];return!1},load:function(a,b,c){google.x({id:a+l++},function(){google.load(a,b,c
rome={});window.chrome.sv=2.00;window.chrome.searchBox||(window.chrome.searchBox={});var m=function(){var a=encodeURICompon
rch({q:a,sourceid:"chrome-psyapi2"},!1,!0)}}(a))};window.chrome.searchBox.onsubmit=m;})();
bhp";google.timers={};google.startTick=function(a,b){google.timers[a]={t:{start:google.time()},bfr:!!b}};google.tick=functi
.startTick(a);google.timers[a].t[b]=g||google.time()};google.startTick("load",!0);
me&&window.chrome.csi&&Math.floor(window.chrome.csi().pageT);}catch(d){}})();
var h=this,k=Date.now||function(){return+new Date};var t=function(c,b){return function(a){a||(a=window.event);return b.call
st(navigator.userAgent),v="undefined"!=typeof navigator&&!/Opera/.test(navigator.userAgent)&&/WebKit/.test(navigator.userAg
2,COMBOBOX:13,LINK:13,LISTBOX:13,MENU:0,MENUBAR:0,MENUITEM:0,MENUITEMCHECKBOX:0,MENUITEMRADIO:0,OPTION:13,RADIO:32,RADIOGRO
.d=[];this.p={};this.k=null;this.g=[];y(this,"_custom")},A="undefined"!=typeof navigator&&/iPhone|iPad|iPod/.test(navigator
_type)return;b=a.detail._type}var d;e:{d=b;if("click"==d&&(u&&a.metaKey||!u&&a.ctrlKey||2==a.which||null==a.which&&4==a.but
||a.target,m=(e.getAttribute("role")||e.type||e.tagName).toUpperCase(),g;(g="keydown"!=a.type)||(g=(e.getAttribute("role")|
rCase(),g=!("TEXT"!=g&&"TEXTAREA"!=g&&"PASSWORD"!=g&&!e.isContentEditable)||a.ctrlKey||a.shiftKey||a.altKey||a.metaKey||13!
srcElement||a.target;e&&e!=this;e=e.__owner||e.parentNode){m=e;var l=m;g=d;var n=l.__jsaction;if(!n){n={};l.__jsaction=n;va
ngth:0;q<H;q++){var p=l[q];if(p){var s=p.indexOf(":"),w=-1!=s,I=w?p.substr(0,s).replace(/^\s+/,"").replace(/\s+$/,""):"clic
lick||(g="clickonly");g=(n=n[g])?{i:g,action:n,w:!1}:void 0;if(g){if(g.w)break;d={eventType:g.i,event:a,targetElement:f,act
actionElement.tagName&&"click"==b&&(a.preventDefault?a.preventDefault():a.returnValue=!1),c.k)c.k(d);else{var r;if((f=h.doc
ventObject)try{r=f.createEventObject(a)}catch(M){r=a}else r=a;d.event=r;c.g.push(d)}}},D=function(c,b){return function(a){v
entListener){if("focus"==d||"blur"==d||"error"==d||"load"==d)e=!0;a.addEventListener(d,f,e)}else a.attachEvent&&("focus"==d
.attachEvent("on"+d,f));return{i:d,s:f,v:e}}},y=function(c,b){if(!c.p.hasOwnProperty(b)&&"mouseenter"!=b&&"mouseleave"!=b){
null,f.a))}"click"==b&&y(c,"keydown")}};z.prototype.s=function(c){return this.p[c]};var L=function(c){var b=E,a=new F(c);e:
lse{J(b,a);b.a.push(a);a=b.d.concat(b.a);c=[];for(var d=[],f=0;f<b.a.length;++f){var e=b.a[f];if(K(e,a)){c.push(e);for(var
,l.s,l.v):g.detachEvent&&g.detachEvent("on"+l.i,l.s)}e.d=[]}else d.push(e)}for(f=0;f<b.d.length;++f)e=b.d[f],K(e,a)?c.push(
);for(a=0;a<c.o.length;++a)b.d.push(c.o[a].call(null,b.a))},F=function(c){this.a=c;this.d=[]},K=function(c,b){for(var a=0;a
)b=b.parentNode;return c==b};var E=new
entElement);y(E,"click");y(E,"focus");y(E,"focusin");y(E,"blur");y(E,"focusout");y(E,"error");y(E,"load");y(E,"change");y(E
ouseup");y(E,"speech");window.google.jsad=function(c){var b=E;b.k=c;b.g&&(0<b.g.length&&c(b.g),b.g=null)};window.google.jsa
ntById(a.id.substring(1)).href;return!0};</script><style>@-webkit-keyframes gb__a{0%{opacity:0}50%{opacity:1}}@keyframes gb
olute;top:0;-webkit-user-select:none;width:100%}.gb_Ab{font:13px/27px Arial,sans-serif;position:relative;height:60px;width:
n:middle}.gb_Ab::before{background:#e5e5e5;bottom:0;content:'';display:none;height:1px;left:0;position:absolute;right:0}.gb
ne}.gb_p .gb_Ab,.gb_q .gb_Ab{background:transparent}.gb_p .gb_Ab::before{background:#e1e1e1;background:rgba(0,0,0,.12)}.gb_
:#333;background:rgba(255,255,255,.2)}.gb_k{display:inline-block;-webkit-flex:0 0 auto;flex:0 0 auto}.gb_k.gb_4b{float:righ
gb_jb{min-width:980px}.gb_5b,.gb_k{margin-left:0!important;margin-right:0!important}.gb_h{background-image:url('//ssl.gstat
bkit-min-device-pixel-ratio:1.25),(min-device-pixel-ratio:1.25){.gb_h{background-image:url('//ssl.gstatic.com/gb/images/v2_
-child,#gbsfw:first-child+.gb_Va{padding-left:0}.gb_La{position:relative}.gb_s{display:inline-block;outline:none;vertical-a
;height:30px;width:30px}#gb#gb a.gb_s{color:#404040;cursor:default;text-decoration:none}#gb#gb a.gb_s:hover,#gb#gb a.gb_s:f
;border-width:0 8px 8px;display:none;position:absolute;left:7px;top:37px;z-index:1;height:0;width:0;-webkit-animation:gb__a
8px;display:none;position:absolute;left:7px;z-index:1;height:0;width:0;-webkit-animation:gb__a .2s;animation:gb__a .2s;bord
bottom-color:#ccc}.gb_t{background:#fff;border:1px solid #ccc;border-color:rgba(0,0,0,.2);box-shadow:0 2px 10px rgba(0,0,0,
tion:gb__a .2s;-webkit-border-radius:2px;border-radius:2px;-webkit-user-select:text}.gb_Va.gb_pa .gb_S,.gb_Va.gb_pa .gb_T,.
-scrollbar{height:15px;width:15px}.gb_Ab ::-webkit-scrollbar-button{height:0;width:0}.gb_Ab ::-webkit-scrollbar-thumb{backg
:10px;min-height:20px;min-width:20px;height:5px;width:5px}.gb_Ab ::-webkit-scrollbar-thumb:hover,.gb_Ab ::-webkit-scrollbar
Bb{display:none!important}.gb_a{background-size:64px 64px}#gb136 .gb_a{background-image:url('//ssl.gstatic.com/gb/images/a/
com/gb/images/a/c03dda0b34.png')}gb217 .gb_a{background-image:url('//ssl.gstatic.com/gb/images/a/b19d3468df.png')}#gb228 .g
l('//ssl.gstatic.com/gb/images/a/29adc12d690.png')}#gb261 .gb_a{background-image:url('//ssl.gstatic.com/gb/images/a/0b26f6f
.25){#gb136 .gb_a{background-image:url('//ssl.gstatic.com/gb/images/a/48165cc026.png')}#gb211 .gb_a{background-image:url('/
com/gb/images/a/d8c8b405fa.png')}#gb228 .gb_a{background-image:url('//ssl.gstatic.com/gb/images/a/82532ae36e.png')}#gb260 .
l('//ssl.gstatic.com/gb/images/a/9001dae971.png')}}.gb_b{display:inline-block;vertical-align:top;height:100px;width:88px}.g
ty:visible;z-index:1001;-webkit-box-shadow:0 0 3px #ddd;box-shadow:0 0 3px #ddd}.gb_e{opacity:.5}.gb_b.gb_d a{color:#404040
```

If that's not enough



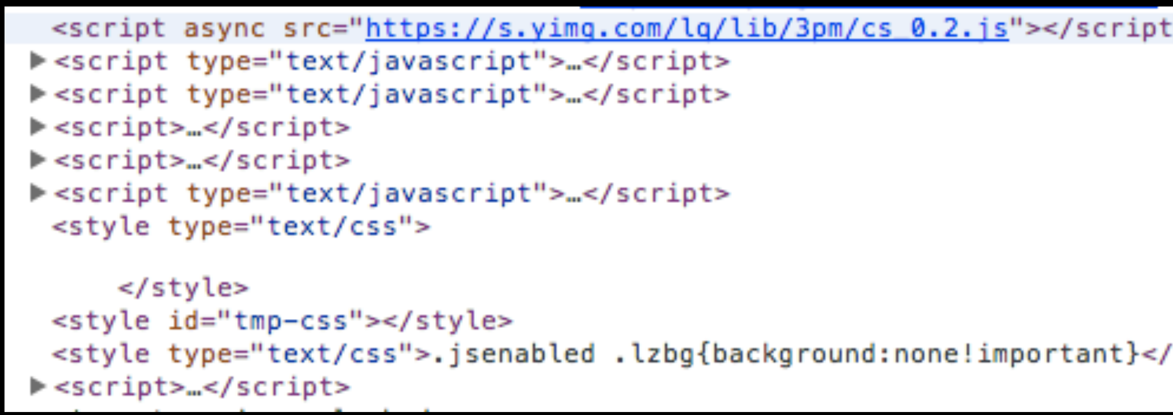
```
ory /zz/combo?yui:3.9.1/build/yui/yui-min.js&os/mit/media/p/common/rmp-min-1675959.js&os/mit/m
ght 2013 Yahoo! Inc. http://yuilibrary.com/license/ */
I=YUI);var YUI=function(){var e=0,t=this,n=arguments,r=n.length,i=function(e,t){return e&&e.hasOwnProperty&&e instanceof
pplyConfig(YUI.GlobalConfig),s&&t.applyConfig(s),r||t._setup()):t=new YUI;if(r){for(;e<r;e++)t.applyConfig(n[e]);t._setup(
.yahooapis.com/",s="yui3-js-enabled",o="yui3-css-stamp",u=function(){},a=Array.prototype.slice,f={"io.xdrReady":1,"io.xdr
=h&&h.documentElement,d=p&&p.className,v={},m=(new Date).getTime(),g=function(e,t,n,r){e&&e.a
e.removeEventListener(t,n,r)}catch(i){}else e&&e.detachEvent&&e.detachEvent("on"+t,n)},b=func
,i=YUI.Env,s=i.mods;return n?(n.ignoreRegistered=!1,n.onEnd=null,n.data=null,n.required=[],n.
),YUI.Env.core=e.Array.dedupe([].concat(YUI.Env.core,r)),n},E=function(e,t){for(var n in t)t.
"@")>-1&&(n="3.5.0"),e={applyConfig:function(e){e=e||u;var t,n,r=this.config,i=r.modules,s=r.
n=="groups"?E(s,t):n=="win"?(r[n]=t&&t.contentWindow||t,r.doc=r[n]?r[n].document:null):n!="_y
.version=n;if(!u){r.Env={core:["get","features","intl-base","yui-log","yui-later","loader-base
0,_used:{},_attached:{},_missed:[],_yidx:0,_uidx:0,_guidp:"y",_loaded:{},_BASE_RE:/(?:\?(?:[
gExp.leftContext||e.slice(0,e.indexOf(n[0])),i=n[3],n[1]&&(r+="?"+n[1]),r={filter:i,path:r}),
ength;o<a;++o){f=n[o].src;if(f){s=r.Env.parseBasePath(f,t);if(s){e=s.filter,i=s.path;break}}}
ace(/[^a-z0-9_]+/g,"_");else if(YUI._YUI){s=YUI._YUI.Env,u._yidx+=s._yidx,u._uidx+=s._uidx;fo
0,doc:h,fetchCSS:!0,throwFail:!0,useBrowserConsole:!0,useNativeES5:!0,win:c,global:Function(
ant; visibility: hidden !important"></div>',YUI.Env.cssStampEl=t.firstChild,h.body?
mpEl):p.insertBefore(YUI.Env.cssStampEl,p.firstChild)):h&&h.getElementById(o)&&!YUI.Env.cssSt
e||r.Env.getBase(r.Env._BASE_RE);if(!e||!"mindebug".indexOf(e))e="min";e=e?"-"+e:e,r.config.lo
e||[].concat(YUI.Env.core);for(e=0;e<i.length;e++)r[i[e]]&&n.push(i[e]);t._attach(["yui-base"
ength;o+=1)s=s[i[o]],s||this.log("applyTo not found: "+t,"warn","yui");return s&&s.apply(r,n)
n,details:r},o={},u,a,f,l=i.versions;i.mods[e]=s,l[n]=l[n]||{},l[n][e]=s;for(f in v)v.hasOwnP
].temp)&&u.addModule(r,e)));return this},_attach:function(e,t){var n,r,i,s,o,u,a,f=YUI.Env.mo
,b.push(r);if(d&&d.conditions[r])for(h in d.conditions[r])d.conditions[r].hasOwnProperty(h)&&
(c)),y&&b.push(g.name))}e=b,m=e.length;for(n=0;n<m;n++)if(!v[e[n]]){r=e[n],i=f[r];if(l&&l[r]&
c.Env._missed.push(r),c.Env._missed=c.Array.dedupe(c.Env._missed),c.message("NOT loaded: "+r,
","warn","yui"),c.Env._missed.splice(h,1));if(d&&p&&p[r]&&p[r].temp){d.getRequires(p[r]),o=[];for(h in
duleInfo[r].expanded_map.hasOwnProperty(h)&&o.push(h);c._attach(o)}s=i.details,o=s.requires,u=s.use,a=s.after,s.lang&&(o=
if(a)for(h=0;h<a.length;h++)if(!v[a[h]]){if(!c._attach(a,!0))return!1;break}if(i.fn)if(c.config.throwFail)i.fn(c,r);else
th;h++)if(!v[u[h]]){if(!c._attach(u))return!1;break}}return!0},_delayCallback:function(e,t){var n=this,r=["event-base"];
&r.push("event-synthetic"),function(){var i=arguments;n._use(r,function(){n.on(t.event,function(){i[1].delayUntil=t.event
ng.isFunction(t)?(e.pop(),n.config.delayUntil&&(t=n._delayCallback(t,n.config.delayUntil))):t=null,n.Lang.isArray(e[0])&&
n._notify(t,S,e),n}return n._loading?(n._useQueue=n._useQueue||new n.Queue,n._useQueue.add([e,t])):n._use(e,function(n,r)
rrorFn)this.config.loadErrorFn.call(this,this,e,t,n);else if(e){this.Env._missed&&this.Env._missed.length&&(t.msg="Missin
ss=!1);if(this.config.throwFail)e(this,t);else try{e(this,t)}catch(r){this.error("use callback error",r,n)}}},_use:functi
=o.Env,l=f._used,c=u.aliases,h=u._loaderQueue,p=e[0],d=o.Array,v=o.config,m=v.bootstrap,g=[],y,b=[],E=!0,S=v.fetchCSS,x=f
]]&&!a[e[r]]?i=[].concat(i,c[e[r]]):i.push(e[r]);e=i}o=e.length;for(r=0;r<o;r++){s=e[r],t||b.
&&x(h),p&&p.length&&x(p,1)}},T=function(n){var r=n||{success:!0,msg:"not dynamic"},i,s,u=!0,a
e(g,function(){o._attach(a)&&o._notify(t,r,a)})):(a&&(u=o._attach(a)),u&&o._notify(t,r,e)),o.
return E=o._attach(e),E&&T(),o}return(a.loader||a["loader-base"])&&!o.Loader&&o._attach(["loa
stered=!0,i._boot=!0,i.calculate(null,S?null:"js"),e=i.sorted,i._boot=!1),x(e),r=g.length,r&&
.context=o,i.data=e,i.ignoreRegistered=!1,i.require(g),i.insert(null,S?null:"js")):m&&r&&o.Ge
tstrapped=!0,u._bootstrapping=!1,o._attach(["loader"])&&o._use(e,t)},u._bootstrapping?h.add(s
ace:function(){var e=arguments,t,n=0,i,s,o;for(;n<e.length;n++){t=this,o=e[n];if(o.indexOf(r)
:u,dump:function(e){return""+e},error:function(e,t,n){var r=this,i;r.config.errorFn&&(i=r.con
:function(e){var t=this.Env._guidp+"_"+ ++this.Env._uidx;return e?e+t:t},stamp:function(e,t)
n}catch(r){n=null}}return n},destroy:function(){var e=this;e.Event&&e.Event._unload(),delete
ction(e){if(!e)return;YUI.GlobalConfig&&this.prototype.applyConfig.call(this,YUI.GlobalConfig
d=g,YUI.Env.remove=y,typeof exports=="object"&&(exports.YUI=YUI,YUI.setLoadHook=function(e){Y
l.slice.call(e,t)}catch(s){i=[];for(r=e.length;t<r;++t)i.push(e[t]);return i}return[e]}functi
rototype.toString,s={"undefined":"undefined",number:"number","boolean":"boolean",string:"stri
rror"},o=/\{\s*([^|}]+?)\s*(?:\|([^}]*))?\s*\}/g,u=/^\s+|\s+$/g,a=/\{\s*\[(?:native code|func
(t))},n.isArray=n._isNative(Array.isArray)?Array.isArray:function(e){return n.type(e)==="arra
=="Invalid Date"&&!isNaN(e)},n.isFunction=function(e){return n.type(e)==="function"},n.isNull
ect=function(e,t){var r=typeof e;return e&&(r==="object"||!t&&(r==="function"||n.isFunction(e
n(e){var t=n.type(e);switch(t){case"number":return isFinite(e);case"null":case"undefined":ret
r){return n.isUndefined(t[r])?e:t[r]}):e},n.trim=r.trim?function(e){return e&&e.trim?e.trim(
e.replace(/^\s+/,"")},n.trimRight=r.trimRight?function(e){return e.trimRight()}:function(e){r
ct.prototype.hasOwnProperty;e.Array=h,h.dedupe=function(e){var t={},n=[],r,i,s;for(r=0
(t,i)||(t[i]=1,n.push(i));return n},h.each=h.forEach=f._isNative(l.forEach)?function(t,n,r){r
},h.hash=function(e,t){var n={},r=t&&t.length||0,i,s;for(i=0,s=e.length;i<s;++i)i in e&&(n[e[
,t,n){var r=e.length;n=+n||0,n=(n>0||-1)*Math.floor(Math.abs(n)),n<0&&(n+=r,n<0&&(n=0));for(
```

- Anonymous functions



```
> (function(){
      window.onload = function(){alert(document.location)}
  })()
  undefined
> window.onload
  function (){alert(document.location)}
> |
```

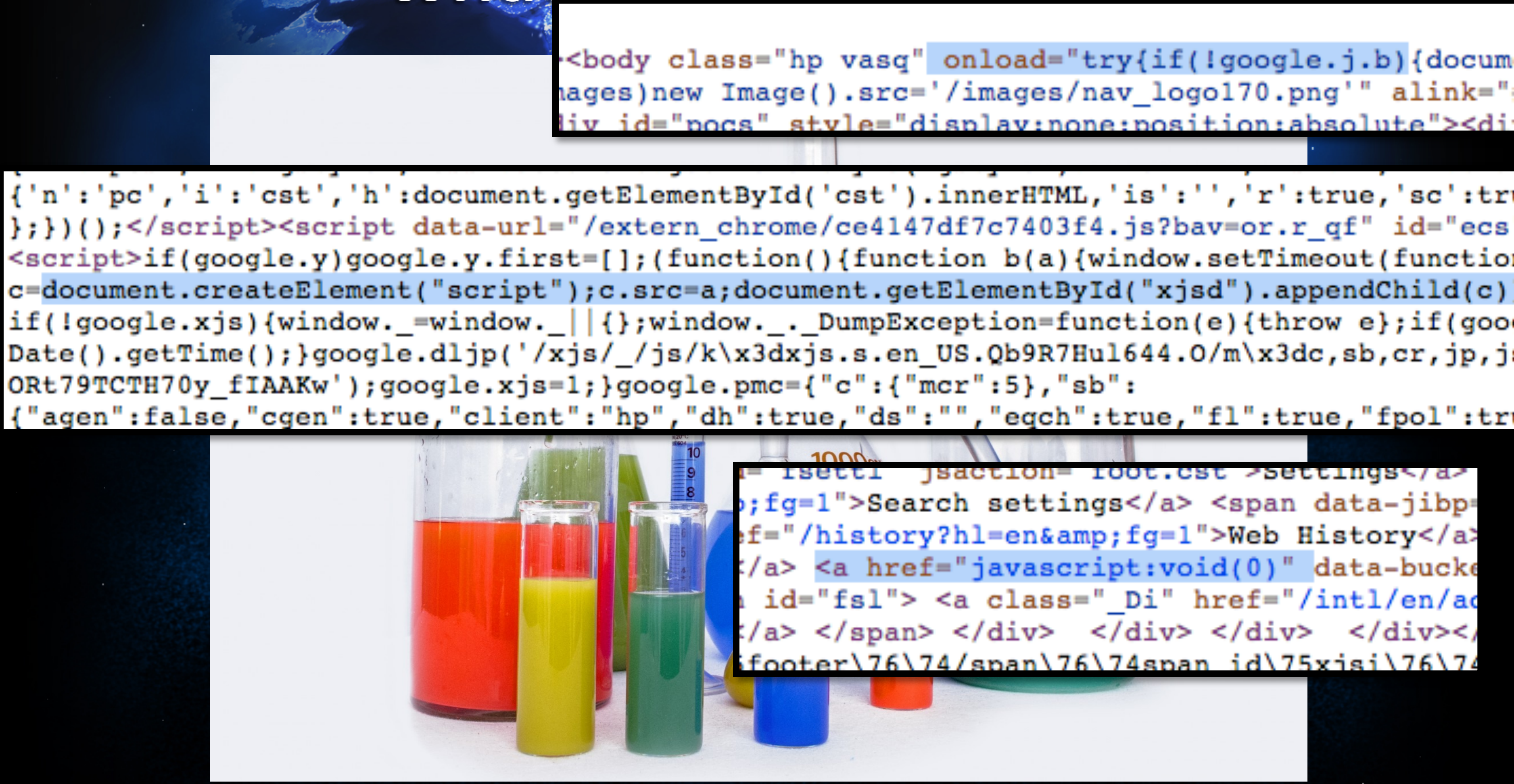
- Dynamic loading



```
  <script async src="https://s.yimg.com/lq/lib/3pm/cs_0.2.js"></script
▶<script type="text/javascript">…</script>
▶<script type="text/javascript">…</script>
▶<script>…</script>
▶<script>…</script>
▶<script type="text/javascript">…</script>
 <style type="text/css">

    </style>
 <style id="tmp-css"></style>
 <style type="text/css">.jsenabled .lzbg{background:none!important}</
▶<script>…</script>
```

The Chemistry of DOM what is executable?

The Chemistry of DOM
what is executable?



```
<body class="hp vasq" onload="try{if(!google.j.b){docum
ages)new Image().src='/images/nav_logo170.png'" alink="
iv id="pocs" style="display:none;position:absolute"><di
```

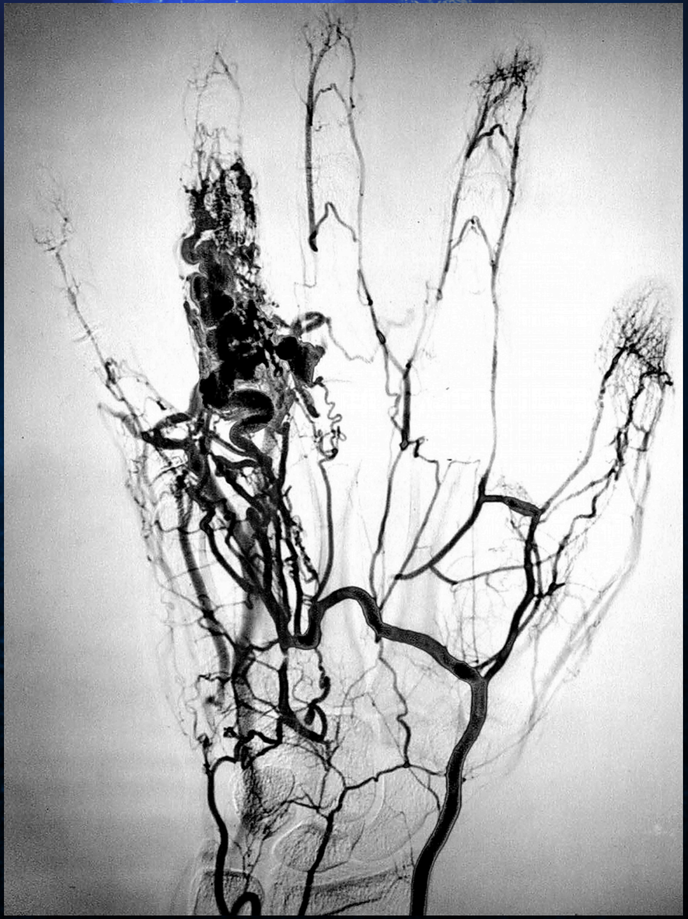
```
{'n':'pc','i':'cst','h':document.getElementById('cst').innerHTML,'is':'','r':true,'sc':tr
};})();</script><script data-url="/extern_chrome/ce4147df7c7403f4.js?bav=or.r_qf" id="ecs
<script>if(google.y)google.y.first=[];(function(){function b(a){window.setTimeout(functio
c=document.createElement("script");c.src=a;document.getElementById("xjsd").appendChild(c)
if(!google.xjs){window._=window._||{};window._._DumpException=function(e){throw e};if(goo
Date().getTime();}google.dljp('/xjs/_/js/k\x3dxjs.s.en_US.Qb9R7Hu1644.O/m\x3dc,sb,cr,jp,j
ORt79TCTH70y_fIAAKw');google.xjs=1;}google.pmc={"c":{"mcr":5},"sb":
{"agen":false,"cgen":true,"client":"hp","dh":true,"ds":"","eqch":true,"fl":true,"fpol":tr
```

```
="fsettl" jsaction="foot.cst">Settings</a>
;fg=1">Search settings</a> <span data-jibp=
f="/history?hl=en&amp;fg=1">Web History</a>
/a> <a href="javascript:void(0)" data-bucke
 id="fsl"> <a class="_Di" href="/intl/en/ac
/a> </span> </div>  </div> </div>  </div></
footer\76\74/span\76\74span id\75xjsi\76\74
```

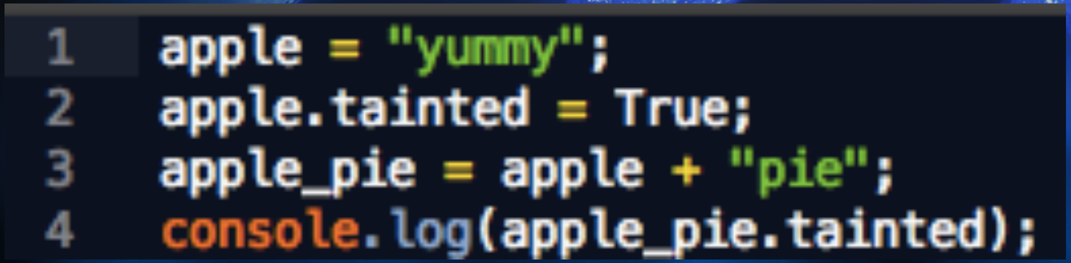
DOM XSS DETECTION

What we want to do

- Analysis how "antigen" (untrusted data) get into our "body" (DOM)



char*



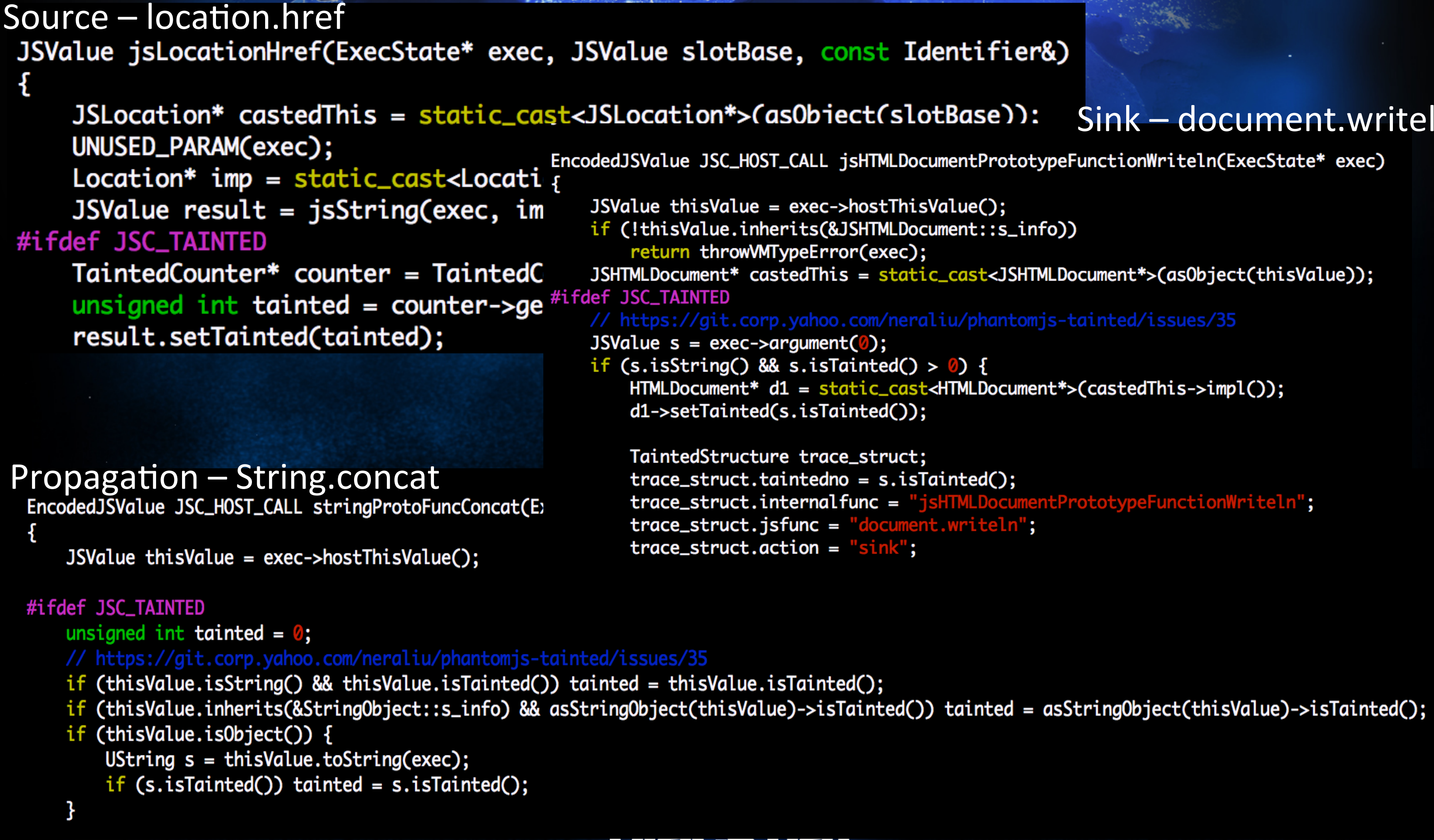
```
apple = "yummy";
apple.tainted = True;
apple_pie = apple + "pie";
console.log(apple_pie.tainted);
```

- All arithmetic operations need to be overridden
- Enable to propagate through different context (HTML/CSS/JS)

Tainted Phantomjs

- Hacking the JavaScriptCore and WebKit engine by propagating the tainted signal during the javascript execution.

Source code of Tainted PhantomJS



Source – location.href

```
JSValue jsLocationHref(ExecState* exec, JSValue slotBase, const Identifier&)
{
    JSLocation* castedThis = static_cast<JSLocation*>(asObject(slotBase));
    UNUSED_PARAM(exec);
    Location* imp = static_cast<Locati
    JSValue result = jsString(exec, im
#ifdef JSC_TAINTED
    TaintedCounter* counter = TaintedC
    unsigned int tainted = counter->ge
    result.setTainted(tainted);
```

Sink – document.writeln

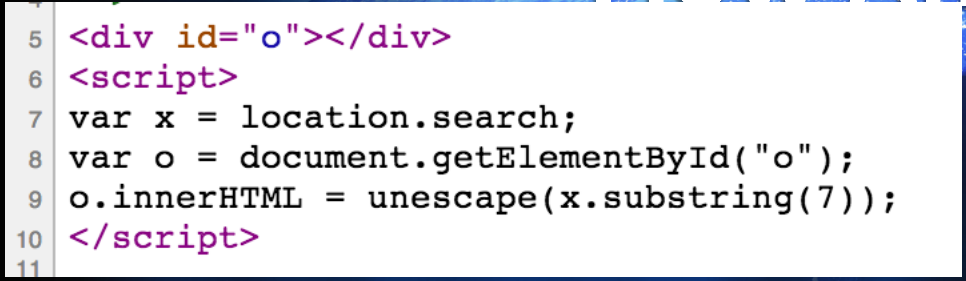
```
EncodedJSValue JSC_HOST_CALL jsHTMLDocumentPrototypeFunctionWriteln(ExecState* exec)
{
    JSValue thisValue = exec->hostThisValue();
    if (!thisValue.inherits(&JSHTMLDocument::s_info))
        return throwVMTypeError(exec);
    JSHTMLDocument* castedThis = static_cast<JSHTMLDocument*>(asObject(thisValue));
#ifdef JSC_TAINTED
    // https://git.corp.yahoo.com/neraliu/phantomjs-tainted/issues/35
    JSValue s = exec->argument(0);
    if (s.isString() && s.isTainted() > 0) {
        HTMLDocument* d1 = static_cast<HTMLDocument*>(castedThis->impl());
        d1->setTainted(s.isTainted());

        TaintedStructure trace_struct;
        trace_struct.taintedno = s.isTainted();
        trace_struct.internalfunc = "jsHTMLDocumentPrototypeFunctionWriteln";
        trace_struct.jsfunc = "document.writeln";
        trace_struct.action = "sink";
```

Propagation – String.concat

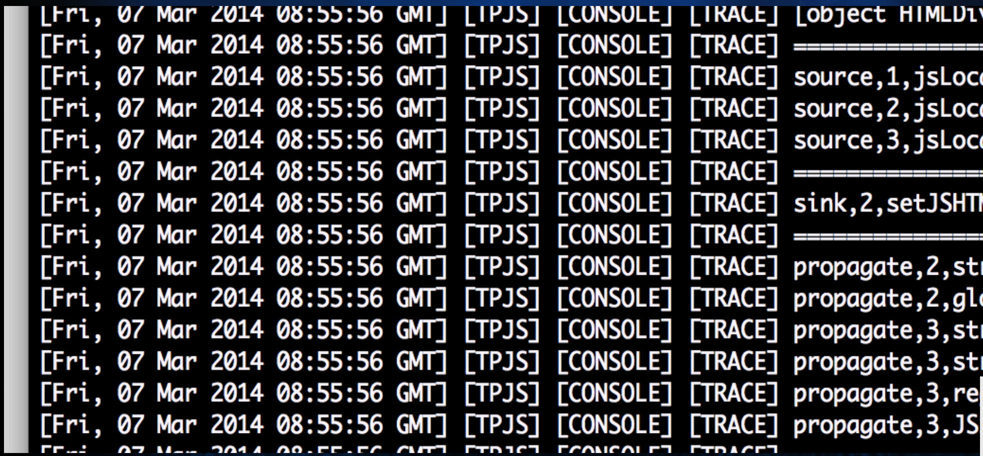
```
EncodedJSValue JSC_HOST_CALL stringProtoFuncConcat(E
{
    JSValue thisValue = exec->hostThisValue();

#ifdef JSC_TAINTED
    unsigned int tainted = 0;
    // https://git.corp.yahoo.com/neraliu/phantomjs-tainted/issues/35
    if (thisValue.isString() && thisValue.isTainted()) tainted = thisValue.isTainted();
    if (thisValue.inherits(&StringObject::s_info) && asStringObject(thisValue)->isTainted()) tainted = asStringObject(thisValue)->isTainted();
    if (thisValue.isObject()) {
        UString s = thisValue.toString(exec);
        if (s.isTainted()) tainted = s.isTainted();
    }
```

Flow Analysis

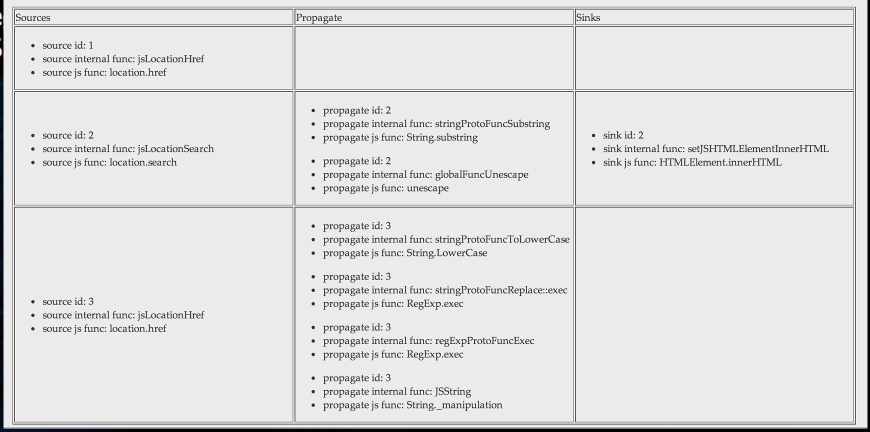
Flow Analysis



```html
<div id="o"></div>
<script>
var x = location.search;
var o = document.getElementById("o");
o.innerHTML = unescape(x.substring(7));
</script>
```



```
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] [object HTMLDivElement] id:o tainted:2
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] ==================
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] source,1,jsLocationHref,location.href,about:blank
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] source,2,jsLocationSearch,location.search,?1394182556085&
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] source,3,jsLocationHref,location.href,http://tinyknight.c
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] ==================
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] sink,2,setJSHTMLElementInnerHTML,HTMLElement.innerHTML,2556085&
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] ==================
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] propagate,2,stringProtoFuncSubstring,String.substring,?1394182556085&
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] propagate,2,globalFuncUnescape,unescape,2556085&
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] propagate,3,stringProtoFuncToLowerCase,String.LowerCase,http://tinyknight.c
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] propagate,3,stringProtoFuncReplace::exec,RegExp.exec,http://tinyknight.c
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] propagate,3,re
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE] propagate,3,JS
[Fri, 07 Mar 2014 08:55:56 GMT] [TPJS] [CONSOLE] [TRACE]
```



Sources	Propagate	Sinks
• source id: 1 • source internal func: jsLocationHref • source js func: location.href		
• source id: 2 • source internal func: jsLocationSearch • source js func: location.search	• propagate id: 2 • propagate internal func: stringProtoFuncSubstring • propagate js func: String.substring • propagate id: 2 • propagate internal func: globalFuncUnescape • propagate js func: unescape	• sink id: 2 • sink internal func: setJSHTMLElementInnerHTML • sink js func: HTMLElement.innerHTML
• source id: 3 • source internal func: jsLocationHref • source js func: location.href	• propagate id: 3 • propagate internal func: stringProtoFuncToLowerCase • propagate js func: String.LowerCase • propagate id: 3 • propagate internal func: stringProtoFuncReplace::exec • propagate js func: RegExp.exec • propagate id: 3 • propagate internal func: regExpProtoFuncExec • propagate js func: RegExp.exec • propagate id: 3 • propagate internal func: JSString • propagate js func: String._manipulation	

Usable Security

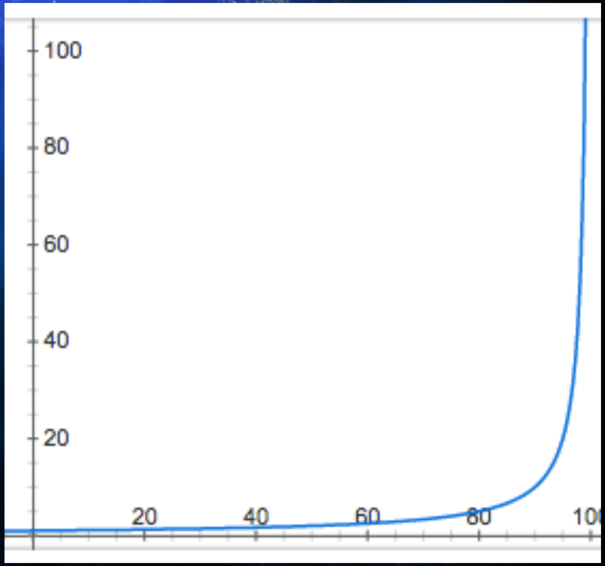
False alarm rate

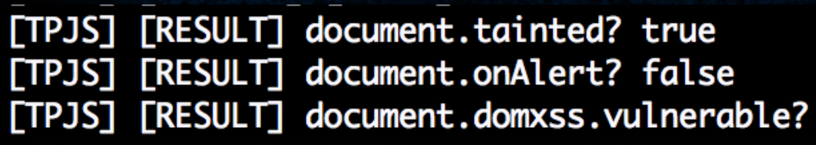
= non-issues / issues reported

More you fix, the higher the false alarm rate

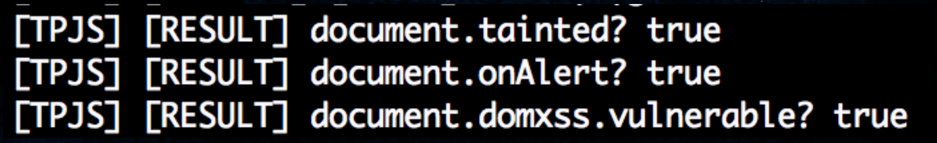
Our ultimate goal:

0 false alarm = 0% rate!





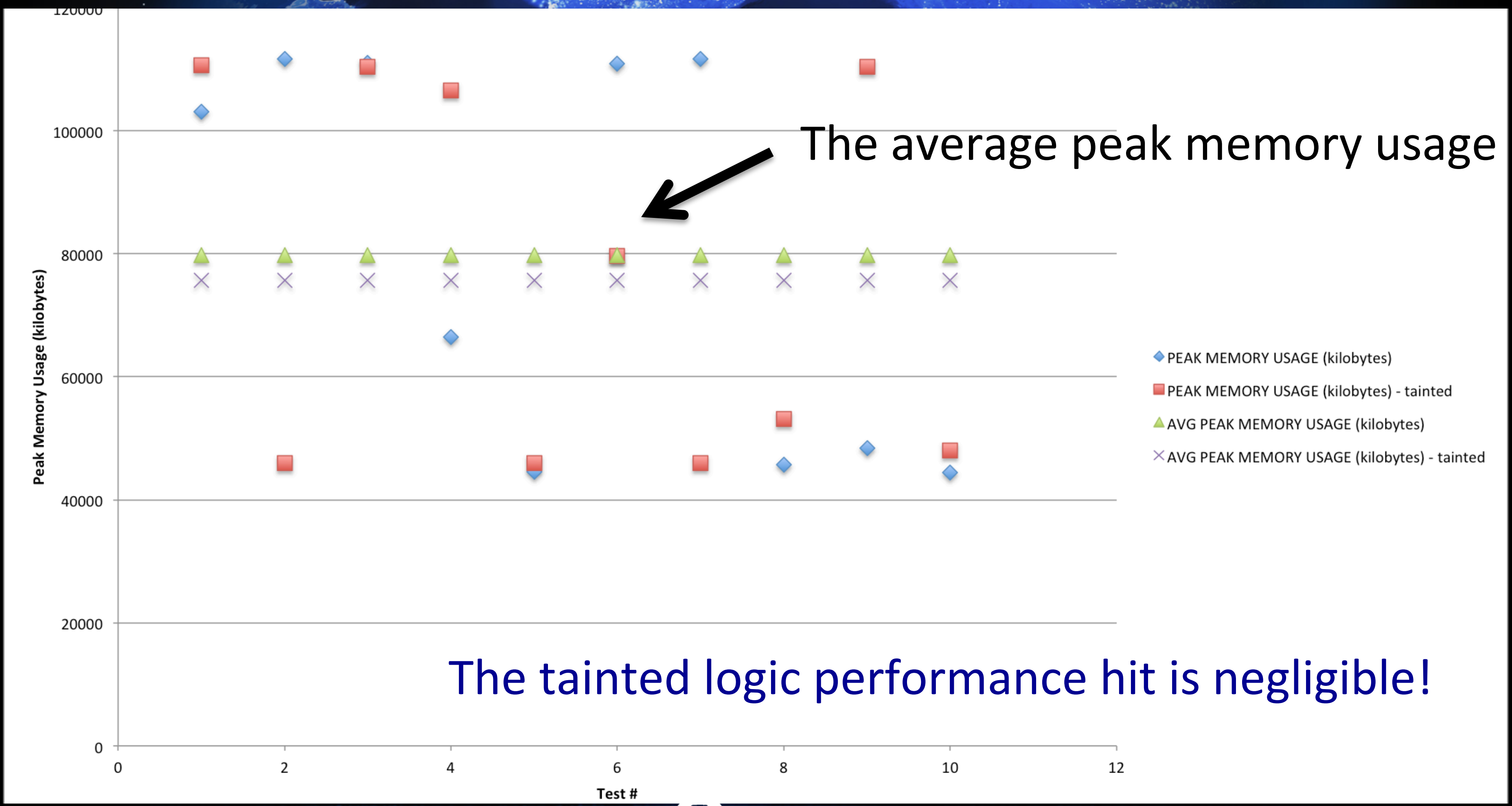
```
[TPJS] [RESULT] document.tainted? true
[TPJS] [RESULT] document.onAlert? false
[TPJS] [RESULT] document.domxss.vulnerable?
```



```
[TPJS] [RESULT] document.tainted? true
[TPJS] [RESULT] document.onAlert? true
[TPJS] [RESULT] document.domxss.vulnerable? true
```

Benchmark and Comparisons

peak memory usage



The average peak memory usage

The tainted logic performance hit is negligible!

DEMO

http://www.youtube.com/watch?v=VU3YnAwc2Ag

Creative Commons

- http://www.flickr.com/photos/58053205@N06/6999839463/
- http://www.flickr.com/photos/67272961@N03/6123892769/
- http://upload.wikimedia.org/wikipedia/commons/7/75/UCLA_dorm_room.JPG
- http://www.flickr.com/photos/44124348109@N01/4682168995/
- http://www.flickr.com/photos/15923063@N00/3150765076/
- http://www.flickr.com/photos/88063120@N00/3529818070/
- http://en.wikipedia.org/wiki/File:Angiome_annulaire.JPG
- http://www.flickr.com/photos/free-stock/4817475664/
- http://www.flickr.com/photos/78428166@N00/9604922912/

black hat ASIA 2014

THANK YOU!