JS Checklist

This is a small JS checklist that helped me score a few bounties with DOM-based vulnerabilities.
If this helped you, know that there's a way to automate this using Nova Security Scanner.

- [ ] **DOM-based DOS** can be induced if user-input lands in `requestFileSystem()` or `RegExp()`
- [ ] **Client-side SQLi** can exist if user-input lands in `executeSql()` (*database is created via the* `var db = openDatabase()` *function, and later called via* `db.transaction(function(tx) {tx.executeSql("...")})`)
- [ ] **DOM-based open redirection** can exist if user-input lands into one of the following sinks:

```
location
location.host
location.hostname
location.href
location.pathname
location.search
location.protocol
location.assign()
location.replace()
open()
element.srcdoc
XMLHttpRequest.open()
XMLHttpRequest.send()
jQuery.ajax()
$.ajax()
```

- [ ] **DOM-based link manipulation** can be caused by one of the following sinks:

```
element.href
element.src
element.action
```

☐ **DOM-based cookie manipulation** can exist if arbitrary user-input gets injected inside the `document.cookie` sink

☐ **DOM-based javascript injection** can be caused if arbitrary user-input ends in one of the following sinks:

```
eval()
Function()
setTimeout()
setInterval()
setImmediate()
execCommand()
execScript()
msSetImmediate()
range.createContextualFragment()
crypto.generateCRMFRequest()
```

☐ **DOM-based local file-path manipulation** can be induced by one of the following sinks:

```
FileReader.readAsArrayBuffer()
FileReader.readAsBinaryString()
FileReader.readAsDataURL()
FileReader.readAsText()
FileReader.readAsFile()
FileReader.root.getFile()
```

☐ **DOM-based Ajax request-header manipulation** can be caused by one of the following sinks:

```
XMLHttpRequest.setRequestHeader()
XMLHttpRequest.open()
XMLHttpRequest.send()
jQuery.globalEval()
$.globalEval()
```

Follow @0xblackbird on Twitter for more like this!