

Forum: [Hack Forums](#)

Thread: [Prototype pollution is it actual bad coding or false positive results from my scanner](#)

konaboy808 - April 23, 2025, 10:00 pm

I was using a prototype scanner that I wrote some code for and I was scanning a site and this is what I found. Is this my scanner returning a bunch of bullshit or is this a site that is really that messed up and dont know what they are doing. Input would be appreciated and maybe some direction in tuning my scanner to not return false issues in the future. I can send you my code for the scanner also. If you tweek the code for my scanner please provide the corrections it would be of great help. ???

```
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"createSummaryTransaction",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"createTemplateSummaryTransaction",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"getEligibleSubsidiariesFor",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"getEvaluationOptions",{enumerable:!0,get:function()
? Line 411: [HIGH] object_mutation -
Object.defineProperty(e,"generateAuthorizeCancelSuccessModal",{enumerable:!0,get:function()
? Line 411: [HIGH] object_mutation -
Object.defineProperty(e,"generateAuthorizeFailureModal",{enumerable:!0,get:function()
? Line 411: [HIGH] object_mutation -
Object.defineProperty(e,"isTransactionPutOnHold",{enumerable:!0,get:function()

? Line 1570: [HIGH] dangerous_operations - Object.freeze({toString:()
? Line 1570: [HIGH] dangerous_operations - Object.freeze({})
Line 2089: [CRITICAL] prototype_manipulation - Object.setPrototypeOf(i,n.prototype)
Line 2427: [CRITICAL] prototype_manipulation - .prototype.serialize=
Line 2807: [CRITICAL] prototype_manipulation - .prototype.isNamespace=

Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"ACCOUNT_MAP_QUERY_PARAMS",{enumerable:!0,get:function()
? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"ACCOUNT_MAP_REFRESH_STATUS",{enumerable:!0,get:function()
? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"ACCOUNT_QUERY_PARAMS",{enumerable:!0,get:function()
? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"AccountMapExtendedSearch",{enumerable:!0,get:function()
? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"accountIsEligible",{enumerable:!0,get:function()
? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"postAccountsFetch",{enumerable:!0,get:function()
? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"postSingleAccountFetch",{enumerable:!0,get:function()
? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"stringToMatch",{enumerable:!0,get:function()

```

? Line 396: [HIGH] object_mutation -
Object.defineProperty(e,"updateAccountBalanceAndStatus",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"ACCOUNT_INTERMEDIARY_PROPERTIES",{enumerable:!0,get:function()
)
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"ACCOUNT_RECEIVER_PROPERTIES",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"ACH_ACCOUNT_PROPERTIES",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"COMMON_ACCOUNT_PROPERTIES",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"PROPERTY_TYPES",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"RECIPIENT_ACCOUNT_PROPERTIES",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"RECIPIENT_DETAIL_PROPERTIES",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"RTP_ACCOUNT_PROPERTIES",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"WAGE_GARNISHMENT_ADDENDA_PROPERTIES",{enumerable:!0,get:f
unction()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"wageGarnishmentAccountProperties",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"hasActualChanges",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"hasAddedProperty",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"hasRemovedProperty",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"hasUpdatedProperty",{enumerable:!0,get:function()
? Line 403: [HIGH] object_mutation -
Object.defineProperty(e,"fetchAndPopulateWageGarnishmentForm",{enumerable:!0,get:function()
? Line 405: [HIGH] object_mutation -
Object.defineProperty(e,"generateAuthorizeFailureModal",{enumerable:!0,get:function()
? Line 405: [HIGH] object_mutation -
Object.defineProperty(e,"generateAuthorizeSuccessModal",{enumerable:!0,get:function()
? Line 405: [HIGH] object_mutation -
Object.defineProperty(e,"generateDraftSuccessModal",{enumerable:!0,get:function()
Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"fromAccountFilter",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"getAccountDisplayText",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"toAccountFilter",{enumerable:!0,get:function()
Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"PaymentOptionsMapping",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"getPaymentActions",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"BankPolicyTypes",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -

```
Object.defineProperty(e,"addCompanySubsidiary",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"capabilityCheck",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"createAccountMap",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"createCompanySubsidiary",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"createPaymentSummaryTransaction",{enumerable:!0,get:function()
? Line 406: [HIGH] object_mutation -
Object.defineProperty(e,"createSummaryTransaction",{enumerable:!0,get:function()

```

```
data:text/plain;base64,dmFyIHEgPSBnYXRoLmZsb29yKG5ldyBEYXRIKCkuZ2V0VGltZSgpLzMwM
DAwMcK7dmFyIHM9ZG9jdW1lbnQuY3JlYXRIRWxlbnVudCgic2NyaXB0lik7d2luZG93LI9fQk9CTGI
2ZUNoYXQgPSB7fTtzLnNyYz0iaHR0cHM6Ly9zZGstY2RuLm9ubGluZWJjY2VzcyEuY29tL3Nkay1
uZ2lueC1hd3NwcmQvc2RrY2RuLzQxOTQtMDEtcHJkLWRiby00MTk0LXRyYWJpYW4tYmVjdS1xc
2RrL0JPQkxpdmdVdaGF0L2Fzc2V0cy91dXhfcGF5bG9hZC5qc28iK3E7cy5zZXRBdHRyaWJ1dGUo
J2FzeW5jJyx0cnVKTtZLnNldEF0dHJpYnV0ZSgnY3Jvc3NvcmlnaW4nLCAAnYW5vbnltb3VzJyk7ZG9
jdW1lbnQucXVlcnlTZWxly3RvcigiYm9keSlpLmFwcGVuZENoaWxkKHMPow==: No connection
adapters were found for
'data:text/plain;base64,dmFyIHEgPSBnYXRoLmZsb29yKG5ldyBEYXRIKCkuZ2V0VGltZSgpLzMw
MDAwMcK7dmFyIHM9ZG9jdW1lbnQuY3JlYXRIRWxlbnVudCgic2NyaXB0lik7d2luZG93LI9fQk9CT
GI2ZUNoYXQgPSB7fTtzLnNyYz0iaHR0cHM6Ly9zZGstY2RuLm9ubGluZWJjY2VzcyEuY29tL3Nkay
1uZ2lueC1hd3NwcmQvc2RrY2RuLzQxOTQtMDEtcHJkLWRiby00MTk0LXRyYWJpYW4tYmVjdS1x
c2RrL0JPQkxpdmdVdaGF0L2Fzc2V0cy91dXhfcGF5bG9hZC5qc28iK3E7cy5zZXRBdHRyaWJ1dGU
oJ2FzeW5jJyx0cnVKTtZLnNldEF0dHJpYnV0ZSgnY3Jvc3NvcmlnaW4nLCAAnYW5vbnltb3VzJyk7ZG
9jdW1lbnQucXVlcnlTZWxly3RvcigiYm9keSlpLmFwcGVuZENoaWxkKHMPow=='

```

PercevalFox - April 24, 2025, 12:14 am

Hello =)

Normal :

The usage of Object.defineProperty() with getters is a normal usage of framework JS or packaged code. Not really dangerous if there is no network access, DOML or eval in the getters

Object.freeze() is save except if combined with other malicious mutation

Potentially dangerous :

Object.setPrototypeOf() or .prototype.* = ... can lead to prototype pollution, that's hot if it's accessible via externals inputs

The base 64 script inject dynamicly JS frm an external domain (sdk-cdn.onlineaccess1.com) via document.createElement("script")

Classic from a live chat, but also used for phishing or XSS, if it's not a trust domain : RED FLAG

Other :

TOOOOOO MUCH object_mutation, you have to filter like :

Flag only if getters are non-trivials (access to DOM, do fetch/ajax, or even user eval())

Keep thoses prototype_manipulation flags in CRITICAL, this is a real risk

You can send me the code, i'll help you if you need to make you code with less false positives and more pertinent