

Open in app ↗

Sign up

Sign in

Medium

Search

Write



Malicious OPEN Redirection *CVE-2025-61166*



Nikhil Thakur

Follow

2 min read · Feb 11, 2026



SigningHub by Ascertia v.10.0 — Malicious OPEN Redirection

Discovered by: Nikhil Thakur

```
#####
# Title: SigningHub by Ascertia v.10.0 - Malicious OPEN Redirection
# Author: Mr. Nikhil Thakur
# Vendor Homepage: https://www.signinghub.com/
# Version: v10.0
# Tested on: Latest version of Chrome, Firefox on Windows and Linux.
# CVE: CVE-2025-61166
#####
```

----- OPEN Redirection -----

Open redirection arises when a script writes controllable data into the target of a redirection in an unsafe way. An attacker may be able to use the

vulnerability to construct a URL that, if visited by another application user, will cause a redirection to an arbitrary external domain. This behavior can be leveraged to facilitate phishing attacks against users of the application. The ability to use an authentic application URL, targeting the correct domain and with a valid SSL certificate (if SSL is used), lends credibility to the phishing attack because many users, even if they verify these features, will not notice the subsequent redirection to a different domain. If an attacker can control the start of the string that is passed to the redirection API, then it may be possible to escalate this vulnerability into a JavaScript injection attack, by using a URL with the javascript: pseudo-protocol to execute arbitrary script code when the URL is processed by the browser.

Reproduction Steps:

Step 1: Initial Discovery and Reconnaissance:

As an unauthenticated user, navigate to the target application's base URL (e.g., [https://.signinghub.com](https://*.signinghub.com)). Using browser developer tools (F12 → Network tab) or an intercepting proxy like Burp Suite, spider/crawl the application to identify all endpoints. Look specifically for parameters named url, redirect, return, next, or destination. You should identify the endpoint: /OAuth/OIDCAuthenticate?url=*

Step 2: Craft the Malicious Request:

Construct a GET request to the vulnerable endpoint with an external domain in the url parameter:

[https://.signinghub.com/OAuth/OIDCAuthenticate?url=https://evil.com](https://*.signinghub.com/OAuth/OIDCAuthenticate?url=https://evil.com)*

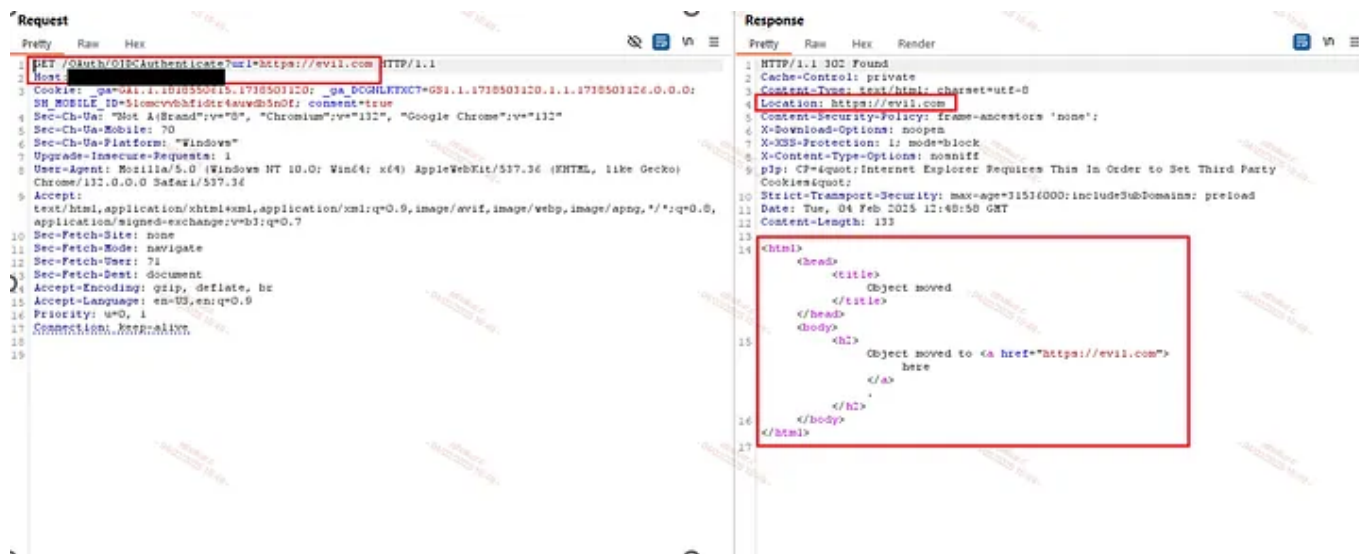
(Replace url= value with the actual subdomain with a domain you control or a trusted external site like <https://evil.com> for testing)

Step 3: Execute and Observe:

Submit the crafted URL directly in a browser address bar or via a crafted link.

Observe if the application immediately redirects the browser to <https://evil.com> without any user warning, interstitial page, or validation prompt.

Step 4: Traffic will be redirected to <https://evil.com> ;)



Successfully Redirected to <https://evil.com>

****An unauthenticated attacker can able to find this vulnerable “url=” parameter endpoint by just spidering the SigningHub application portal url to identify associated endpoints.****

Get Nikhil Thakur's stories in your inbox

Join Medium for free to get updates from this writer.



Remember me for faster sign in

— — — Many Thanks — — —



Written by Nikhil Thakur

3 followers · 1 following



No responses yet



Write a response

What are your thoughts?

More from Nikhil Thakur

```

Request
Pretty Raw Hex
1 GET /Instinct_UI.WebClient_AMC_SA_v6.5.0/Tandori/Instinct-webportal-01
  inst/assets/logo.html [redacted] HTTP/2
2 Host: instinc
3 Sec-Ch-Ua: " ; chrome=";v="55", "Chromium";v="102", "Google
  Chrome";v="112"
4 Sec-Ch-Ua-Mobile: ?0
5 Upgrade-Insecure-Requests: 1
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.0.0
  Safari/537.36
7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
  image/avif,image/svg+xml;q=0.8,application/signed-exchange;v=b3;q=0.6
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: navigate
10 Sec-Fetch-Dest: document
11 Referer: https://instinct-internal/Instinct_UI.WebClient_AMC_SA_v6.5.0/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.5
14 Cookie: [redacted]
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Cache-Control: no-cache, no-store, must-revalidate
3 Content-Type: text/html
4 Last-Modified: Thu, 15 Jun 2023 13:01:56 GMT
5 Accept-Ranges: bytes
6 ETag: "01a000000001:0"
7 Vary: Accept-Encoding
8
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Headers: Content-Type, Authorization
11 Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
12 X-Frame-Options: DENY
13 Content-Security-Policy: default-src 'self' http://localhost:4200/
  https://chrome.cloudflare.com/js/inline.html;
  'unsafe-inline' 'unsafe-eval' data: frame-ancestors 'self';
  Strict-Transport-Security: max-age=31536000
14 X-Content-Type-Options: nosniff
15 Date: Wed, 10 Aug 2023 00:50:23 GMT
16 Content-Length: 101
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

```

Nikhil Thakur

```

Request
Pretty Raw Hex
1 GET /page/changepass/overco
  [redacted] [redacted] [redacted]
2 Cookie: [redacted]
3 Accept: application/json, text/plain, */*
4 Sec-Fetch-Dest: empty
5 Sec-Fetch-Mode: cors
6 Referrer: https://instinct-internal/Instinct_UI.WebClient_AMC_SA_v6.5.0/
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
Response
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Cache-Control: no-cache, no-store, must-revalidate
3 Content-Type: text/html
4 Last-Modified: Thu, 15 Jun 2023 13:01:56 GMT
5 Accept-Ranges: bytes
6 ETag: "01a000000001:0"
7 Vary: Accept-Encoding
8
9 Access-Control-Allow-Origin: *
10 Access-Control-Allow-Headers: Content-Type, Authorization
11 Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
12 X-Frame-Options: DENY
13 Content-Security-Policy: default-src 'self' http://localhost:4200/
  https://chrome.cloudflare.com/js/inline.html;
  'unsafe-inline' 'unsafe-eval' data: frame-ancestors 'self';
  Strict-Transport-Security: max-age=31536000
14 X-Content-Type-Options: nosniff
15 Date: Wed, 10 Aug 2023 00:50:23 GMT
16 Content-Length: 101
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

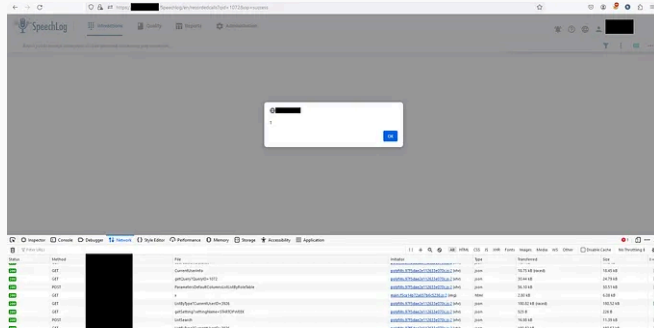
```

Nikhil Thakur

DOM Based Malicious Redirection *CVE-2024-28287*

Instinct Web UI v.6.5.0 — DOM-Based Malicious Redirection

Mar 22, 2024 150



Nikhil Thakur

Stored Cross Site Scripting *CVE-2024-33819*

SpeechLog v.8.1 — Stored XSS

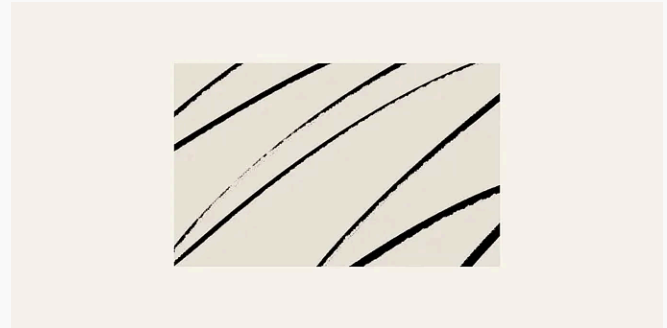
May 10, 2024 50



Insecure Direct Object References *CVE-2024-33818*

SpeechLog v.8.1 — Privilege Escalation

May 10, 2024 50



Nikhil Thakur

Stored XSS in Chat Box Component *CVE-2025-56320*

CobbleStone Software — Enterprise Contract Management Software v.22.2.1

Oct 14, 2025



See all from Nikhil Thakur

Recommended from Medium



In ILLUMINATION by Sufyan Maan, M.Eng

I Woke Up at 4:30 AM Every Day for 30 Days — Here Is What Nobody...

Here is what actually happened, from someone who did it & tracked everything.

2d ago 6.7K 298



Krishna Kumar

From SSRF to AWS Pwnage: A Hacker's Guide to Cloud-Native...

Ever found a bug that lets you make a server visit a URL? It might seem small, but...

Feb 27 6

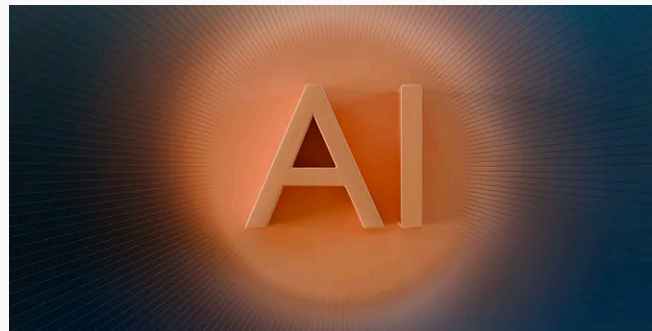


Manya Agarwal

Understanding Kubernetes Internals: CRI, Taints, Affinity &...

Container Runtime Interface (CRI) & Docker Removal

5d ago

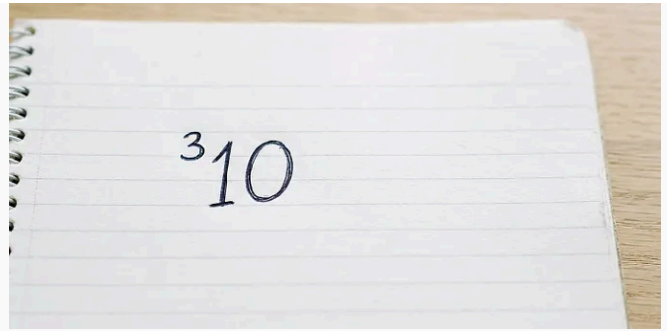
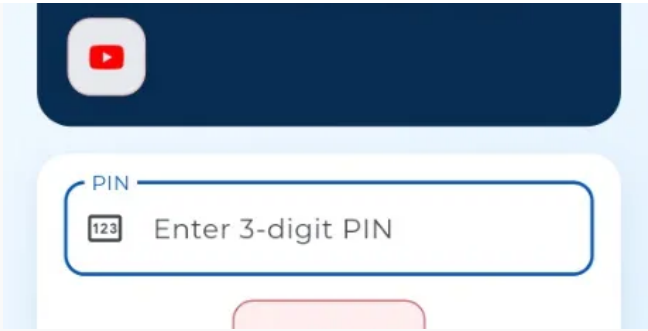


In Predict by Tasmia Sharmin

Palantir CEO Says Only Two Types Will Survive AI (And Elite Degrees...

Alex Karp told Gen Z there are “basically two ways to know you have a future.” Vocational...

Mar 27 2.3K 195




B Bejiamen

Mobile CTF: Cracking an Android App PIN with ADB Brute-Forcing

Introduction

Mar 30



 In Variables & Values by Pradeep Mishra

I Was 32 Before I Saw a Number Written Like This. Nobody Warne...

The operation above exponentiation that makes the universe feel embarrassingly...



Mar 27



5.2K



122



See more recommendations