

[Code](#) [Issues](#) **32** [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** yesterday

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/system/status>) 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`

This behavior enables loading of external resources from attacker infrastructure and may allow phishing attacks or user redirection.

PoC

Send a crafted request with a malicious Host header:

The screenshot shows the Burp Suite interface. On the left, the 'Request' tab is active, displaying a GET / HTTP/1.1 request. A red arrow points to the 'Host: localhost:8080' header. On the right, the 'Response' tab is active, showing the HTML response from the server. A red box highlights the following HTML elements:

```

<link rel="apple-touch-icon" sizes="180x180" href="
http://localhost:8080/apple-touch-icon.png">
<link rel="shortcut icon" type="image/x-icon" href="
http://localhost:8080/favicon.ico">
<link rel="manifest" href="http://localhost:8080/site.webmanifest"
crossorigin="use-credentials">
<link rel="mask-icon" href="http://localhost:8080/safari-pinned-tab.svg"
color="#5bbad5">
<meta name="msapplication-TileColor" content="#da532c">
<meta name="theme-color" content="#ffffff">

```

The screenshot shows the Burp Suite interface with a request to google.com. A red arrow points to the 'Host: google.com' header in the request. The response tab shows the HTML response from google.com. A red box highlights the following HTML elements:

```

<link rel="apple-touch-icon" sizes="180x180" href="
http://google.com/apple-touch-icon.png">
<link rel="shortcut icon" type="image/x-icon" href="
http://google.com/favicon.ico">
<link rel="manifest" href="http://google.com/site.webmanifest" crossorigin
="use-credentials">
<link rel="mask-icon" href="http://google.com/safari-pinned-tab.svg" color
="#5bbad5">
<meta name="msapplication-TileColor" content="#da532c">
<meta name="theme-color" content="#ffffff">

```

At the bottom of the response tab, a search bar contains 'localhost' and shows '37 matches'. A red arrow points to this search bar.

The screenshot shows the Burp Suite interface. On the left, the 'Request' tab is active, displaying various headers like 'Host: google.com', 'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36', and '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'. On the right, the 'Response' tab is active, showing HTML code for a navigation menu. A red box highlights a portion of the response containing the following code:

```
<a class="navbar-brand" href="http://google.com" title="Dashboard"
>

</div>
<div class="collapse navbar-collapse" id="app-navbar-collapse">
<ul class="nav navbar-nav">
<li class="">
<a href="http://google.com/mailbox/1">
Mailbox
</a>
</li>
<li class="dropdown">
<a href="#" class="dropdown-toggle" data-toggle="dropdown"
role="button" aria-expanded="false" aria-haspopup="true" v-pre
>
Manage <span class="caret">
</span>
</a>
</li>
<ul class="dropdown-menu">
<li class="">
<a href="http://google.com/app-settings">
Settings
</a>
</li>
<li class="">
<a href="http://google.com/mailboxes">
Mailboxes
</a>
</li>
</ul>
</ul>
```

At the bottom of the interface, a search bar contains 'google.com' and indicates '35 matches'. A red arrow points to this search bar.

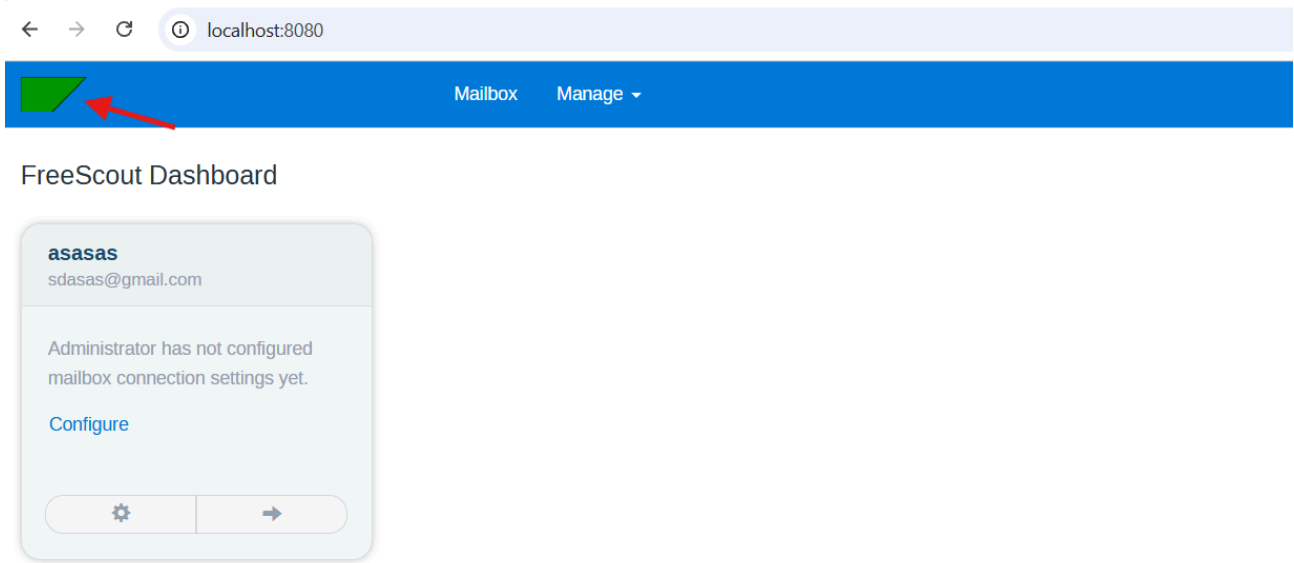
The screenshot shows a web browser window with two tabs: 'Dashboard - FreeScout' and 'Dashboard - FreeScout'. The address bar shows 'localhost:8080'. The page content includes a blue navigation bar with 'Mailbox' and 'Manage' items. A blue arrow points to the 'Mailbox' item.

FreeScout Dashboard

The screenshot shows the mailbox configuration panel in FreeScout. It displays the email address 'sdasas@gmail.com' and a message: 'Administrator has not configured mailbox connection settings yet.' Below the message is a blue 'Configure' link and a button with a gear icon.

The screenshot shows a browser address bar with the URL 'google.com/mailbox/1'. A blue arrow points to the address bar.

External Resource Loading

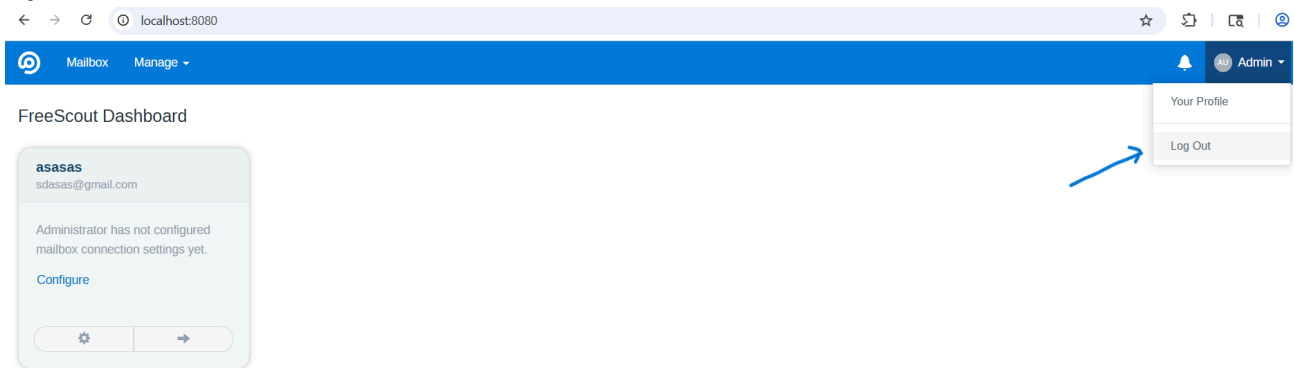


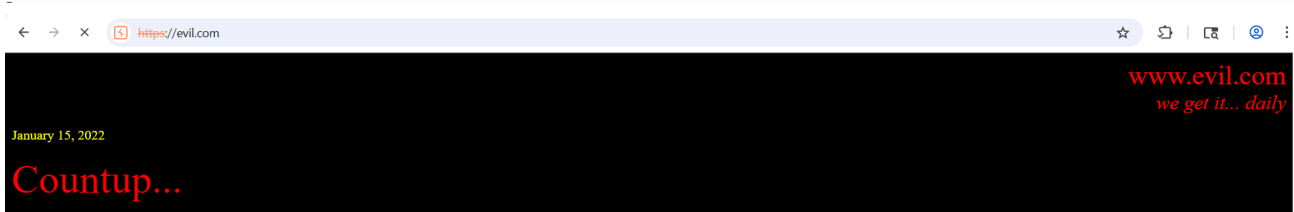
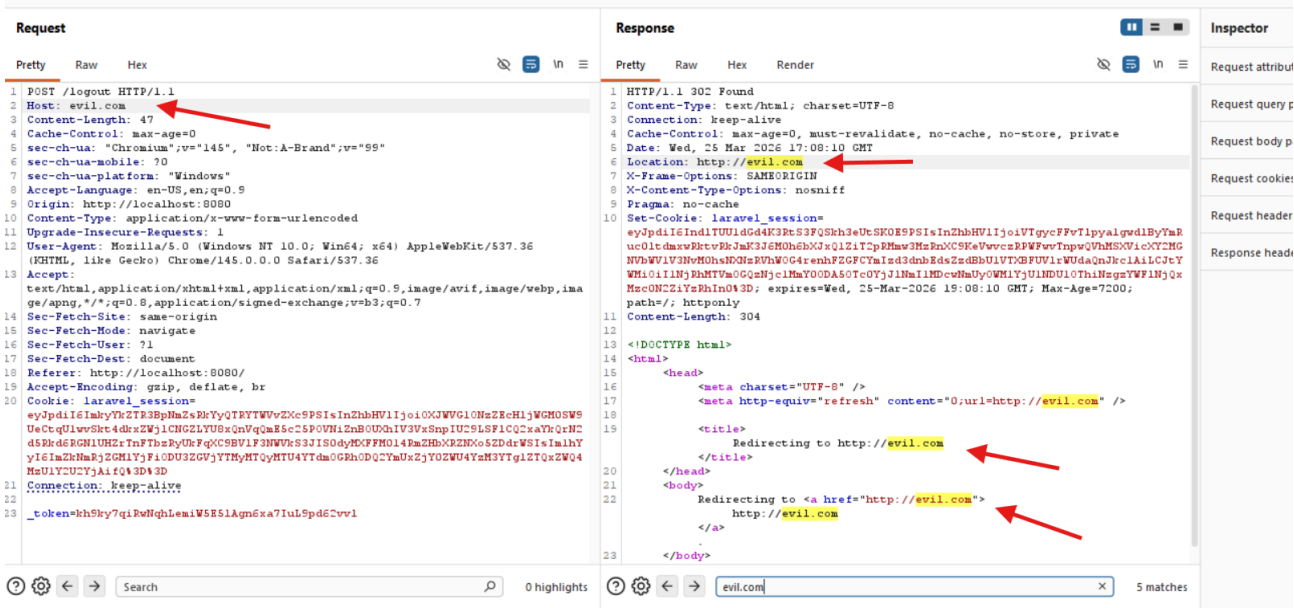
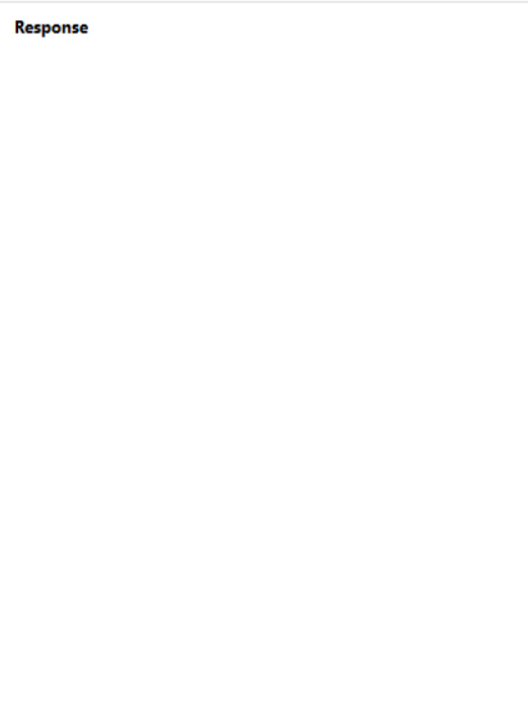
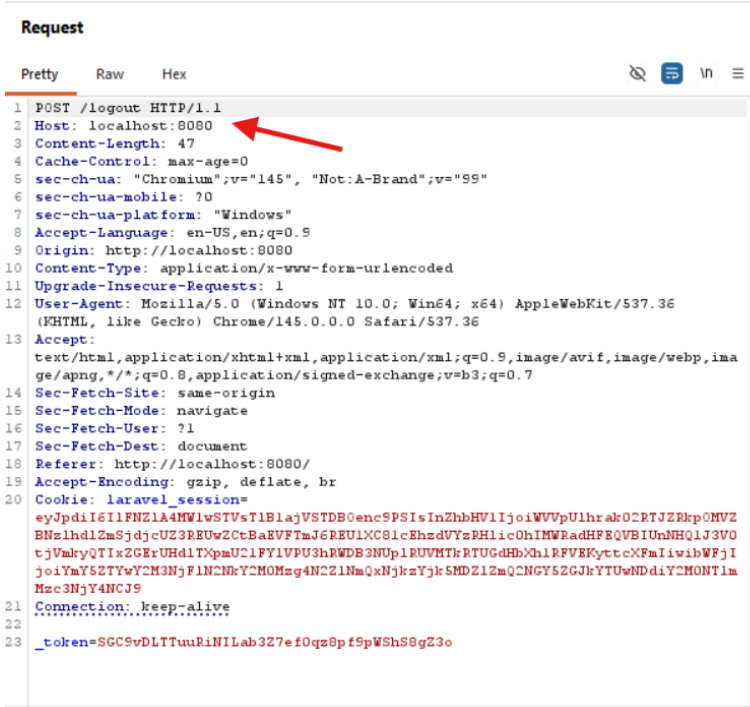
```
(root@kali)-[~/kali/Desktop]
# python3 -m http.server

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





Impact

- Open Redirect vulnerability
- External Resource Loading
- Possible phishing attacks
- UI redressing / brand impersonation
- User traffic redirection to attacker infrastructure

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