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	Patched versions
<1.8.211	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

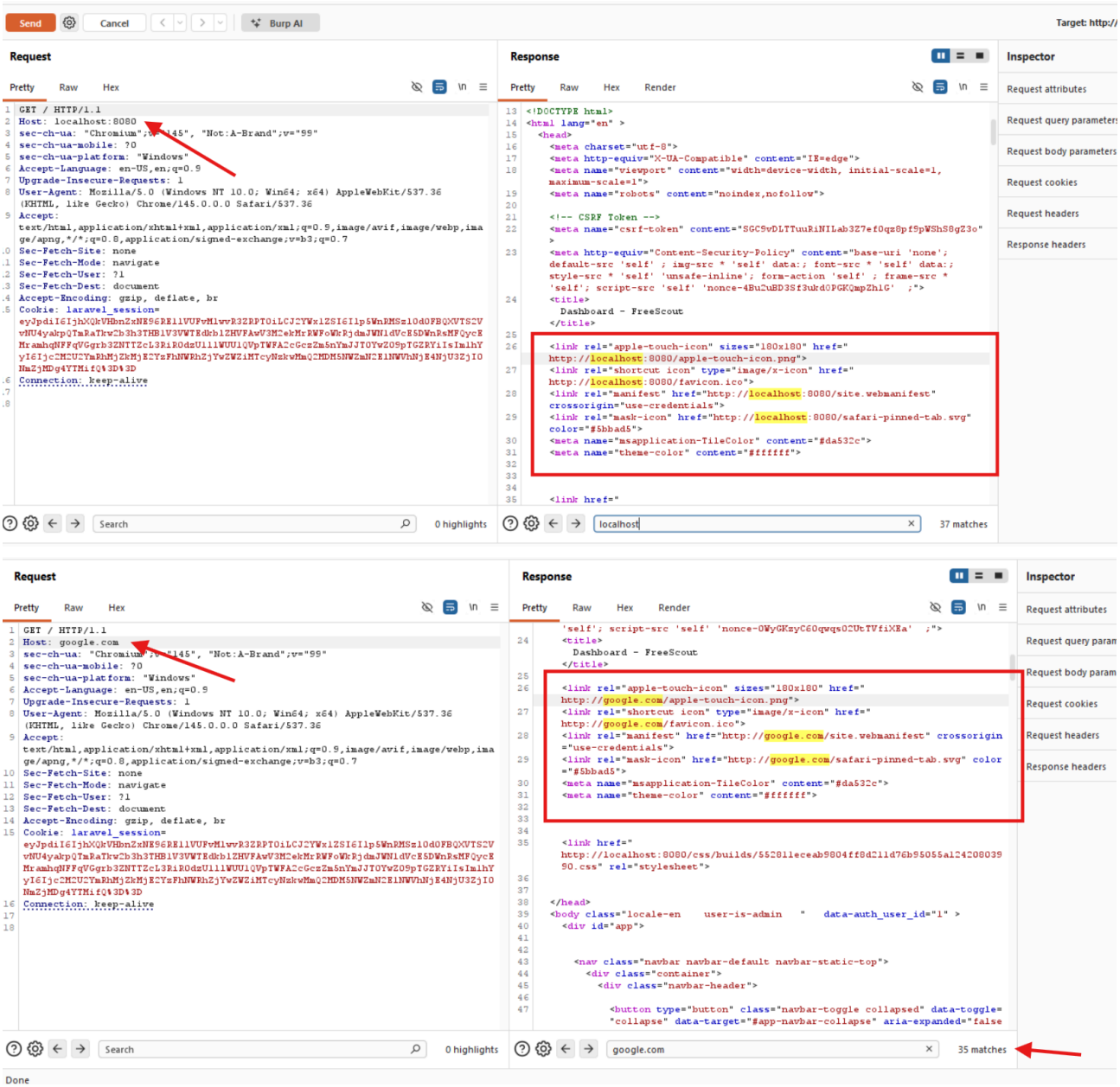
When the manipulated host is processed, the application generates responses containing attacker-controlled URLs. These URLs are reflected in:

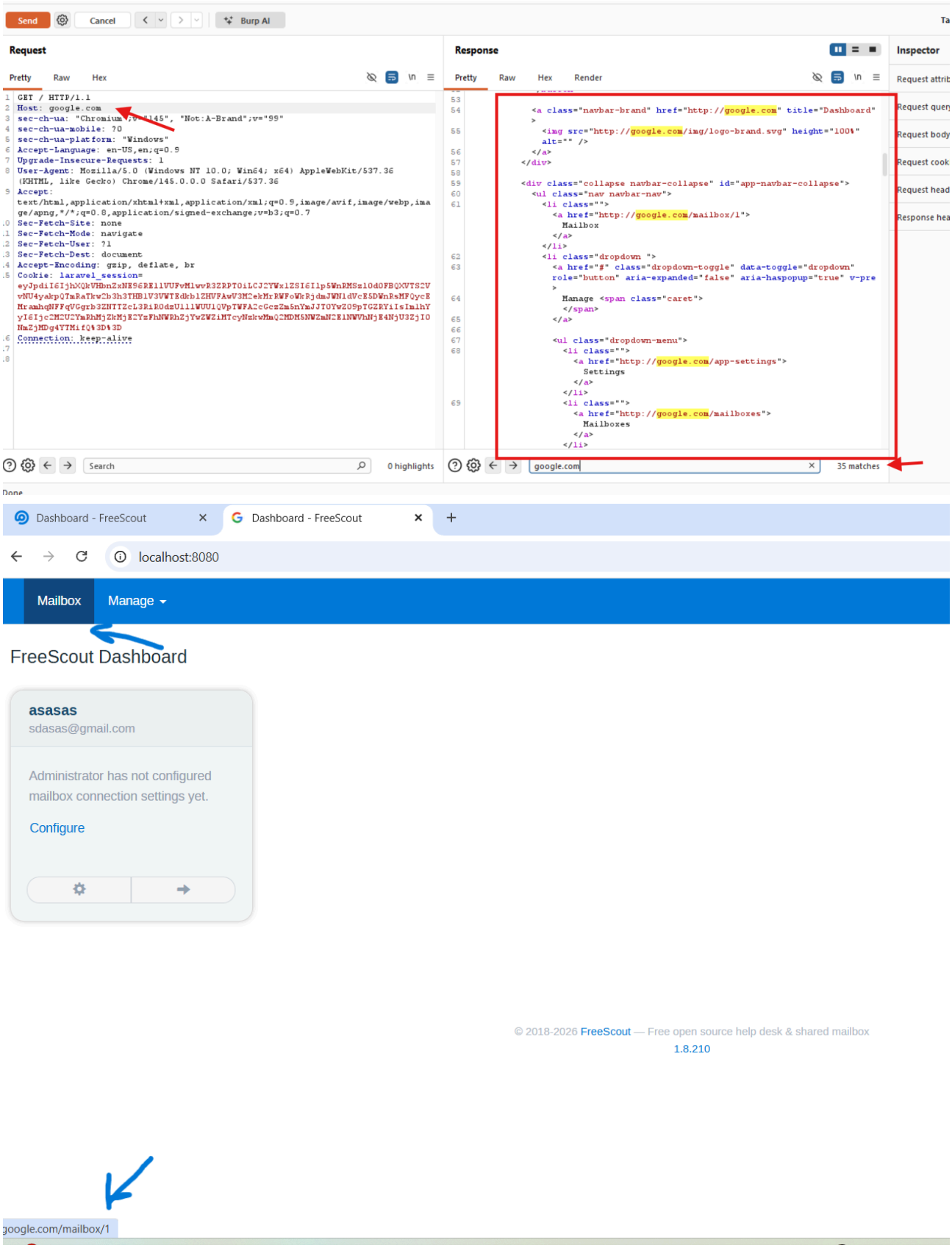
Redirect responses (Location header)
Navigation links
Image resources
Favicon and manifest references
AJAX endpoints such as /conversation/ajax-html/default_redirect

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

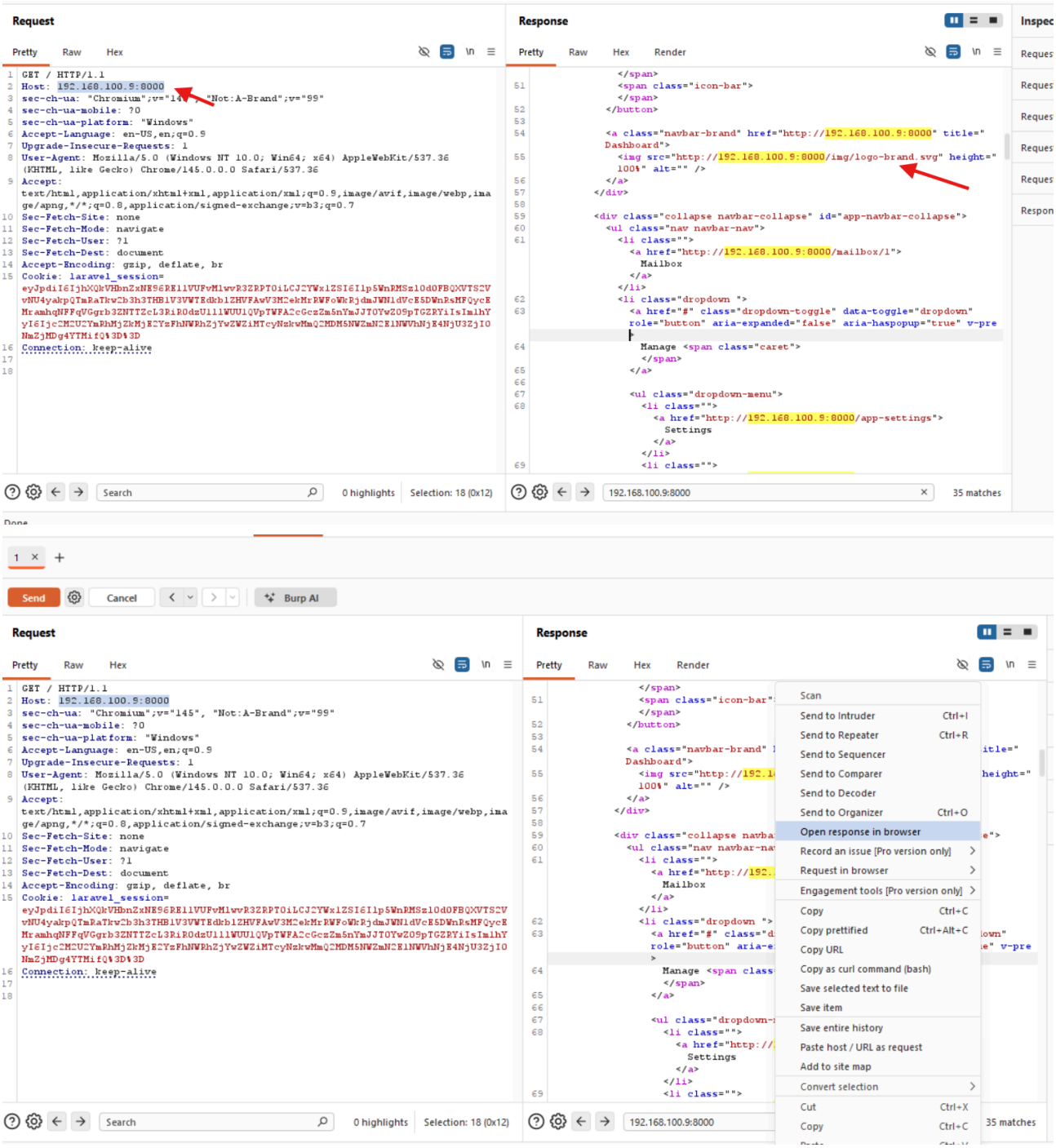
PoC

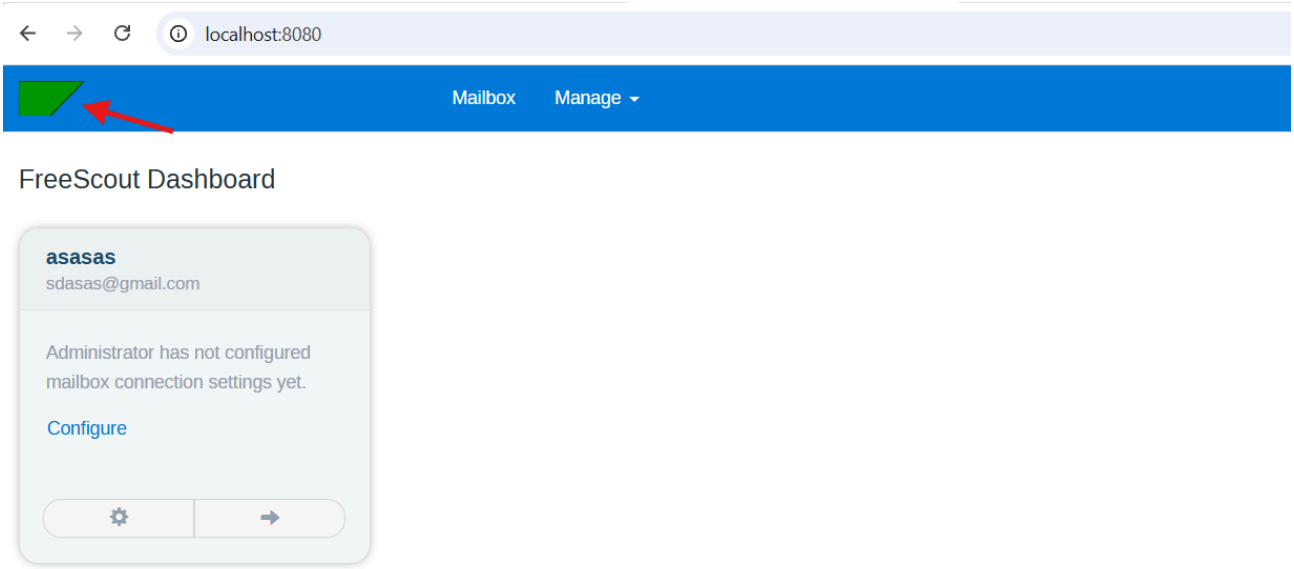
Send a crafted request with a malicious Host header:

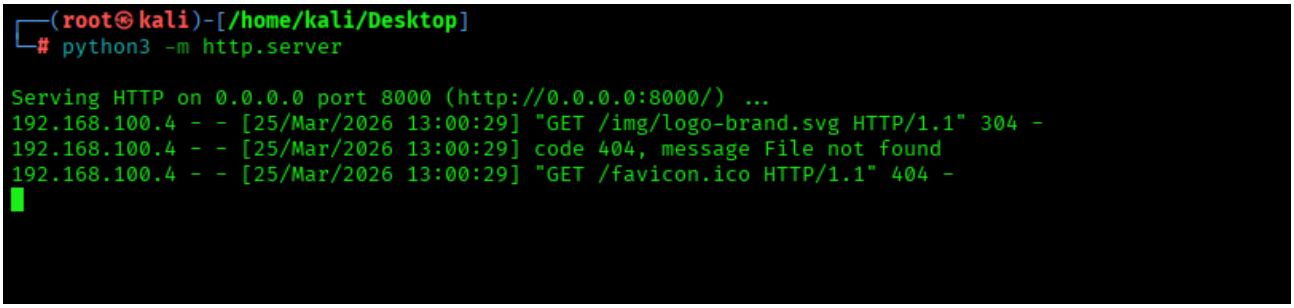




External Resource Loading

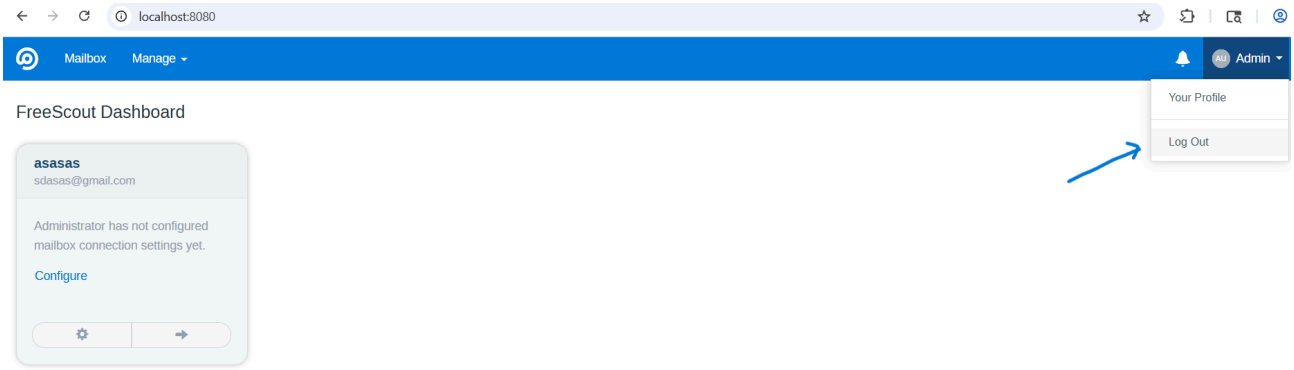

Request
Response
Pretty
Raw
Hex
Render
GET / HTTP/1.1
Host: 192.168.100.9:8000
Search
0 highlights
Selection: 18 (0x12)
192.168.100.9:8000
35 matches
Send
Cancel
Burp AI
Scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Send to Organizer Ctrl+O
Open 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

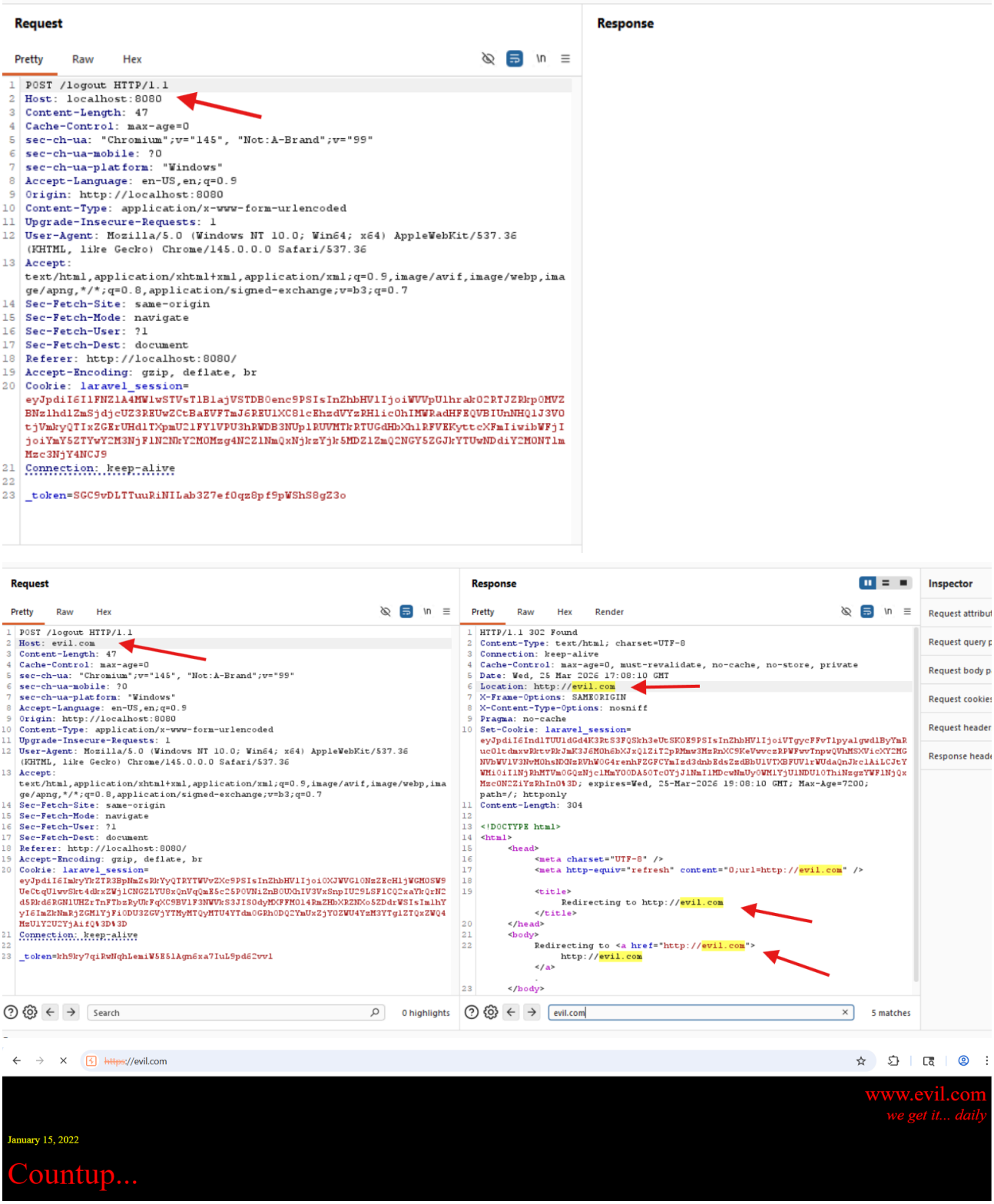




When a victim visits the affected page, the browser loads resources from the attacker-controlled domain.

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