

milesdcc / shynet Public[Code](#) [Issues](#) 53 [Pull requests](#) 9 [Actions](#) [Projects](#) [Security and quality](#)

# Remove wildcard ALLOWED\_HOSTS default to prevent password reset poisoning #345

Mergedmilesdcc merged 2 commits into `master` from `claude/fix-host-header-injection-...`

3 weeks ago

[Conversation](#) 0[Commits](#) 2[Checks](#) 3[Files changed](#) 5milesdcc commented [3 weeks ago](#) • edited ▾Owner

## Summary

Fixes a Host header injection vulnerability in the password reset flow. The default `ALLOWED_HOSTS = "*"`  disabled Django's Host header validation, allowing an unauthenticated attacker to poison password reset emails with links to their own domain — capturing valid reset tokens when victims (or email link-preview scanners) click them.

## Root cause

`django-allauth` builds the `{{ password_reset_url }}` in reset emails using `request.build_absolute_uri()`, which derives the hostname from the `Host` header. Django's `ALLOWED_HOSTS` setting is the security boundary that validates this header — but `"*"` disables it entirely.

Attack: `curl -X POST http://<shynet-ip>/accounts/password/reset/ -H "Host: attacker.com" -d "email=admin@..."` → admin receives an email linking to `http://attacker.com/accounts/password/reset/key/<valid-token>/`.

## Fix

Change the default to `localhost,127.0.0.1`. With `ALLOWED_HOSTS` properly restricted, Django's `CommonMiddleware` rejects spoofed Host headers with a 400 before any view runs — making `request.get_host()` inherently safe downstream.

File	Change
settings.py	Default * → localhost,127.0.0.1 . Uses or instead of getenv 's default arg so an empty-string env var falls through correctly.
Dockerfile	Healthcheck shell fallback matches the new Python default, so it still passes when the env var is unset.
app.json	Heroku one-click deploy now <b>requires</b> the user to enter their domain (no default).
kubernetes/secrets_template.yml	Removed the * placeholder.
GUIDE.md	Changed "consider setting" → "make sure is set", with an explicit warning about * .

## Upgrade note

Existing deployments that did not set ALLOWED\_HOSTS will need to set it after upgrading. [TEMPLATE.env](#) already documented the correct value.

**claude** added 2 commits [3 weeks ago](#)

[Remove wildcard ALLOWED\\_HOSTS default to prevent Host header injection](#) ✓ [c022dd9](#)

[Require explicit ALLOWED\\_HOSTS in Heroku deploy instead of subdomain ...](#) ✓ [530c026](#)

**milesMcC** merged commit [ca35cab](#) into [master](#) [3 weeks ago](#)  
3 checks passed

[View details](#)

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

### Reviewers

No reviews

**Assignees**

No one assigned

---

**Labels**

None yet

---

**Projects**

None yet

---

**Milestone**

No milestone

---

**Development**

Successfully merging this pull request may close these issues.

None yet

---

**2 participants**

