Zesty.io Incident Report

Date: 11/07/2025
Affected Instance: HTTP Requests
Zesty.io Service: CDN, WAF, Webengine

Summary

During the transition to a new Web Application Firewall (WAF), customer traffic was served but inadvertently redirected to the internal Zesty.io origin domain. As a result, end-users saw the correct content but under the platform's origin URL instead of the customer's branded domain. These redirects were intended to be internal and add additional security to the Zesty.io origin URLs.

Root Cause Analysis

Every point in the request chain to the downstream Zesty.io WebEngine service presents an opportunity to make an encrypted Hypertext Transfer Protocol Secure (HTTPS) connection using Transport Layer Security (TLS). One of these points is the connection between the Content Delivery Network (CDN) and the Zesty.io origin. Which is exposed by a Uniform Resource Locator (URL) which takes the form of zesty-io.webengine.origin.zesty.zone

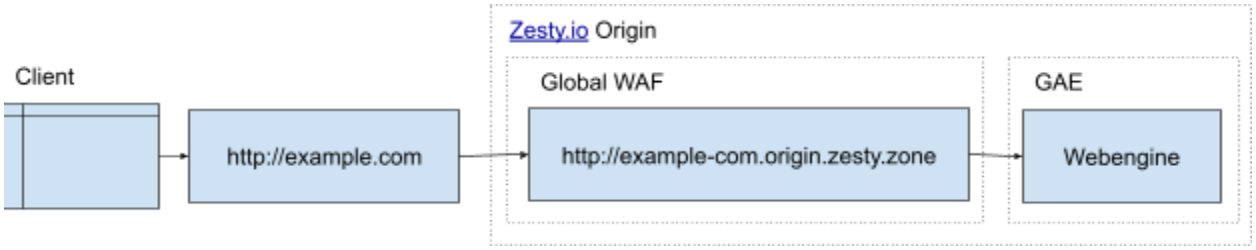
Historically the Zesty.io origin has supported Hypertext Transfer Protocol (HTTP) connections. As many domains operated without TLS certificates before their proliferation by letsencrypt.org. Additionally there was a point in time when Zesty.io operated without a CDN in front of the origin. This meant that in order to support HTTP domains we needed infrastructure that would handle direct connections without enforcing HTTPS.

Now with a CDN between customer domains and the Zesty.io origin it presented an opportunity to secure the CDN to origin connection. This is because the connection point between the customer domain and the CDN is different from the connection point between the CDN and the origin. However, the new infrastructure configuration did not account for the need to follow the generated redirect. Consequently, the system returned the redirect instruction itself to the customer's domain request, rather than the intended content. Leading to the incident of returning Zesty.io origin redirects to customer domain requests.

Note: zesty.dev URLs were affected by this incident. As they are also configured to support historical HTTP requests.

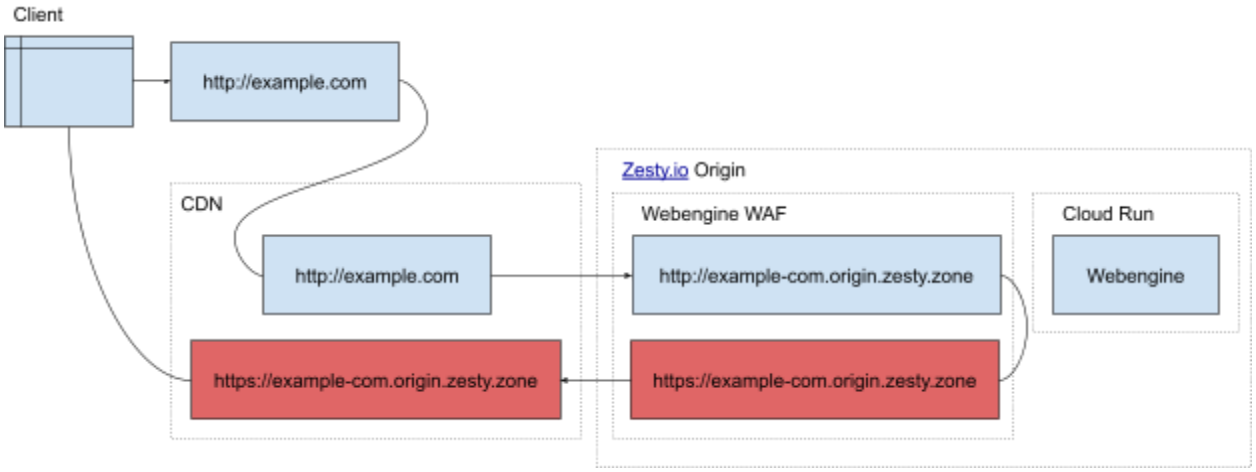
Previous Infrastructure Configuration

The previous infrastructure configuration included a dedicated HTTP WAF to route non-https traffic to webengine. Allowing HTTP connections through the entire request chain. This was necessary to support historical customer connection needs.



Introduced Infrastructure Configuration

We implemented a redirect in the newly introduced WAF to direct HTTP requests to HTTPS. This was done to enforce secure connections to the origin.



Solution

By reintroducing a dedicated HTTP WAF we allowed for upstream customer HTTP traffic to proceed to the WebEngine service without a redirect being present in the request chain.

Additional Details

Private Caches

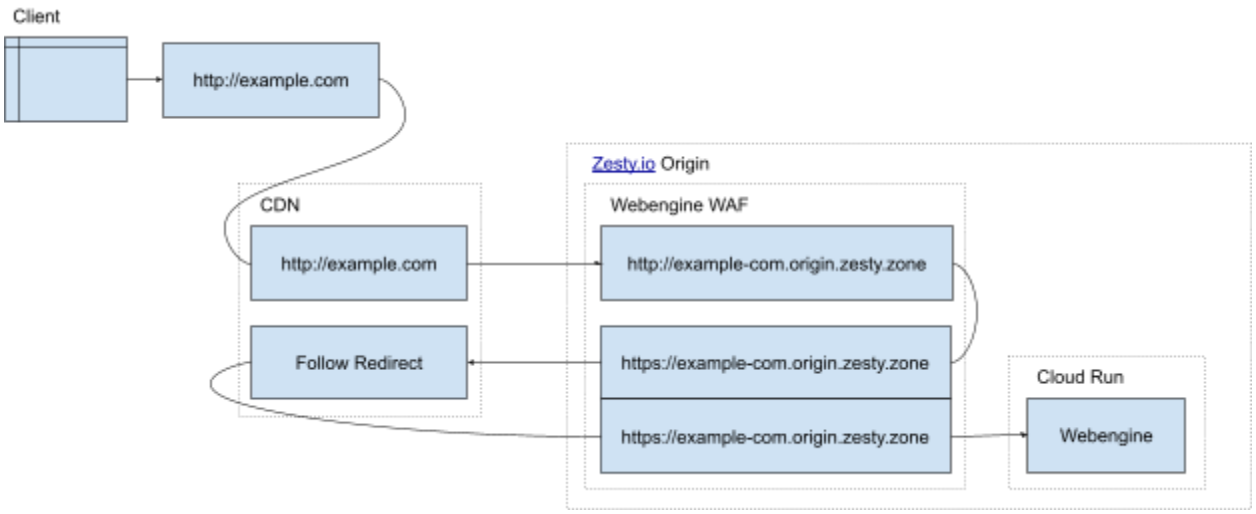
Customers have the option to operate their own caches in front of the Zesty.io platform. This configuration allows customers control over headers and cache instructions. Consequently, for customers with this setup, the origin URL redirect responses may have been cached at the requester's browser, extending the duration of the issue for some end-users.

HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) is a simple and widely supported standard to protect visitors by ensuring that their browsers always connect to a website over HTTPS – https://https.cio.gov/hsts/

What this means is that once you visit a site over HTTPS your browser will remember and then force HTTPS when HTTP is requested. This led to testing scenarios where HTTP was believed to be working correctly.

Future Prevention



There will be additional functionality added to follow the HTTP to HTTPS redirect. This will allow support for historical customer configurations but enforce HTTPS connections to origin URLs. However, to ensure the highest level of security and performance, we encourage all customers to use HTTPS variants of URLs where possible.

For example;

- **https**://zesty-io.zesty.dev
- **https**://zesty-io.webengine.origin.zesty.zone