Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated.

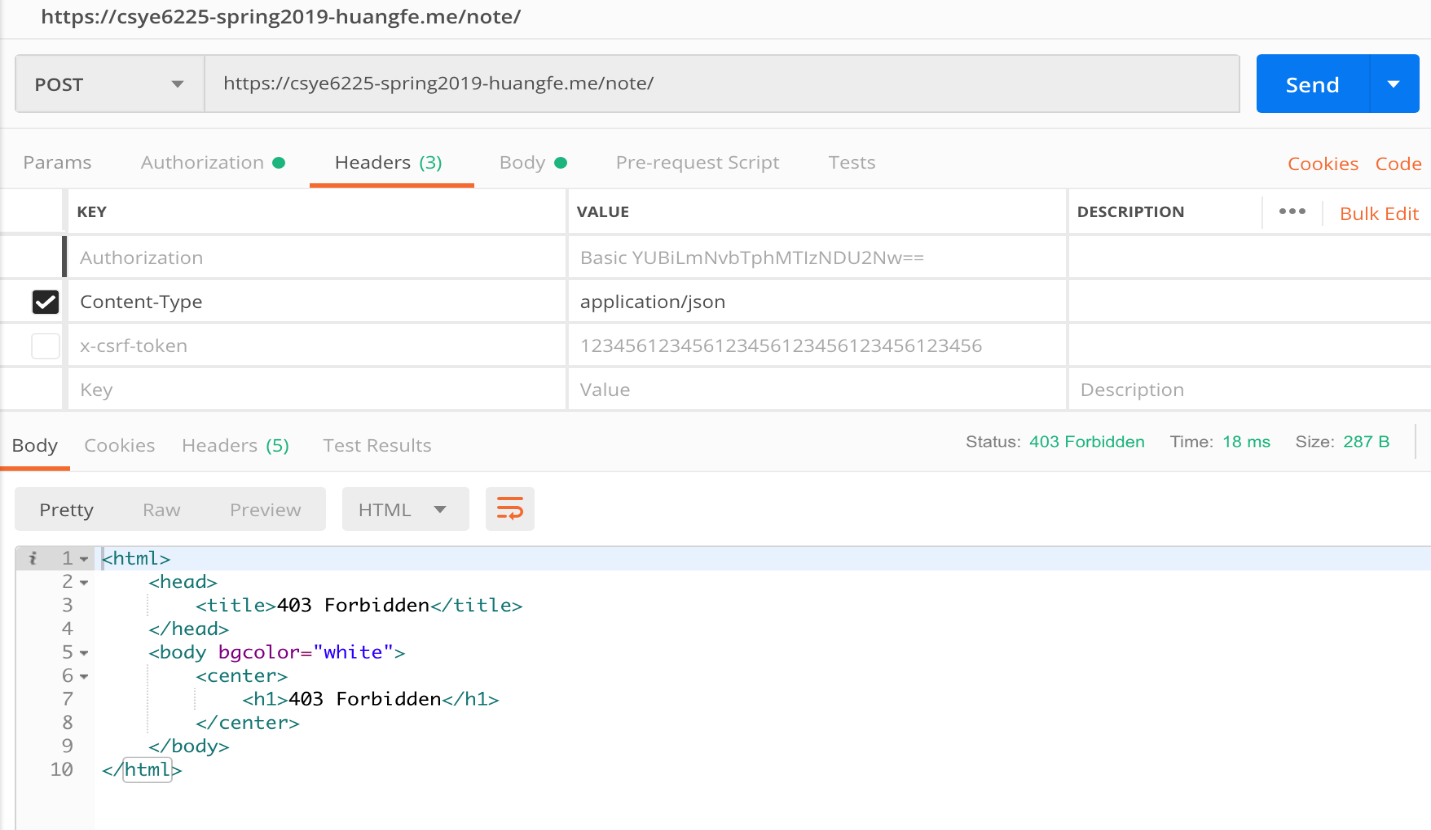
CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.

Since we use REST API for our web application, which is stateless, and we don’t render actual web pages, in fact there is no need to detect CSRF.

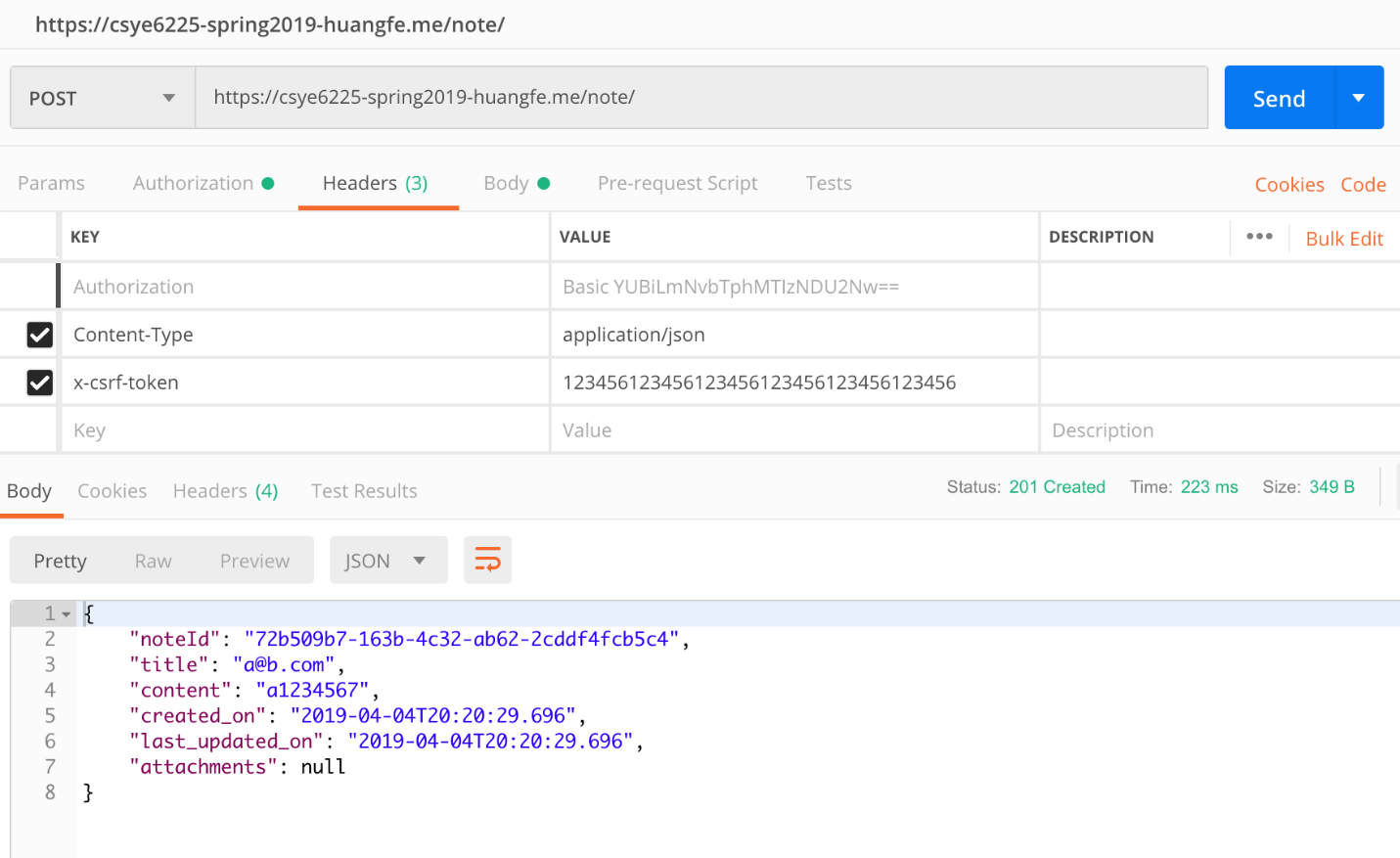
We enforce csrf to meet assignment requirements.



Result: If we enforce CSRF in AWS WAF, any post requests without x-csrf-token header will be blocked. Since we don’t check the actual value of x-csrf-token, any value of 36 length will be allowed.

without x-csrf-token header:

with x-csrf-token header:



Why do we choose this attack?

For most of web applications, it is developer’s responsibility to consider all kinds of attack, and CSRF is one of the most common attacks to think about. Therefore we select this attack.