

mallory.csrf.jp
(Attacker)

csrf.jp
(Attacker)

alice.csrf.jp
(Victim)

Invoke XHR with DELETE method

Preflight

Access-Control-Max-Age: 50000
Alt-Svc: h2="alice.csrf.jp:8020"

DELETE is permitted!

DELETE request

Invoke XHR with DELETE method again

DELETE request without preflight

Pwned...

