Cyber Defense
6.11.2024

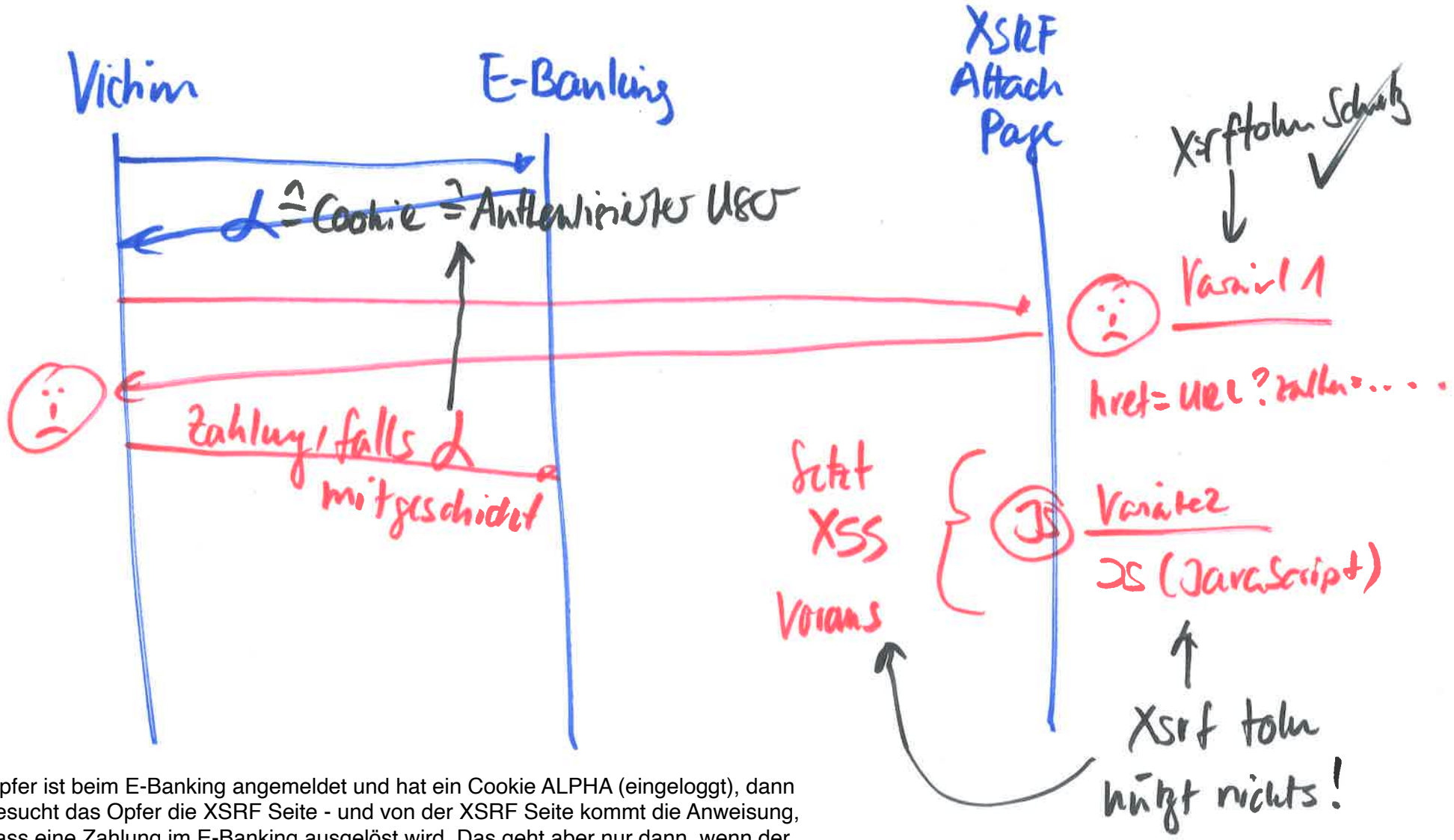
Heute sprechen wir wieder zuerst über ein Advisory. Ich habe ein XSRF Advisory gewählt, weil es einen DNS Change Angriff gibt für Home Router

Advisory: https://nvd.nist.gov/vuln/detail/CVE-2020-7780

Auf den folgenden Seiten findet ihr die Erklärung über XSRF

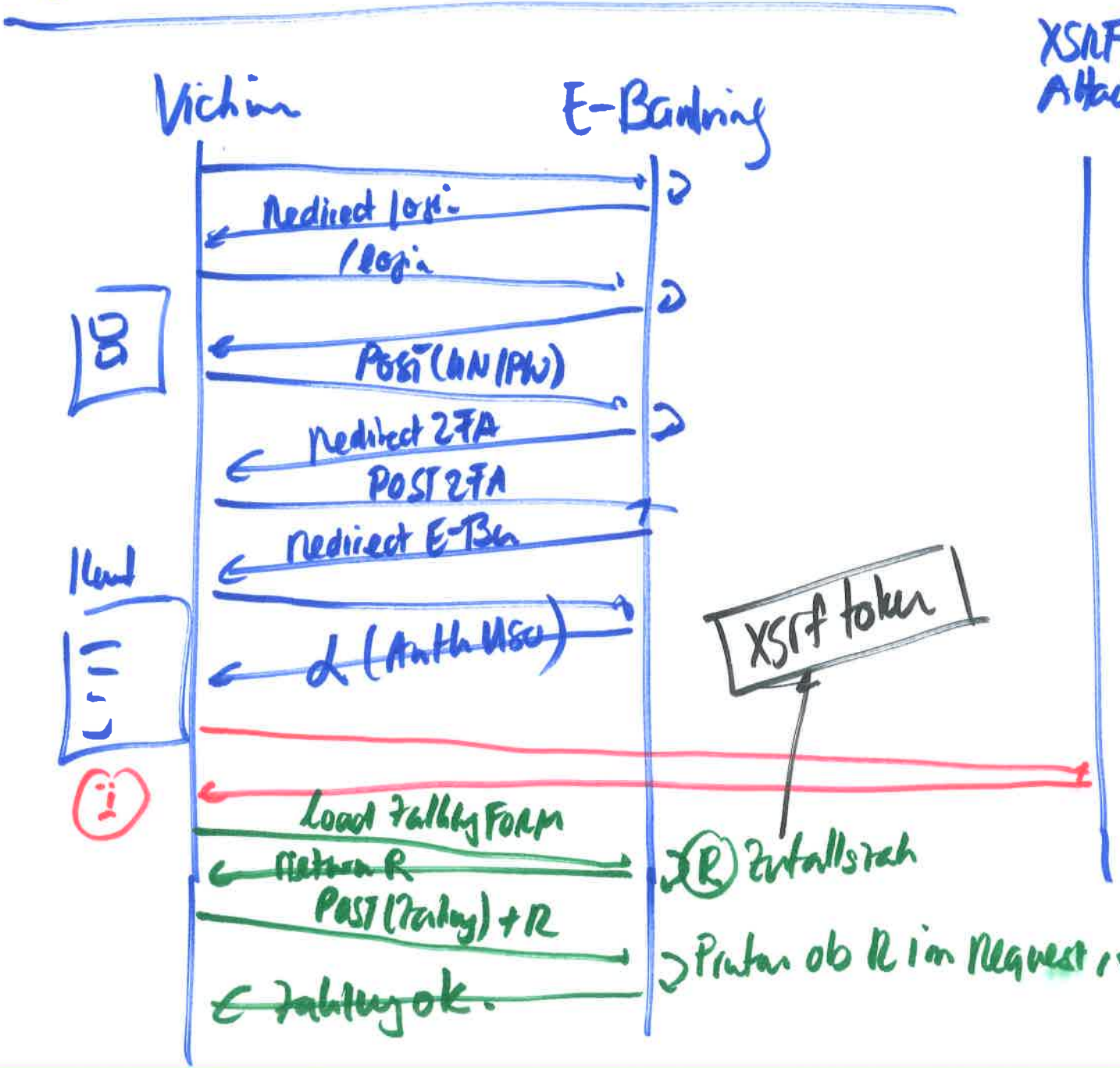
Man muss die Angriffe kennen, damit man die Advisories versteht.

XSRF ≙ Cross Site Request Forgery



Opfer ist beim E-Banking angemeldet und hat ein Cookie ALPHA (eingeloggt), dann besucht das Opfer die XSRF Seite - und von der XSRF Seite kommt die Anweisung, dass eine Zahlung im E-Banking ausgelöst wird. Das geht aber nur dann, wenn der Browser das ALPHA Cookie zum E-Banking mitschickt, wenn der Request von der XSRF Seite initiiert wird (siehe unten SameSite)

Gegenmassnahme XSRF (alt)



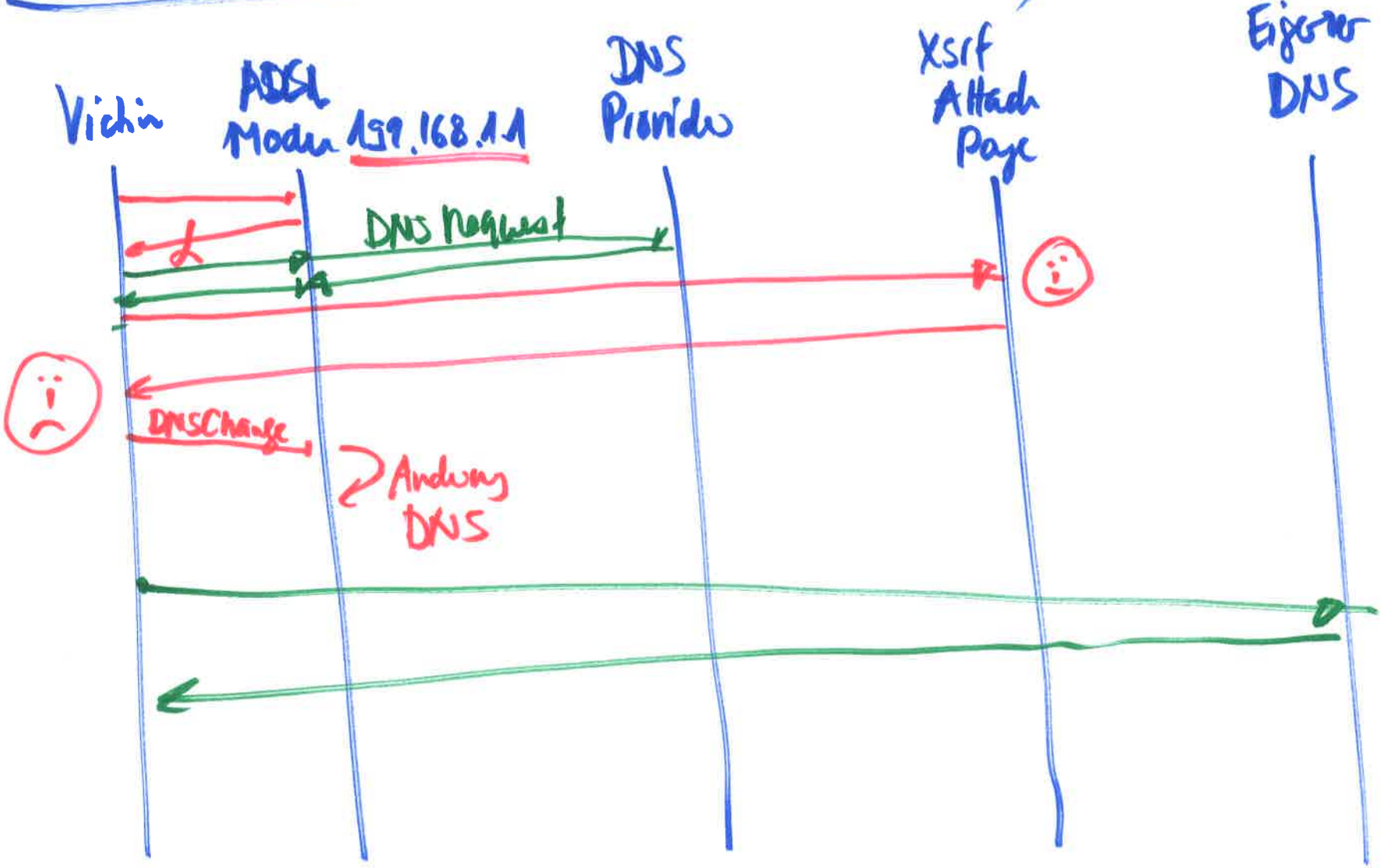
Die alte Gegenmassname war, dass man eine Webseite so baut, dass ein Formular über 2 Requests abgefüllt wird.

Als Antwort auf den ersten Request (Anforderung Formular) erzeugt der Server eine Zufallszahl (wird auch xsrf token genannt) und dem Client mitgeteilt

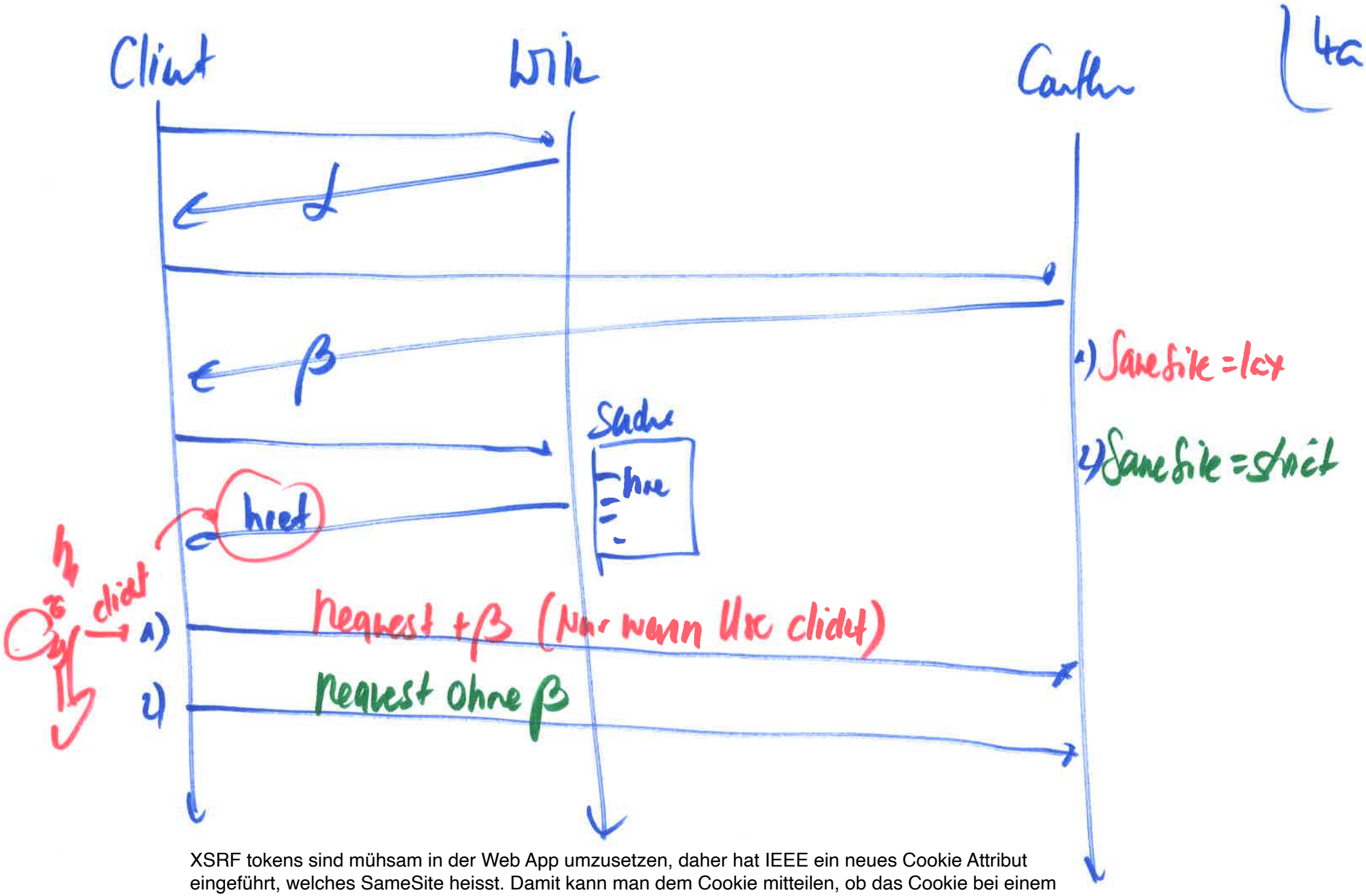
Danach schickt der Client die Form Daten mit dem xsrf token und natürlich dem Cookie ALPHA

Der Server prüft das Vorhandensein des xsrf token und ALPHA und nur wenn beides gültig ist, wird die Zahlung akzeptiert.

XSRF - DNS Attack (Home Router Attacke)



Gleiches Beispiel wie oben, aber nicht um eine E-Banking Zahlung aufzugeben, aber um beim Home Router eine DNS Change Config Attacke durch zu führen. Das geht vielleicht, weil der Home Router auf einer bekannten IP liegt 192.168.1.1 oder so



XSRF tokens sind mühsam in der Web App umzusetzen, daher hat IEEE ein neues Cookie Attribut eingeführt, welches SameSite heisst. Damit kann man dem Cookie mitteilen, ob das Cookie bei einem Cross Domain Request (einem Request der von einer Drittseite initiiert wird) mit ALPHA oder ohne ALPHA Cookie gemacht wird. Bei SameSite=Strict wird das Cookie NIE mitgeschickt. Bei lax dann, wenn der User “klickt” (aber im Hintergrund ohne clicken auch nicht)