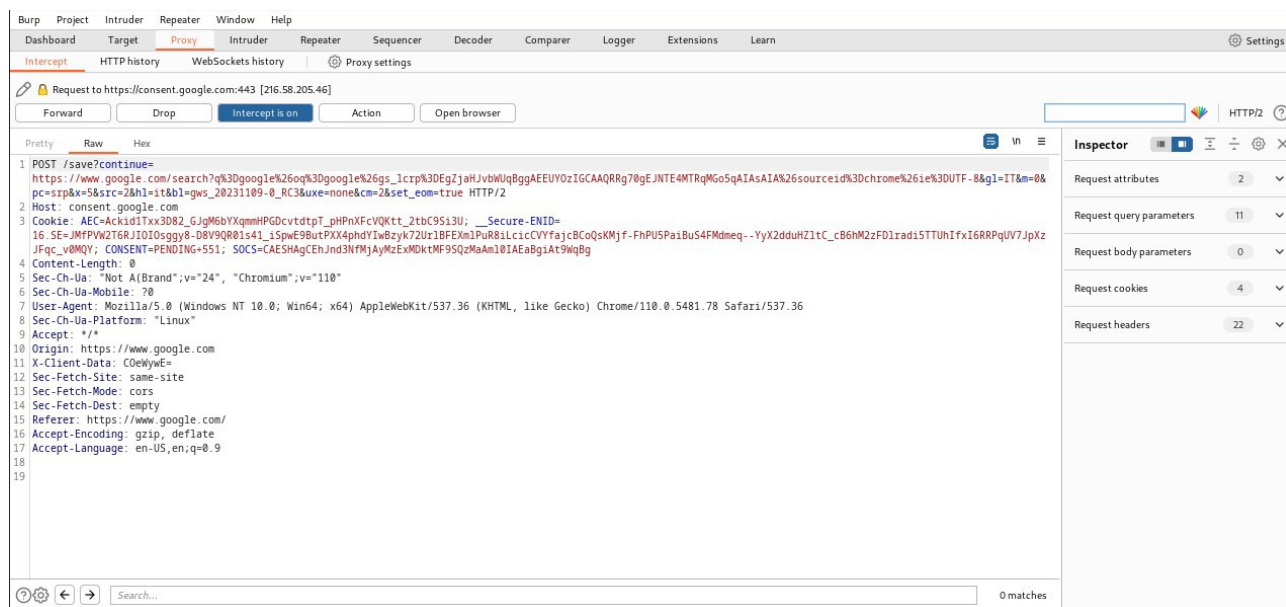


Applicazioni Web (7)

Dopo aver avviato Burpsuite apro il browser tramite “open browser”, in questo caso apre Chromium una versione di Google Chrome solo per Kali.

Su Burpsuite vado su Proxy per vedere tutte le richieste che fa il browser prima di arrivare alla pagina effettiva



Una volta scelto il target mando la richiesta che mi interessa all'Intuder che mi da la possibilità di fare un attacco alla pagina in caso di vulnerabilità



Invece nella parte di Repeater ho la possibilità di vedere la richiesta interettata come cambio se modifico qualche parametro

Request

PrettyRawHex

1 POST /save?continue=
https://www.google.com/search?q%3Dgoogle%26oq%3Dgoogle%26gs_lcrp%3DEgZjaHJvbWUqB
ggAEUyOzIGCAAQRrg70gEJNTE4MTRqMG65qAIAIA%26sourceid%3Dchrome%26ie%3DUTF-8&gl=
IT&m=0&pc=srp&x=5&src=2&hl=it&bl=gws_20231109-0_RC3&uxe=none&cm=2&set_eom=true
HTTP/2
2 Host: consent.google.com
3 Cookie: AEC=AckidITxx3D82_GJgM6bYXqmmHPGDcvtdtpT_pHPnXFcVQKtt_2tbC9S13U;
__Secure-ENID=
16.SE=JMFpVW2T6RJIOI0sggy8-D8V9QR01s41_iSpwE9ButPXX4phdYIwBzyk72Ur1BFEXm1PuR8ilc
icCVYfajcBCoQsKMjff-FhPU5PaibuS4FMdmeq--YyX2dduH21tC_cB6hM2zFD1radi5TTUuIfxIGRRRPq
UV7JpXzJFqc_v0MQY; CONSENT=PENDING+551; SOCS=
CAESHAqCEhJnd3NFMjAyMzExMDktMF9S0zMaAm10IAEaBg1At9WqBg
4 Content-Length: 0
5 Sec-Ch-Ua: "Not A(Brand)";v="24", "Chromium";v="110"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/110.0.5481.78 Safari/537.36
8 Sec-Ch-Ua-Platform: "Linux"
9 Accept: */*
10 Origin: https://www.google.com
11 X-Client-Data: C0eWYwE=
12 Sec-Fetch-Site: same-site
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://www.google.com/
16 Accept-Encoding: gzip, deflate

0 matches

Response

PrettyRawHexRender

1 HTTP/2 204 No Content
2 Content-Type: text/html; charset=utf-8
3 Access-Control-Allow-Origin: https://www.google.com
4 Access-Control-Allow-Credentials: true
5 Cache-Control: no-cache, no-store, max-age=0, must-revalidate
6 Pragma: no-cache
7 Expires: Mon, 01 Jan 1990 00:00:00 GMT
8 Date: Thu, 16 Nov 2023 02:07:30 GMT
9 Permissions-Policy: ch-ua-arch=*, ch-ua-bitness=*, ch-ua-full-version=*,
ch-ua-full-version-list=*, ch-ua-model=*, ch-ua-wow64=*, ch-ua-form-factor=*,
ch-ua-platform=*, ch-ua-platform-version=*,
10 Content-Security-Policy: require-trusted-types-for 'script';report-uri
/_/ConsentHttp/cspreport
11 Content-Security-Policy: script-src 'report-sample'
'nonce-k15n5lik0WdJX1kkUvgxlg' 'unsafe-inline';object-src 'none';base-uri
'self';report-uri _/_/ConsentHttp/cspreport;worker-src 'self'
12 Content-Security-Policy: script-src 'unsafe-inline' 'self'
https://apis.google.com https://ssl.gstatic.com https://www.google.com
https://www.googletagmanager.com https://www.gstatic.com
https://www.google-analytics.com;report-uri _/_/ConsentHttp/cspreport/allowlist
13 Accept-Ch: Sec-CH-UA-Arch, Sec-CH-UA-Bitness, Sec-CH-UA-Full-Version,
Sec-CH-UA-Full-Version-List, Sec-CH-UA-Model, Sec-CH-UA-WoW64,
Sec-CH-UA-Form-Factor, Sec-CH-UA-Platform, Sec-CH-UA-Platform-Version
14 Cross-Origin-Opener-Policy: unsafe-none
15 Server: ESF
16 Content-Length: 0

0 matches