AI for Cyber Security with IBM Qradar

Assignment- 4

Name: MAYANDI VARUN

What is Burp Suite?

Burp Suite is a Java based Web Penetration Testing framework.

Burp Suite is a software security application used for penetration testing of web applications. It has become an industry standard suite of tools used by information security professionals.

Burp Suite helps you identify vulnerabilities and verify attack vectors that are affecting web applications.It was created by PortSwigger Web Security. Burp Suite provides a range of powerful features that can be used to perform security assessments of web applications

Burp Suite can be classified as an Interception Proxy. While browsing their target application, a penetration tester can configure their internet browser to route traffic through the Burp Suite proxy server.

Burp Suite then acts as a (sort of) Man In The Middle by capturing and analyzing each request to and from the target web application so that they can be analyzed. Penetration testers can pause, manipulate and replay individual HTTP requests in order to analyze potential parameters or injection points. Injection points can be specified for manual as well as automated fuzzing attacks to discover potentially unintended application behaviors, crashes and error messages.

Why is Burp Suite Used in Cybersecurity?

Burp Suite is a comprehensive framework that may be used to carry out several activities, including:

1. Identification of Security Vulnerabilities: Burp Suite helps identify various security vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and many others. By using Burp Suite, security experts can discover these vulnerabilities before malicious hackers do, allowing organizations to fix these issues before they are exploited.

2. Web Application Security Testing: Burp Suite is specifically designed for testing the security of web applications. It can intercept, inspect, and modify the traffic between a web browser and the target application. This capability is crucial for understanding how an application behaves under different conditions and inputs.

3. Automation of Security Testing: Burp Suite can automate various aspects of security testing, such as scanning for common vulnerabilities or performing brute-force attacks. Automation saves time and allows security professionals to focus on analyzing the results and understanding the context of vulnerabilities.

4. Customization and Extensibility: Burp Suite is highly customizable and extensible. Security experts can create custom plugins and scripts to tailor the tool according to the specific requirements of the application being tested. This flexibility is valuable when dealing with unique or complex web applications.

5. Manual Testing Capabilities: While automation is crucial, manual testing is equally important. Burp Suite's tools, such as the Repeater and Intruder, allow testers to manually explore and manipulate individual requests, enabling them to discover vulnerabilities that automated scanners might miss.

6. Real-time Analysis and Feedback: Burp Suite provides real-time feedback on HTTP requests and responses. Security professionals can immediately see how the

application responds to various inputs and attacks, allowing for efficient testing and analysis.

7. Learning and Skill Development: Burp Suite is widely used in the cybersecurity community. Learning how to use Burp Suite effectively is a valuable skill for security professionals, penetration testers, and ethical hackers. It provides hands-on experience in web application security testing, helping individuals enhance their expertise in the field.

8. Comprehensive Reporting: Burp Suite generates detailed reports that can be shared with development teams and stakeholders. These reports outline discovered vulnerabilities, potential risks, and recommended remediation steps, aiding organizations in prioritizing and addressing security issues.

Burp Suite is an essential tool for web application security testing because it provides a comprehensive set of features, allowing security professionals to systematically assess the security posture of web applications, discover vulnerabilities, and help organizations secure their digital assets. Burp suite also has the advantage of being built into the Chrome browser.

Burp Suite is a prominent web application security solution. It gives us the ability to manually test for vulnerabilities, intercepts HTTP messages, and change a message's body and header.

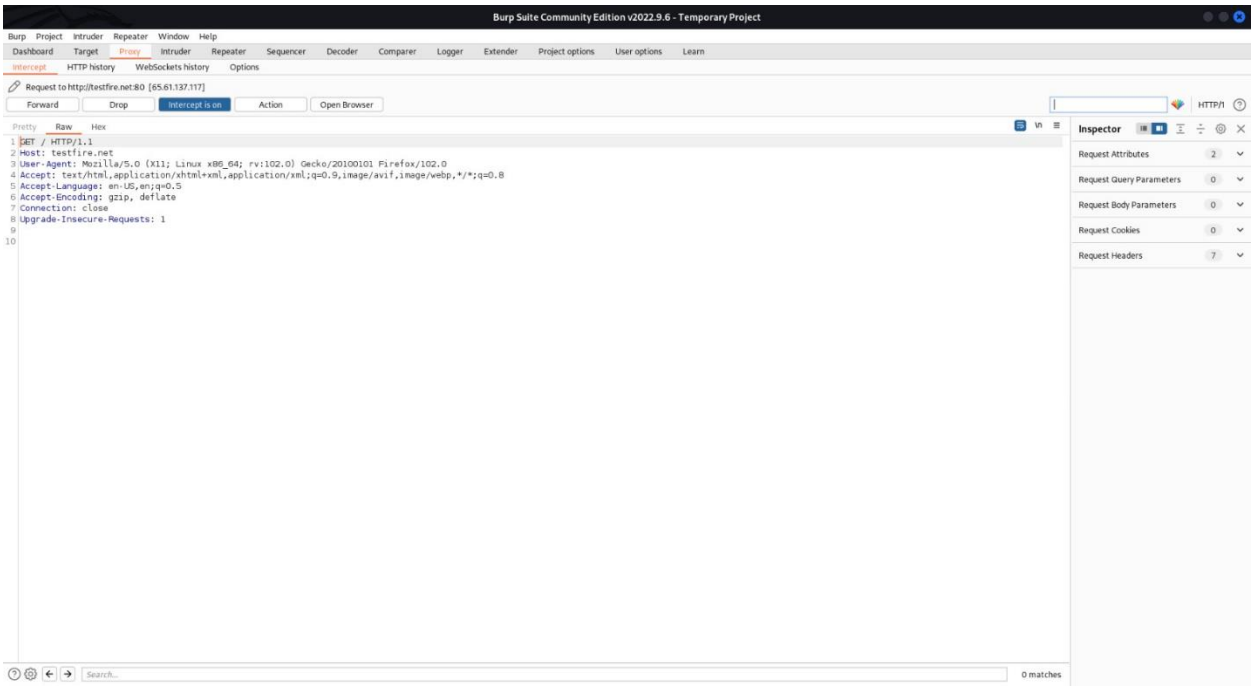
What are the features of Burp Suite?

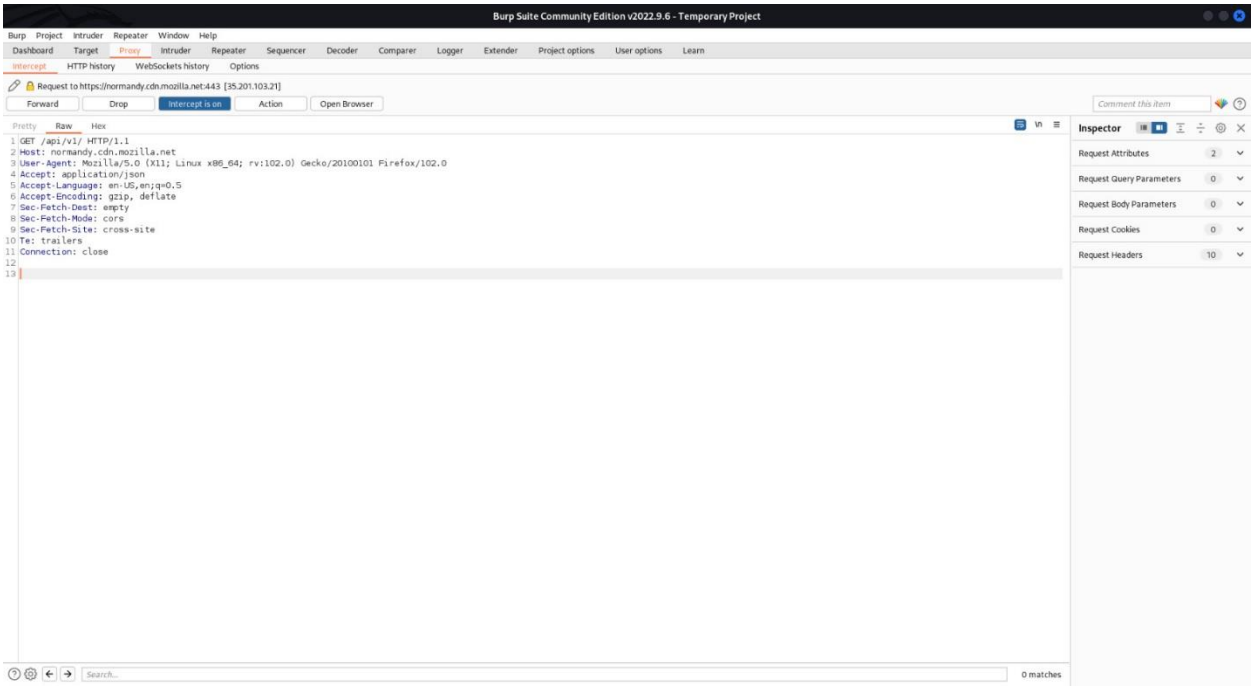
1. Spider:

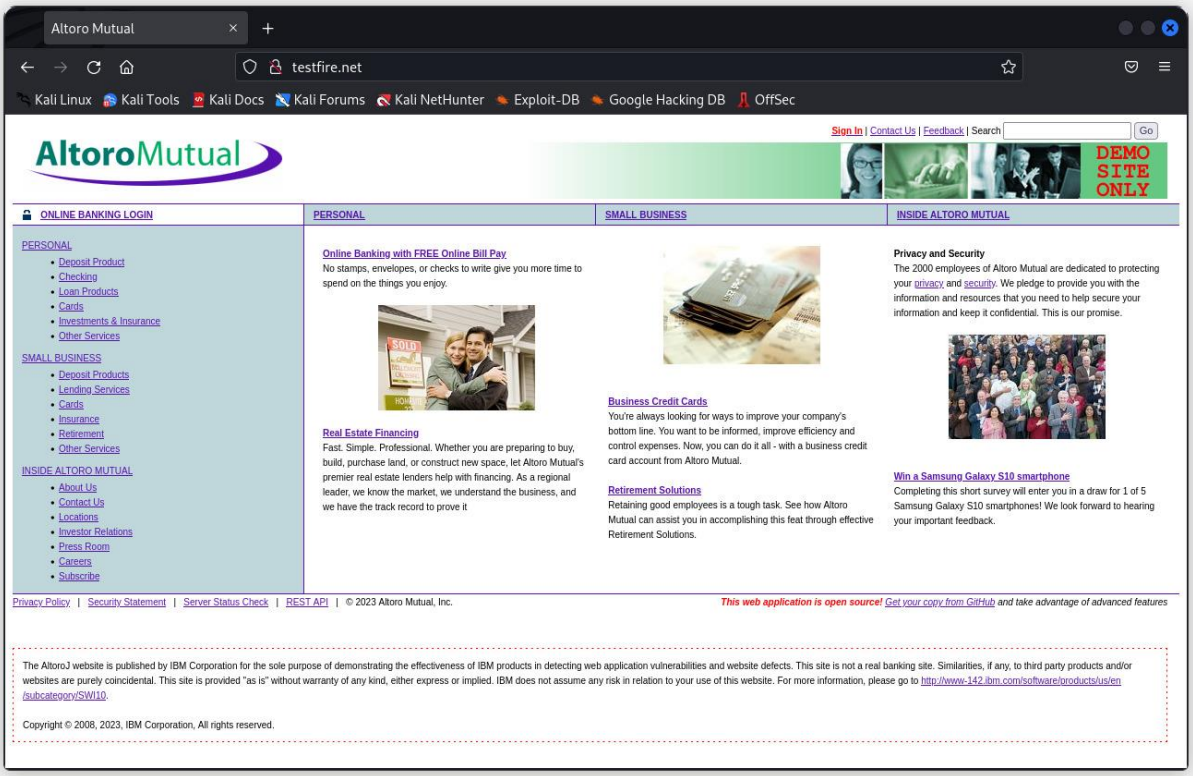
It is a web spider/crawler that is used to map the target web application. The objective of the mapping is to get a list of endpoints so that their functionality can be observed and potential vulnerabilities can be found. Spidering is done for a simple reason that the more endpoints you gather during your recon process, the more attack surfaces you possess during your actual testing.

2. Proxy:

Burp Suite contains an intercepting proxy that lets the user see and modify the contents of requests and responses while they are in transit. It also lets the user send the request/response under monitoring to another relevant tool in Burp Suite, removing the burden of copy-paste. The proxy server can be adjusted to run on a specific loop-back ip and a port. The proxy can also be configured to filter out specific types of request-response pairs.


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://testfire.net:80 [65.61.137.117]
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
1 GET / HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 0
Request Headers 7
Search...
0 matches

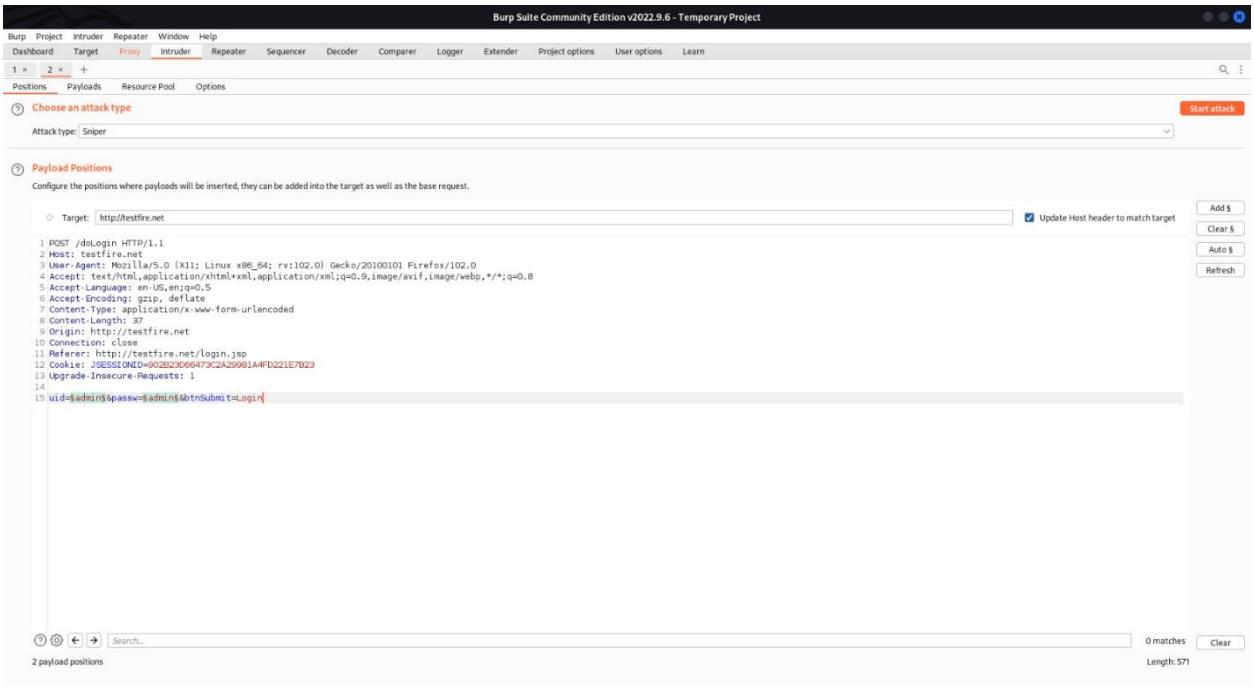

Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to https://normandy.cdn.mozilla.net:443 [35.201.103.21]
Forward Drop Intercept is on Action Open Browser
Comment this item
Pretty Raw Hex
1 GET /api/v1/ HTTP/1.1
2 Host: normandy.cdn.mozilla.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: application/json
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Sec-Fetch-Dest: empty
8 Sec-Fetch-Mode: cors
9 Sec-Fetch-Site: cross-site
10 Te: trailers
11 Connection: close
12
13
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 0
Request Cookies 0
Request Headers 10
Search...
0 matches

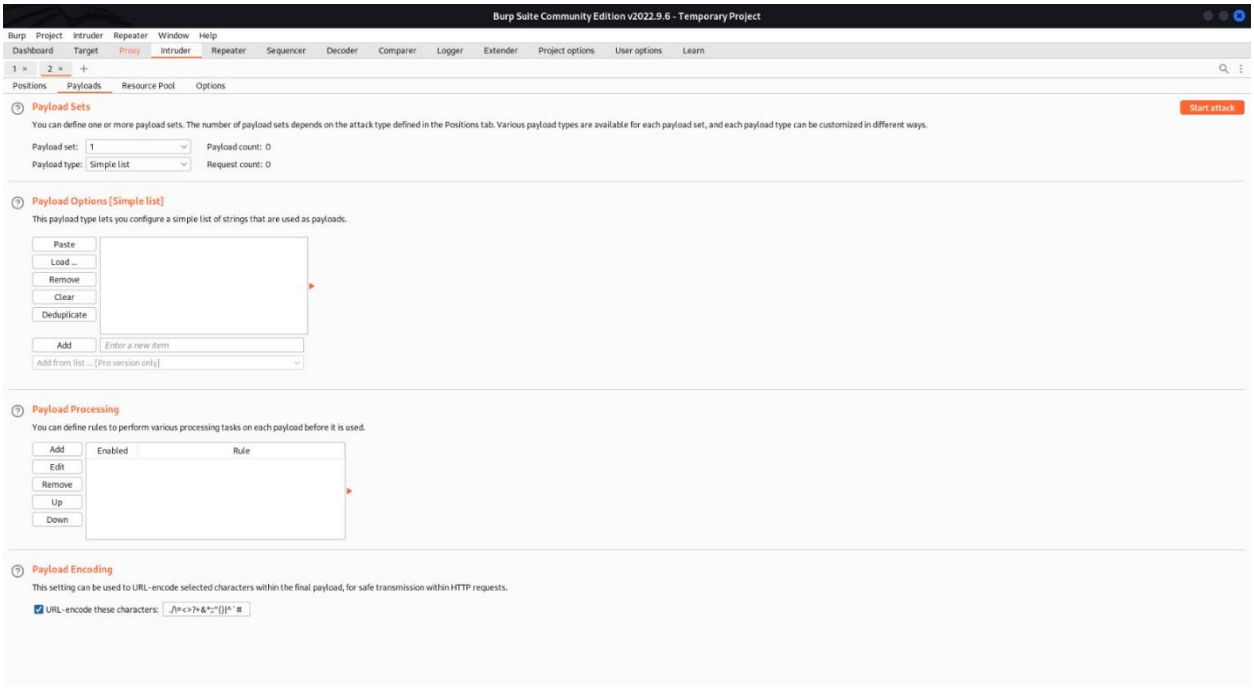


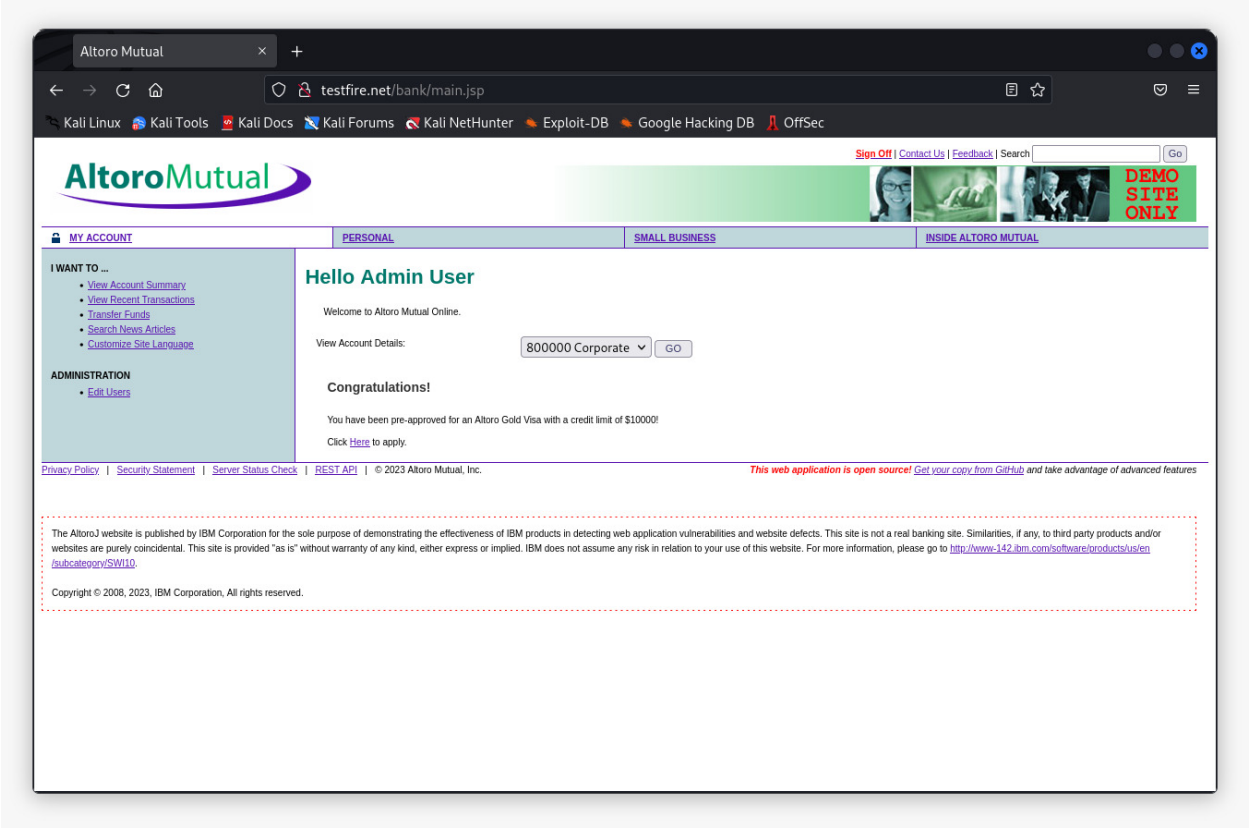
3. Intruder:

It is a fuzzer. This is used to run a set of values through an input point. The values are run and the output is observed for success/failure and content length. Usually, an anomaly results in a change in response code or content length of the response. Burp Suite allows brute-force, dictionary file and single values for its payload position. The intruder is used for:

- Brute-force attacks on password forms, pin forms, and other such forms.
- The dictionary attack on password forms, fields that are suspected of being vulnerable to XSS or SQL injection.
- Testing and attacking rate limiting on the web-app.


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Choose an attack type
Start attack
Attack type: Sniper
Payload Positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://testfire.net
Update Host header to match target
Add §
Clear §
Auto §
Refresh
1 POST /doLogin HTTP/1.1
2 Host: testfire.net
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 37
9 Origin: http://testfire.net
10 Connection: close
11 Referer: http://testfire.net/login.jsp
12 Cookie: JSESSIONID=902B23D66473C2A29901A4FD221E7B23
13 Upgrade-Insecure-Requests: 1
14
15 uid=§admin§&passw=§admin§&btnSubmit=Login
Search...
0 matches
Clear
2 payload positions
Length: 571


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 × 2 ×
Positions Payloads Resource Pool Options
Payload Sets
Start attack
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 1
Payload count: 0
Payload type: Simple list
Request count: 0
Payload Options [Simple list]
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Payload Processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload Encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters: ./\=<>?+&*;:"{}|^`#



4. Repeater:

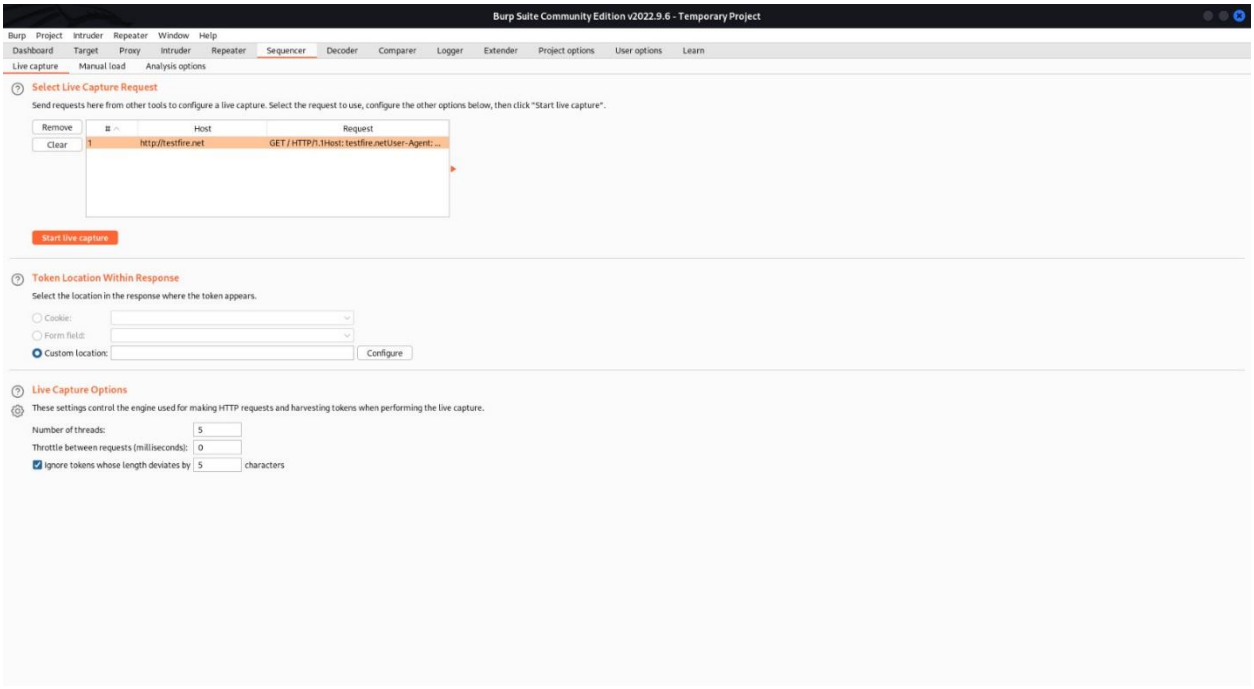
Repeater lets a user send requests repeatedly with manual modifications. It is used for:

- Verifying whether the user-supplied values are being verified.
- If user-supplied values are being verified, how well is it being done?
- What values is the server expecting in an input parameter/request header?
- How does the server handle unexpected values?
- Is input sanitation being applied by the server?
- How well the server sanitizes the user-supplied inputs?
- What is the sanitation style being used by the server?
- Among all the cookies present, which one is the actual session cookie.
- How is CSRF protection being implemented and if there is a way to bypass it?

5. Sequencer:

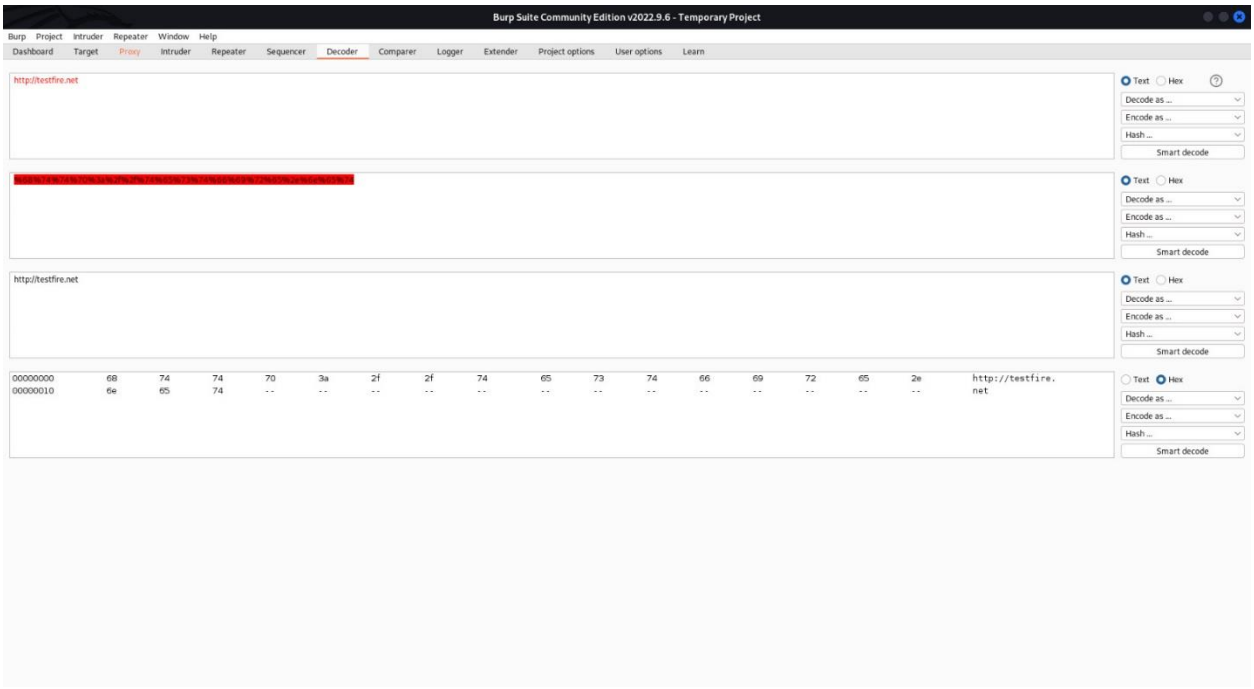
The sequencer, an entropy checker, verifies the unpredictability of tokens produced by the webserver. These tokens, like cookies and anti-CSRF tokens, are typically used for authentication in sensitive processes. The ideal way to produce these tokens is completely random, which will distribute the likelihood of each potential character appearing at each location equally. Bitwise and character wise approaches should be used to accomplish this. This hypothesis' validity is examined with an entropy analyzer.

This is how it works: first, it is thought that the tokens are random. The tokens are then put to the test using specific criteria for certain traits. The definition of a "significance level" is a minimal value of probability that a token will demonstrate for a characteristic, such that the token's randomness hypothesis will be rejected if the token's characteristic probability is below the significance level. This utility may be used to discover weak tokens and show how they are made.



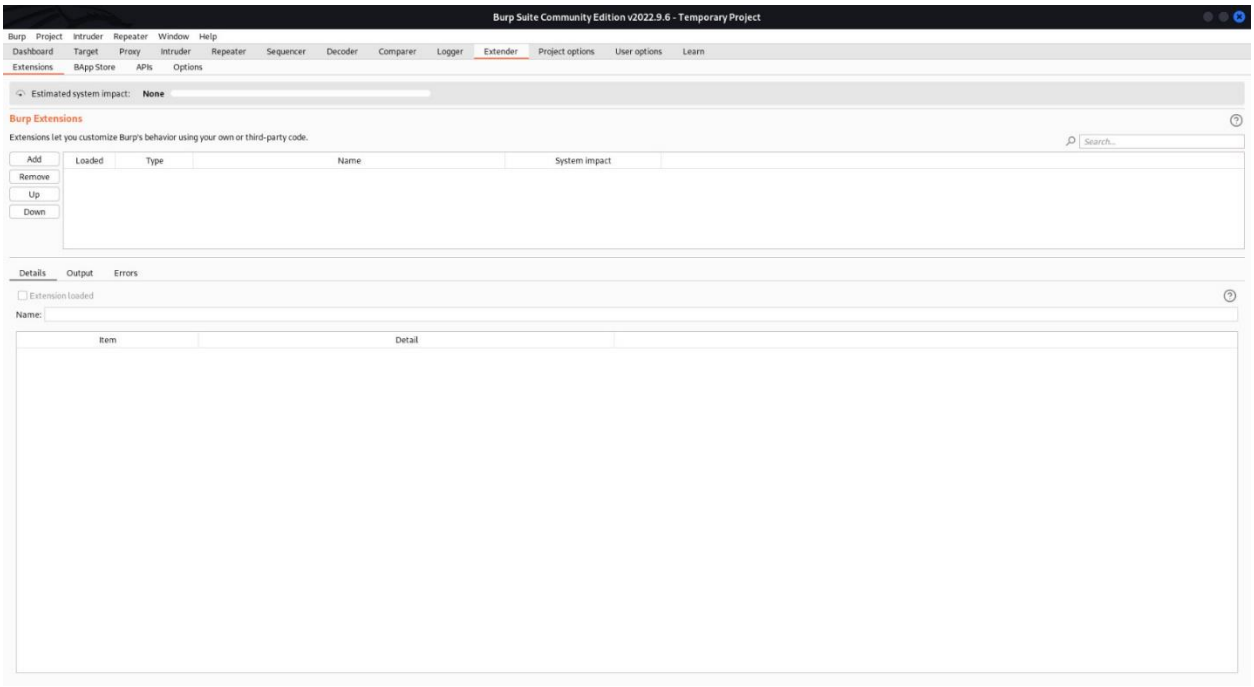
6. Decoder:

The decoder provides a list of common encoding techniques such as URL, HTML, Base64, Hex, and so on. When searching for specific data chunks inside the values of parameters or headers, this tool is quite helpful. Additionally, it is employed in the development of payloads for several vulnerability classes. Primary instances of IDOR and session hijacking are also uncovered using it.



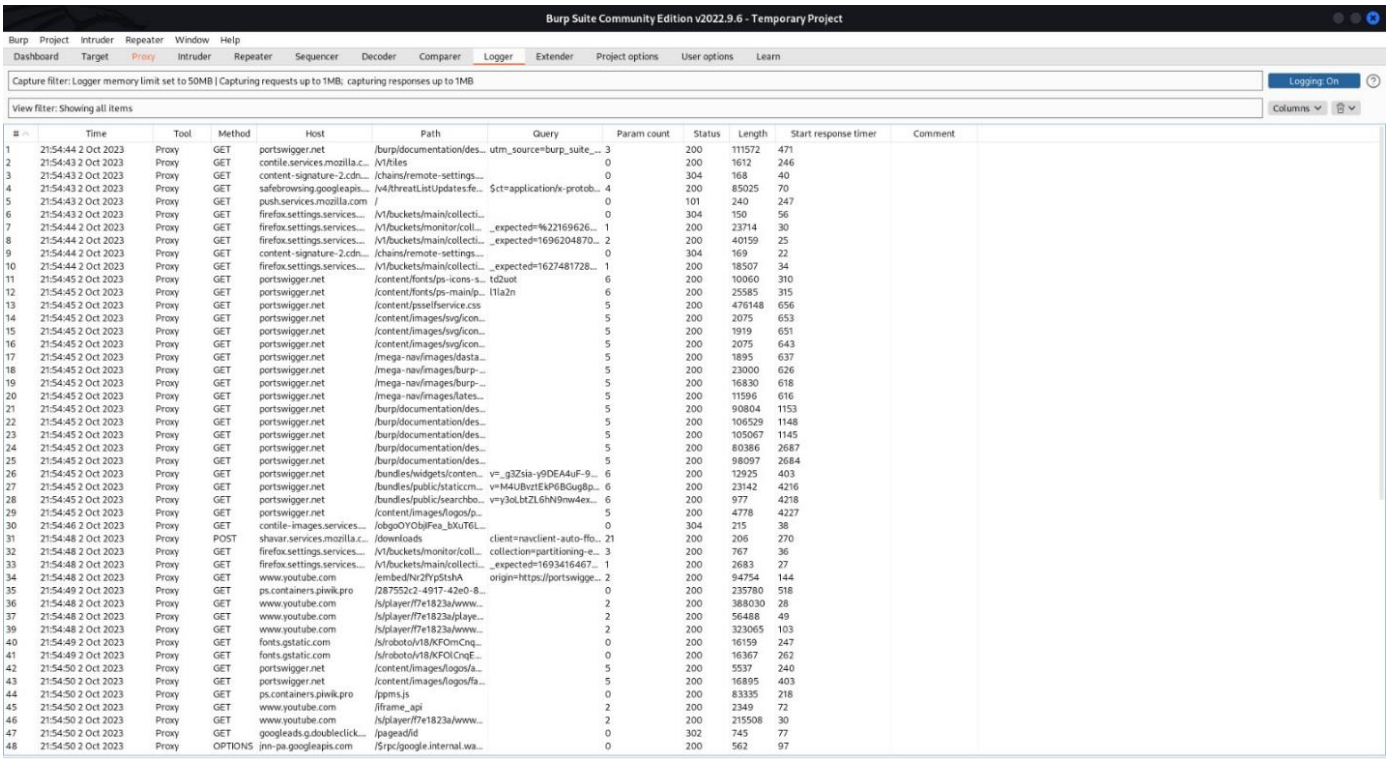
7. Extender:

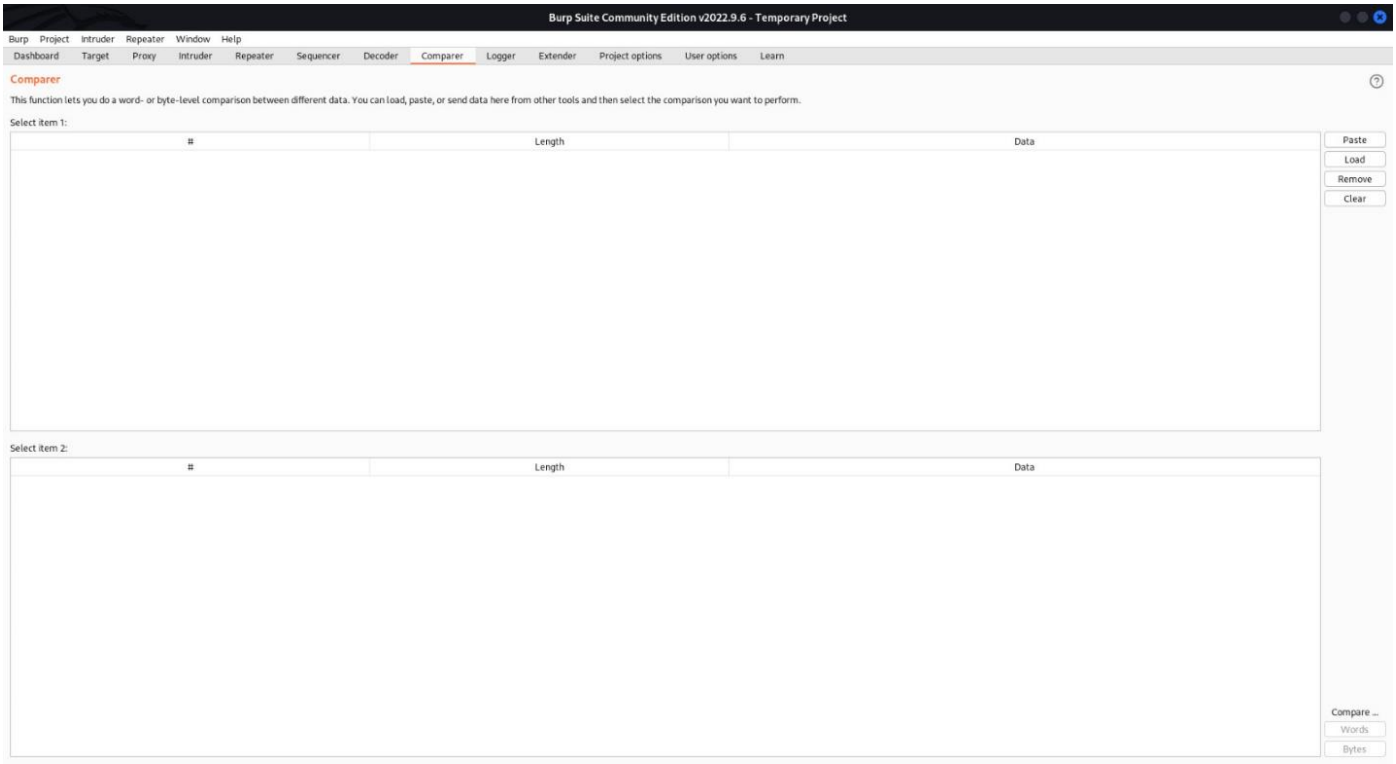
Burp Suite enables the integration of extra components into the toolkit to expand its functionality. These external components are referred to as BApps. These perform the same tasks as browser extensions... The Extender window allows you to examine, modify, install, and remove them. Some of them are supported by the free community version, while others need the professional version, which is a paid upgrade.



8. Scanner:

The community edition does not have a scanner. It automatically analyses the website for a variety of common vulnerabilities and provides them together with details on the reliability of each discovery and the difficulty of exploiting them. It is routinely updated to add brand-new, and lesser-known vulnerabilities.


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Capture filter: Logger memory limit set to 50MB | Capturing requests up to 1MB; capturing responses up to 1MB
Logging: On
View filter: Showing all items
Columns
Time Tool Method Host Path Query Param count Status Length Start response timer Comment
1 21:54:44 2 Oct 2023 Proxy GET portswigger.net /burp/documentation/des... utm_source=burp_suite_... 3 200 111572 471
2 21:54:43 2 Oct 2023 Proxy GET contile.services.mozilla.c... /v1/tiles 0 200 1612 246
3 21:54:43 2 Oct 2023 Proxy GET content-signature-2.cdn.... /chains/remote-settings.... 0 304 168 40
4 21:54:43 2 Oct 2023 Proxy GET safebrowsing.googleapis.... /v4/threatListUpdates:fe... $ct=application/x-protob... 4 200 85025 70
5 21:54:43 2 Oct 2023 Proxy GET push.services.mozilla.com / 0 101 240 247
6 21:54:43 2 Oct 2023 Proxy GET firefox.settings.services.... /v1/buckets/main/collecti... 0 304 150 56
7 21:54:44 2 Oct 2023 Proxy GET firefox.settings.services.... /v1/buckets/monitor/coll... _expected=%22169626... 1 200 23714 30
8 21:54:44 2 Oct 2023 Proxy GET firefox.settings.services.... /v1/buckets/main/collecti... _expected=1696204870... 2 200 40159 25
9 21:54:44 2 Oct 2023 Proxy GET content-signature-2.cdn.... /chains/remote-settings.... 0 304 169 22
10 21:54:44 2 Oct 2023 Proxy GET firefox.settings.services.... /v1/buckets/main/collecti... _expected=1627481728... 1 200 18507 34
11 21:54:45 2 Oct 2023 Proxy GET portswigger.net /content/fonts/ps-icons-s... td2uot 6 200 10060 310
12 21:54:45 2 Oct 2023 Proxy GET portswigger.net /content/fonts/ps-main/p... l1la2n 6 200 25585 315
13 21:54:45 2 Oct 2023 Proxy GET portswigger.net /content/psselfservice.css 5 200 476148 656
14 21:54:45 2 Oct 2023 Proxy GET portswigger.net /content/images/svg/icon... 5 200 2075 653
15 21:54:45 2 Oct 2023 Proxy GET portswigger.net /content/images/svg/icon... 5 200 1919 651
16 21:54:45 2 Oct 2023 Proxy GET portswigger.net /content/images/svg/icon... 5 200 2075 643
17 21:54:45 2 Oct 2023 Proxy GET portswigger.net /mega-nav/images/dasta... 5 200 1895 637
18 21:54:45 2 Oct 2023 Proxy GET portswigger.net /mega-nav/images/burp-... 5 200 23000 626
19 21:54:45 2 Oct 2023 Proxy GET portswigger.net /mega-nav/images/burp-... 5 200 16830 618
20 21:54:45 2 Oct 2023 Proxy GET portswigger.net /mega-nav/images/lates... 5 200 11596 616
21 21:54:45 2 Oct 2023 Proxy GET portswigger.net /burp/documentation/des... 5 200 90804 1153
22 21:54:45 2 Oct 2023 Proxy GET portswigger.net /burp/documentation/des... 5 200 106529 1148
23 21:54:45 2 Oct 2023 Proxy GET portswigger.net /burp/documentation/des... 5 200 105067 1145
24 21:54:45 2 Oct 2023 Proxy GET portswigger.net /burp/documentation/des... 5 200 80386 2687
25 21:54:45 2 Oct 2023 Proxy GET portswigger.net /burp/documentation/des... 5 200 98097 2684
26 21:54:45 2 Oct 2023 Proxy GET portswigger.net /bundles/widgets/conten... v=_g3Zsia-y9DEA4uF-9... 6 200 12925 403
27 21:54:45 2 Oct 2023 Proxy GET portswigger.net /bundles/public/staticcm... v=M4UBvztEkP6BGug8p... 6 200 23142 4216
28 21:54:45 2 Oct 2023 Proxy GET portswigger.net /bundles/public/searchbo... v=y3oLbtZL6hN9nw4ex... 6 200 977 4218
29 21:54:45 2 Oct 2023 Proxy GET portswigger.net /content/images/logos/p... 5 200 4778 4227
30 21:54:46 2 Oct 2023 Proxy GET contile-images.services.... /obgoOYObjlFea_bXuT6L... 0 304 215 38
31 21:54:48 2 Oct 2023 Proxy POST shavar.services.mozilla.c... /downloads client=navclient-auto-ffo... 21 200 206 270
32 21:54:48 2 Oct 2023 Proxy GET firefox.settings.services.... /v1/buckets/monitor/coll... collection=partitioning-e... 3 200 767 36
33 21:54:48 2 Oct 2023 Proxy GET firefox.settings.services.... /v1/buckets/main/collecti... _expected=1693416467... 1 200 2683 27
34 21:54:48 2 Oct 2023 Proxy GET www.youtube.com /embed/Nr2fYpStshA origin=https://portswigge... 2 200 94754 144
35 21:54:49 2 Oct 2023 Proxy GET ps.containers.piwik.pro /287552c2-4917-42e0-8... 0 200 235780 518
36 21:54:48 2 Oct 2023 Proxy GET www.youtube.com /s/player/f7e1823a/www... 2 200 388030 28
37 21:54:48 2 Oct 2023 Proxy GET www.youtube.com /s/player/f7e1823a/playe... 2 200 56488 49
39 21:54:48 2 Oct 2023 Proxy GET www.youtube.com /s/player/f7e1823a/www... 2 200 323065 103
40 21:54:49 2 Oct 2023 Proxy GET fonts.gstatic.com /s/roboto/v18/KFOmCnq... 0 200 16159 247
41 21:54:49 2 Oct 2023 Proxy GET fonts.gstatic.com /s/roboto/v18/KFOlCnqE... 0 200 16367 262
42 21:54:50 2 Oct 2023 Proxy GET portswigger.net /content/images/logos/a... 5 200 5537 240
43 21:54:50 2 Oct 2023 Proxy GET portswigger.net /content/images/logos/fa... 5 200 16895 403
44 21:54:50 2 Oct 2023 Proxy GET ps.containers.piwik.pro /ppms.js 0 200 83335 218
45 21:54:50 2 Oct 2023 Proxy GET www.youtube.com /iframe_api 2 200 2349 72
46 21:54:50 2 Oct 2023 Proxy GET www.youtube.com /s/player/f7e1823a/www... 2 200 215508 30
47 21:54:50 2 Oct 2023 Proxy GET googleads.g.doubleclick.... /pagead/id 0 302 745 77
48 21:54:50 2 Oct 2023 Proxy OPTIONS jnn-pa.googleapis.com /$rpc/google.internal.wa... 0 200 562 97


Burp Suite Community Edition v2022.9.6 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Comparer
This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.
Select item 1:
Length Data
Paste
Load
Remove
Clear
Select item 2:
Length Data
Compare ...
Words
Bytes