# LAB ASSIGNMENT - 4

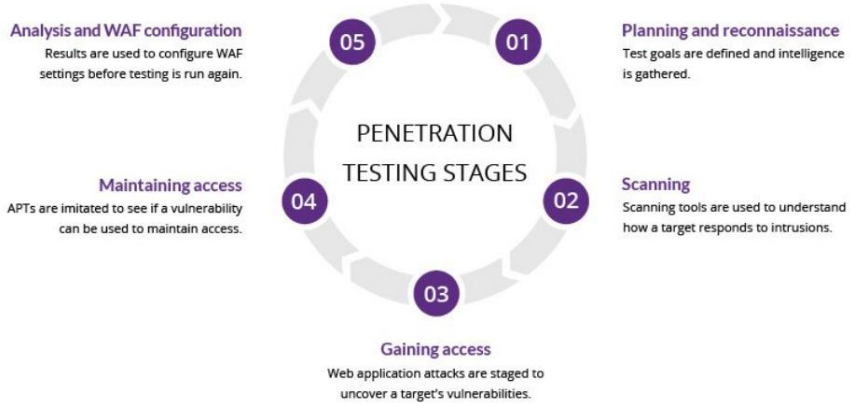
**Name:** Ashwin Balaji
**Roll Number:** 2020PMD4221
**Course:** M.Tech (Mobile Computing and Data Analytics)

**Title:** To perform the web penetration testing using Burp Suite

**Software Requirements:** Burp Suite 6.3 Community Edition

## Theory:

**Penetration Testing:** A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as end-user adherence to security policies. **Penetration testing is typically performed using manual or automated technologies** to systematically compromise servers, endpoints, web applications, wireless networks, network devices, mobile devices and other potential points of exposure. Once **vulnerabilities have been successfully exploited on a particular system, testers may attempt to use the compromised system to launch subsequent exploits at other internal resources**, specifically by trying to incrementally achieve higher levels of security clearance and deeper access to electronic assets and information via privilege escalation. **Information about any security vulnerabilities successfully exploited through penetration testing is typically aggregated and presented to IT and network system managers to help those professionals make strategic conclusions and prioritize related remediation efforts.** The fundamental purpose of penetration testing is to measure the feasibility of systems or end-user compromise and evaluate any related consequences such incidents may have on the involved resources or operations.




**Penetration testing methods:**

**External testing:** External penetration tests target the assets of a company that are visible on the internet, e.g., the web application itself, the company website, and email and domain name servers (DNS). The goal is to gain access and extract valuable data.

**Internal testing:** In an internal test, a tester with access to an application behind its firewall simulates an attack by a malicious insider. This isn't necessarily simulating a rogue employee. A common starting scenario can be an employee whose credentials were stolen due to a phishing attack.

**Blind testing:** In a blind test, a tester is only given the name of the enterprise that's being targeted. This gives security personnel a real-time look into how an actual application assault would take place.

**Double-blind testing:** In a double blind test, security personnel have no prior knowledge of the simulated attack. As in the real world, they won't have any time to shore up their defenses before an attempted breach.

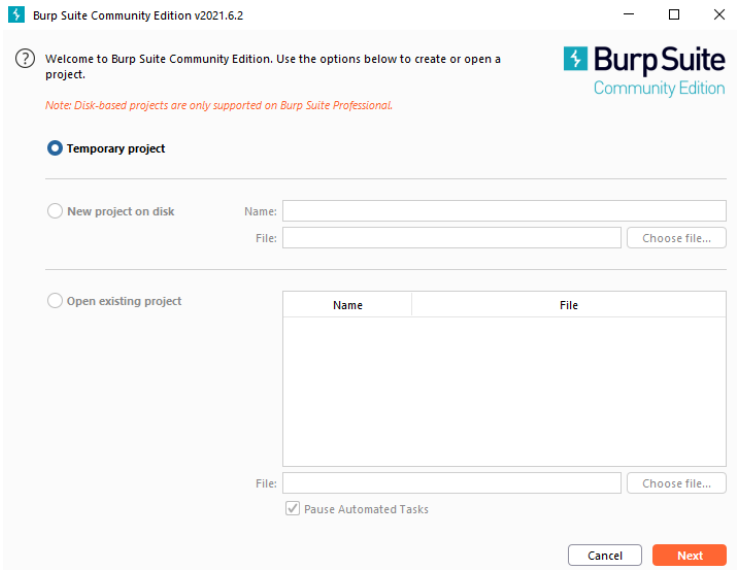
**Targeted testing:** In this scenario, both the tester and security personnel work together and keep each other appraised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

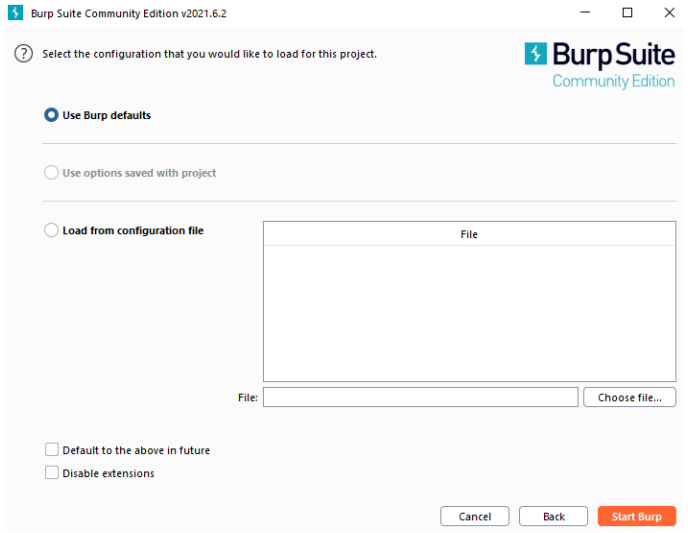
**While vulnerability scans provide a valuable picture of what potential security weaknesses are present, penetration tests can add additional context by seeing if the vulnerabilities could be leveraged to gain access within your environment. Pen tests can also help prioritize remediation plans based on what poses the most risk.**

**Burp Suite:** Burp Suite is the most popular **penetration testing and vulnerability finder tools**, and is often used for checking web application security. "Burp," as it is commonly known, is a proxy-based tool used to evaluate the security of web-based applications and do hands-on testing.

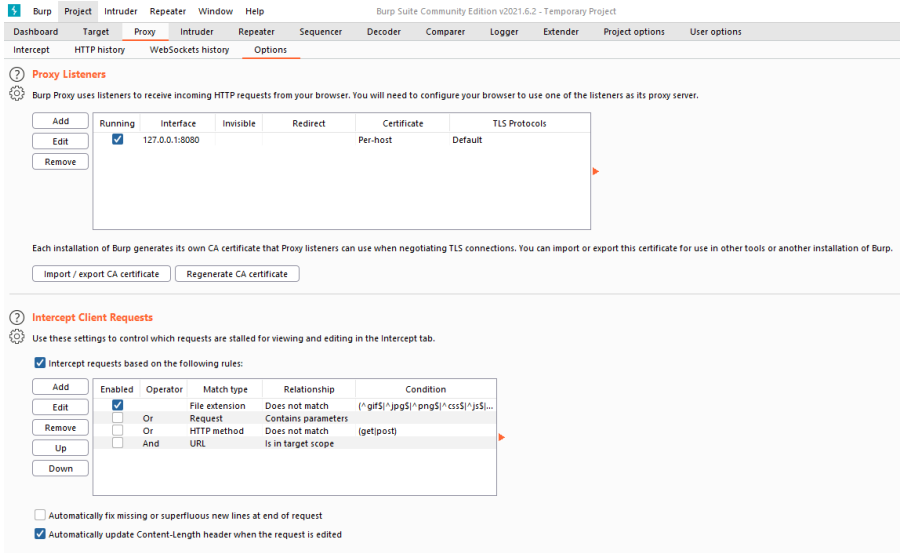
## Procedure:

1. Download and install **Burp Suite**
2. After installation, create **Temporary Project**
3. Click **Next -> Start Burp**

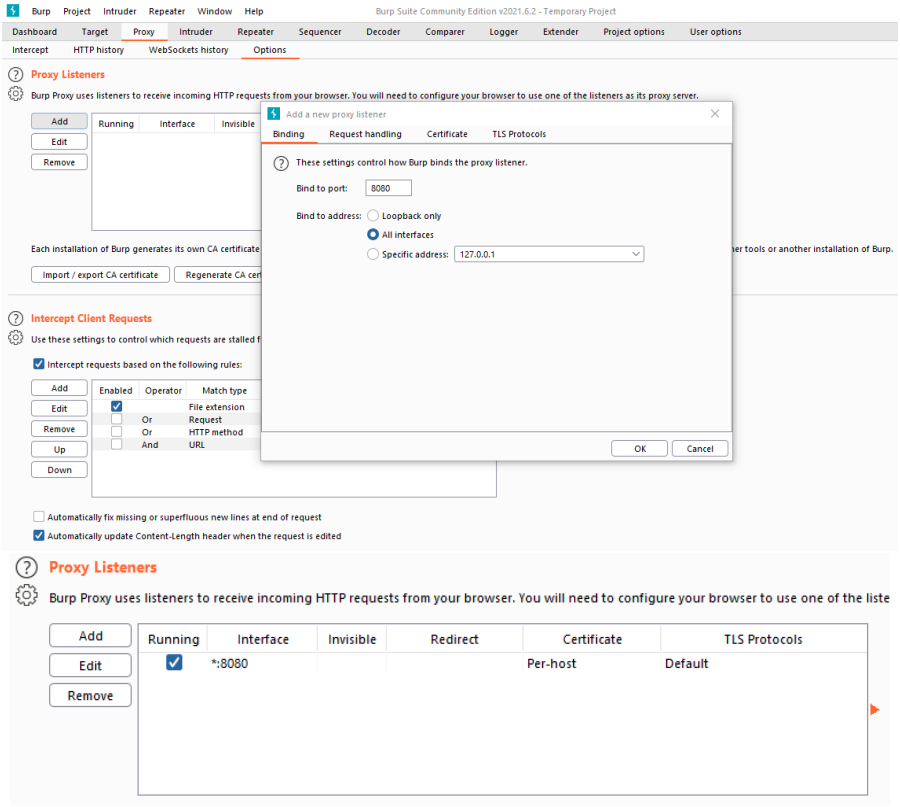


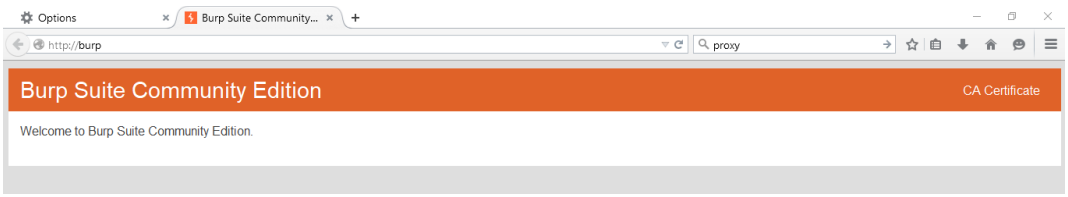

4. To configure Proxy: **Proxy -> Options**



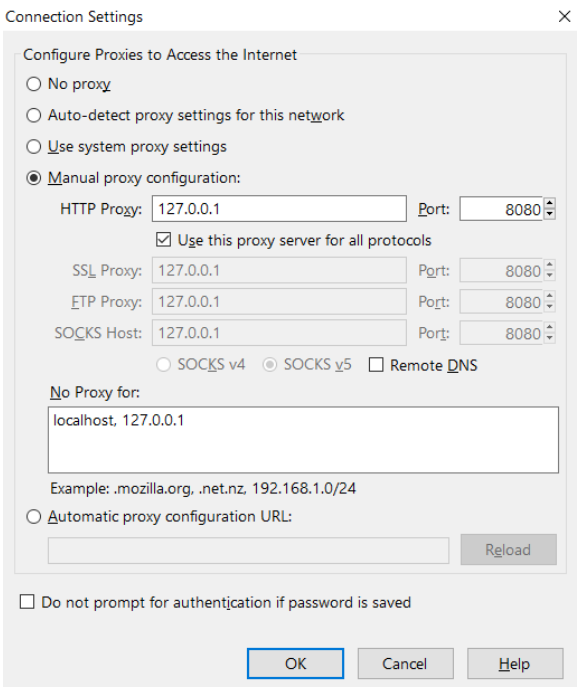
5. To set **proxy listener port**, If **localhost is not set**, Click **Add-> Bind Port : 8080 -> Bin Address: All Interfaces -> OK -> Yes** (For testing purposes)



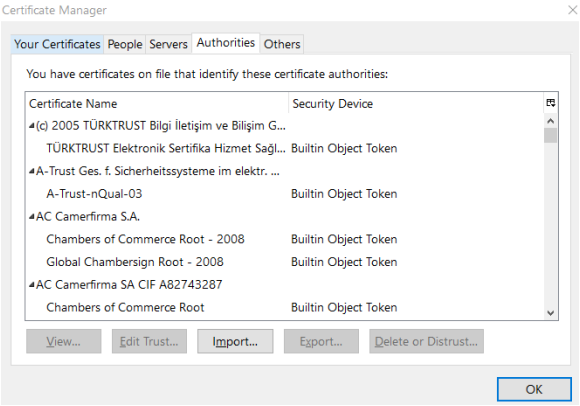

6. To Install **Certificate in the device (example., Browser)**
   a) In the browser, search **Proxy setting -> Manual proxy configuration -> set Proxy Address & Port -> Tick "Also use this proxy for FTP and HTTPS protocols" -> OK**
   b) Run [http://burp](http://burp)



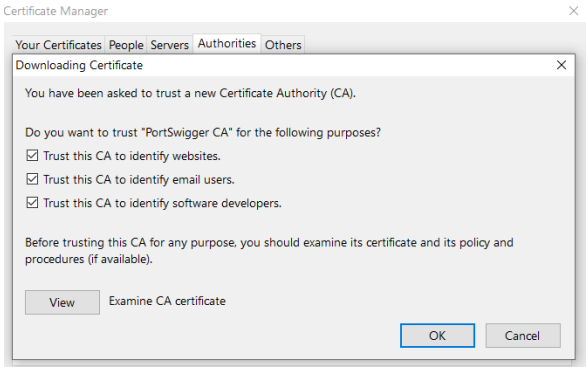

   c) Click on **CA Certificate -> Download/Save cacert.der file**



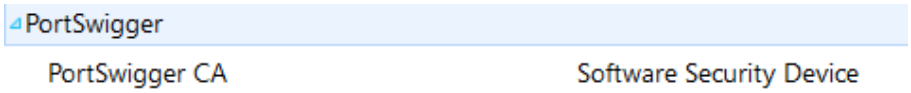

d) Import downloaded certificate to the browser




e) Search for **certificates in the browser settings -> Import -> cacert.der -> Tick boxes**




f) **PortSwigger CA** successfully installed

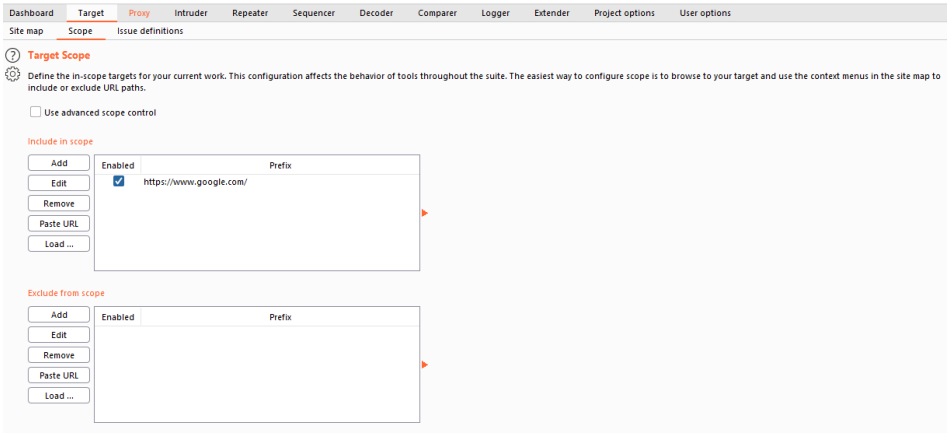



g) Now we can **intercept traffic** using BurpSuite/PortSwigger certificate authority.

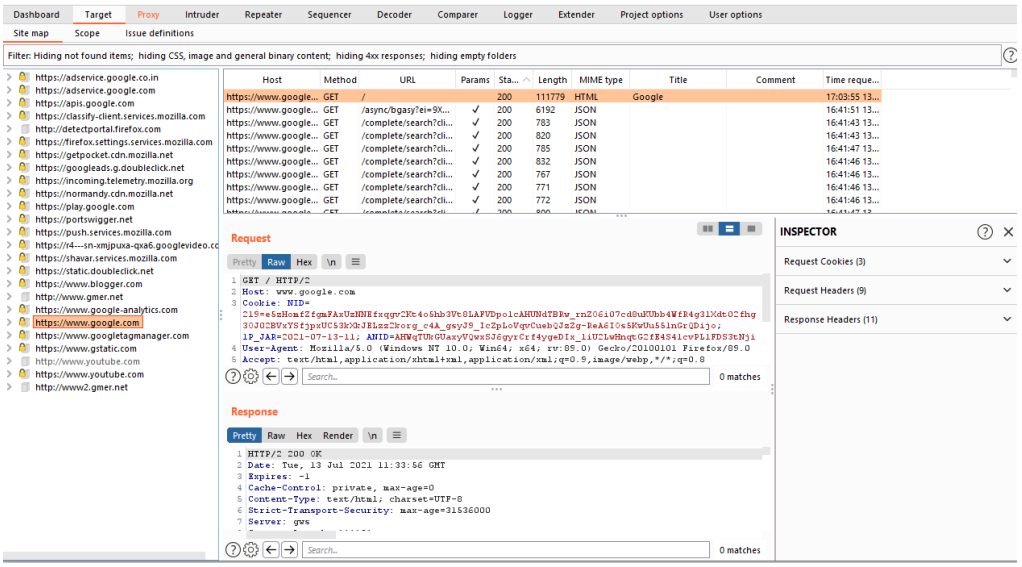
## TARGET SCOPE

**7.** The target scope configuration lets you tell Burp, at a suite-wide level, exactly what hosts and URLs constitute the target for your current work. You can think of the **target scope as, roughly, the items that you are currently interested in and willing to attack.**

8. The **scope definition uses two lists of URL-matching rules - an "include" list and an "exclude" list**. When Burp evaluates a URL to decide if it is within the target scope, it will be deemed to be in scope if the URL matches at least one "include" rule and does not match any "exclude" rules. This enables you to define specific hosts and directories as being generally within scope, and yet exclude from that scope specific subdirectories or files (such as logout or administrative functions).

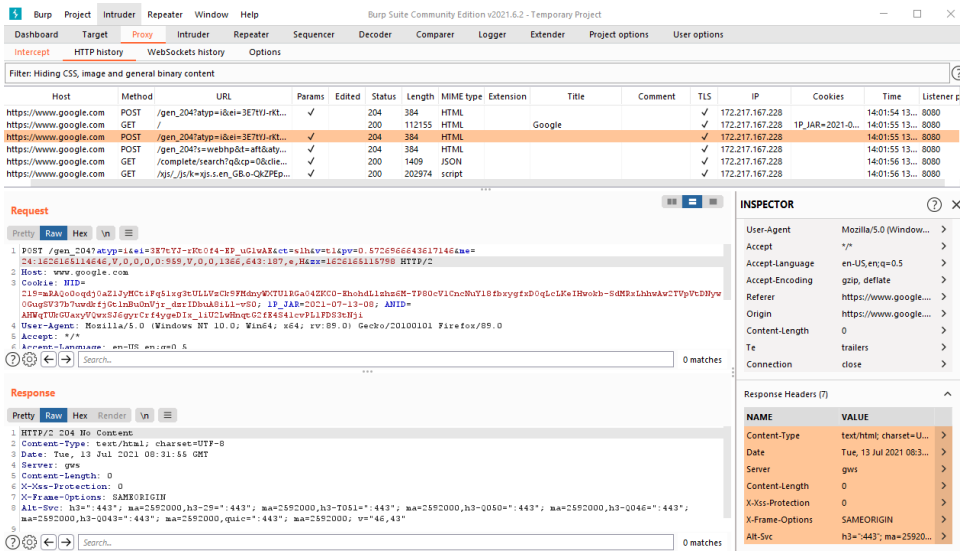



9. You can add or edit rules on the "include" and "exclude" lists using the URL-matching rule editor. However, in most cases, by far the easiest way to define your target scope is via the site map. As you map out the target application via Burp Proxy, the application's content will appear in the site map. You can then select one or more hosts and folders, and use the context menu to include or exclude these from the scope. This process is extremely easy and in most situations will let you quickly define all of the rules necessary for your testing.

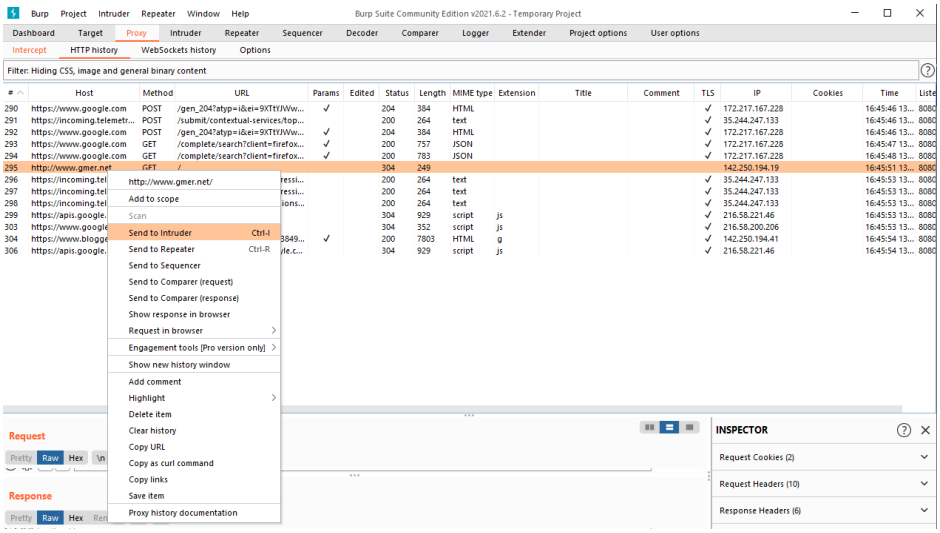


## PROXY INTERCEPTION

10. In intercept tab, **Turn on Intercept**
11. To check the traffic i.e., GET/POST, run https://google.com, traffic can be analyzed in **HTTP history** tab
12. Tap on google.com POST to see the request and response.
    Request headers parameters like, **POST, Host-Name, Cookie, User-Agent, Accept-Encoding, Referrer, Origin, Content-Length etc.**
    Response headers parameters like, **Content-type, Date, Server, Content-Length, XSS-Protection, X-Frame options etc.**



13. From here we can categorize the request to intruder, repeater, sequencer, decoder, comparer, logger, extender section by right clicking on the request.




## SCANNER

14. Burp Scanner automates the task of scanning web sites for content and vulnerabilities. Depending on configuration, the Scanner can crawl the application to discover its content and functionality, and audit the application to discover vulnerabilities. By default, all scans will use Burp's embedded browser to ensure maximum coverage through browser-powered scanning. You can also provide sets of user credentials so that Burp Scanner can discover and audit content that is only accessible to authenticated users.
15. Types of Scanning:

    **a) Scan from specific URLs.**

    This performs a scan by crawling the content within one or more provided URLs, and optionally auditing the crawled content. To do this, go to the Burp Dashboard, and click the "New scan" button. This will open the scan launcher which lets you configure details of the scan.

    **b) Scan selected items**

    This lets you perform an audit-only scan (no crawling) of specific HTTP requests. To do this, select one or more requests anywhere within Burp, and select "Scan" from the context menu. This will open the scan launcher which lets you configure details of the scan.

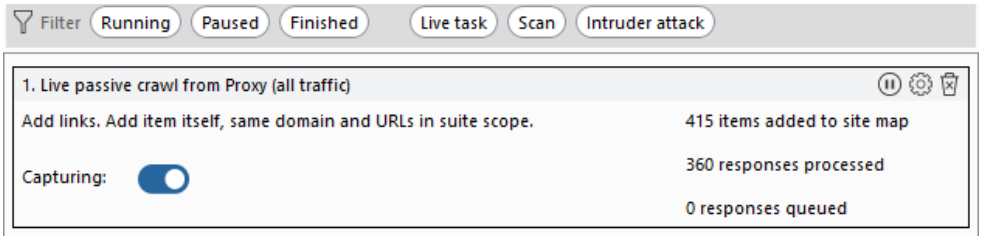
    **c) Live scanning**

    You can use live scans to automatically scan requests that are processed by other Burp tools, such as the Proxy or Repeater tools. You can configure precisely which requests are processed, and whether they should be scanned to identify content or audit for vulnerabilities. To do this, go to the Burp Dashboard, and click the "New live task" button. This will open the live scan launcher which lets you configure details of the task.

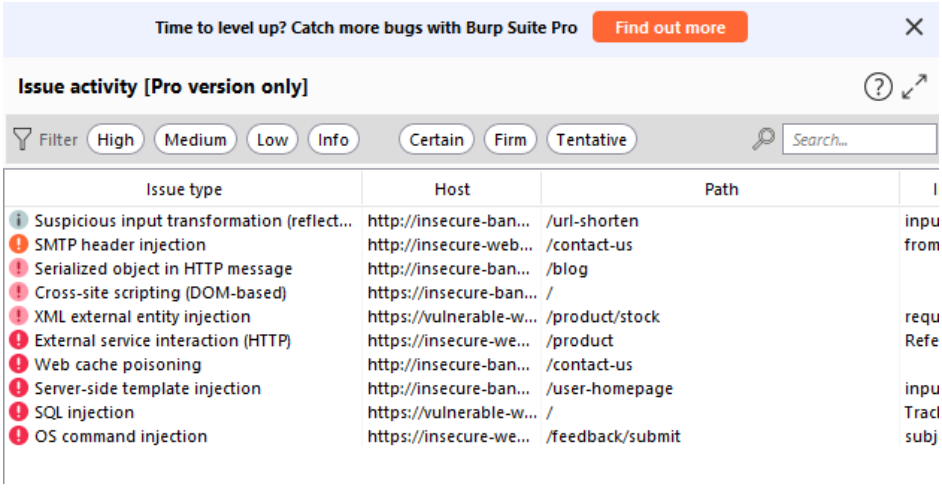
    **d) Instant scanning**

    You can also launch instant active or passive scans from the context menu. This means you can quickly check for vulnerabilities without having to open the scan launcher. You can access these

options by right-clicking on a request. Alternatively, you can configure hotkeys for triggering instant scans.

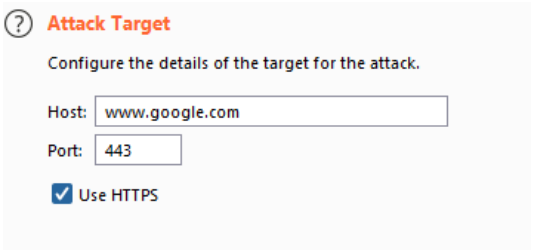



16. Analysed traffic (recorded while surfing) will automatically categorize the severity of issues by performing web crawling.




## INTRUDER

17. This allows you to perform customized automated attacks, to carry out all kinds of testing tasks.
18. Send the request to intruder, **Tick HTTPS**, Port will be set to 443 and the website on which intrusion need to be performed.




19. Click on **Positions -> Clear$**
20. You may find many parameters for which automated brute-force testing attack need to be carried off. Consider the snippet:

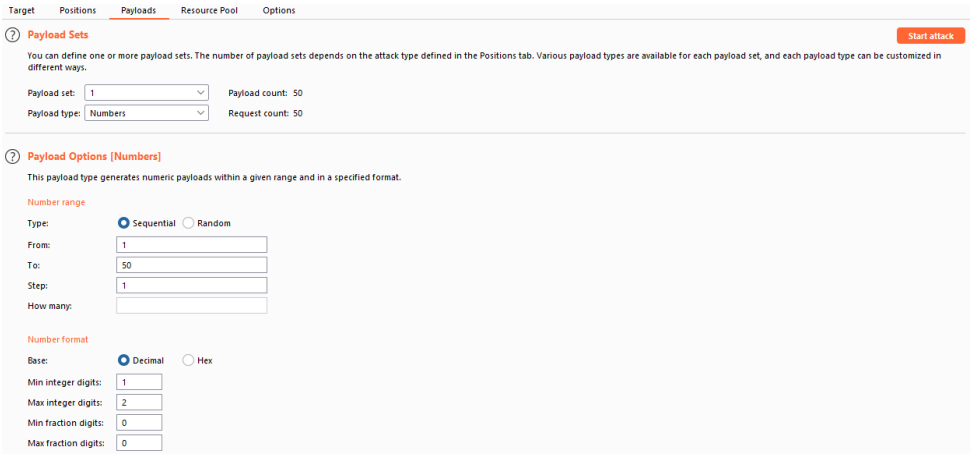
```
POST /gen_204?s=webhp&t=aft&atyp=csi&ei=JHrtYN_1AqPF4-
EPjsoE&rt=wsrt.327,aft.153&imn=1&ima=0&imad=0&aftp=-1&bl=nKur
HTTP/2
Host: www.google.com
```

```
Cookie:
NID=219=e5zHomfZfgmFAxUzNNEfxqgv2Kt4o5hb3Vt8LAFVDpolcAHUNdTBRw_
rnZO6i07cd8uKUbb4WfR4g3lXdt02fhg3OJ02BVxYSfjpxUC53kXkJELzz2korg
_c4A_gsyJ9_IcZpLoVqvCuebQJzZg-ReA6IOs5KwUu551nGrQDijo;
1P_JAR=2021-07-13-11;
ANID=AHWqTUkGUaxyVQwxSJ6gyrCrf4ygeDIx_liU2LwHnqtG2fE4S41cvPL1FD
S3tNji
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:89.0)
Gecko/20100101 Firefox/89.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.google.com/
Content-Type: text/plain;charset=UTF-8
Content-Length: 0
Origin: https://www.google.com
Te: trailers
Connection: close
```

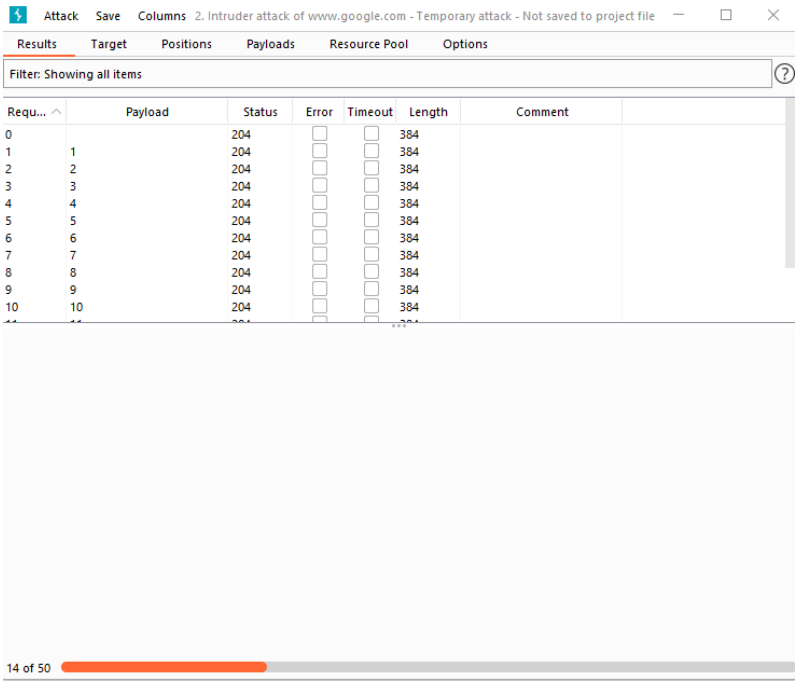
21. **Add $** sign on the paramater which to be considered for attack. Suppose **"imn"** parameter considered for atatck.

```
POST /gen_204?s=webhp&t=aft&atyp=csi&ei=JHrtYN_1AqPF4-
EPjsoE&rt=wsrt.327,aft.153&imn=§1§&ima=0&imad=0&aftp=-
1&bl=nKur HTTP/2
```

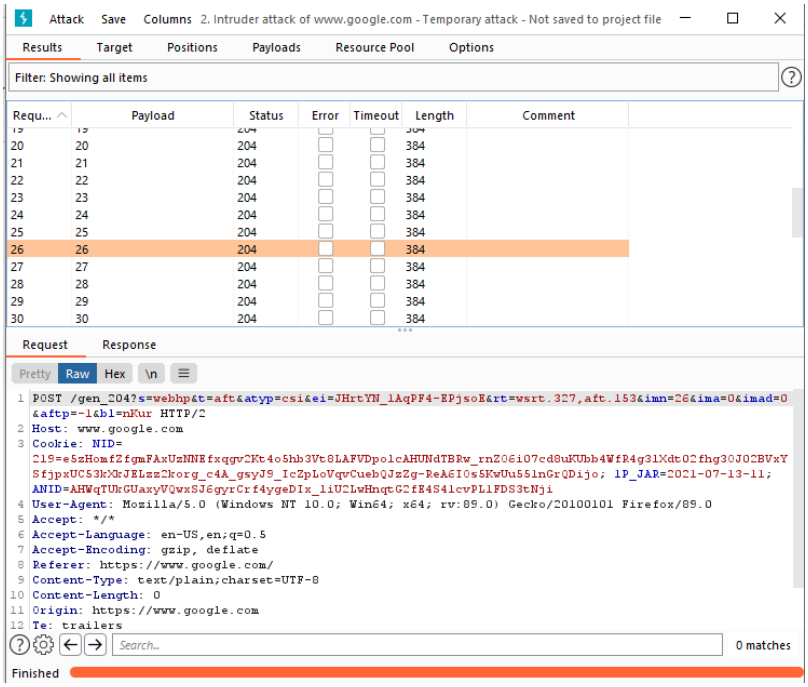

22. Click on Payloads. **Set Payload sets -> Payload Options -> Payload Processing -> Payload Encoding.** All these settings initialization may vary based on the nature of the parameter considered.




23. Click on **Start Attack**




24. Attack inititated from **imn count 1 to 50 value and responses from the server are captured.**

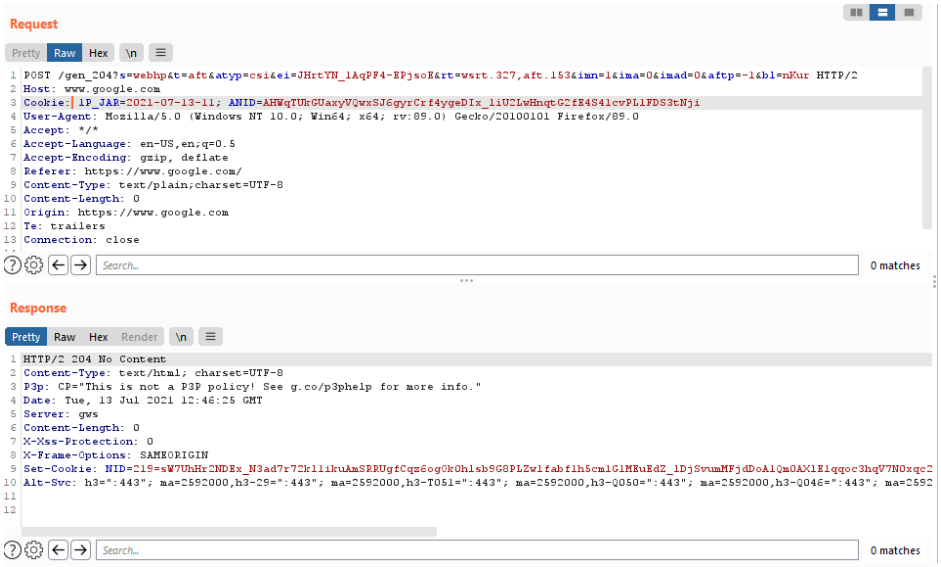



25. Like this way, attacks are possible like password attacks (combinations of digits and alphabets) by creating custom list of combinations of alphanumeric characters in a brute-force manner **(one of the use-case)**

## REPEATER

26. This is used to manually modify and reissue individual HTTP requests over and over.
27. Fetch any Post/Get request-> Right Click on the request -> Send to repeater.
28. We will check, how the server will respond for the changes happened in request packet.


29. Removed **NID** to see how the server responds.




30. **Response received** from the server and here, **NID has been set automatically as it was unavailable in the request**. We can change whatever the information to check the response.

## SEQUENCER

31. This is used to analyze the quality of randomness in an application's session tokens.

## DECODER

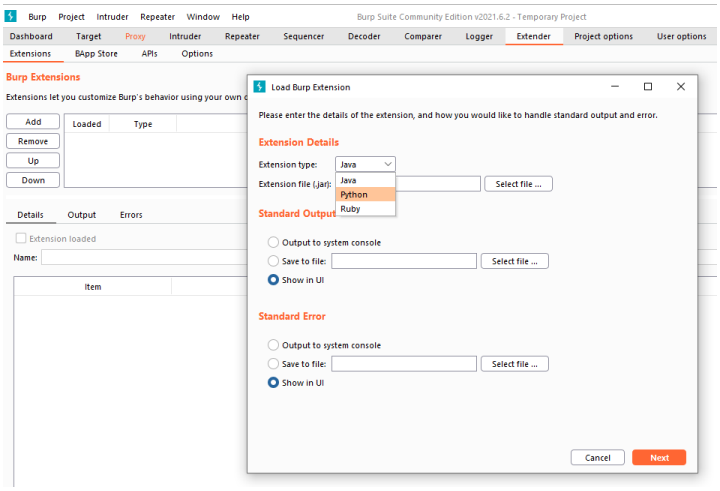
32. This lets you transform bits of application data using common encoding and decoding schemes.

## COMPARER

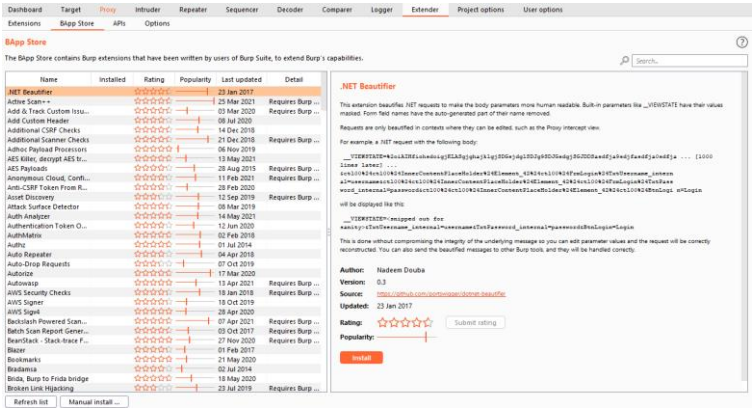
33. This is used to perform a visual comparison of bits of application data to find interesting differences.

## EXTENDER

34. This is used to install plugins used for security testing
35. Extension type can be installed manually **-> Java, Python or Ruby.**




36. Can also be installed through **BApp Store, these extensions are written Burp Suite users to extended the capabilites of BurpSuite.**




37. Burp's behavior can be customised using Burp Extended API to create own extensions.