BURP SUITE:

🛡️ Burp Suite Kya Hota Hai?

Burp Suite ek tool hai jo hackers (ethical hackers), security testers, aur developers use karte hain websites ke **security flaws** dhoondhne ke liye.

Security flaws ka matlab hai:

> Website ya app ke system me aisi galti (bug) ya kamzori (weakness) jisko koi hacker use karke nuksan pohoncha sakta hai.

Iska kaam hota hai: "Website aur user ke beech chalne wali baatein (requests aur responses) ko sunna, samajhna, aur test karna."

https://youtu.be/aUG45BxFwp0?si=0IS8lX57pcOVenGM => burp suite

Use Kaise Karte Hain?

Burp Suite ek middleman (beech wala) ka kaam karta hai:

- Tumhara browser → 🔄 → **Burp Suite** → 🔄 → Website server

Yani jab tum website open karti ho, Burp Suite dekh sakta hai ke kya data ja raha hai aur kya aa raha hai.Tum is data me changes bhi kar sakti ho, jaise hacker karta hai — aur check kar sakti ho ke website me koi security bug hai ya nahi.

Example:

Socho hum aik login page test kar rahy hen:

- Normal user: email + password bhejta hai.
- Burp Suite: hum us password ko intentionally galat bhej kar check karty hy k:
    - Kya error aa raha hai?
    - Kya data encrypt hai ya plain?
    - Kya system weak password accept kar raha hai?

Is tarah tum check karti ho ke website secure hai ya nahi**.**

Use Cases:

- Web Security Testing
- Ethical Hacking etc

Burp suite ki jo official main website hy uska name hy **“PortSwigger.net”.** Burp suite k 3 main editions hy.

1- Burp Suite Enterprise Edition.**(for company level)**

2- Burp Suite Professional. **(for professional level in freelancing)**

3- Burp Suite Community Edition.**(for beginners**

Burp Suite Alternatives:

1- Acunetix

2- OWASP ZAP

3- Netsparker

4- W3af

What is DNS?

Full form of “domain name system” ye dns IP address k liye hota hy.yani jab

Step-by-Step Solution (Import Burp CA Certificate into Firefox):

Step 1: Start Burp Suite and listen on 127.0.0.1:8080

- Make sure Burp is running and the intercept is **off**.
- Go to Proxy > Options and verify the interface is 127.0.0.1:8080.

Step 2: Configure Firefox Proxy

- Go to Firefox Settings → Search: `proxy` → Click Settings.

- Select: Manual proxy configuration
    - HTTP Proxy: `127.0.0.1` | Port: `8080`
    - Check "Use this proxy for all protocols"
- Click OK.

🔹 **Step 3: Download Burp Certificate in Firefox**

1. In Firefox, go to: `http://burp`
2. Click on the link: CA Certificate to download `cacert.der` file.

🔹 **Step 4: Import Certificate in Firefox**

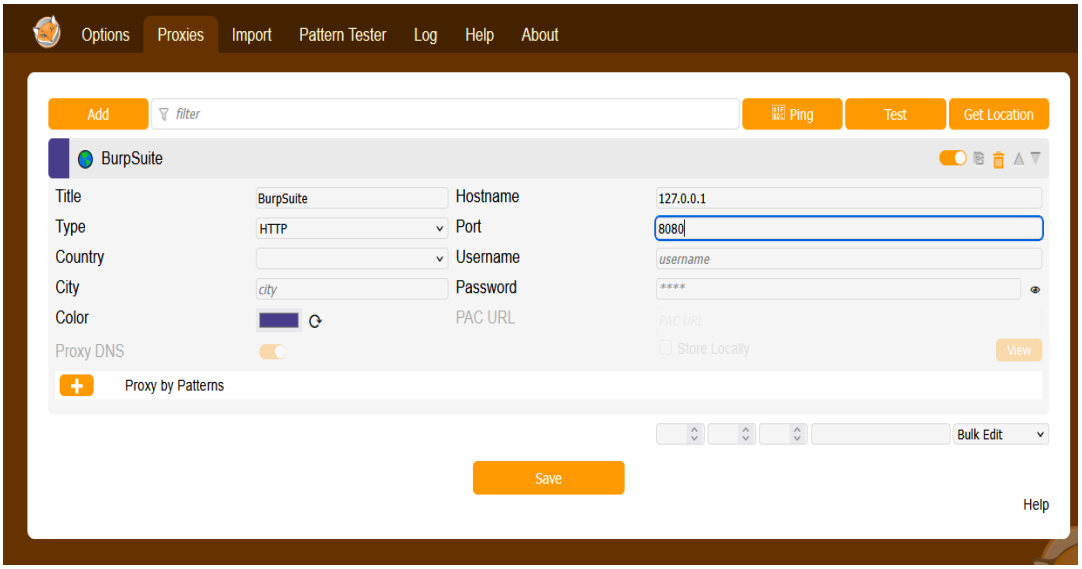
1. Go to Firefox Settings ⟶ Search: **certificates**
2. Click on "View Certificates"
3. Go to Authorities tab ⟶ Click Import
4. Select the `cacert.der` file you downloaded.
5. Check both:
    - "Trust this CA to identify websites"
    - "Trust this CA to identify email users" (optional)
6. Click OK and restart Firefox.

Burp Suite Ka Traffic Log clear method:

- **HTTP history** ya logs bhar jaate hain to Burp slow ho jata hai.
- Jao: `Proxy → HTTP history` ⟶ Right-click ⟶ Clear history.
- `Target` ya `Logger` tabs bhi clear kar do.

*proxy ko bar bar manual setup karny or disable karny sy bohat time waste hota hy to isk liye aik extension hy **“FoxyProxy firefox”**

Foxyproxy setup {options => proxies => add => title



Repeater:

Repeater Burp Suite ka ek tab hai jo aapko **“copy → edit → send → dekh”** ka bahut hi aasan playground deta hai.
Sochiye aap server ko bar-bar ek hi request bhejna chahte hain, har dafa thoda-bhot badal-kar dekhna chahte hain ke response kaisā badalta hai. Repeater isi kaam ke liye bana hai.

Intruder:

Intruder ek Burp Suite ka tool hai jo kisi form ya field (jaise login form) me bar bar automatically different values try karta hai — taake check kare ke koi password match hota hai ya koi error ya weakness milti hai.

Soch lo ke tum bar bar manually password try kar rahi ho — Intruder ye kaam tumhare liye automatic kar deta hai.

Payload

Payload ka matlab hota hai Jo cheez aap kisi field ya request me daal kar test karna chahti ho.Ye ho sakta hai:

- Ek password (e.g., `admin123`)

- Ek username (e.g., `admin`)
- Ek URL, code, script, ya special input (e.g., `<script>alert(1)</script>`, `' OR 1=1--`)

Burp Suite me Payload ka kaam:

Burp Suite ka Intruder tool bar bar request ke kisi part me payload daal kar check karta hai ke:

- Response change hota hai ya nahi?
- Kya vulnerability milti hai?
- Kya koi valid input mil gaya (e.g., sahi password)?

PAYLOAD LIST:

https://github.com/payloadbox/xss-payload-list/tree/master/Intruder

Payload = Test Wala Input

Jab tum kisi form, field, search bar ya URL me kuch type karti ho, wo ek input hota hai.Agar hacker ya security tester kuch aisa input deta hai jo system ka reaction test kare, to usko payload kehte hain.

Types of Attack:

1- Sniper Attack

Sniper attack ek Intruder ka attack mode hai jo sirf ek position (yaani ek jagah) pe bar bar alag alag payloads try karta hai.

Matlab:

- Tum kisi field (jaise password) me ek hi jagah payloads lagana chahti ho
- Burp har baar ek payload dal kar test karega

Example:

Socho ek login request:

```
POST /login

username=admin&password=§test§
```

Tumne password field ko payload position banaya (`§test§`)

Tumhari payload list:

```
123456

admin123

password

letmein
```

Sniper Attack kya karega?

Ye request bar bar repeat hogi, har baar ek naye password ke sath:

```
username=admin&password=123456

username=admin&password=admin123

username=admin&password=password

username=admin&password=letmein
```

- Bas ek hi jagah payload apply hota hai.Burp response ko compare karta hai:

2- Battering Ram:

Battering Ram ek attack mode hai jisme multiple jagahon (positions) par same payload ek saath apply hota hai.

Yani:

- Tum request me 1 se zyada §§ (positions) lagati ho
- Har request me same payload sab positions pe ek saath inject hota hai

Example:

Tumhari login request:

POST /login

username=§test§

password=§test§

Tumhari payload list:

admin

mueza

123456

test123

Battering Ram kya karega? Burp Intruder in payloads ko same waqt par dono positions (username & password) pe inject karega:

username=admin & password=admin

username=mueza & password=mueza

username=123456 & password=123456

username=test123 & password=test123

3- Pitchfork Attack :

Example:

Tumhari Request:

POST /login

username=§username§

password=§password§

Payload List 1 (username field ke liye):

admin

user1

mueza

Payload List 2 (password field ke liye):

123456

pass123

mueza@321

Ye do payloads list banti hy phir selected part par apply hoti hy

§ Symbol in Burp Suite:

Ye § ka matlab hota hai: "Yahan payload inject karo."Jab tum Burp Intruder me request open karti ho, to jo part tum test karna chahti ho, usko § symbols ke beech me daalti ho.

4- Cluster Bomb:

Ye aik math me jo order pairs banaty hy usi tarah ye bhi request k parts ko order pairs ki tarha check karta hy .

Encoder:

Normal message ko special format me badalna.

Decoder:

Special format wale message ko wapis normal banana.

Example:

Tumhara message:

Hello Mueza!

Encoder se ban gaya:

SGVsbG8gTXVlemEh

Decoder se:

SGVsbG8gTXVlemEh → Hello Mueza!

Encode = chhupa dena / badal dena

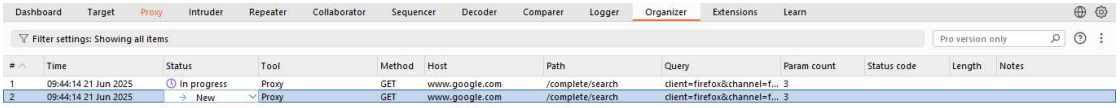
Decode = samajhna / wapis asli form me lana

Comparer in Burp Suite:

> Comparer ek tool hai jo do responses, requests, cookies, ya koi bhi text side-by-side compare karta hai taake tum dekh sako ke unme kya difference ya similarity hai.

Organizer:

Ye aik notepad type hota hy jaisy k agr koi request hy or hum chah rahy hy k apny yaad rakhny k liye uspar koi commit kardy to ye organizer sy hoga.



Sequencer:

Sequencer ka kaam hai check karna ke token ya ID random hai ya nahi.

Jab tum kisi website par login karti ho, ya form submit karti ho, to server tumhe ek “token” ya “session ID” deta hai. Ye token aise lag sakta hai:

AB123XYZ

Har user ko alag token milta hai — taki koi dusra user uska session chura na sake.Agar Token Bar Bar Wahi Ho:

AB123XYZ

AB123XYZ

AB123XYZ

To ye dangerous hai! Hacker easily guess kar sakta hai tumhara session!

Agar Har Baar Naya Token Mile:

AB123XYZ

CD456TUV

JP789LMN

To ye secure hai.

Yahi Burp Ka “Sequencer” Karta Hai:

Kaise?

1. Tum token wala request Burp me “Send to Sequencer” karti ho
2. Burp wo request bar bar send karta hai (jaise 100 ya 500 baar)
3. Har baar naya token collect karta hai
4. Fir check karta hai:

    - Kya har token different hai?
    - Kya usme koi pattern to nahi?

Add to Scope:

> Jab tum Burp Suite me kisi website ya URL ko "Add to Scope" karti ho, to tum Burp ko batati ho ke:
>
> “Ye meri testing ka target hai — is domain par hi focus karo.”

Example:

Tum test kar rahi ho:

https://www.example.com

Is website me kuch links jaise:

- **`example.com/login`**
- **`example.com/dashboard`**
- **`google.com/fonts`** **(external)**
- **`cdn.somewhere.com/script.js`** **(external)**

Agar tum example.com ko “Add to Scope” karti ho to Burp samajhta hai sirf `example.com` par focus karna hai,domains jaise `google.com` ya `cdn.somewhere.com` ignore karo."