{

```
char buffer[1024];
char password[100];
```

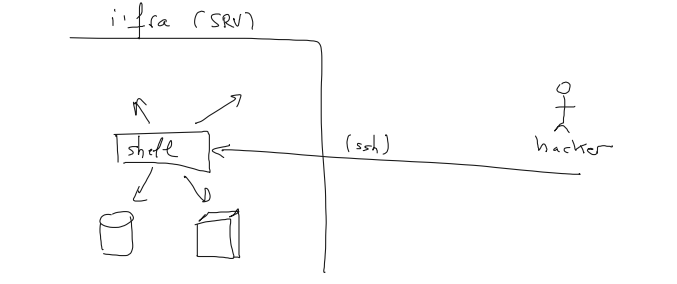
(normalement) Un paquet réseau fait 1 ko

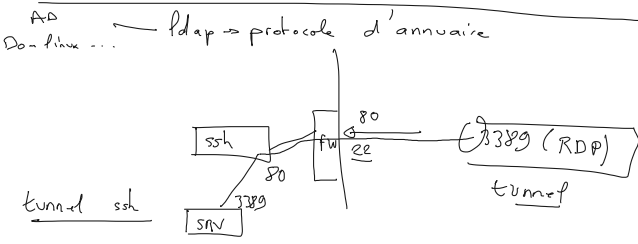
Paquet 1400 octets

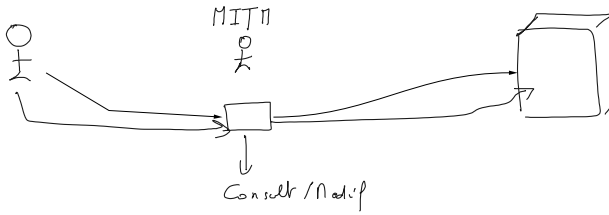
Code

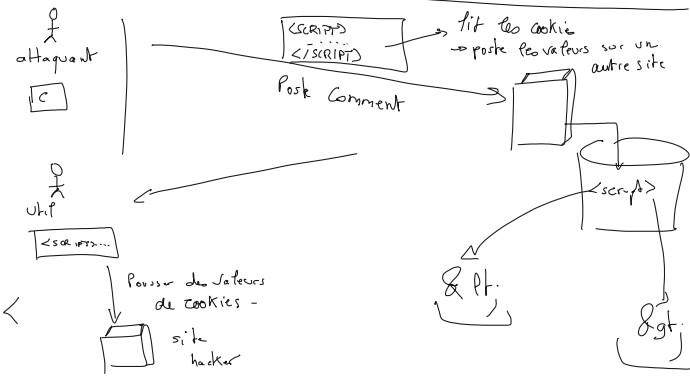
Lecture du paquet
- pas prévu le dépassement

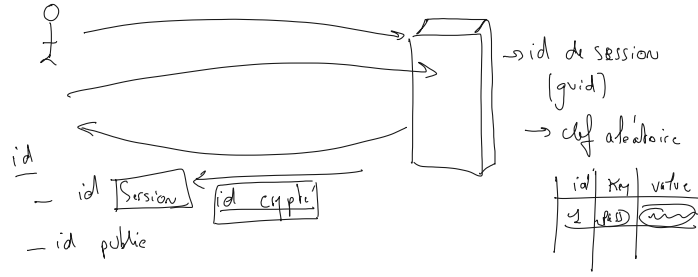
App "malicieuse" | tata






MITM
Consulter / Modif


attaquant
PC
<SCRIPT>
.....
</SCRIPT>
Post Comment
lit les cookie
→ poste les valeurs sur un autre site
<script>
&pt
&gt
Victime
<SCRIPT>...
Pousse des valeurs de cookies -
site hacker


→ id de session (guid)
→ clef aléatoire
id
- id Session
id crypté
- id public
id
key
value
1
RSA

Attaque CSRF.

App: http://srv.interne/user/reset?id=10&p=toto