Sicurezza sul web

oh, mamma!

whoami

Sante Rotondi
saten.r@gmail.com

CIO @ dSmart s.r.l

#polimi
#POuL
#securenetwork
#rubyonrails

Se la chiamano rete...

è perché pullula di ragni :)

La superficie di attacco

- Il **sistema operativo**
- Il **browser**
- I **plugin** del browser
- I siti visitati
- I programmi in esecuzione
- **Ciò che di solito è fra la tastiera e la sedia...**

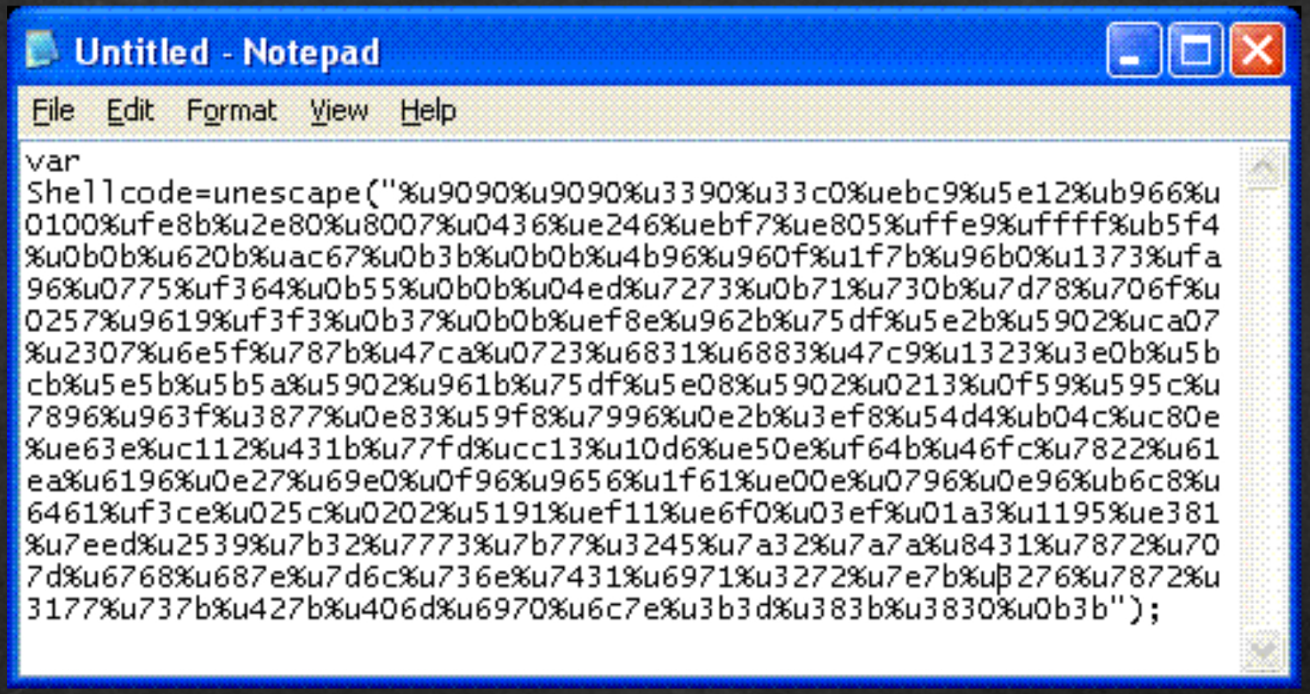
Attacchi comuni

A1: Injection (**SQL**)
A2: Cross-Site Scripting (**XSS**)
A3: Broken Authentication and **Session Management**
A4: Insecure Direct Object References
A5: Cross-Site Request Forgery (**CSRF**)
A6: Security Misconfiguration
A7: Insecure Cryptographic Storage
A8: Failure to Restrict URL Access
A9: Insufficient **Transport Layer Protection**
A10: Unvalidated **Redirects and Forwards**

Sotto attacco!

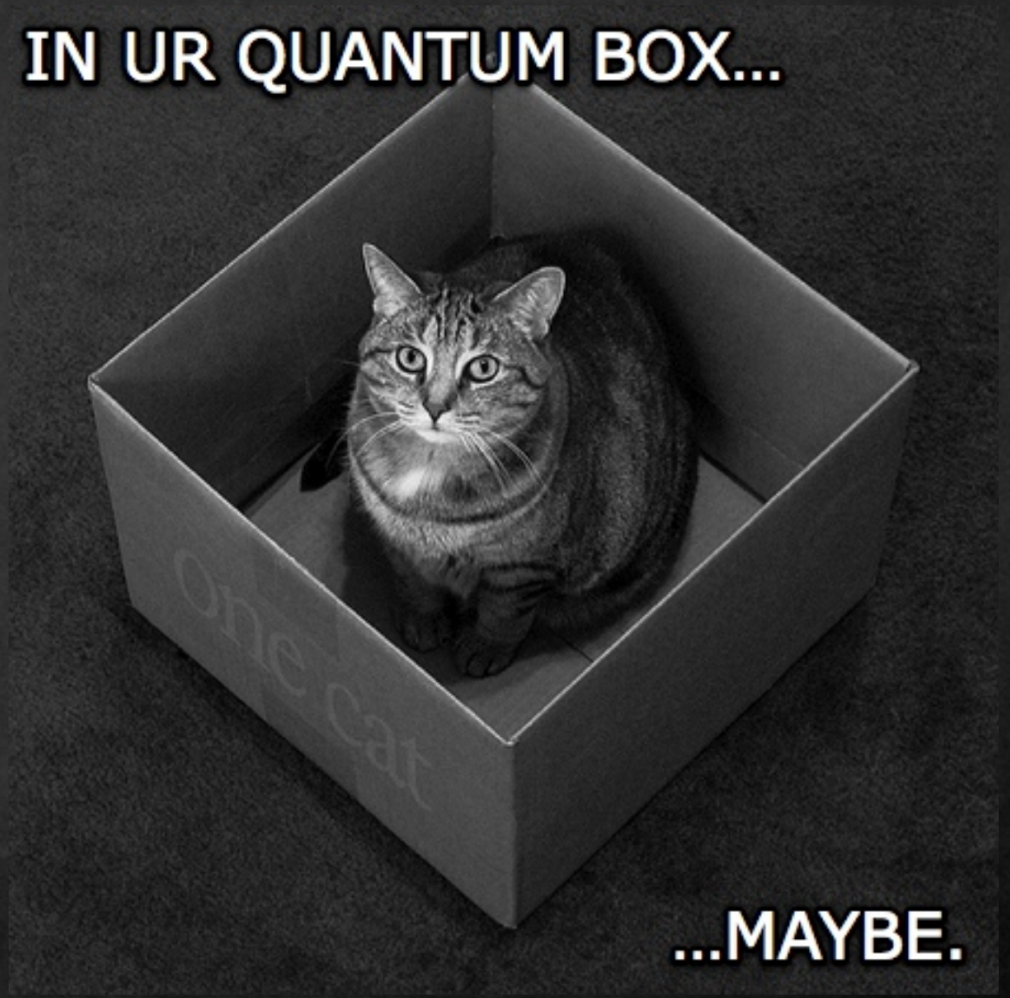
shellcode

La chiave per eseguire comandi sul vostro computer



privilege escalation

Una volta entrati in casa dalla porta sul retro, facciamo entrare i nostri complici...



botnet

Si può perdere il controllo del proprio computer, anche senza rendersene conto..

Difesa!

Una catena è forte quanto il suo anello più debole ...
Bisogna ridurre la superficie di attacco!

domande

?