sicurezza for dummy coders

Sante Rotondi
20/01/2010

Perché?

dSmart

POuL
have a lot of fun...

La stupidità degli utenti è leggendaria..

Che mi dite di quella dei programmatori? :)

Le cause di tutti i mali

- Time To Market
- Sviluppo a Cascata
- Pigrizia del coder :(
- Fantasia dell'hacker :)

dSmart

POuL
have a lot of fun...

Panoramica.. degli orrori

dSmart

POuL
have a lot of fun...

Buffer Overflow

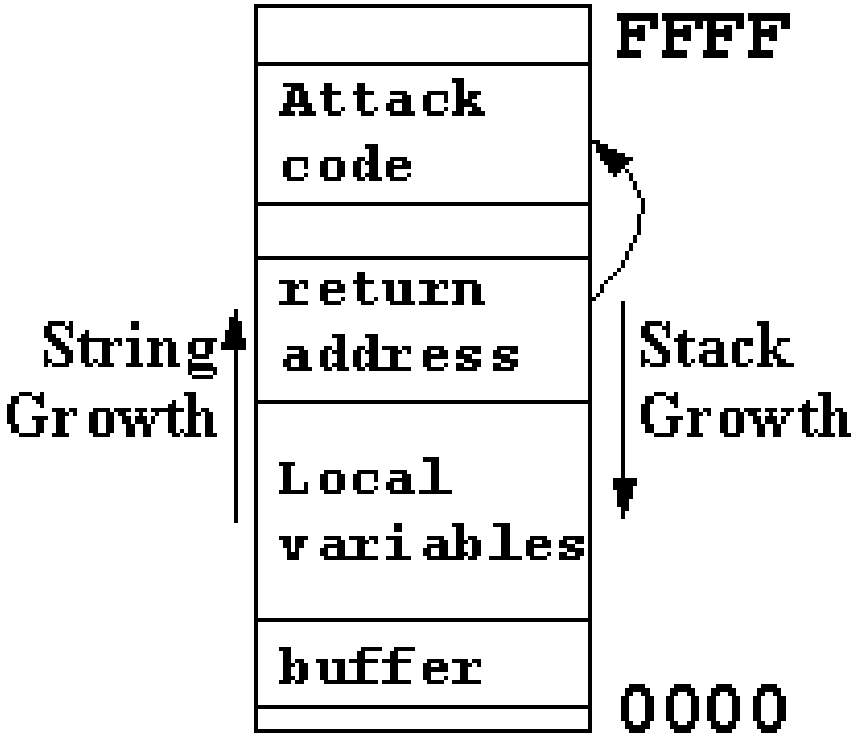
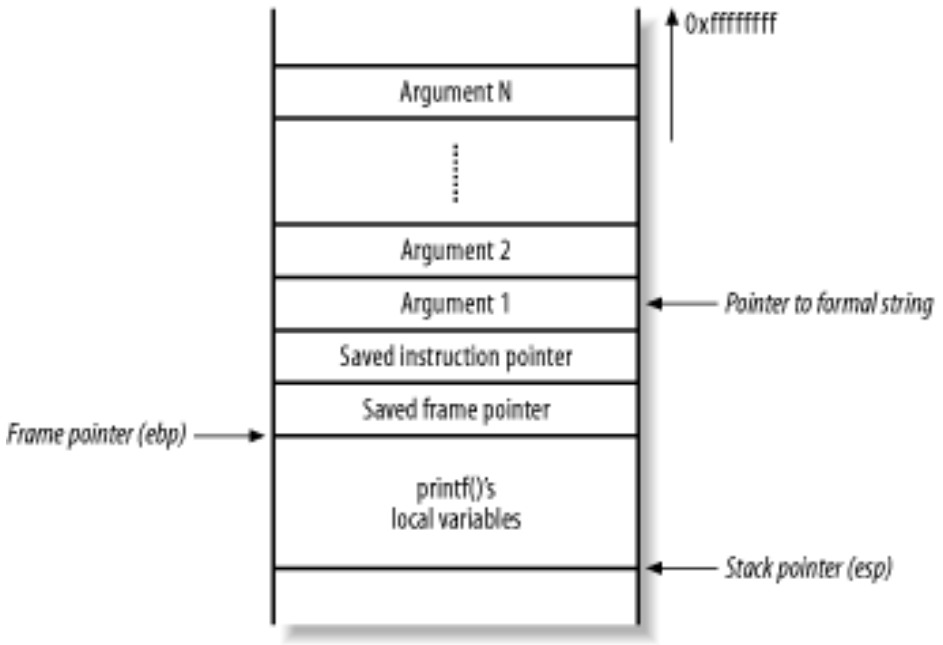


Figure 1: "Stack Smash" Attack Against Activation Record

- Aleph1 (Phrack 49)
- Codice C
- Se ne trovano sempre meno

Format String



- Perché la printf non faceva abbastanza pena :P
- Facili da sbagliare, facili da fixare

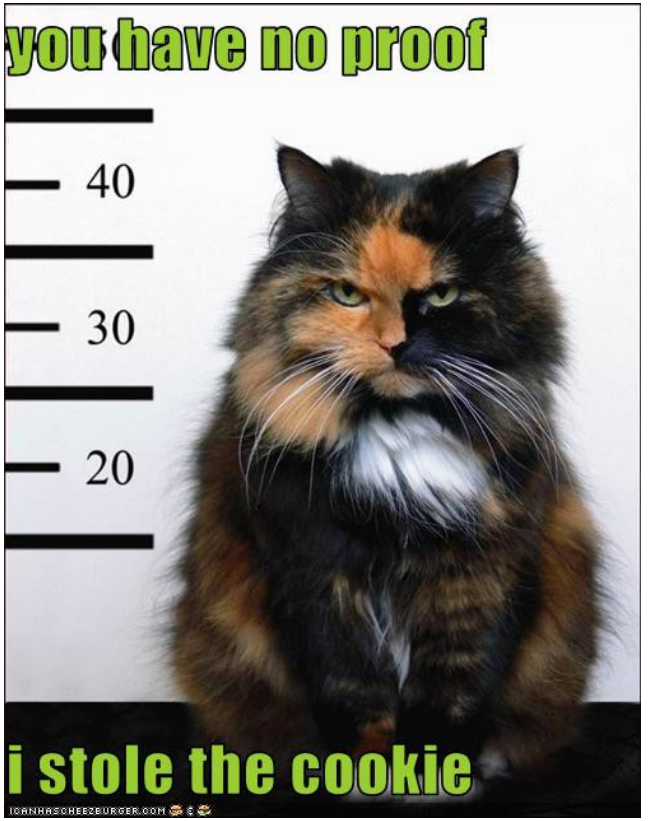
Null Byte Poisoning

- Perl scripts, anyone?
- Espressioni regolari poco sicure

dSmart

POuL
have a lot of fun...

Cookie Insicuri

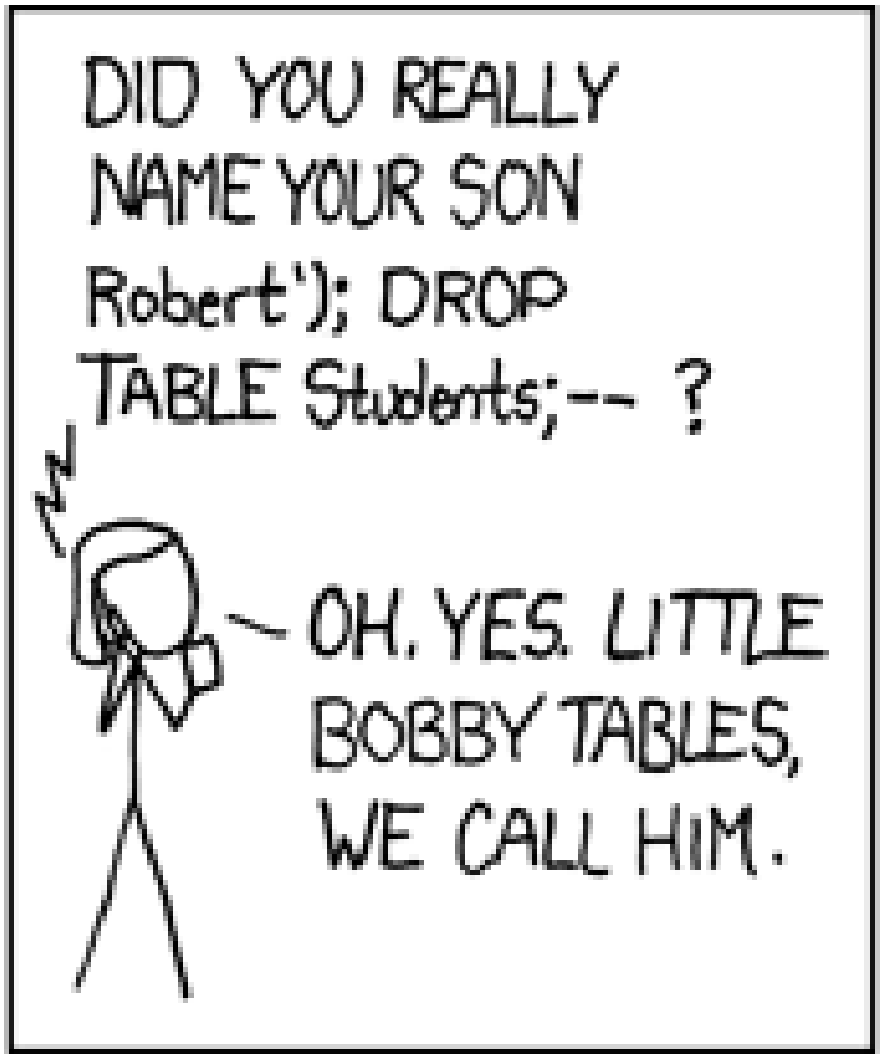


- I cookie possono essere letti e manipolati dal client
- Spesso persino dal JavaScript...

dSmart

POuL
have a lot of fun...

SQL Injection



- Il web ne é pieno
- Query SQL costruite concatenando stringhe con l'input dell'utente

dSmart

POuL have a lot of fun...

Javascript Injection / XSS / CSRF

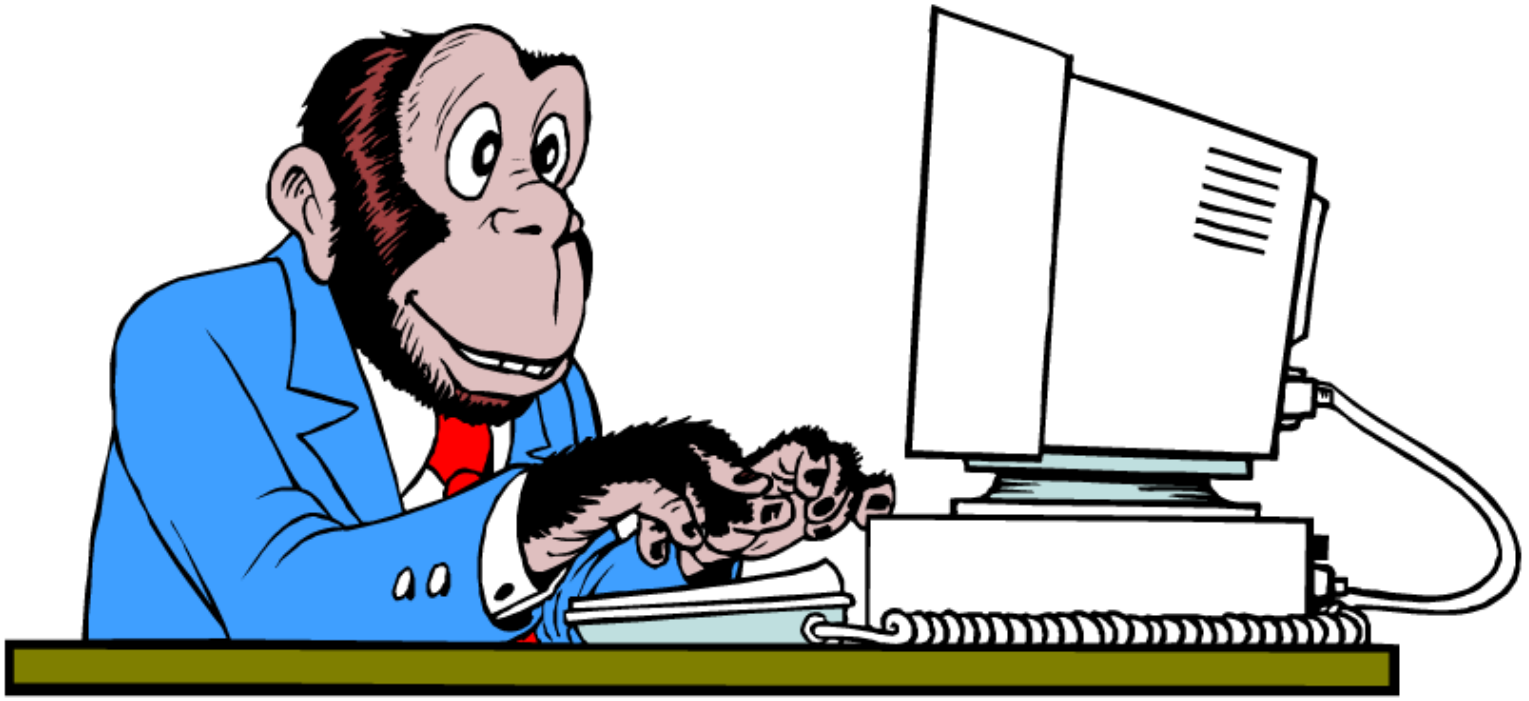
Http Parameter Pollution

- Cosa succede se si specifica più volte un parametro in una richiesta HTTP?
- Linguaggi e Programmi diversi si comportano differentemente
- Alcuni comportamenti sono molto interessanti..

Execute After Redirect

- I browser seguono le richieste di redirezione (HEADER HTTP 30x)
- Non è vietato specificare un corpo per le risposte che contengono una redirezione
- Nella risposta potrebbero essere contenuti dati sensibili

Always Remember



We Could Hire A Trained Monkey

To Do Your Job!

dSmart

POuL
have a lot of fun...

Cosa fare?

- Hack This Site
- Tower Of Hanoi ;-)
- OWASP
- RTFM

- Framework robusti
- Seguire community
- Pensare Agile
- Behaviour Driven Development
- Addestrare Scimmia

dSmart

POuL have a lot of fun...

<a>

- hackthissite.org
- portswigger.net
- owasp.org
- getfirebug.com
- google.com/chrome
- rubyonrails.org

Contatti

saten.r@gmail.com