Cryptography Wargame

MISTIC: Màster Interuniversitari en Seguretat de les Tecnologies de la Informació

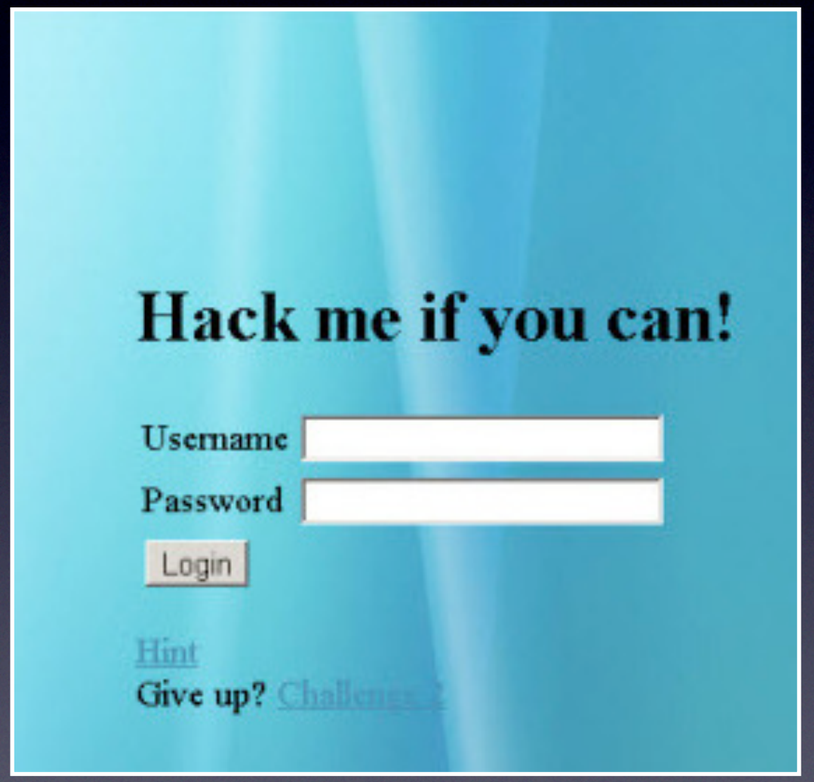
Alumne: Ramon Fuguet Roma
Tutor: Cristina Pérez Solà
21 de juny de 2013

Esquema Presentació

- Introducció
- Objectius
- Planificació
- Metodologia
- Descripció Plataforma
- Conclusions i Linies de Futur

Introducció

- Creació d'una plataforma de wargames criptogràfics
- Que és un wargame?
- Proves criptogràfiques

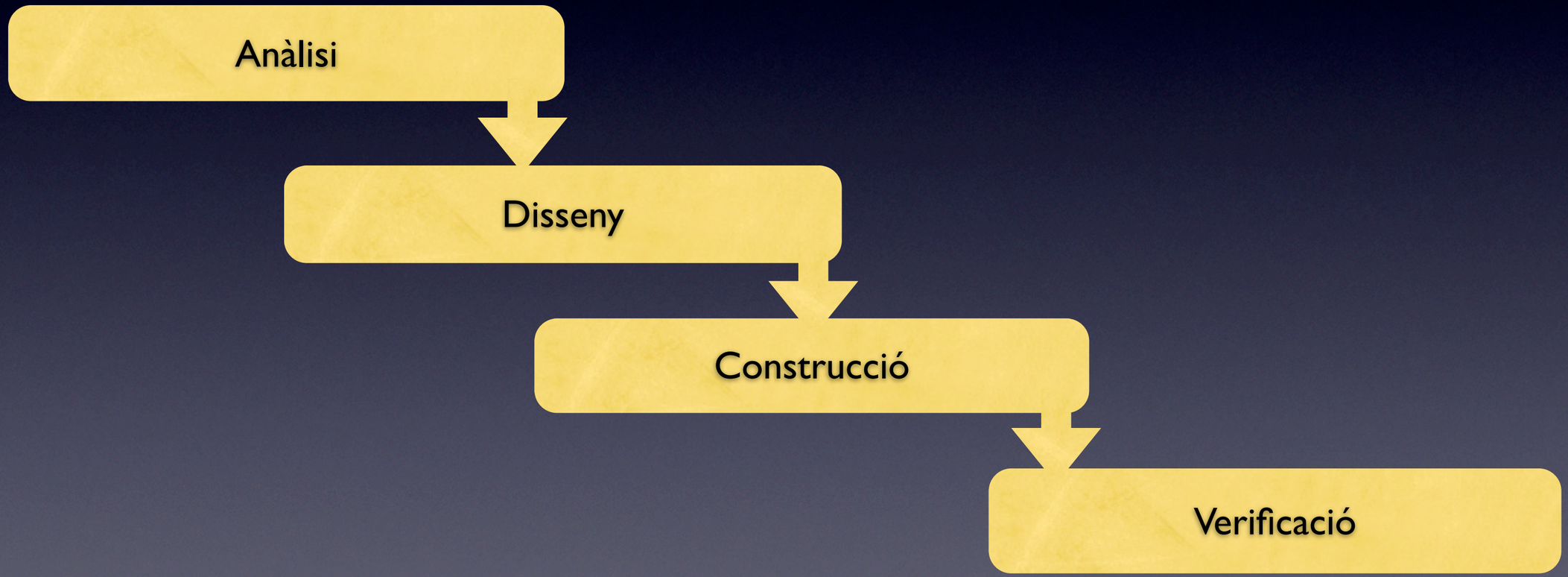


Objectius

- Creació d'un front-end
- Creació d'un back-end
- Securització de la plataforma
- Realització de proves criptogràfiques

Metodologia

Desenvolupament en cascada (clàssic)



Planificació

PAC2	18/03/13	19/04/13
Anàlisi i creació del model de...	18/03/13	19/03/13
[Back] - Gestió de wargames	20/03/13	21/03/13
[Back] - Gestió de quizzes	22/03/13	27/03/13
[User] - Registre i alta user	28/03/13	1/04/13
[User] - Login/Logout	2/04/13	3/04/13
[User] - Veure/editar perfil	4/04/13	8/04/13
[Front] - Llistat wargames	9/04/13	10/04/13
[Front] - Llistat de quizzes	11/04/13	15/04/13
[Front] - Realitzar un quiz	16/04/13	19/04/13
PAC3	22/04/13	22/05/13
[Backend] - Gestió usuaris	22/04/13	29/04/13
[Backend] - Login admin	30/04/13	1/05/13
[Front] - Llistat d'usuaris	2/05/13	6/05/13
[Front] - Estadístiques user	7/05/13	9/05/13
[Front] - Inici/Welcome	10/05/13	13/05/13
[Front] - FAQ	14/05/13	15/05/13
[Front] - Quiz - Control de br...	16/05/13	20/05/13
[Continguts]	21/05/13	22/05/13
Documentació	18/03/13	31/05/13

Eines

- Servidor web: Apache
- Servidor base de dades: MySQL
- Llenguatge de programació: PHP
- Llenguatge de plantilles: TWIG
- Llenguatge de programació client: Javascript + jQuery
- Rich Text Editor: CKEditor
- Documentació: LaTeX









Requeriments Funcionals

- El back-end ha de permetre a un administrador gestionar els wargames, les proves, els usuaris i mostrar-ne estadístiques.
- El front-end ha de permetre als usuaris registrar-se i resoldre les proves creades pels administradors.
- Les proves han de permetre múltiple opcions d'estil.
- Un wargame pot contindre múltiples proves i una prova pot pertànyer a múltiples wargames, podent ser ordenades.
- Les proves poden tenir pistes, que l'usuari pot desbloquejar gastant punts.

Requeriments Seguretat

- Control d'accés
- Registre segur
- Atacs web (SQL Injection, XSS, CSRF,...)
- Protecció via contrasenyes
- Atacs de força bruta

Conclusions

- Creació desde zero
- Objectius aconseguits
- Planificació
- Mecanismes de seguretat
- Documentació

Línies de Futur

- Més continguts
- Proves dinàmiques
- Usuaris poden enviar proves
- Sistema d'assoliments

Demostració