EUSTEMA

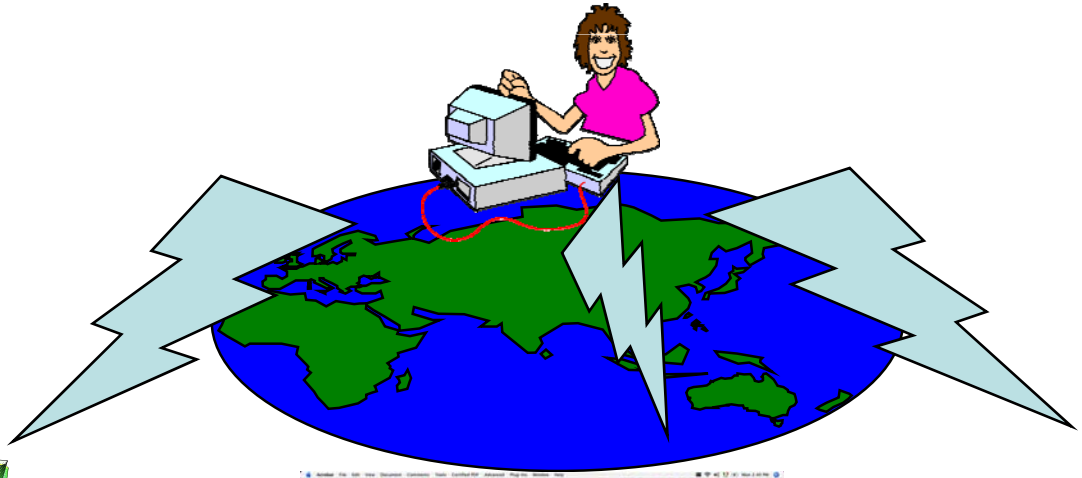
Direzione Tecnica /BU Sicurezza

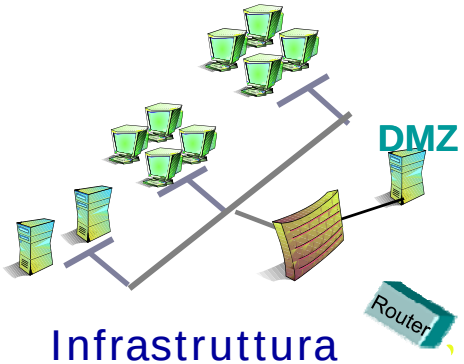
Dott. Marcello Pistilli Business Development Manager

Ethical Hacking, dallo sviluppo del software alla produzione: Code review e Pen testing

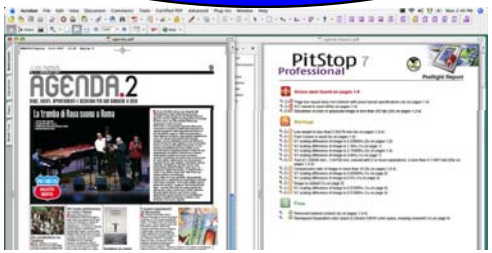
07/05/2008

FATTORE UMANO





Infrastruttura



web

endpoint

L’anello debole

All’interno del processo informatico, il fattore umano ha sempre una rilevanza determinante:

- è presente nella progettazione e sviluppo del software, sia di Sistema che Applicativo;
- quando il suo comportamento non è adeguato, diventa esso stesso un rischio all’interno dei processi informatici;
- incide sensibilmente nell’accettazione e nella consapevolezza della policy di sicurezza emanata dal management aziendale;
- è parte del processo di parametrizzazione e controllo degli apparati di rete e sicurezza;
- è presente sulla diffusione dei nuovi servizi informatici, aziendali e non.

È quindi l’anello debole della sicurezza informatica.

Aree di intervento

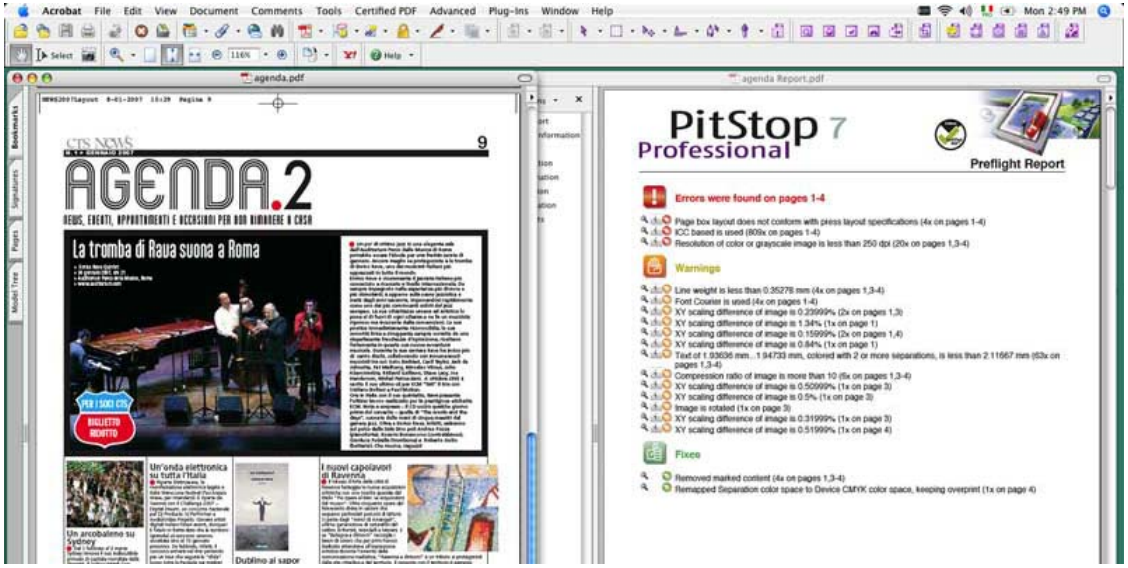
Occorre intervenire nella gestione delle opportune procedure e politiche di sicurezza, in fase di emissione ma ancor di più in fase di verifica.

Ragioniamo sui seguenti punti che riteniamo essere aree di intervento critiche:

- verifica delle vulnerabilità/conformità dell'infrastruttura;
- verifica delle vulnerabilità delle applicazioni legacy e web;
- verifica dell'accettazione delle policy emanate.

EUSTEMA

Verifica vulnerabilità applicazioni legacy e web



EUSTEMA

Verifica vulnerabilità applicazioni legacy e web

La sicurezza del software che viene sviluppato dalle aziende è un problema crescente.

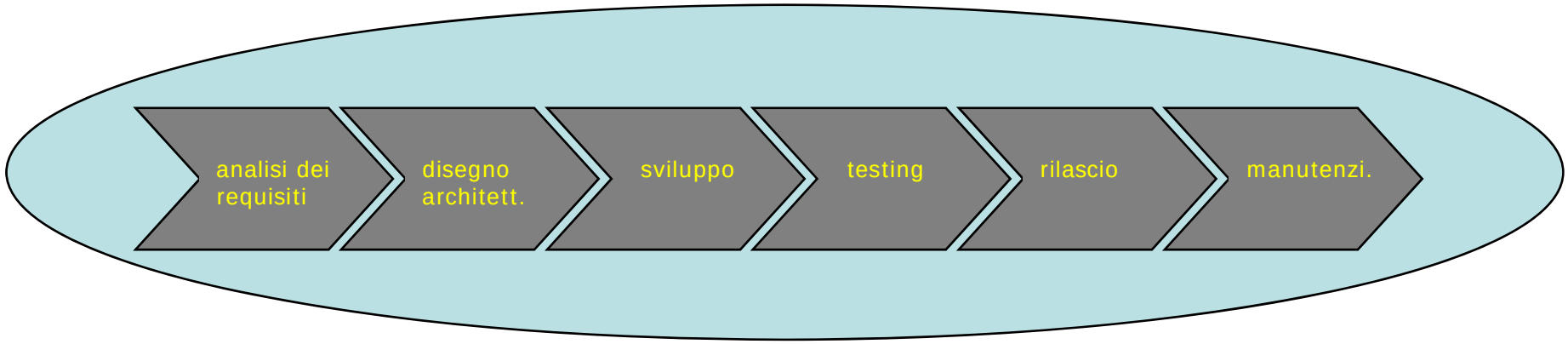
Sempre più si tende a globalizzare l'informazione per cui si richiede una maggiore attenzione alla sicurezza degli sviluppi applicativi. Una vulnerabilità applicativa web può permettere accessi indesiderati e non etici.

Nasce quindi l'esigenza di verificare preventivamente la sicurezza degli applicativi individuando e rimuovendo le vulnerabilità.

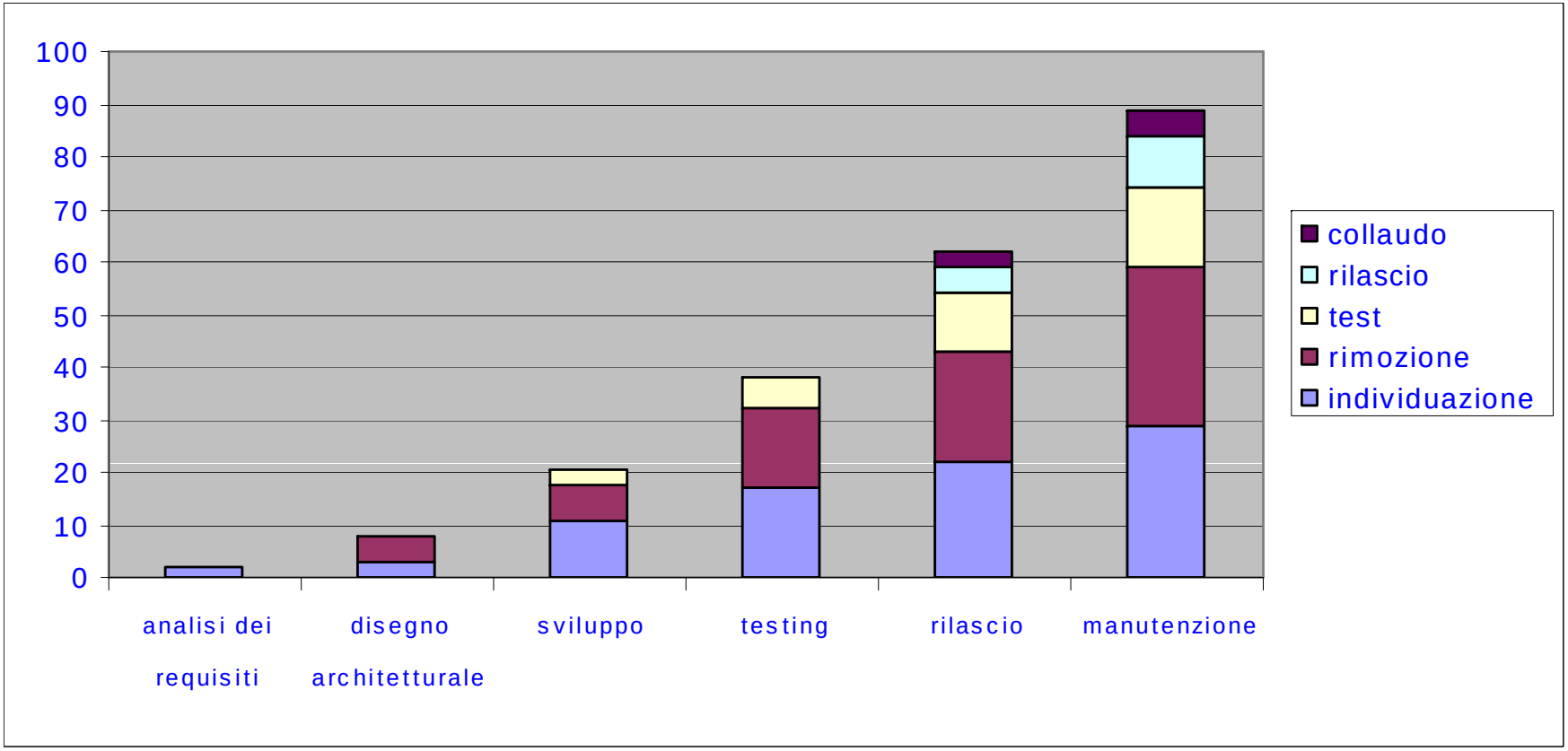
EUSTEMA

SDLC

ciclo di vita del software



I costi del rientro delle vulnerabilità



Incremento dei costi delle correzioni di sicurezza nel “SDLC”

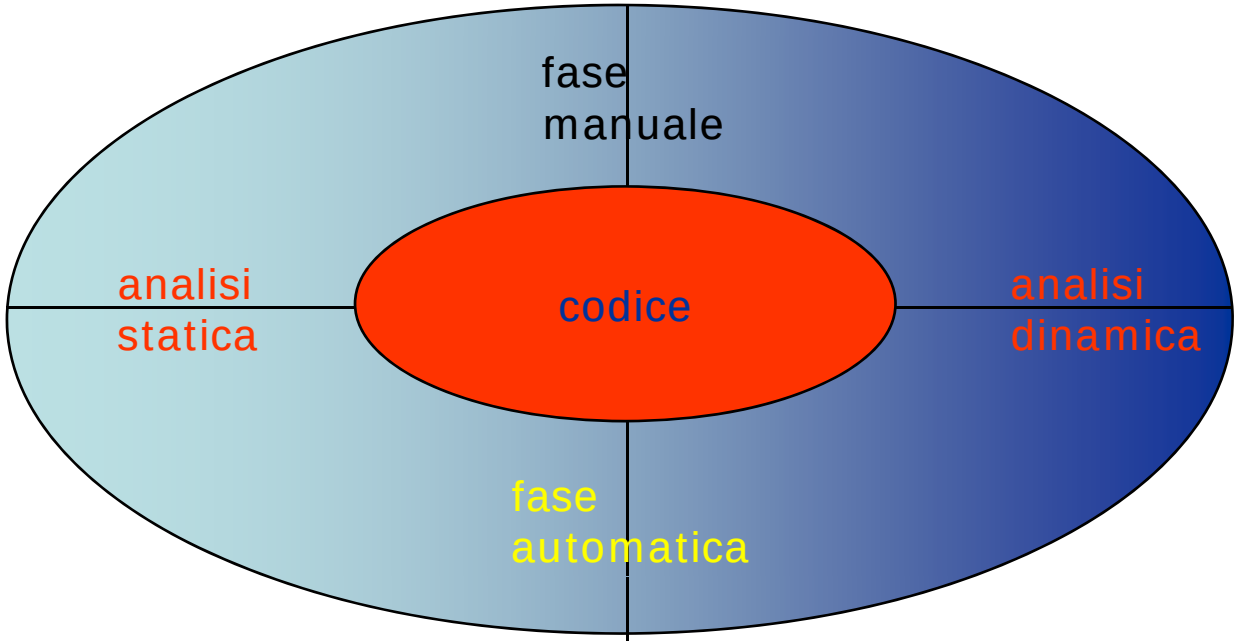
Il processo di verifica

È importante quindi definire un processo per la verifica della correttezza dello sviluppo software che deve strutturarsi attraverso:

1. seminari/corsi di formazione per lo sviluppo di software sicuro;
2. sviluppo di linee guide per la realizzazione di software sicuro;
3. verifica delle vulnerabilità applicative;
4. assistenza ai gruppi di sviluppo per i rientri alle vulnerabilità individuate e la pianificazione delle contromisure.

Fasi & metodologie

Fasi e metodologie per l'analisi delle vulnerabilità :

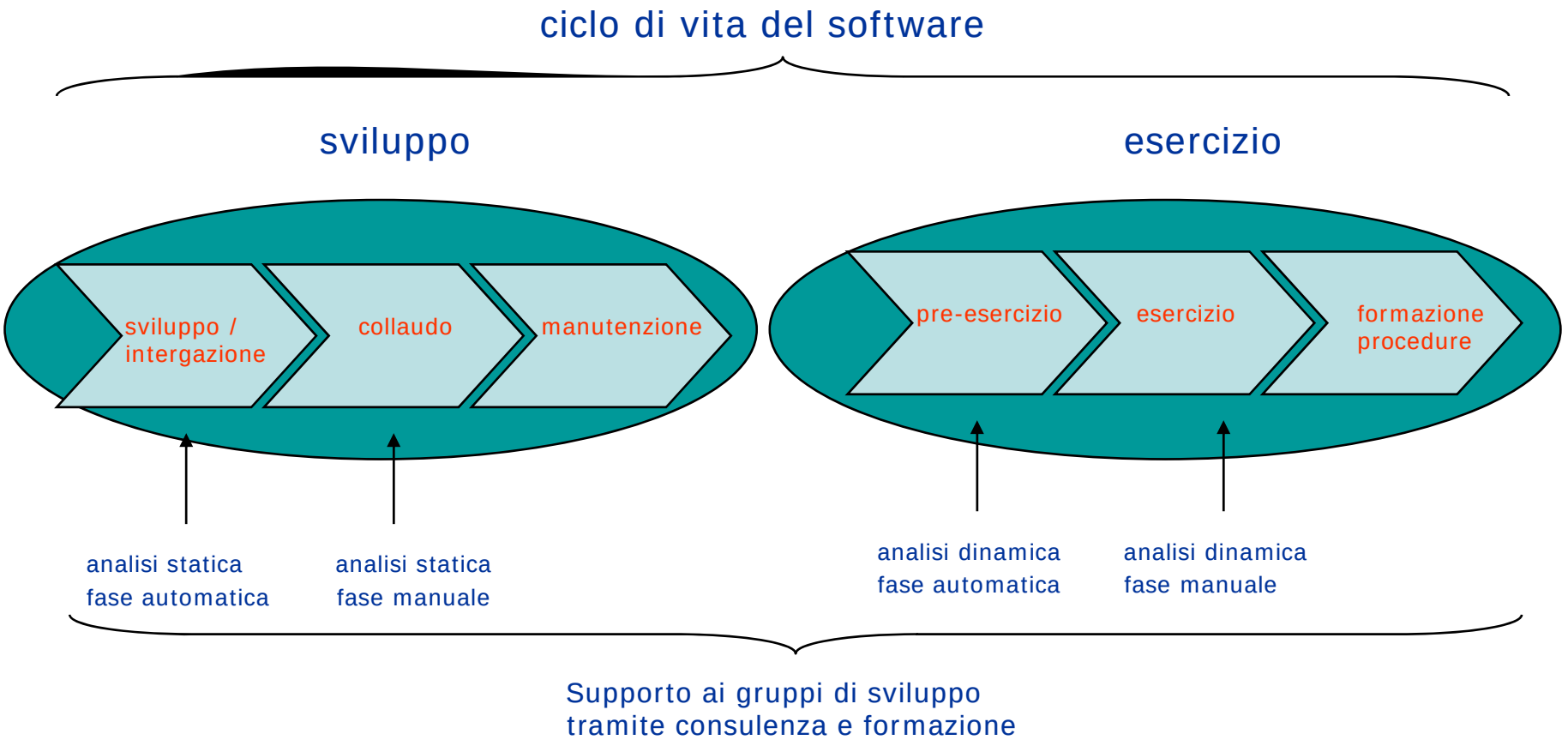


Analisi statica (Code Review)

Analisi dinamica
(Web Application Testing)

EUSTEMA

SDLC



EUSTEMA

Manuale vs automatico

Per le fasi presentate precedentemente esistono prodotti automatici, commerciali e non, atti a supportare le verifiche, essi sono:

Analisi statica o white box (Code Review)
(commerciali)
Fortify; Compuware DP SecurityChe; Ounce Labs Prexis
(open source)
Rough Auditing Tool for Security;

Analisi dinamica o black box (Web Application Penetration Testing)
(commerciali)
IBM Rational Appscan; HP Spydinamics
(open source)
Nikto; OWASP Pantera; OWASP WebScarab; BurpProxy

fonte (Luca Carettoni (luca.carettoni@ikkisoft.com))

Open Web Application Security Project (OWASP)

Il progetto Open Web Application Security Project (OWASP) è una organizzazione dedicata alla creazione e alla diffusione di una cultura per quanto riguarda la sicurezza delle applicazioni web.

portale → www.owasp.org

Alcuni progetti :

- Guida per la progettazione di applicativi web sicuri
- Strumenti di testing e revisione del codice
- OWASP Testing Guide v2 : descrive la metodologia OWASP per testare un'applicativo web
- OWASP code review
- OWASP Top10

OWASP TOP 10 1/4

1. Cross Site Scripting (XSS) - Esecuzione di script nel browser della vittima

Un caso reale: Lo scorso anno PayPal è stato obiettivo di alcuni attaccanti, i quali riuscirono a dirottare i visitatori di PayPal verso una pagina che avvertiva gli utenti che i loro account erano stati compromessi. Le vittime venivano dirottati verso un sito phishing che presentava un'interfaccia per l'inserimento dei dati di login, numeri di sicurezza sociali, e numeri di carta di credito. PayPal ha dichiarato di aver corretto la vulnerabilità nel Giugno del 2006.

2. Injection Flaws - Esecuzioni non volute di codice iniettato o alterazioni dei dati

Un caso reale: Nel Gennaio del 2006 alcuni hackers russi riuscirono a bucare il sito web del governo di Rhode Island rubando i dati relativi alle carte di credito. Gli hackers affermarono di aver sfruttato una falla di tipo SQL Injection per rubare 53000 numeri di carte di credito, anche se il fornitore del servizio di hosting affermò che i numeri di carte di credito rubate erano solo 4113

3. Malicious File Execution - Inclusione di codice ostile anche compromissione totale del server

Caso reale: Nel 2002 un programmatore aveva scoperto che il sito Guess.com era vulnerabile ad un attacco che permetteva di rubare dal database più di 200000 record contenenti i dati dei clienti, compresi nomi, numeri di carte di credito e date di scadenza. L'anno successivo, in seguito ad un'indagine da parte della Federal Trade Commission, Guess ha effettuato l'aggiornamento del suo sistema di sicurezza

Fonte: matteo lucchetti ABI lab & Zone h Jakub Maslowski

4. Insecure Direct Object Reference - Accesso non autorizzato ad oggetti (file, directory, database…)

Un caso reale: Nel 2000, un ufficio delle tasse australiano era stato compromesso da un utente che aveva cambiato il “tax ID” presente nell' URL. Ciò ha permesso all'utente di accedere ai dettagli di circa 17000 aziende. L'hacker ha poi contatto via e-mail le 17000 aziende per avvertirli della falla di sicurezza.

5.Cross Site Request Forgery - Il browser viene forzato ad eseguire azioni per conto della vittima che è loggata in quel momento

Un caso reale: Alla fine del 2005, un hacker conosciuto con lo pseudonimo di “Samy” era riuscito a stabilire più di un milione di contatti “amici” su MySpace. attraverso un worm, il quale in maniera automatica includeva in migliaia di pagine MySpace il messaggio “Samy is my hero”. L'attacco in se non era stato così dannoso, ma aveva dimostrato la potenza della combinazione di un attacco cross site scripting con quello di tipo cross site request forgery. Un altro caso venuto alla luce un anno fa aveva dimostrato come una vulnerabilità di Google poteva permettere a siti esterni di cambiare la lingua predefinita dell'utente Google

Fonte: matteo lucchetti ABI lab & Zone h Jakub Maslowski

6. Information Leakage and Improper Error Handling - Raccolta di informazioni sulla configurazione, il codice e lo stato interno delle applicazioni, da riutilizzare a supporto di altre modalità di attacco

Caso reale: L'information leakage va ben oltre la gestione degli errori, arrivando anche a violazioni dove i dati sensibili sono lasciati completamente in chiaro. La debacle di The ChoicePoint all'inizio del 2005 ne è una dimostrazione. I record di circa 163 mila clienti erano stato compromessi dopo che alcuni criminali finsero di essere dei clienti legittimi di ChoicePoint accedendo alle informazioni personali delle persone presenti nel database della compagnia. ChoicePoint ha successivamente limitato la sue vendite di prodotti informativi contenenti dati sensibili.

7. Broken Authentication and Session Management Reperimento - credenziali utente o amministratore e violazione privacy

Caso reale: Nel 2002, Microsoft aveva eliminato una vulnerabilità in Hotmail che poteva essere sfruttata attraverso dei javascript malevoli per rubare le password dell'utente. Il problema, segnalato da un rivenditore di prodotti per la rete, veniva sfruttato attraverso dei messaggi email contenenti un trojan che alterava l'interfaccia utente, forzando le vittime a reinserire la password che sarebbe poi stata inviata inconsapevolmente agli hackers.

Fonte: matteo lucchetti ABI lab & Zone h Jakub Maslowski

OWASP TOP 10 4/4

8. Insecure Cryptographic Storage - Perdita di dati riservati e violazione privacy

Caso Reale: Una falla di sicurezza nei sistemi della TJX aveva portato alla divulgazione di circa 45,7 milioni di numeri di carte di credito/debito. Un'indagine del governo canadese aveva imputato alla TJX di non aver aggiornato il suo sistema crittografico prima di essere stato oggetto di un'intercettazione elettronica nel Luglio del 2005

9. Insecure Communications - Comunicazioni non criptate

Caso reale: Ancora TJX. Un'indagine avevano portato alla conclusione che alcuni hackers avevano usato un'antenna telescopica ed un pc portatile per rubare i dati scambiati via wireless tra i dispositivi per il controllo dei prezzi, i registri di cassa, e i computer del magazzino.

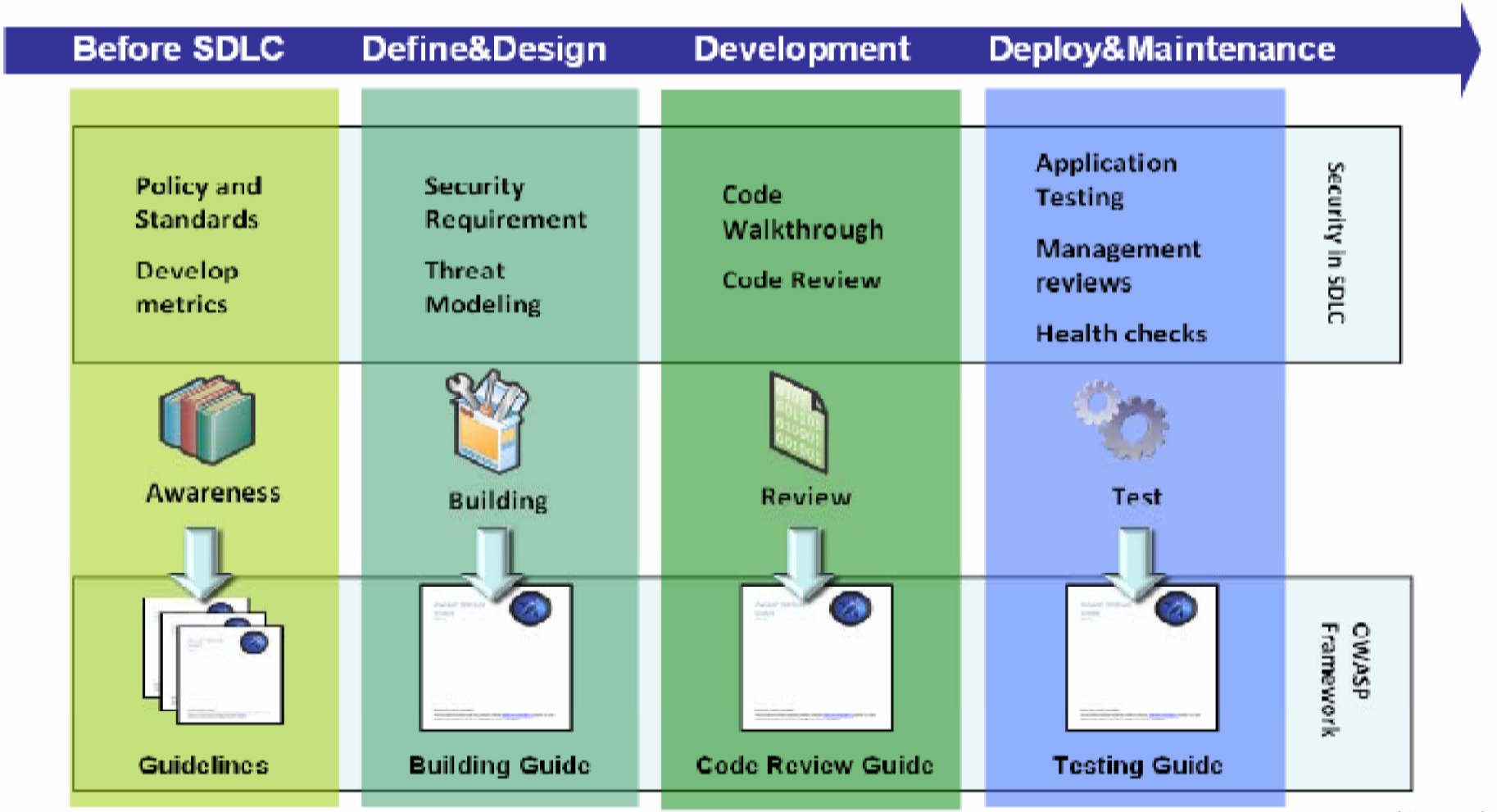
10. Failure to Restrict URL - Accesso non autorizzato ad URL non protetti, ma riservati

Caso Reale: Una falla nel sito web della MacWorld Conference aveva permesso agli utenti di ottenere dei pass “Platinum” del valore di circa 1700 dollari, oltre ad uno speciale accesso al keynote di Steve Jobs, il tutto gratuitamente. La falla era presente nel codice lato client, invece che lato server, che verificava i privilegi dell'utente. Ciò permetteva a chiunque di ottenere dei pass gratuiti manipolando il codice javascript dal browser.

Fonte: matteo lucchetti ABI lab & Zone h Jakub Maslowski

EUSTEMA

SDLC e OWASP



Fonte: matteo meucci OWASP it

Cultura della sicurezza

Emanare policy e procedure chiare ed applicabili, promuovere attraverso seminari e corsi di "informazione" la crescita individuale e collettiva della sicurezza. Sensibilizzare il personale tutto al rispetto delle policy e delle procedure per una sempre maggiore consapevolezza alla sicurezza,

al fine di

creare una cultura della sicurezza

Eustema e la Sicurezza

Eustema ha una pluriennale esperienza nell'Information Security.

La nascita della Business Unit ha definito e attualizzato un'offerta che caratterizza Eustema nel mercato, tenendo presente le peculiarità delle risorse e le competenze già presenti in azienda.

Business Unit
Information Security

SECURE THE HUMAN FACTOR


EUSTEMA
Eustema S.p.A.
00195 Roma · Via Carlo Mirabello, 7
Tel. +39.06.372721 - +39.06.374931 · Fax +39.06.37351735
info@eustema.it
www.eustema.it
RINA
ISO 9001 - SA 8000
Certified integrated Systems