

SQL Injection
Homograph Attack
Cross-Site Scripting

Applicazioni di Rete - M. Ribaudò - DISI

SQL Injection

"SQL Injection is a technique for exploiting web applications that use client-supported data in SQL queries without stripping potentially harmful characters first"

Applicazioni di Rete - M. Ribaudò - DISI

SQL Injection

```
$sql = "SELECT * FROM client WHERE  
username='\" . $username . \"' AND \"  
password='\" . $password . \"\"";
```

Esempi

```
SELECT * FROM client WHERE  
username='Rossi' AND password='****'
```

```
SELECT * FROM client WHERE  
username='Rossi' OR 1=1 --
```

Commento in molti DBMS!

Applicazioni di Rete - M. Ribaudò - DISI

SQL Injection

Area ad accesso riservato ...

Username
Password

Ecco i tuoi dati

Nome	Cognome	VISA	Scadenza	Modifica
Mario	Rossi	1111	13/05/2004	modifica

[Esempio \(in ASP\)](#)

Applicazioni di Rete - M. Ribaudò - DISI

SQL Injection

- Username:rossi, Password:*****
- Username:verdi, Password:*****
- Username: ' OR ''='
Password: ' OR ''='

```
SELECT * FROM client WHERE  
username=' ' OR ''=' AND  
password=' ' OR ''=' true !!
```

Applicazioni di Rete - M. Ribaudò - DISI

SQL Injection

Area ad accesso riservato ...

Username
Password

Ecco i tuoi dati

Nome	Cognome	VISA	Scadenza	Modifica
Mario	Rossi	1111	13/05/2004	modifica
Gianni	Bianchi	2222	12/06/2005	modifica
Paolo	Verdi	3333	11/03/2005	modifica
Luca	Bruni	4444	18/11/2004	modifica

GAAAAAASP !!!!

[Esempio \(in ASP\)](#)

Applicazioni di Rete - M. Ribaudò - DISI

SQL Injection

- Username: `' ; DROP TABLE clienti--`

(per Transact-SQL, usato da SQL server)

- userId: `123; shutdown--`

Per saperne di più
www.nextgenss.com/papers/advanced_sql_injection.pdf

Applicazioni di Rete - M. Ribaudò - DISI

Soluzione?

- **Validare** sempre molto bene i dati in **input** usando, se possibile, le **espressioni regolari**
- **Suggerimento**: considerate quali sono i dati validi e rifiutate tutto il resto ...

Applicazioni di Rete - M. Ribaudò - DISI

Homograph Attack

- Il problema sorge a causa dell'**equivalenza visiva** tra le lettere di alfabeti diversi
- Siamo abituati a confondere 0 (zero) con O (o maiuscola) ma esistono altri caratteri che pur essendo visivamente simili, sono semanticamente molto diversi!
- Nel **cirillico** ci sono per esempio le lettere a, c, e, p, y, x, ...

Applicazioni di Rete - M. Ribaudò - DISI

Homograph Attack

- John Hacker "imita" il nome del sito web della vostra banca
- Installa un proxy che instrada in modo trasparente tutte le vostre richieste alla vostra banca
- "Inserisce" il suo link nei portali più importanti

Applicazioni di Rete - M. Ribaud - DISI

Homograph Attack

- Poichè la maggior parte delle volte clicchiamo sui link e non li scriviamo direttamente nella location bar
- ... John Hacker ha accesso a login e password dei clienti della banca ☺
- Per saperne di più
www.cs.technion.ac.il/~gabr/papers/homograph_full.pdf

Applicazioni di Rete - M. Ribaud - DISI

Rappresentazione canonica

- "Do not make any security decision based on the name of a resource, especially a filename"
- Esistono **nomi diversi** per identificare la stessa risorsa
/home/stud/2000s000/index.html
~2000s000/index.html
/home/./home/stud/ ...
- Il nome canonico è quello più "semplice" (lo standard)

Applicazioni di Rete - M. Ribaud - DISI

Bypassing Napster Name Filtering

- Canonicalization bug ☺
- Il blocco delle canzoni è stato fatto sulla base del nome della canzone e non ci è voluto molto a bypassare il filtro ...
- .. changes the file names of songs inside a person's Napster directory into a spelling inspired by **Pig Latin**. The Radiohead song "Karma Police," for example, would be transformed into "armaK oliceP."

Applicazioni di Rete - M. Ribaudo - DISI

Cross-Site Scripting (XSS)

"An intruder causes a legitimate web server to send a page to a victim's browser that contains malicious scripts chosen by the intruder"

Applicazioni di Rete - M. Ribaudo - DISI

Cross-Site Scripting (XSS)

Cross site scripting (also known as XSS) occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it.

The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in **HEX** (or other encoding methods) so the request is less suspicious looking to the user when clicked on.

Applicazioni di Rete - M. Ribaudo - DISI

Cross-Site Scripting (XSS)

"What can I do to protect myself?"

This is a simple answer. **Never trust user input and always filter metacharacters**. This will eliminate the majority of XSS attacks. Converting < and > to < and > is also suggested when it comes to script output.

Filtering < and > alone will not solve all cross site scripting attacks and it is suggested you also attempt to filter out (and) by translating them to (and), and also # and & by translating them to # (#) and & (&).

Applicazioni di Rete - M. Ribaudò - DISI

Cross-Site Scripting (XSS)

▪ Come posso verificare se il mio codice è attaccabile tramite XSS?

1. Scrivo tutti gli entry point dell'applicazione web (campi di un modulo, querystring, HTTP headers, cookies, dati in arrivo da un database)
2. Seguo ciascun dato nel suo "attraversamento" dell'applicazione
3. Verifico se viene restituito in output
4. Se sì, verifico che ogni dato sia "ripulito" da meta-caratteri pericolosi

Applicazioni di Rete - M. Ribaudò - DISI

Web cookies: not just a privacy risk

- DoubleClick (e altri) usa i cookie per tracciare gli utenti e per mandare messaggi pubblicitari mirati. Ma questo non è un vero pericolo ...
- Il pericolo nasce quando i cookie vengono usati per l'**autenticazione** e, soprattutto, quando vengono fornite informazioni personalizzate ...

Applicazioni di Rete - M. Ribaudò - DISI

Web cookies: not just a privacy risk

- La specifica dei cookie si basa infatti su un'idea di **collaborazione tra browser e server** e molti siti non salvano i cookie in modo sicuro
- Diventa facile "forgiare" un nuovo cookie per impersonare un altro utente
- Quindi, è opportuno **non affidarsi mai** al solo meccanismo dei cookie per restituire **informazioni sensibili**

Applicazioni di Rete - M. Ribaudo - DISI

Progettare un sito web

Interattivo e Usabile

Applicazioni di Rete - M. Ribaudo - DISI

Il team

- I siti web professionali non sono sviluppati da una sola persona, ma sono il frutto di un **lavoro di gruppo**. Ad esempio:

- ✓ Project Manager
- ✓ Client Representative
- ✓ Technology Researcher

Applicazioni di Rete - M. Ribaudo - DISI

Il team

✓ Content Developer / Writer

Sa scrivere!!! e deve scegliere il "tono" adeguato per il web

✓ Information Architect

Deve pianificare la navigazione del sito e le caratteristiche interattive di base

✓ Graphic Designer

È il responsabile dell'identità visiva del sito, del layout delle pagine ... crea il **look & feel**

Applicazioni di Rete - M. Ribaudo - DISI

Il team

✓ Multimedia Designer

È il responsabile dei contenuti audio/video

✓ Technical Designer

Sceglie le tecnologie per la realizzazione delle caratteristiche interattive. Deve conoscere i **linguaggi di programmazione** e, possibilmente, **principi di interazione con l'utente** e di **progettazione di interfacce**

Applicazioni di Rete - M. Ribaudo - DISI

Il team

✓ Content Producer

Deve convertire i contenuti originali e le immagini in pagine HTML. Lavora a fianco del programmatore

✓ System Administrator

Si occupa della gestione del server web, del DBMS server, ... dei backup e della sicurezza

✓ Test/Focus Group Coordinator

Si occupa dell'analisi dell'**usabilità del sito** dal punto di vista dell'utente e dal punto di vista della **robustezza del codice**

Applicazioni di Rete - M. Ribaudo - DISI

Usabilità?

- Why
- Who
- Where

- What
- When

Applicazioni di Rete - M. Ribaudo - DISI

Why?

**"Usability rules the Web.
Simply stated if the customer
can't find a product she will
not buy it. [...] It is so easy
to go elsewhere; all the
competitors in the world are
but a mouseclick away"**

Jakob Nielsen: Designing Web Usability

Applicazioni di Rete - M. Ribaudo - DISI

Who?

Noi stessi, gli utenti

Applicazioni di Rete - M. Ribaudo - DISI

Where?

Sul web ma non solo,
l'usabilità coinvolge le
nostre esperienze con ogni
tipo di artefatto

Applicazioni di Rete - M. Ribaudo - DISI

What?

Non esiste una
definizione univoca

Applicazioni di Rete - M. Ribaudo - DISI

Usabilità

ISO 9241

La efficacia e soddisfazione
con cui specificati utenti
raggiungono specificati
obiettivi in particolari
ambienti

Applicazioni di Rete - M. Ribaudo - DISI

Usabilità

Efficacia

La accuratezza e la completezza con cui gli utenti possono raggiungere determinati obiettivi in particolari ambienti

Applicazioni di Rete - M. Ribaudò - DISI

Usabilità

Efficienza

Le risorse spese in relazione all'accuratezza e alla completezza degli obiettivi raggiunti

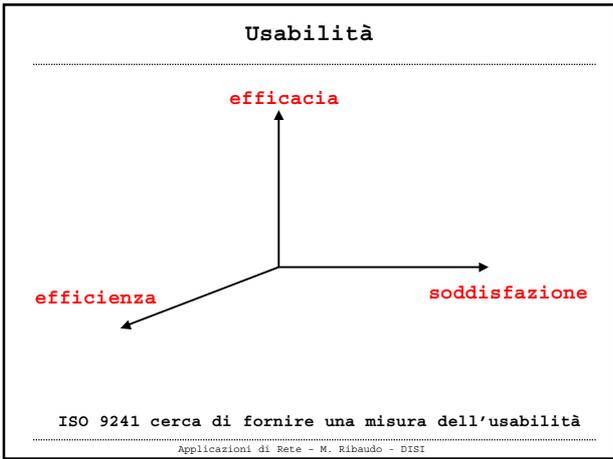
Applicazioni di Rete - M. Ribaudò - DISI

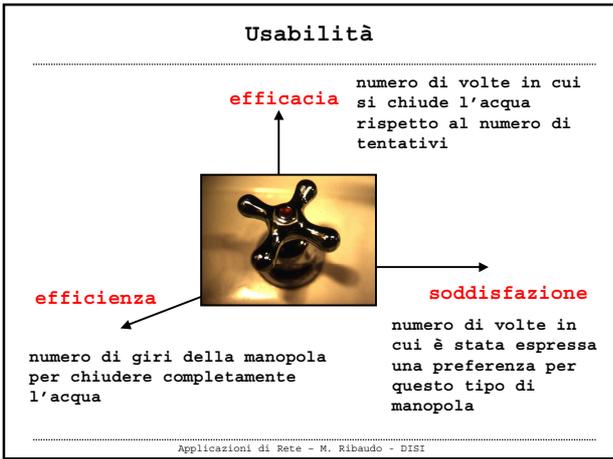
Usabilità

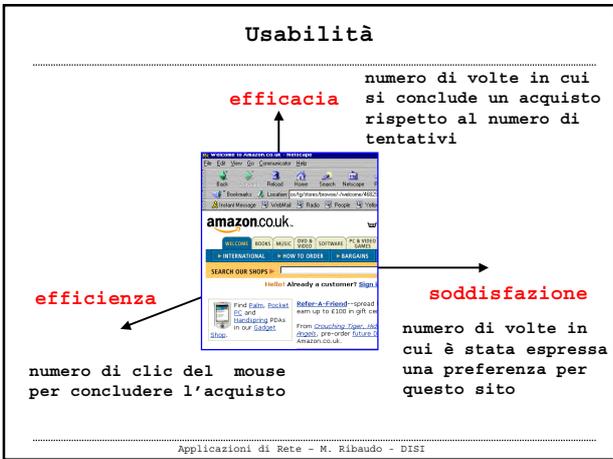
Soddisfazione

Il comfort e l'accettabilità del sistema di lavoro per i suoi utenti e per altre persone influenzate dal suo uso

Applicazioni di Rete - M. Ribaudò - DISI







Principi di usabilità

Non esiste un "catalogo" di principi di usabilità per le applicazioni interattive

Vediamo alcuni "suggerimenti" validi in generale, che vanno reinterpretati per il web

Applicazioni di Rete - M. Ribaudo - DISI

Riconoscere vs Ricordare



Rendere gli oggetti e le azioni visibili

Applicazioni di Rete - M. Ribaudo - DISI

Esplicitare le affordance



Segnali che ci indicano come usare gli oggetti

Applicazioni di Rete - M. Ribaudo - DISI

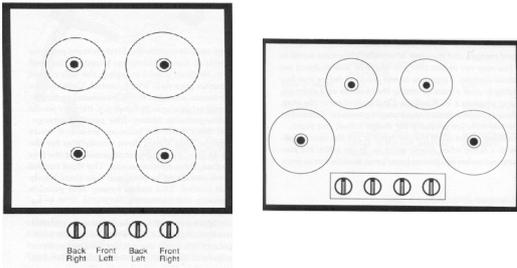
... less is more ...

Si deve cercare di
minimizzare il carico
cognitivo dell'utente

7 +/- 2

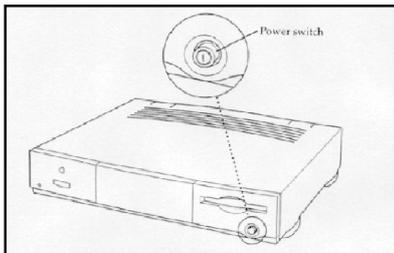
Applicazioni di Rete - M. Ribaud - DISI

Usare mapping corretti



Applicazioni di Rete - M. Ribaud - DISI

Usare mapping corretti



Applicazioni di Rete - M. Ribaud - DISI

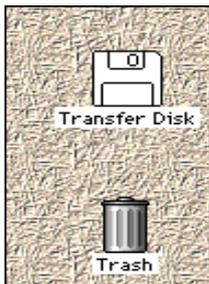
Essere consistenti

Non usare sinonimi

**Attenzione all'uso delle
metafore**

Applicazioni di Rete - M. Ribaudo - DISI

Esempio di metafora non consistente



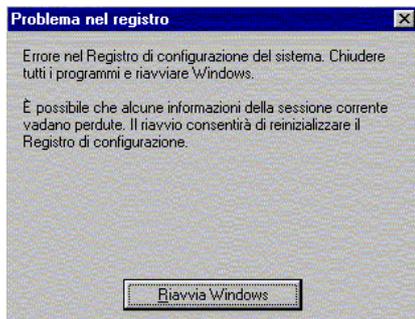
Applicazioni di Rete - M. Ribaudo - DISI

Usare il linguaggio dell'utente

**Chi usa l'interfaccia
non deve conoscere
il gergo informatico**

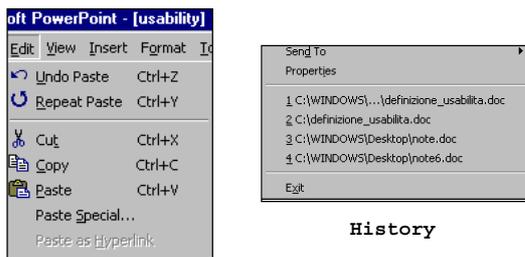
Applicazioni di Rete - M. Ribaudo - DISI

Usare il linguaggio dell'utente



Applicazioni di Rete - M. Ribaudò - DISI

Meccanismi di azione efficienti



Acceleratori

History

Applicazioni di Rete - M. Ribaudò - DISI

Gestire gli errori

Se possibile prevenire gli errori, altrimenti fornire meccanismi di Undo

Applicazioni di Rete - M. Ribaudò - DISI

Fornire uscite chiare

Cancel
Exit

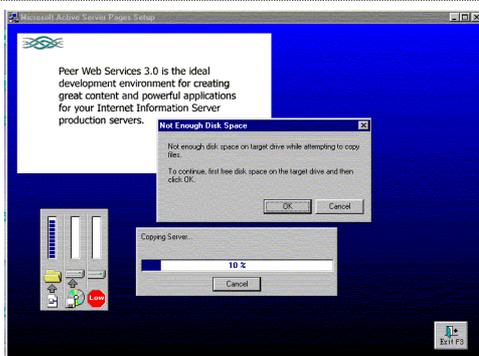
Applicazioni di Rete - M. Ribaudo - DISI

Rendere visibile lo stato del sistema

Fornire feedback

Applicazioni di Rete - M. Ribaudo - DISI

Rendere visibile lo stato del sistema



Applicazioni di Rete - M. Ribaudo - DISI

Fornire informazioni persistenti

La comunicazione vocale
non è persistente,
quella visiva sì

Applicazioni di Rete - M. Ribaudo - DISI

Usabilità

- Why
- Who
- Where

- What
- **When**

Applicazioni di Rete - M. Ribaudo - DISI

When?

Secondo la disciplina della
Usability Engineering - che pone
l'enfasi sui criteri che devono
essere adottati per valutare un
prodotto rispetto alla sua
usabilità - questa analisi deve
essere fatta a partire **dalle fasi
iniziali del ciclo di sviluppo
del software ...**

Applicazioni di Rete - M. Ribaudo - DISI

Come si valuta?

- Interviste
- Focus Group
- Analisi di log
- Test in laboratorio
- ...

... per quanto riguarda il vostro progetto, chiedete ai compagni di "fare un giro" nel vostro sito ed osservate (magari senza intervenire) le loro difficoltà e i loro errori

Applicazioni di Rete - M. Ribaud - DISI
