

Agenda

- ✓ Concetti base
- ✓ Esempio reale (SQL code injection)
- ✓ Come cambia lo scenario della sicurezza
- ✓ Sviluppare applicazioni sicure
- ✓ Acquistare applicazioni sicure

Concetti base

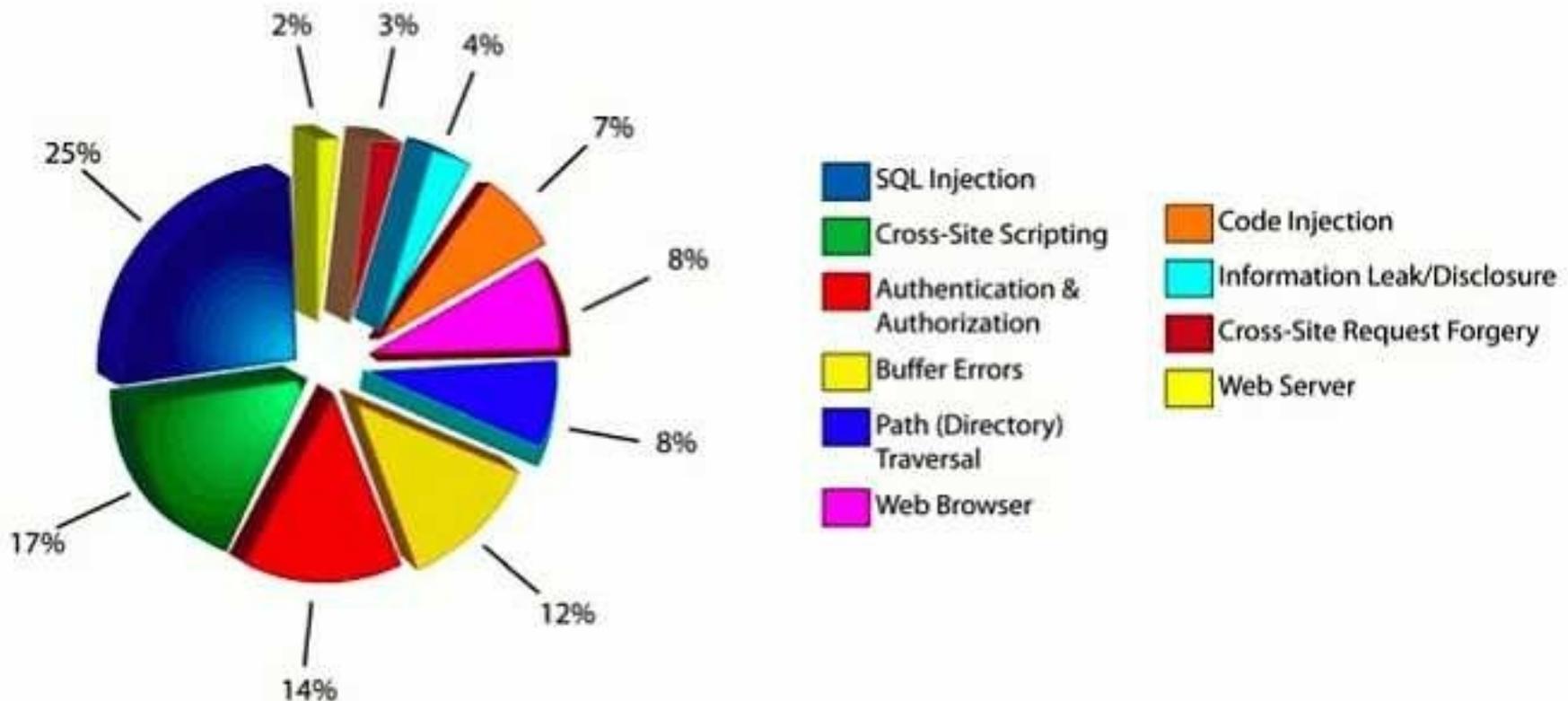
- ✓ Servizi web esposti al mondo
- ✓ Applicazioni custom complesse
- ✓ Struttura a tre livelli (web, application, DB)
- ✓ SSL non aiuta, anzi !
- ✓ Falso senso di sicurezza

Errori più comuni

- ✓ Fidarsi dell'input dell'utente
- ✓ Caratteri speciali non filtrati
- ✓ Output HTML non filtrato
- ✓ Eccesso permessi alle applicazioni
- ✓ Commenti o versioni obsolete
- ✓ Consentire il listing delle directory
- ✓ Non gestire errori
- ✓ Fidarsi

Esempio reale - SQL code injection

Web Vulnerabilities by Class
Q1-Q2 2009



Esempio reale - SQL code injection



Inserisci i tuoi dati

Utente:

Password:

Entra >

Esempio reale - SQL code injection

```
<form action='login.php' method='post'>  
  Username: <input type='text'  
name='user' />  
  Password: <input type='password'  
name='pwd' />  
  <input type='submit' value='Login' />  
</form>
```

Esempio reale - SQL code injection

```
<?php
$query = "SELECT * FROM users WHERE
user='".$_POST['user']."' AND pwd='".$_
_POST['pwd']."'";
$sql = mysql_query($query,$db);
if(mysql_affected_rows($sql)>0)
{
// Consenti l'accesso
}
?>
```

Esempio reale - SQL code injection

```
/login.php?user=pippo&pwd=pluto
```

```
"SELECT * FROM users WHERE user='".  
$_POST['user']."' AND pwd='".  
$_POST['pwd'].""
```

```
select * from users where user=  
'pippo' and pwd='pluto'
```

Esempio reale - SQL code injection

```
/login.php?user=' or 1=1; -- &pwd=
```

```
"SELECT * FROM users WHERE user='".  
$_POST['user']."' AND pwd='".  
$_POST['pwd'].""
```

```
select * from users where user=' ' or  
1=1; -- 'and pwd=' '
```

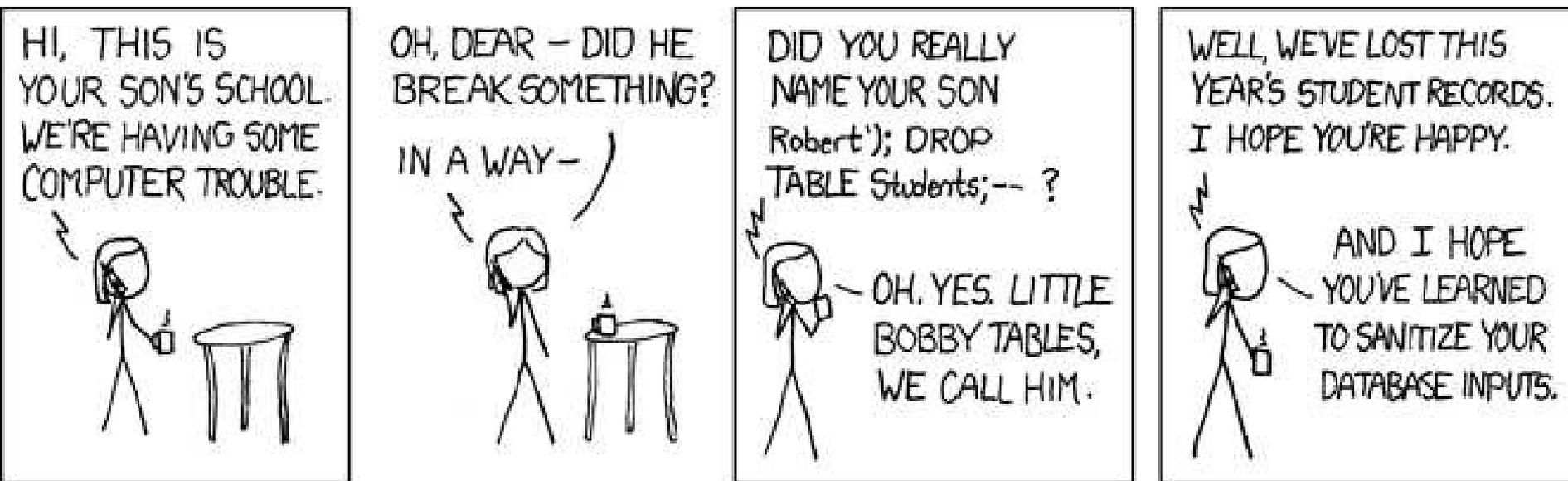
Esempio reale - SQL code injection

```
/login.php?user=' ; drop table users ;  
-- &pwd=
```

```
"SELECT * FROM users WHERE user='".  
$_POST['user']."' AND pwd='".  
$_POST['pwd'].""
```

```
select * from users where user=' '  
drop table users; -- 'and pwd=' '
```

Esempio reale - SQL code injection



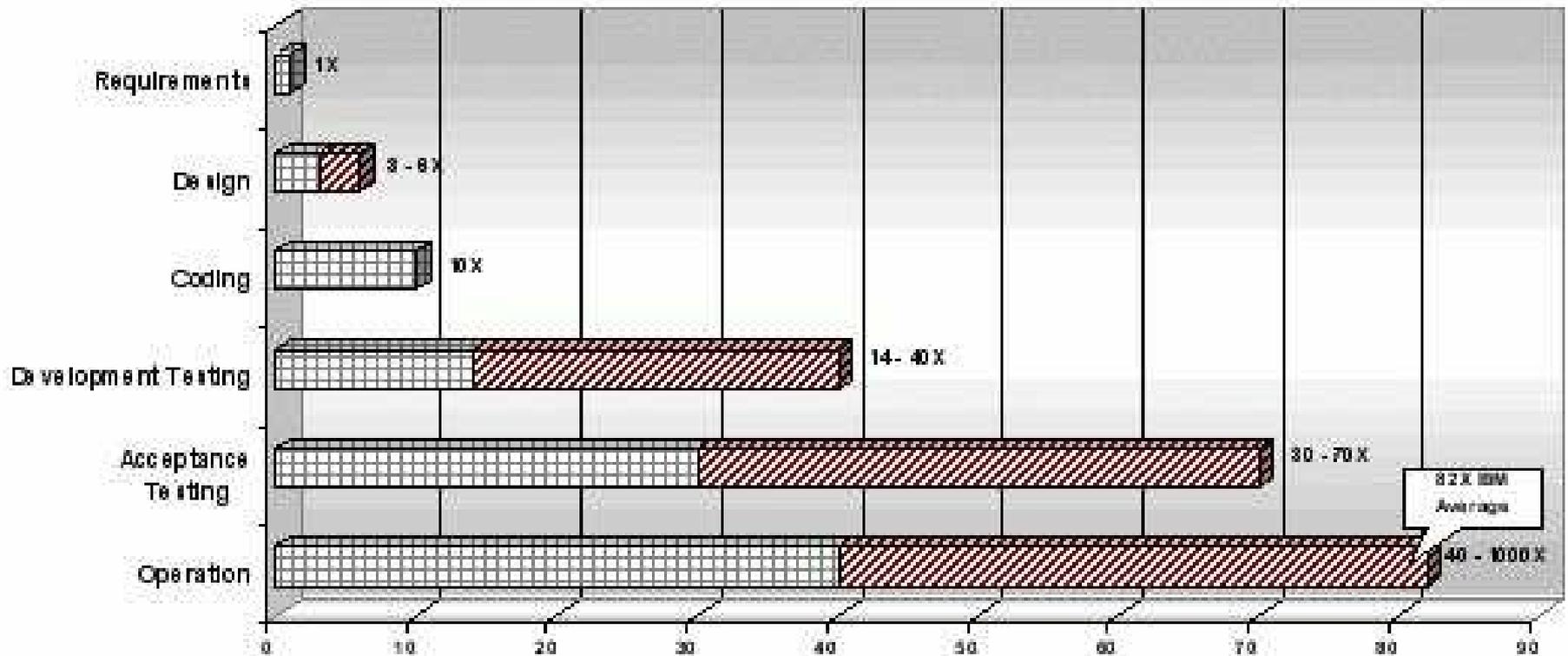
<http://xkcd.com/327/>

Lo scenario della sicurezza

- ✓ Non esistono tecniche di audit automatico veramente affidabili
- ✓ Analisi delle variazioni delle “baseline”
- ✓ Analisi del codice sorgente
- ✓ Analisi “greybox”
- ✓ Analisi “blackbox”
- ✓ Ambienti di test separati interni

Sviluppare applicazioni sicure

Relative Costs to Fix an Error



Sviluppare applicazioni sicure

- ✓ Identificare i security requirement
- ✓ Liste di controllo
- ✓ Linee guida
- ✓ Generare “abuse case”
- ✓ Generare security patterns
- ✓ Simulare modelli di attacco
- ✓ Framemork di sviluppo sicuro
- ✓ KISS

Acquistare applicazioni sicure

- ✓ Semplice da usare e ricca di funzioni
- ✓ Prezzo ragionevole
- ✓ Sicura

Acquistare applicazioni sicure

- ✓ Semplice da usare e ricca di funzioni
- ✓ Prezzo ragionevole
- ✓ Sicura

... Puoi sceglierne due su tre ...

Acquistare applicazioni sicure

(applicazioni custom)

- ✓ Predisporre un disciplinare
- ✓ Imporre degli standard
- ✓ Liste di controllo
- ✓ Security testing
- ✓ Coinvolgere terze parti

(applicazioni off-the-shelf)

- ✓ FOSS oppure ... devi fidarti

Acquistare applicazioni sicure

2. Applicabilità

3. Principi generali

3.1 Applicazioni sicure

3.2 Architettura applicativa

4. Design e sviluppo dell'applicazione

4.1 Analisi dei requisiti e design

4.2 Autenticazione

4.3 Autorizzazione

4.4 Validazione dei dati

4.5 Gestione delle sessioni utente

4.6 Logging

4.7 Crittografia e disponibilità dei dati

5. Test, deployment e gestione dell'applicazione

6. Requisiti minimi previsti dalla normativa vigente

Appendice A: Glossario

Appendice B: Liste di controllo

B.1 Design e sviluppo dell'applicazione

B.2 Test, deployment e gestione dell'applicazione

Acquistare applicazioni sicure

Appendice B: Liste di controllo

B.1 Design e sviluppo dell'applicazione

Analisi dei requisiti e design	
Nell'analisi dei requisiti è stato considerato il valore dei dati e delle informazioni trattate dall'applicazione	<input type="checkbox"/>
L'applicazione viene utilizzata per il trattamento di dati personali	<input type="checkbox"/>
L'applicazione viene utilizzata per il trattamento di dati sensibili e/o giudiziari	<input type="checkbox"/>
È stata eseguita l'analisi dei rischi incombenti sui dati	<input type="checkbox"/>
Sono stati considerati i vincoli architetturali e tecnologici imposti dall'infrastruttura esistente (servizi, porte, protocolli, tecnologie, ecc.)	<input type="checkbox"/>
Sono state documentate le porte ed i protocolli di comunicazione utilizzati dall'applicazione	<input type="checkbox"/>
Sono stati definiti i requisiti hardware e software necessari per il corretto funzionamento dell'applicazione	<input type="checkbox"/>
Sono stati previsti meccanismi di autenticazione degli utenti	<input type="checkbox"/>
Sono stati previsti meccanismi di autorizzazione e profilatura utenti	<input type="checkbox"/>
Sono stati previsti meccanismi di validazione dei dati in ingresso e in uscita	<input type="checkbox"/>
Sono stati previsti meccanismi di gestione sicura delle sessioni utente	<input type="checkbox"/>
Sono stati previsti meccanismi di conservazione e gestione dei log	<input type="checkbox"/>
Sono stati previsti meccanismi di disponibilità dei dati	<input type="checkbox"/>
Sono stati previsti meccanismi di cifratura dei dati	<input type="checkbox"/>

Per ulteriori informazioni

- + Owasp
- + W3 security guidelines
- + Web Application Security Consortium
- + Are You Part Of The Problem?
- + Top 25 Most Dangerous Progr. Errors
- + Google
- + Wikipedia