



Internet Banking e Web Security

Giorgio Fedon

Chief Operation Officer
Minded Security S.r.l.

giorgio.fedon@mindedsecurity.com

OWASP-Day II
Università "La Sapienza", Roma
31st, March 2008

Copyright © 2008 - The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the GNU Free Documentation License.

The OWASP Foundation
<http://www.owasp.org>

Alcune informazioni sul Relatore

Background

- ▶ Chief Operation Officer @ Minded Security
- ▶ Penetration Testing, Code Review Formazione
- ▶ Principali attività di testing su portali Finance
- ▶ Pubblicazione Advisory e Articoli di Ricerca

Owasp Foundation

- ▶ Testing Guide Contributor
- ▶ Membro di Owasp Italian Chapter



Introduzione



Financial Web Security Incidents 2007

- 29 January 2007
 - ▶ Vulnerabilità in una Banca Brasiliana permette di accedere ai dati di altri utenti
- 10 Ottobre 2007
 - ▶ Commerce Bank, furto di informazioni tramite SQL Injection
- 3 Settembre 2007
 - ▶ La pagina principale del portale di benvenuto di Bank of India viene compromesso per diffondere Malware

...



Black Market

Rank	Item	Percentage	Range of Prices
1	Credit Cards	22%	\$0.50–\$5
2	Bank Accounts	21%	\$30–\$400
3	Email Passwords	8%	\$1–\$350
4	Mailers	8%	\$8–\$10
5	Email Addresses	6%	\$2/MB–\$4/MB
6	Proxies	6%	\$0.50–\$3
7	Full Identity	6%	\$10–\$150
8	Scams	6%	\$10/week
9	Social Security Numbers	3%	\$5–\$7
10	Compromised UNIX® Shells	2%	\$2–\$10

Fonte: Symantec Threat Report 2007



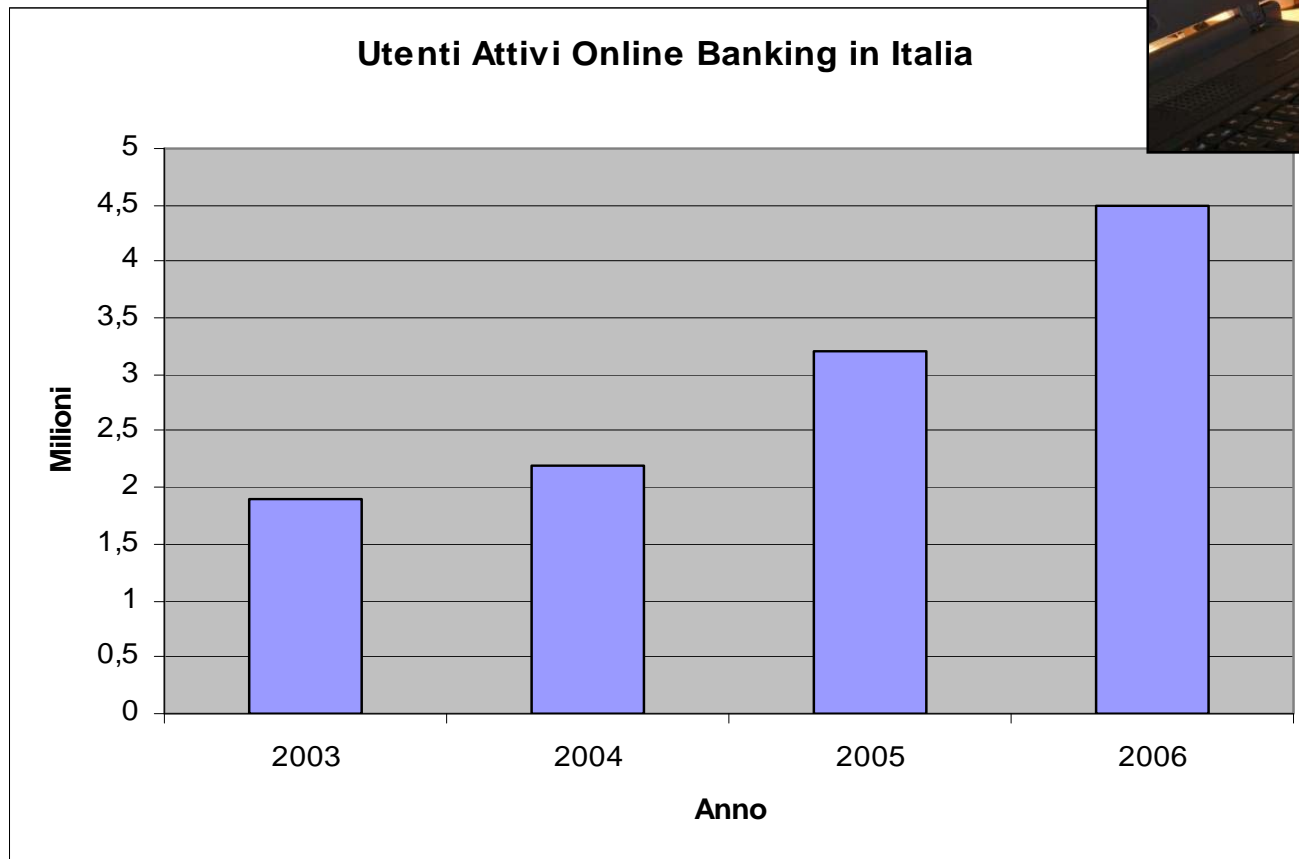
TREND 2007 - 2008

Vulnerabilità WEB nei portali di Internet Banking in Italia



Utilizzo dei portali di Internet Banking

- Crescita del 150% dal 2003 al 2006

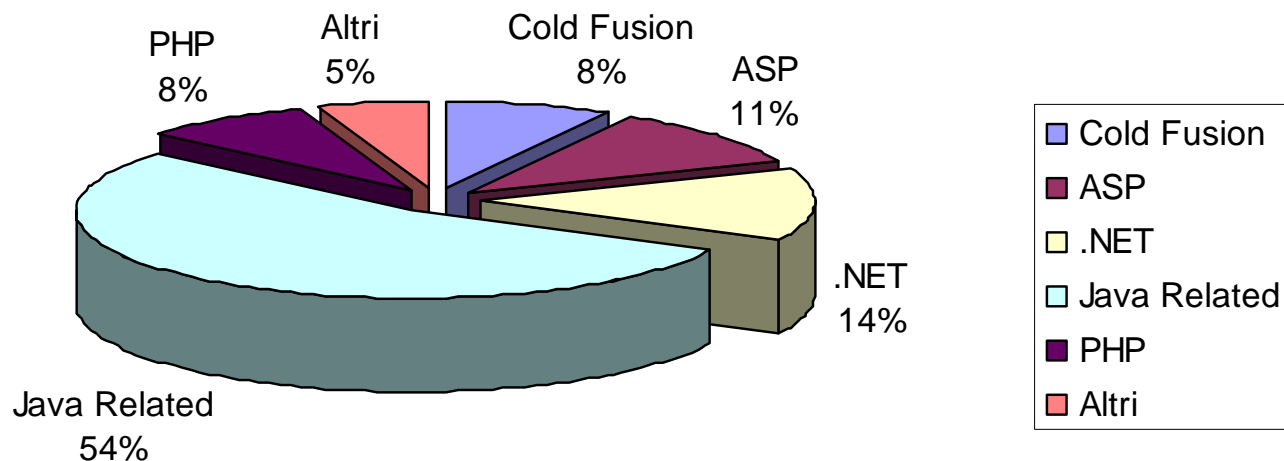


Fonte: Centro Studi Abi



Tecnologie Web e Internet Banking

Distribuzione Tecnologie per Pagine e Portali di Benvenuto

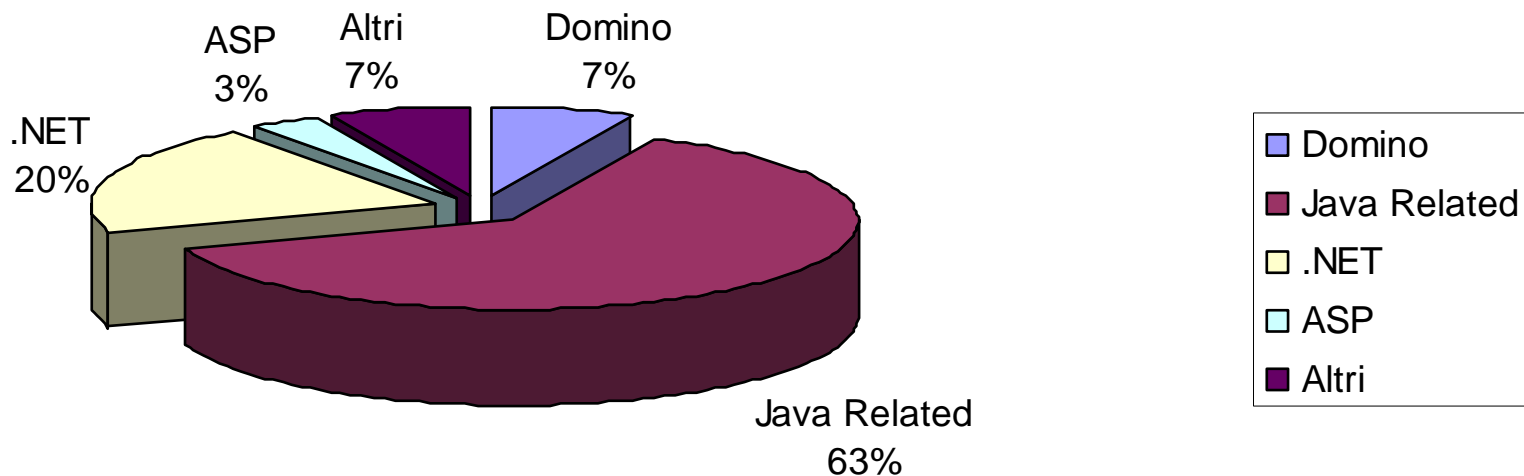


Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



Tecnologie Web e Internet Banking

Distribuzione Tecnologie per Sezioni Sicure



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



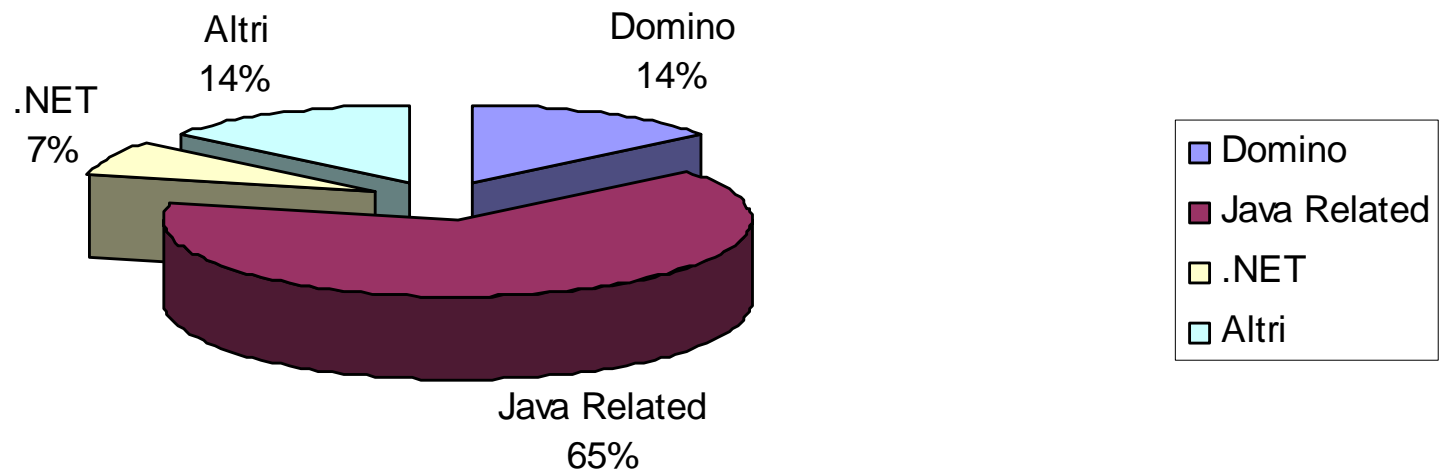
Portali di Benvenuto Vs Sezioni Sicure

- I portali di benvenuto usano una gamma di tecnologie più vasta
 - ▶ Utilizzo ad esempio di tecnologie quali PHP e Cold Fusion
- Più orientati a mostrare contenuti grafici
 - ▶ Presenza spesso di problematiche connesse con l'utilizzo di contenuti multimediali
- Sviluppati spesso da team differenti rispetto alla "Parte Sicura"
 - ▶ Importanza di creare un piano di Risposta comune vista l'integrazione fra entrambe le sezioni



Tecnologie Web e Internet Banking

Tecnologie Più Utilizzate dagli Outsourcer



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



Outsourcer e Tecnologie Web

- Outsourcer di servizi finanziari offrono piattaforme Web che vengono personalizzate e adattate per più Istituti differenti
- La scelta delle piattaforme da utilizzare nasce da esigenze di integrazione
 - ▶ Grande esperienza nell'utilizzo e gestione Mainframe
 - ▶ Forti legami storici con il vendor delle proprie applicazioni

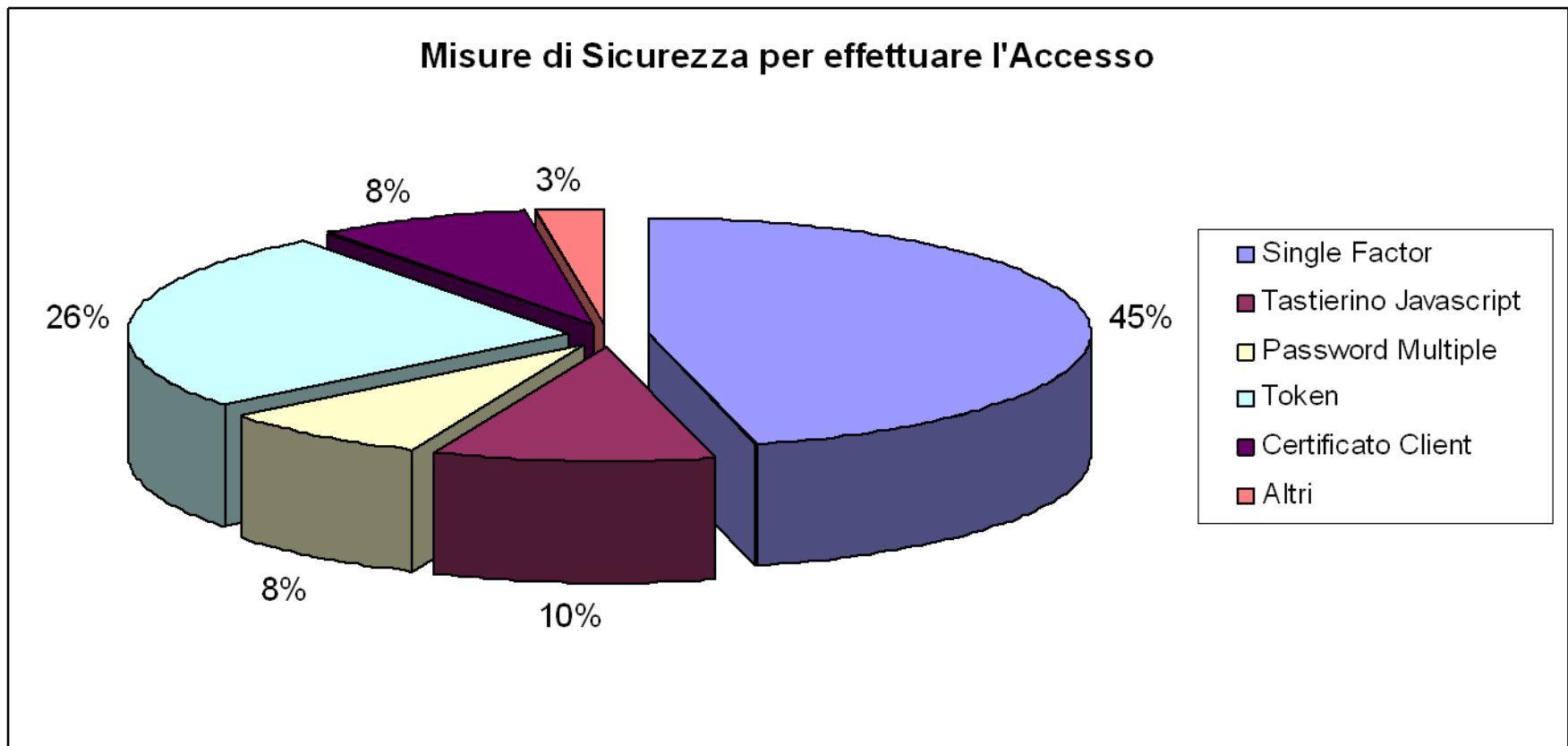


Outsourcer e Tecnologie Web

- Una vulnerabilità a livello di Framework, spesso impatta più banche
- Al contempo maggiore frequenza e granularità dei controlli, essendo richiesti da soggetti diversi

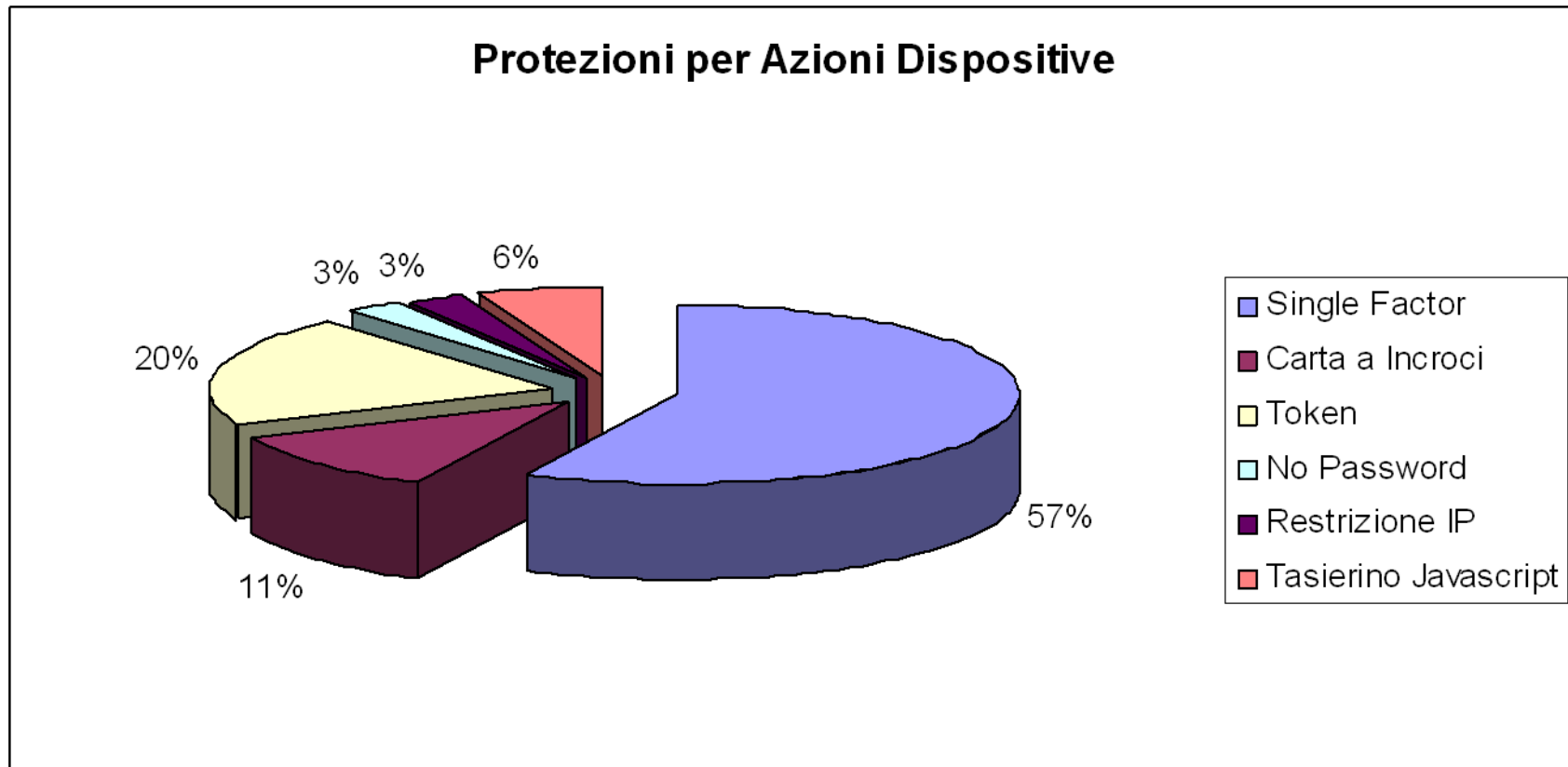


Tecnologie Web e Internet Banking



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia

Tecnologie Web e Internet Banking



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia

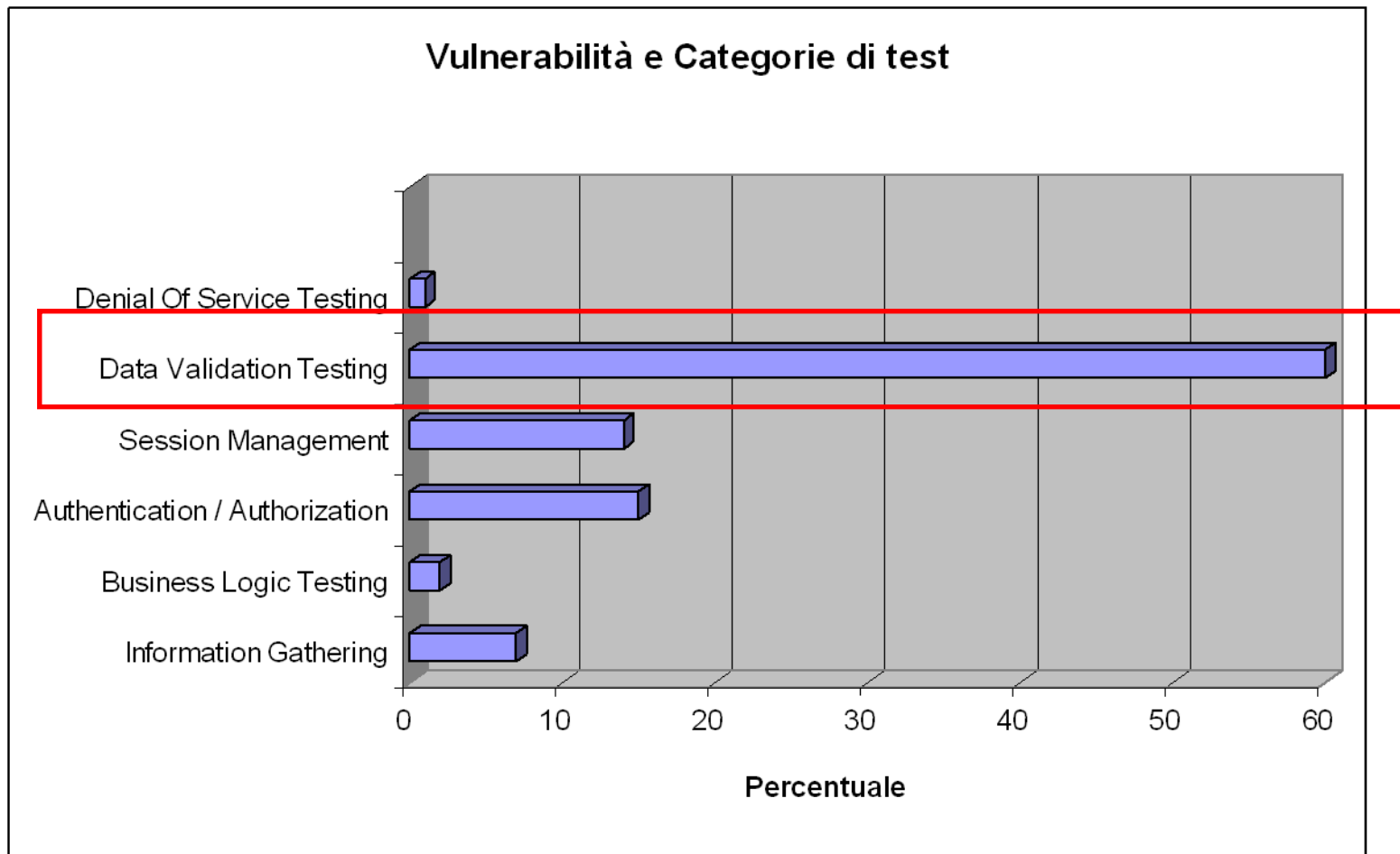


Considerazioni riguardo all'Accesso ai servizi

- Utilizzo ancora preponderante della comune password di Accesso
 - ▶ Anche le banche che offrono tecnologie di autenticazione innovative, continuano a mantenere attivo il "vecchio accesso" basato su password
- Uso del Token OTP in incremento
 - ▶ Protezione efficace contro Password Stealing
 - ▶ Investimento come interesse attivo nel campo della sicurezza
- Altre tecnologie usate:
 - ▶ Certificati Client per Strong Authentication
 - ▶ Tastierino Javascript, altre tecnologie di contenimento



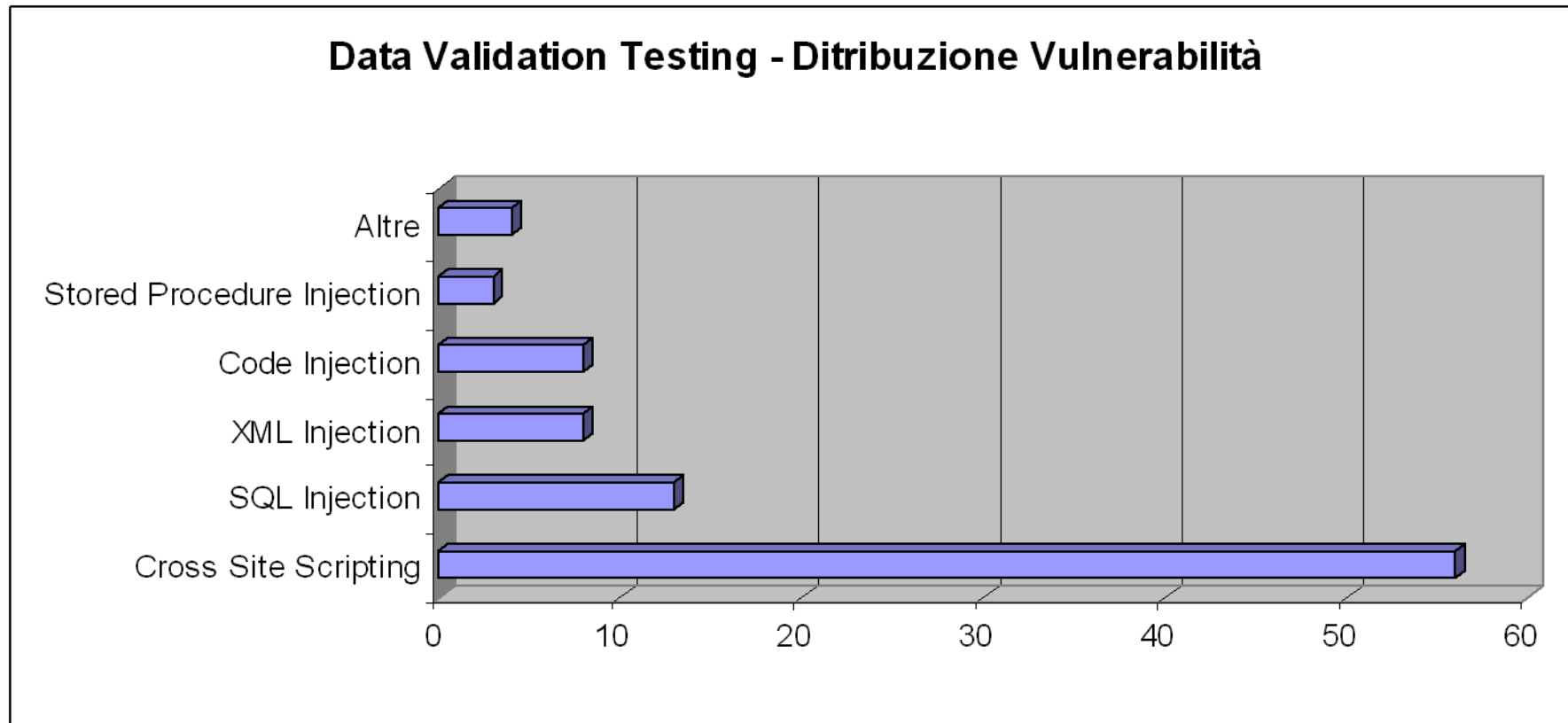
Vulnerabilità Web e Internet Banking



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



Data Validation Testing



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



Impatti sul Business

La presenza di vulnerabilità come le precedenti all'interno di un sito Web Aziendale può causare i seguenti impatti sul business:

Perdite Dirette

- Furti, Perdite Monetarie
- Risorse Informatiche
- Segreti Aziendali
- Informazioni sui Consumatori

Perdite Indirette

- Perdite Commerciali
- Impatto Negativo sul Brand
- Perdite di Vantaggio Competitivo

Perdite nella Produttività

- Spese per il ripristino della continuità
- Corruzione di Dati
- Spese di Recovery dei Dati

Esposizioni Legali

- Impossibilità di concludere Contretti
- Failure to Meet Privacy Regulations
- Attività Illegali



Software Security Vs Application Security

VENDOR



SICUREZZA DEL SOFTWARE

CORPORATE



SDLC Security
Defense in Depth
Operational Security

Processi



Secure Code Review
Penetration Test Appl.
Security Check Periodici



Software

SICUREZZA APPLICATIVA



Tutela dei propri utenti

- Necessità di garantire un ambiente sicuro
 - ▶ Gestione del codice applicativo
 - ▶ Code review periodici
 - ▶ Penetration Test Periodici
 - ▶ Supervisione dei Log

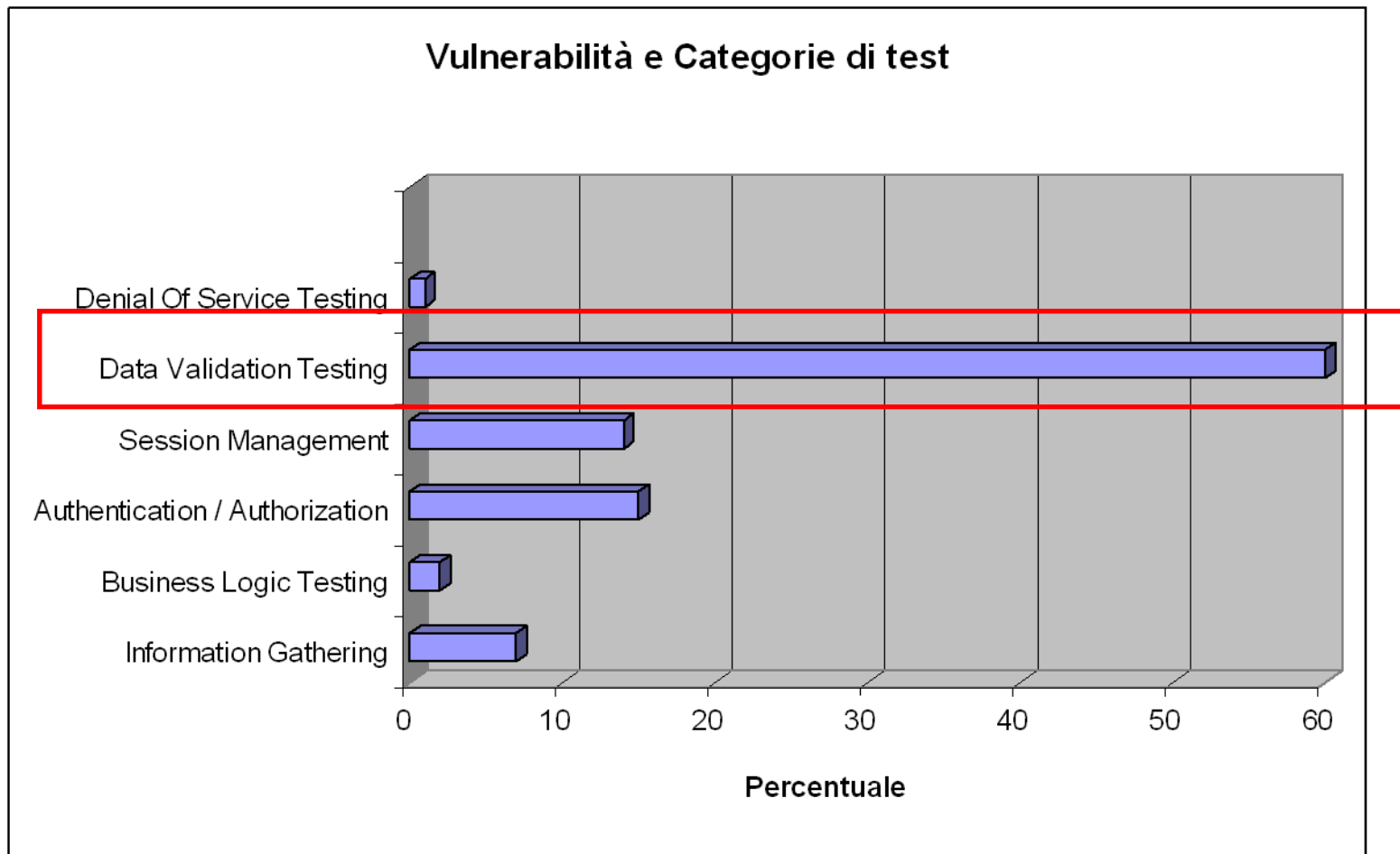


Principali Vulnerabilità 2007-2008

Dettagli delle vulnerabilità più diffuse



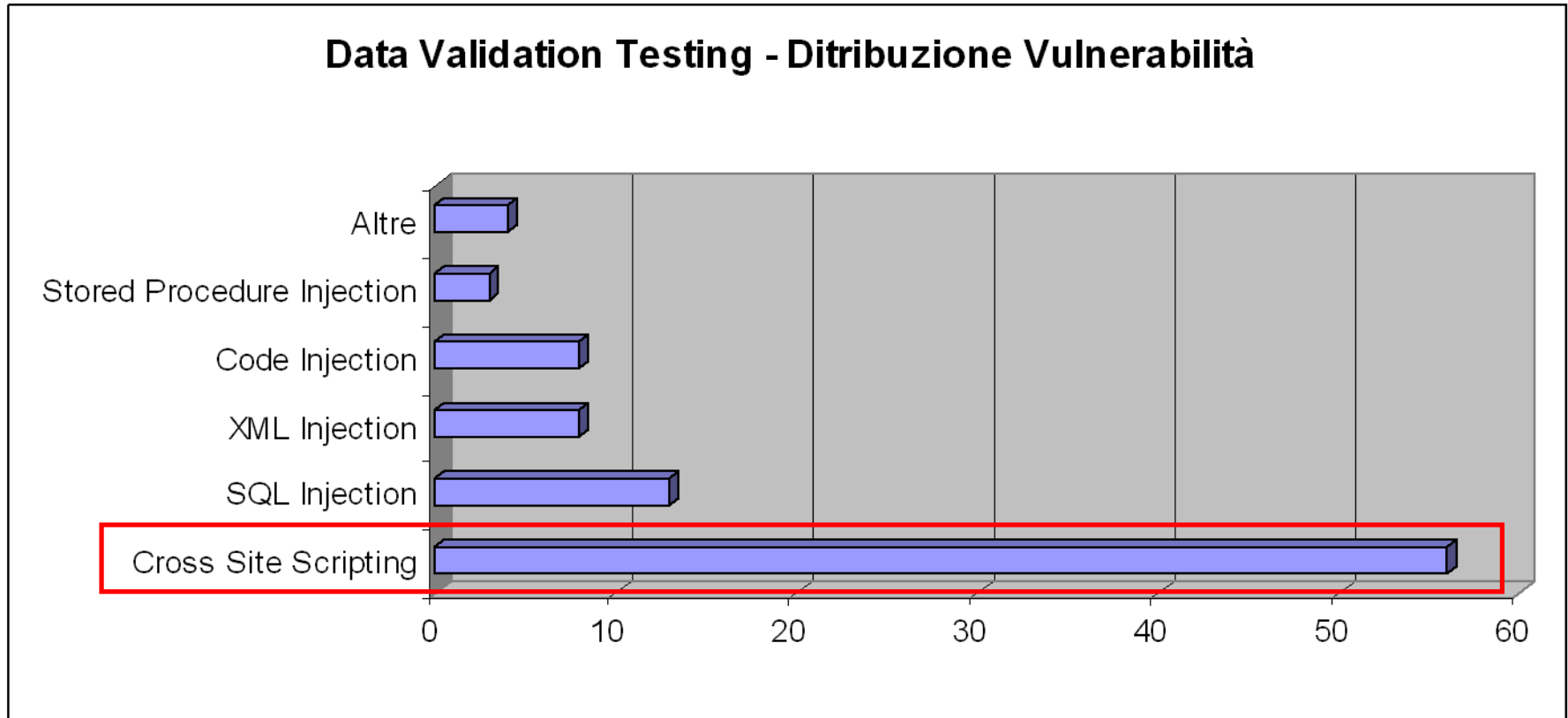
Vulnerabilità Web e Internet Banking



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



Data Validation Testing



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia

Cross-Site Scripting (XSS)

Cos'è un XSS?

- ▶ Problematica di sicurezza che consiste nel poter indurre il browser dell'utente ad eseguire del codice Javascript

Un problema per gli utenti...

- ▶ Il crimine organizzato assolda spesso gruppi di hacker che manomettono siti istituzionali aggiungendo stored XSS per attaccare gli utenti (Phishing e Malware)

E per le aziende...

- ▶ Sono vulnerabilità estremamente comuni



Attacchi di Phishing...

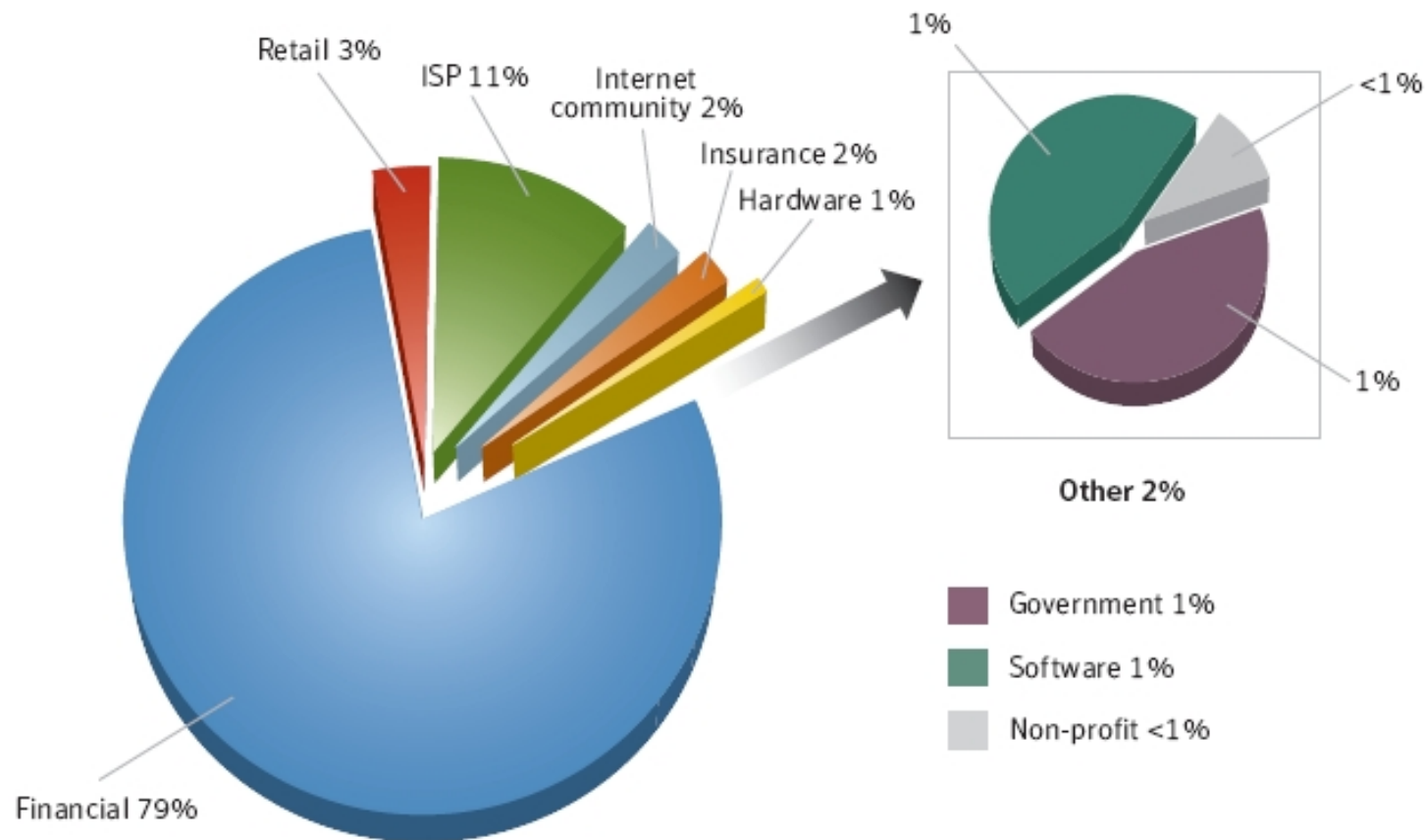


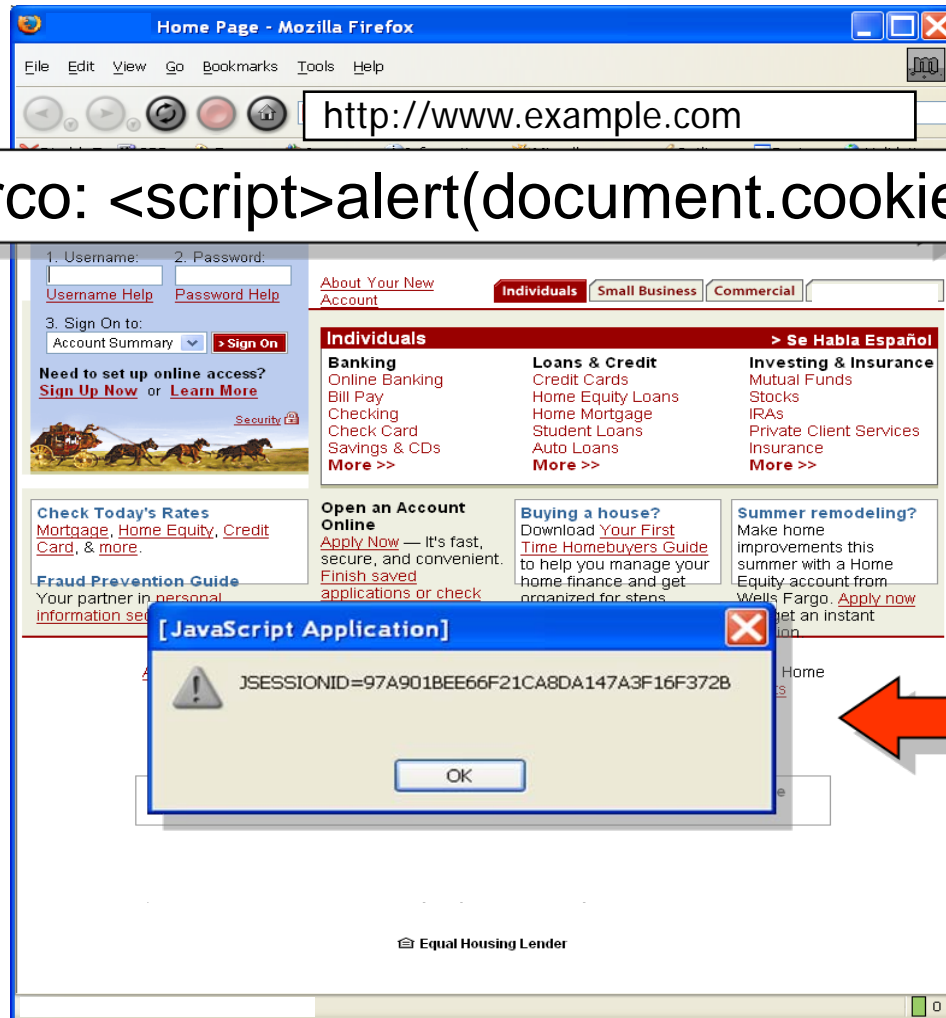
Figure 33. Brands phished by sector
Source: Symantec Corporation



Cross Site Scripting

Il campo di ricerca
so riporta le
parole ricercate a
video.

Il sito invia lo script
all'utente e
visualizza un cookie
di sessione in una
finestra di pop-up.



Attacco di Phishing tramite XSS



Tipologie di Cross-Site Scripting (XSS)

Reflected

- ▶ La richiesta del client incorpora il codice che verrà inviato dal server
- ▶ es. `http://sito.com/1.php?1=<script></script>`

Stored

- ▶ Il codice malevolo è stato inserito permanentemente all'interno della pagina web

Dom/Application Based

- ▶ Nuova Generazione!
- ▶ Per risolvere la problematica è necessario intervenire sul client (es. Aggiornamento Plugin; Javascript Secure Coding)



<iframe> Injection, esempio di Stored XSS

Utilizzando un sito Web precedentemente compromesso, un attaccante cerca di installare un malware sul Pc di un Utente.



Vulnerabilità Browser... e plugins!

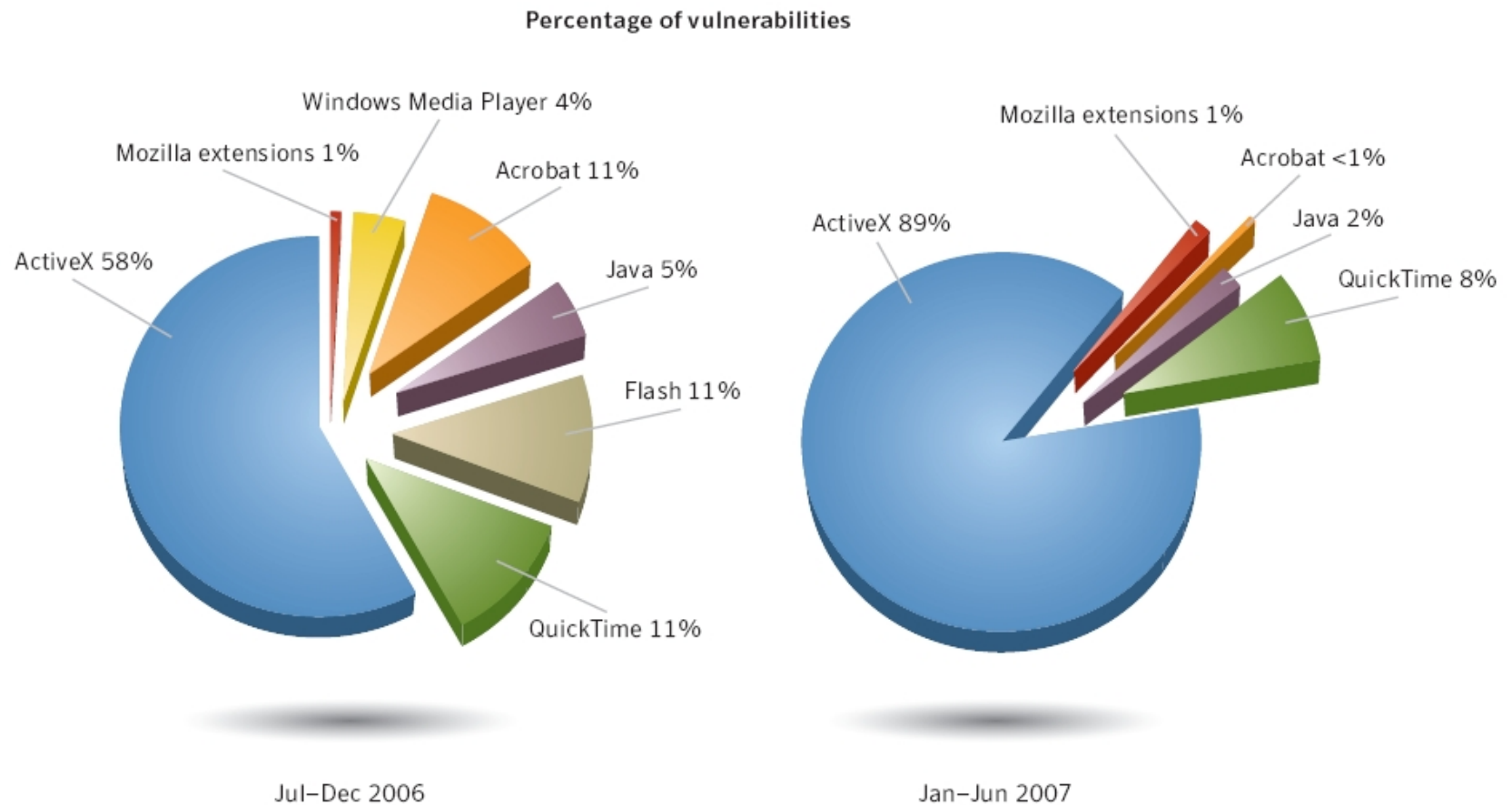
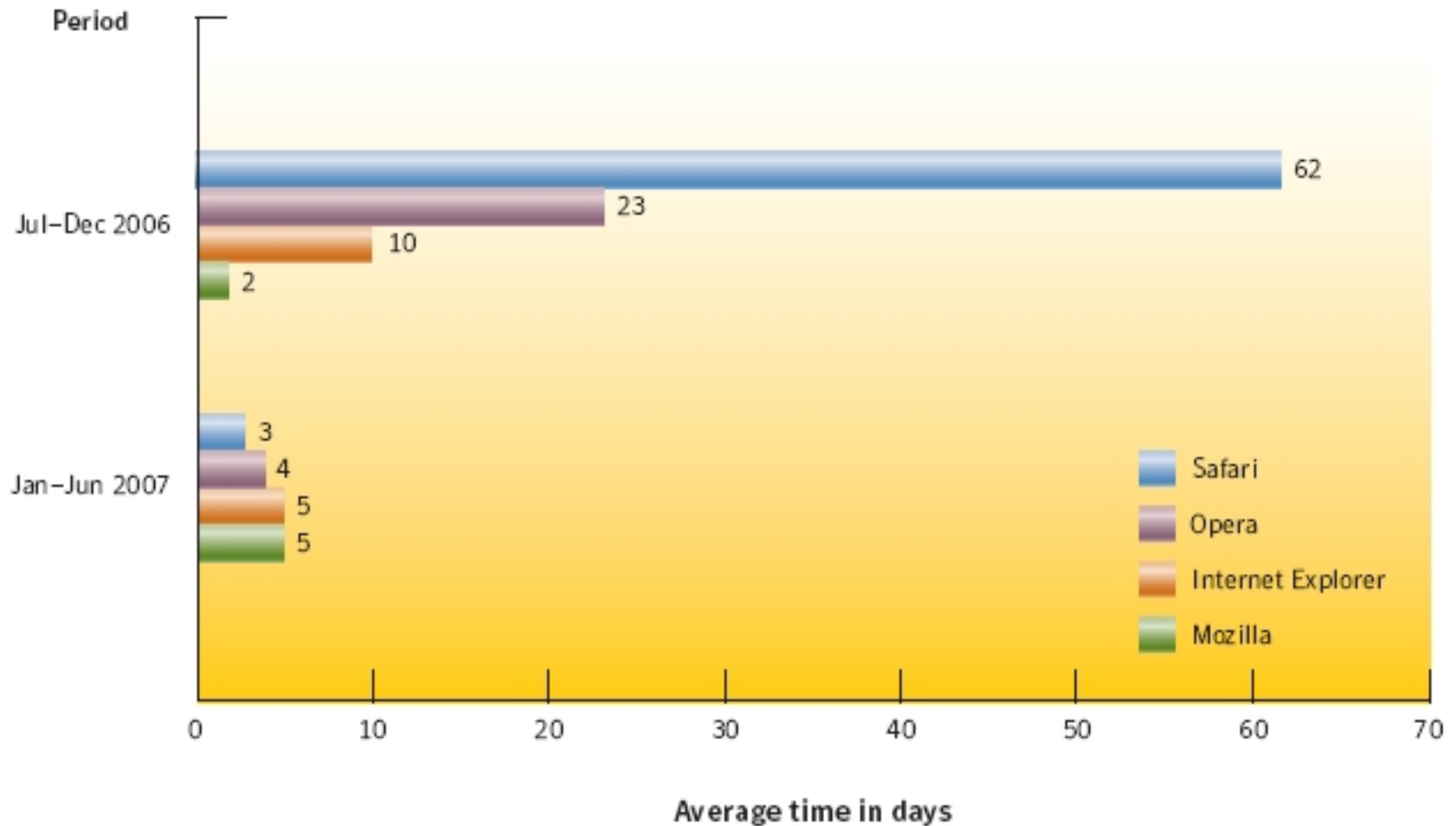


Figure 24. Browser plug-in vulnerabilities

Source: Symantec Corporation

Window Of Exposure 2007-2008



Silent Banker, Malware e Internet Banking

- Malware ad hoc per Internet Banking
 - ▶ Realizzato per scopi criminali
 - ▶ Codice sorgente in vendita per poco più di 1000 euro
 - ▶ Semplice da personalizzare
 - ▶ Intercetta il traffico ed interagisce con il portale di IB
 - ▶ Colpiti utenti di numerose banche intorno al mondo



Data Validation: Injection Flaws

Cos'è una Injection Flaw?

- Problematica di sicurezza che consiste nell'iniettare del codice attivo che viene interpretato.

Dove si trovano queste vulnerabilità.

- Mentre l'XSS è tipicamente una vulnerabilità tipicamente client-side, le Injection Flaws sono vulnerabilità Server Side.

Keywords

- ✓ SQL Injection
- ✓ XML Injection
- ✓ ORM Injection
- ✓ LDAP Injection
- ✓ XPath Injection
- ✓ Code Injection



Data Validation: XML Injection

In cosa consiste questa vulnerabilità?

Il Web Server gira all'Application Server stringhe di dati che interpreta.

Un utente malevolo può essere in grado di inviare strutture XML che vengono elaborate.

`http://www.mybank.ccm/operation.do?User=19900`

Richiesta XML: `<user>19900</user> <callfunc> Balance </callfunc>`

**`http://www.mybank.ccm/operation.do?User=19900</user>
<callfunc>phonecharge;50;3332223232</callfunc>`**

Quali rischi si corrono con queste vulnerabilità?

Parameter Tampering, Transazioni non autorizzate, accesso non autorizzato a Dati.

XML Injection è la nuova SQL Injection



Data Validation: Code Injection

In cosa consiste questa vulnerabilità?

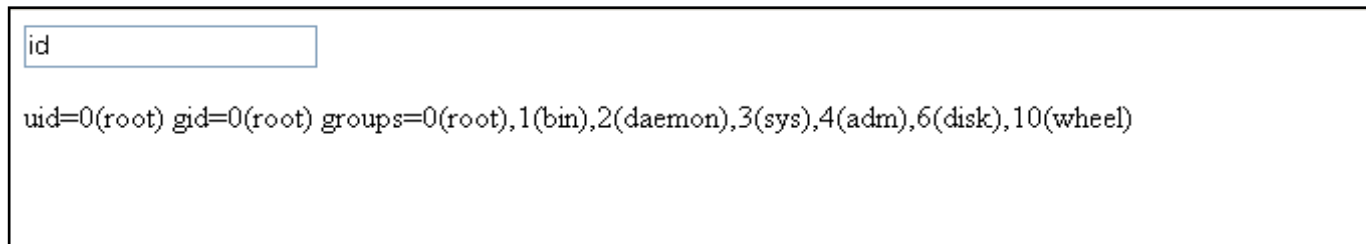
L'applicazione accetta in input stringhe di dati che interpreta.

Ad esempio l'input dell'utente viene passato ad una funzione "eval()" (Javascript Server Side)

Quali rischi si corrono con queste vulnerabilità?

Nel caso in cui i privilegi associati all'interprete siano tali da poter eseguire comandi sul sistema, è possibile eseguire codice in remoto sulla macchina target.

Esempi: "BroadVision", "WebSphere Application server"

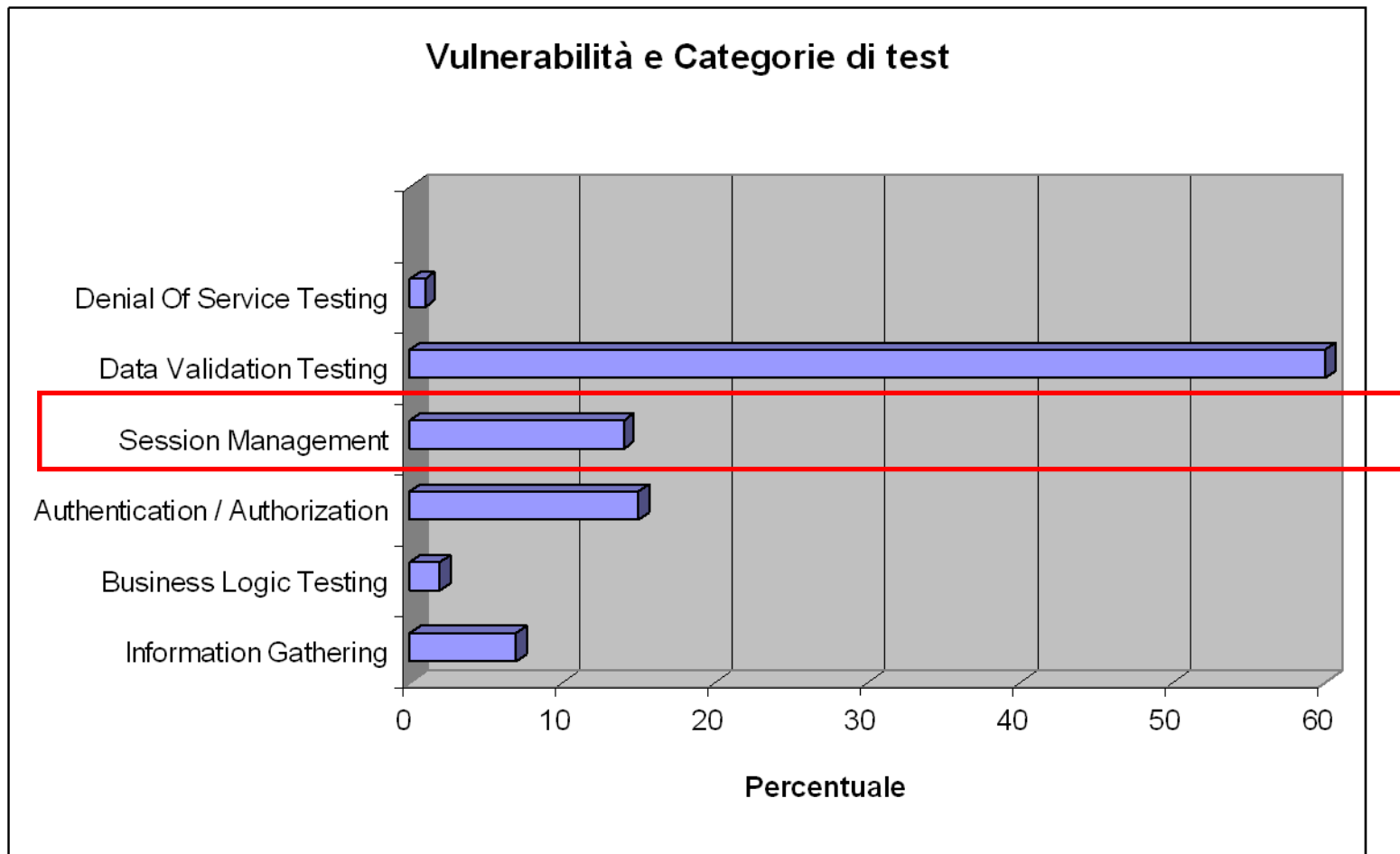


The screenshot shows a web form with a text input field labeled 'id'. Below the input field, the output of a code injection is displayed: `uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)`. This indicates that the injected code successfully executed a command to gain root access on the target system.

Esempio di Code Execution da internet su Web Sphere Application Server



Vulnerabilità Web e Internet Banking



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia

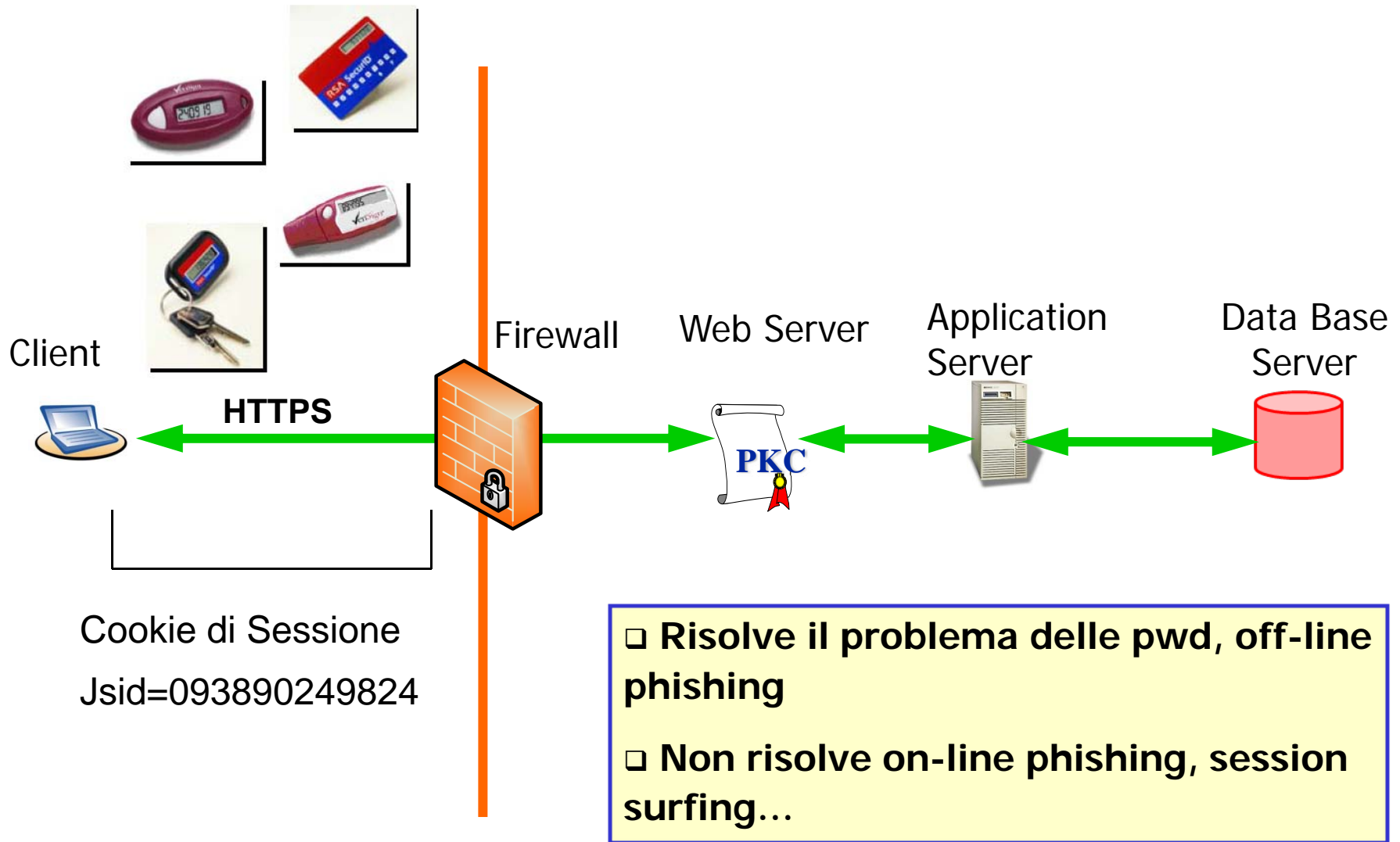


Prima Autenticazione al portale

- Password
 - ▶ Credenziali di accesso costituite da Username e password alfanumerica
- Password + PIN
 - ▶ Password di primo e di secondo livello
- OTP – (One Time Password)
 - ▶ La password cambia ad intervalli regolari



Two Factor Authentication



Source: M.Meucci - IDC Banking Forum – Milano, 18 Nov 05



Cookie di Sessione e comuni problematiche

- Cookie impostato non Secure
 - ▶ Il cookie di sessione viene inviato anche in chiaro, verso la sezione non sicura.
- Cookie impostato non HTTP-Only
 - ▶ Possibilità di leggere il cookie di sessione tramite codice Javascript
- La sessione non va in Expiration
 - ▶ L'utente continua ad essere loggato anche dopo ore



Session Riding: Blended Threat

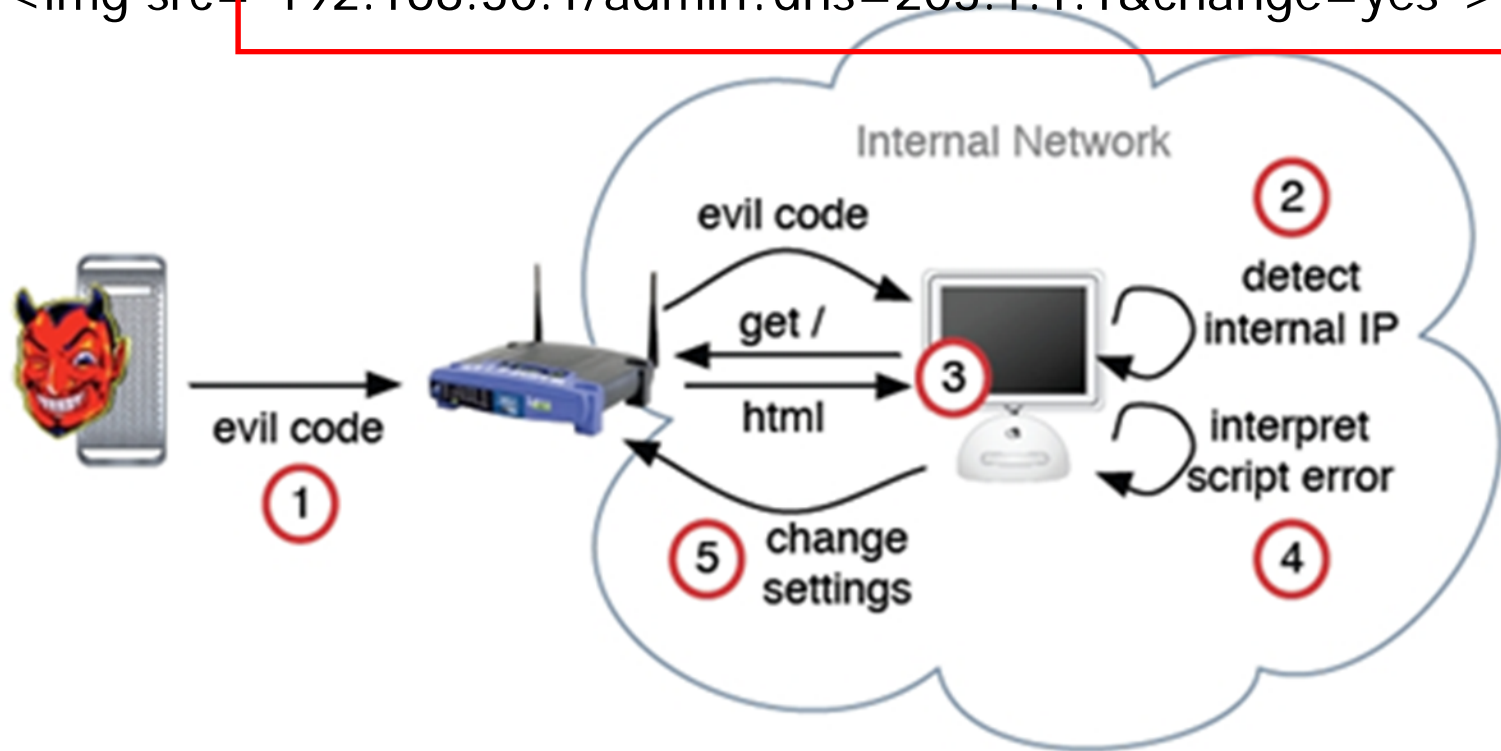
Cos'è una vulnerabilità di tipo Session Riding?

- Problematica di sicurezza che consiste nello sfruttare una sessione già attiva
- E' un attacco efficace contro la sessione, non contro le credenziali

Come viene sfruttata?

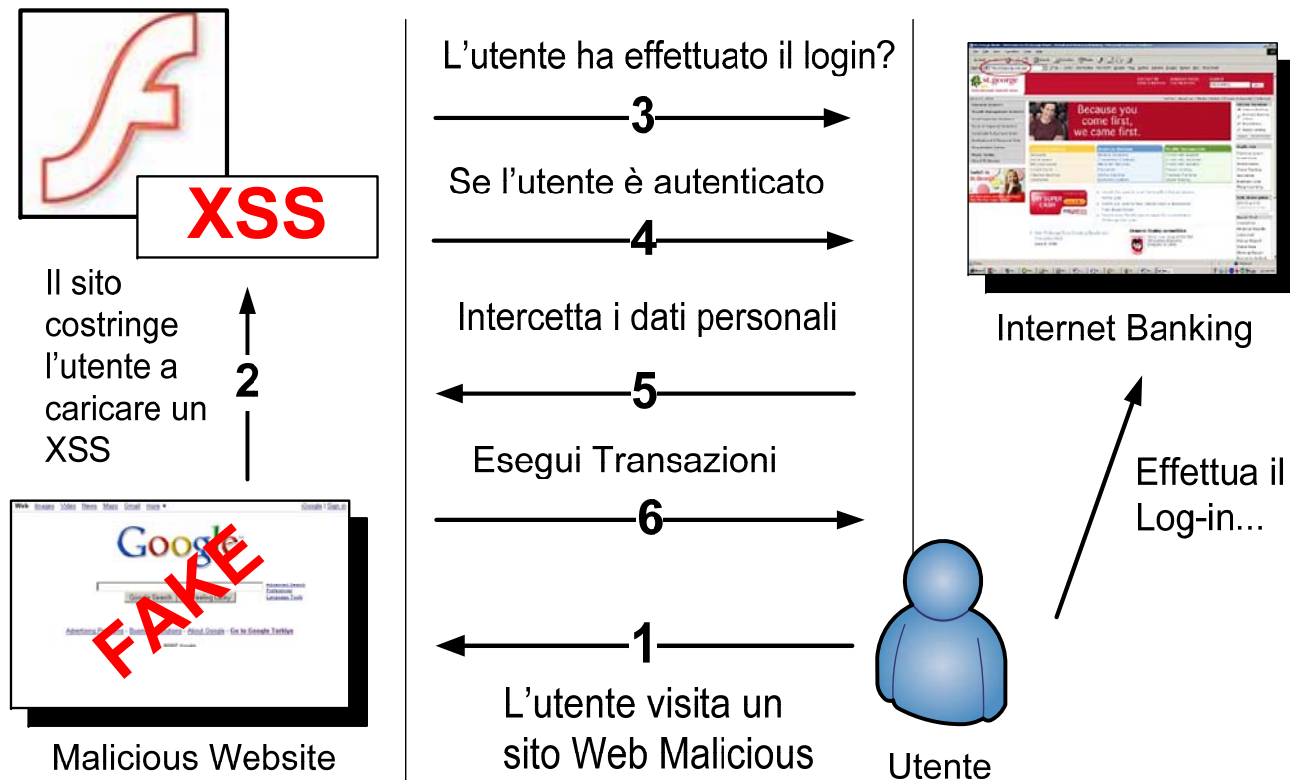
Lo sfruttamento di tale vulnerabilità può avvenire in più modi:

- L'utente mentre naviga con più finestre aperte, visita un sito Malevolo. Mentre la sessione con il sito web sul quale si è autenticato è ancora attiva, l'XSS prende il controllo del suo browser.
- L'attaccante spinge l'utente ad effettuare una richiesta in modo non intenzionale (esempio `
```

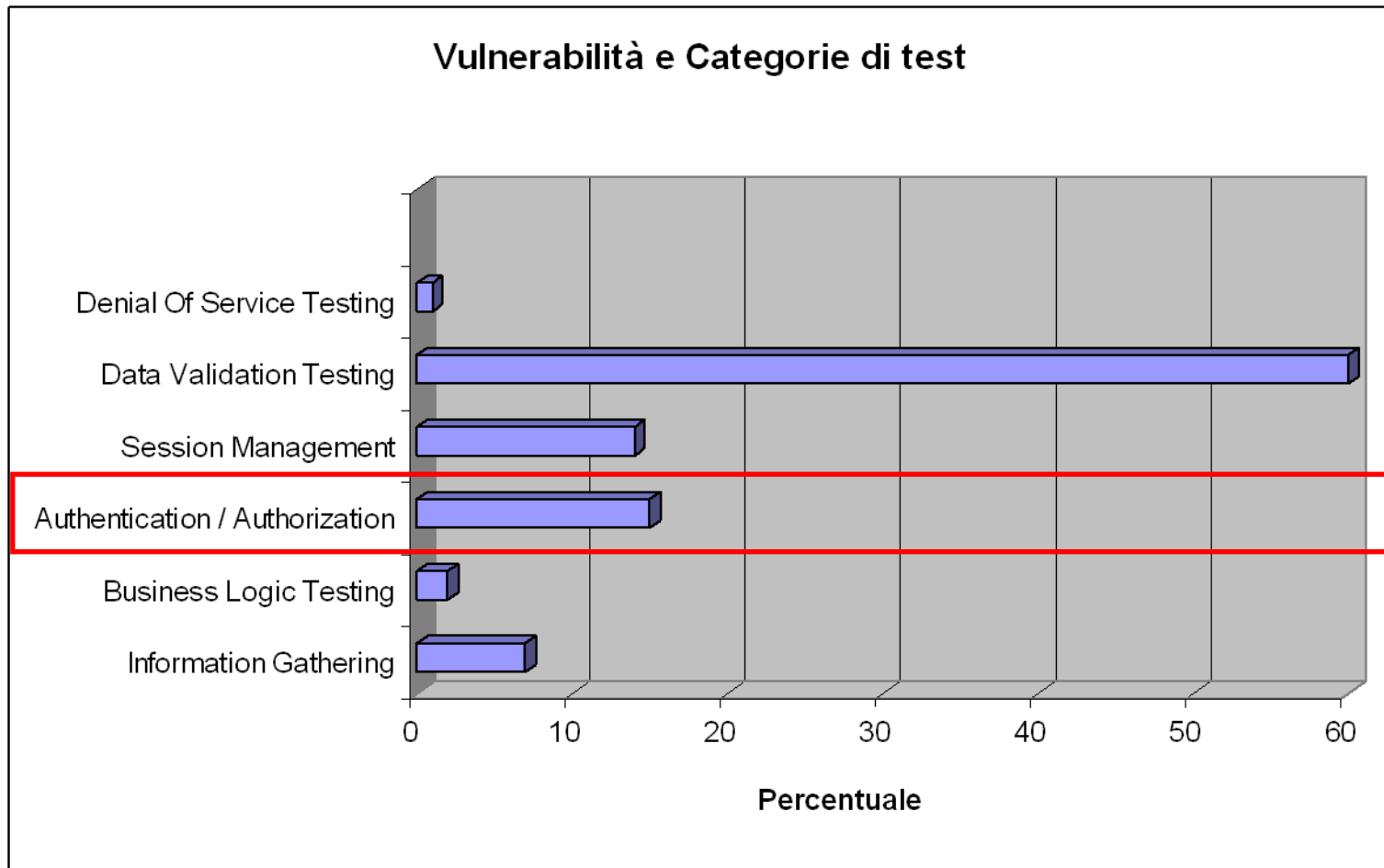


# Sessione Riding Contro Two Factor Authentication

## XSS Proof of Concept – Controllo Remoto di un conto Online



# Vulnerabilità Web e Internet Banking



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



# Authentication / Authorization Testing

## Descrizione

Il controllo è atto a verificare la possibilità di effettuare test approfonditi sul funzionamento del sistema di Autenticazione e Autorizzazione.

Il sistema di Autenticazione è atto a stabilire l'identità di un utente o l'appartenenza di un utente ad un determinato gruppo, mentre il sistema di Autorizzazione è quell'insieme di regole che vietano o permettono ad un determinato utente di compiere delle azioni.

I due sistemi sono a tutti gli effetti complementari, poiché non si può bloccare una certa azione senza aver prima stabilito chi sta cercando di compierla ed al contempo, stabilire l'identità di un utente non è una condizione sufficiente per bloccare un'operazione

## Keywords

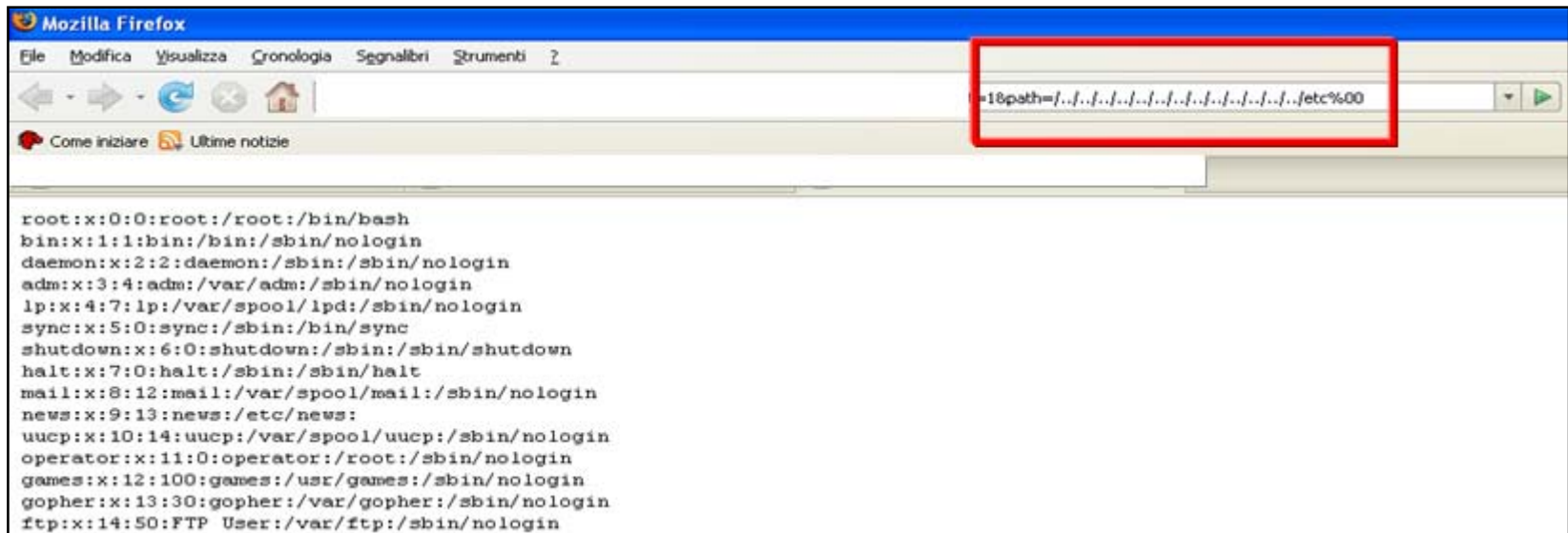
- ✓ Default or guessable account
- ✓ Brute Force
- ✓ Bypassing authentication schema
- ✓ Directory traversal/file include
- ✓ Vulnerable remember password and pwd reset
- ✓ Logout and Browser Cache Management Testing



# Authorization Testing – Path Traversal

Path Traversal ed accesso in lettura a file arbitrari:

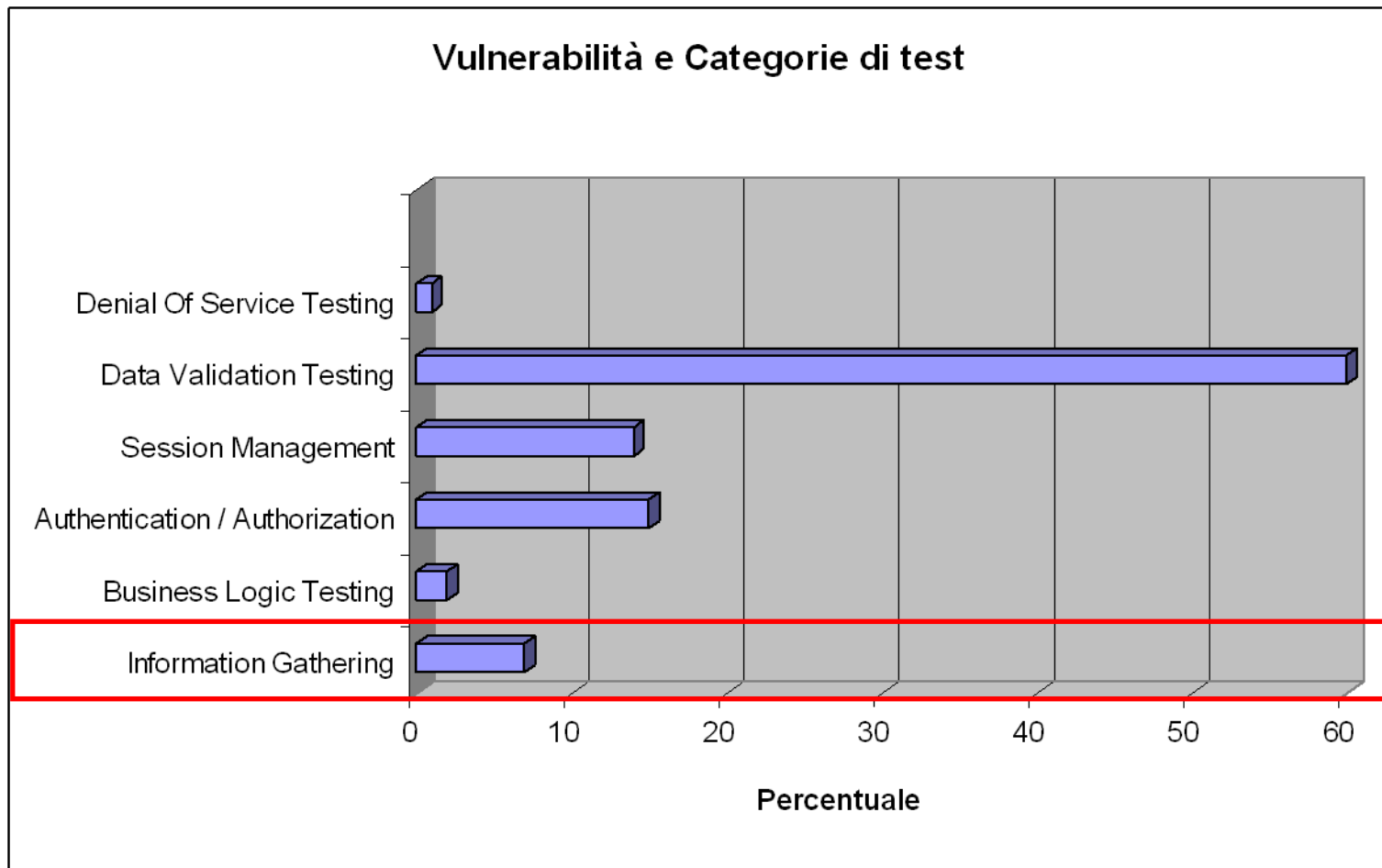
<http://www.sito-.com/sito/download.jsp?id=../../../../../../../../etc/passwd%00>



```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
```



# Vulnerabilità Web e Internet Banking



Fonte: Minded Security Labs – Campione di 20 Banche Online in Italia



# Information Gathering

## Descrizione

Lo scopo di questo controllo è quello di verificare la possibilità di poter accedere ad informazioni riguardanti un determinato target attingendo da ciò che è pubblicamente esposto.

L'attività si compone di fasi differenti, partendo spesso dall'analisi dei servizi esposti per identificarne la versione (versioning), per poi effettuare ricerche avanzate sui motori di ricerca (Power Browsing), concludendo con un'attenta analisi di datamining su quanto è esposto dal sito target.

## Keywords

- ✓ Application Fingerprinting
- ✓ Application Discovery
- ✓ Spidering and googling
- ✓ Analysis of error code
- ✓ SSL/TLS Testing
- ✓ DB Listener Testing
- ✓ File extensions handling
- ✓ Old, backup and unreferenced files





# Information Gathering

## File esposti durante le migrazioni

Google ha una cache che è in grado di conservare per un lungo periodo di tempo le informazioni che raccoglie durante lo spidering e l'aggiornamento dei contenuti presenti all'interno del suo motore.

Spesso accade che durante **una migrazione** vengano fatte delle importanti modifiche al sito web anche **transitorie**. Nel caso in cui vengano accidentalmente esposti dei contenuti importanti, Google è in grado di raccogliarli e conservarli.

Una nota banca ha accidentalmente esposto numerose viste del proprio database DB2 esportate in formato "csv", proprio per questo motivo.

## Attacchi ai dipendenti

Accade spesso che le tecniche di information gathering vengano utilizzate per compromettere la sicurezza aziendale in modo indiretto. La raccolta di informazioni sui dipendenti utilizzando comuni motori di ricerca (es. LinkedIn in primis), può permettere ad un malintenzionato di acquisire dati importanti.

Esempi includono le mail personali dei dipendenti, le loro attitudini, comunità online frequentate.



# Information Gathering

Una gestione degli errori non corretta fornisce un ottimo strumento di information gathering

## Segnala difatti l'evidenza di:

- ✓ SQL Injection
- ✓ Code Execution
- ✓ XML Injection
- ✓ ...

Server Error in '/secure' Application.

### Runtime Error

**Description:** An application error occurred on the server. The current custom error settings for this application prevent the details of the application from being visible to the user on the local server machine.

**Details:** To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "webResource" tag in the application's configuration file. The tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->

<configuration>
 <system.web>
 <customErrors mode="Off"/>
 </system.web>
</configuration>
```

**Notes:** The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->





















<configuration>
 <system.web>
 <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
 </system.web>
</configuration>
```



# Information Gathering

## Esempio di Directory Listing:

### Index of /icons

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">a.gif</a>	21-Nov-2004 15:35	246	
 <a href="#">a.png</a>	21-Nov-2004 15:35	293	
 <a href="#">alert.black.gif</a>	21-Nov-2004 15:35	242	
 <a href="#">alert.black.png</a>	21-Nov-2004 15:35	279	
 <a href="#">alert.red.gif</a>	21-Nov-2004 15:35	247	
 <a href="#">alert.red.png</a>	21-Nov-2004 15:35	298	
 <a href="#">apache_pb.gif</a>	21-Nov-2004 15:35	2.3K	
 <a href="#">apache_pb.png</a>	21-Nov-2004 15:35	1.4K	
 <a href="#">apache_pb2.gif</a>	21-Nov-2004 15:35	2.4K	
 <a href="#">apache_pb2.png</a>	21-Nov-2004 15:35	1.4K	
 <a href="#">apache_pb2_an1.gif</a>	21-Nov-2004 15:35	2.1K	
 <a href="#">back.gif</a>	21-Nov-2004 15:35	216	
 <a href="#">back.png</a>	21-Nov-2004 15:35	284	
 <a href="#">ball.gray.gif</a>	21-Nov-2004 15:35	233	
 <a href="#">ball.gray.png</a>	21-Nov-2004 15:35	277	
 <a href="#">ball.red.gif</a>	21-Nov-2004 15:35	205	
 <a href="#">ball.red.png</a>	21-Nov-2004 15:35	265	
 <a href="#">binary.gif</a>	21-Nov-2004 15:35	246	
 <a href="#">binary.png</a>	21-Nov-2004 15:35	296	



## Information Gathering

Esempio di accesso a funzionalità esposte dall'applicativo (Domino e Lotus Notes): “<http://www.sito-.com/site/cache.nsf>”

▼ 03051A1743		
▶ 20EEF1054103A966C12573D10036AA17		
▼ 03051A1751		
▶ 552D7E5D0CA3A397C12573D10030CB3C		
▶ 8BF0F994CA07A22CC12573D1004D8700		
▼ 03051A1804		
▶ 27F96C77FAF4C501C12573D200638B3E		
▼ 03051A1805		
▼ 3C900B9F55666F75C12573D300141CC1		
	1	17/01/2008 04.40.49
▼ 43098B9297863D7EC12573D30010975A		
		17/01/2008 04.05.27
		17/01/2008 04.03.13
	2	17/01/2008 04.13.41
		17/01/2008 04.13.26
▼ BEC97C10E283D4DAC12573D300182371		
		17/01/2008 05.24.17
		17/01/2008 05.25.47
		17/01/2008 05.26.51
▼ 03051A1821		
▶ 620BB367596D89DAC12573D100515E19		
▶ D215B2AFFDDA1918C12573D2005BDEB7		
▼ 03051A1900		
▶ 3C67E80EC9B8D90DC12573D2002E9E8F		



# Denial Of Service Testing

## Descrizione

Il controllo è atto a verificare la presenza di eventuali Denial of Service all'interno dell'applicazione. Per Denial of Service si intendono tutti quegli attacchi che possono portare ad una interruzione del servizio.

Alcuni attacchi sono una diretta conseguenza di vulnerabilità già viste precedentemente, altri sono la diretta causa di problematiche di varia natura, come ad esempio l'utilizzo di macchine sotto-dimensionate per il carico di lavoro svolto.

## Esempio

- ✓ Presenza di script di Debug (Ambiente di produzione non allineato con l'ambiente di Test.)
- ✓ Utilizzo di un Database di Back-End non adeguato