Sicurezza dei referti online

E-privacy 2013 – Firenze

Gabriele Zanoni

Agenda

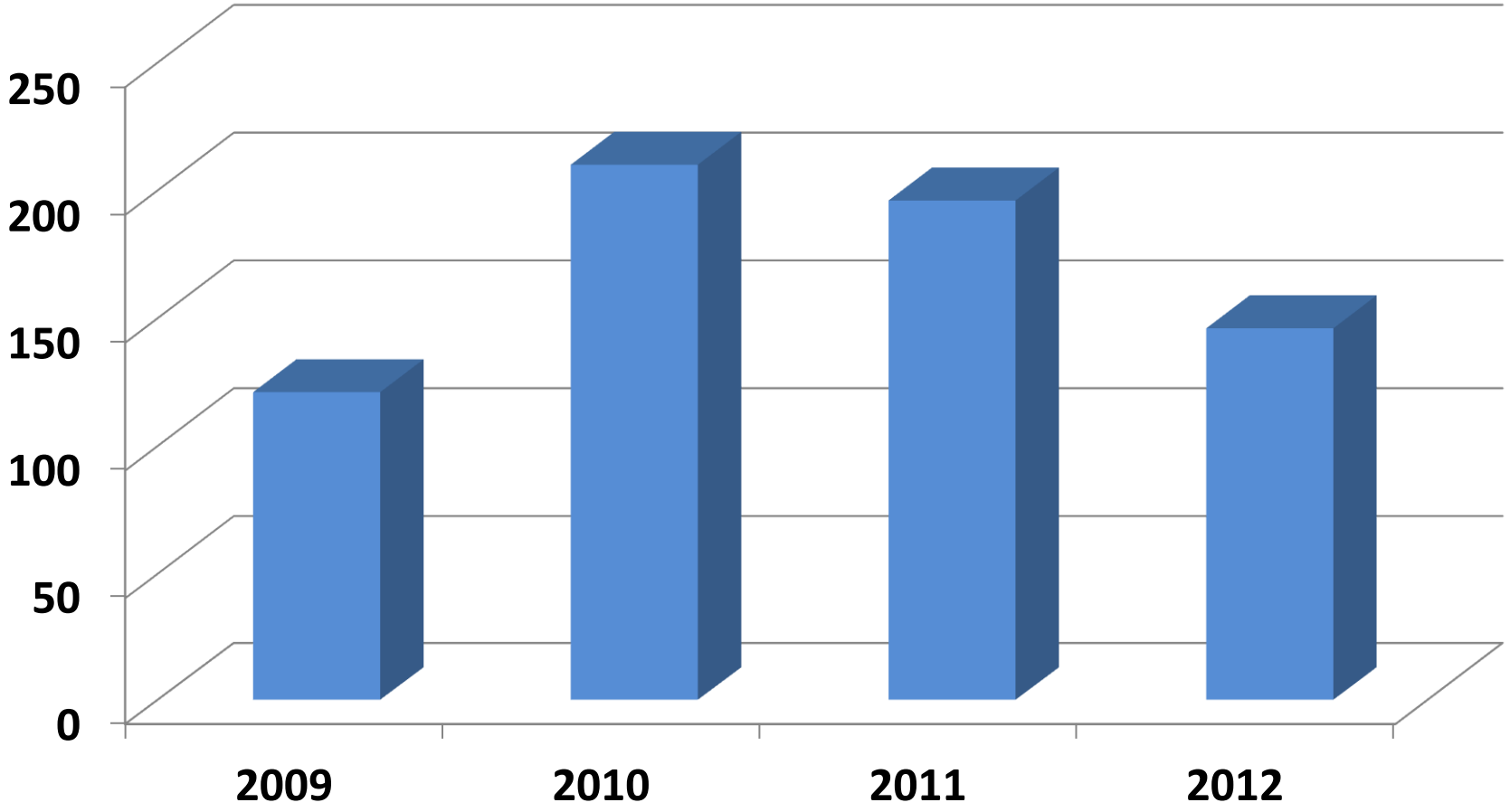
1. Cosa sono i referti online
2. Statistiche
3. Cosa dicono le norme del Garante al riguardo
4. Esempi di attuali servizi di referti online
5. Conclusioni

Esigenza e definizione di referto

Numerose strutture sanitarie, soprattutto private, offrono servizi gratuiti generalmente riconducibili all'espressione *"**referti on-line**"*

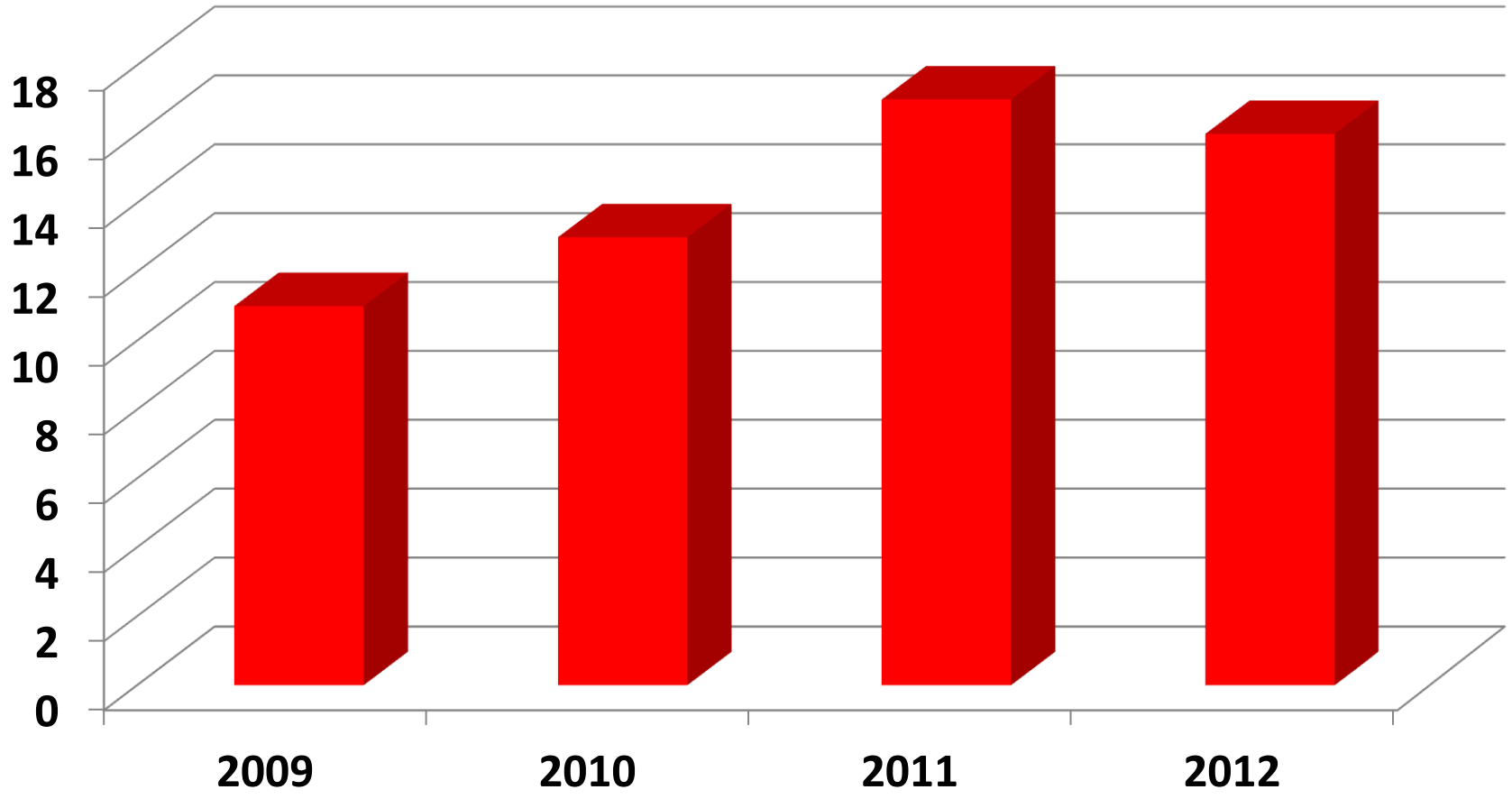
Referto: la relazione scritta rilasciata dal medico sullo stato clinico del paziente dopo un esame clinico o strumentale con modalità informatica.

Statistiche Datalossdb.org – Incidenti per anno



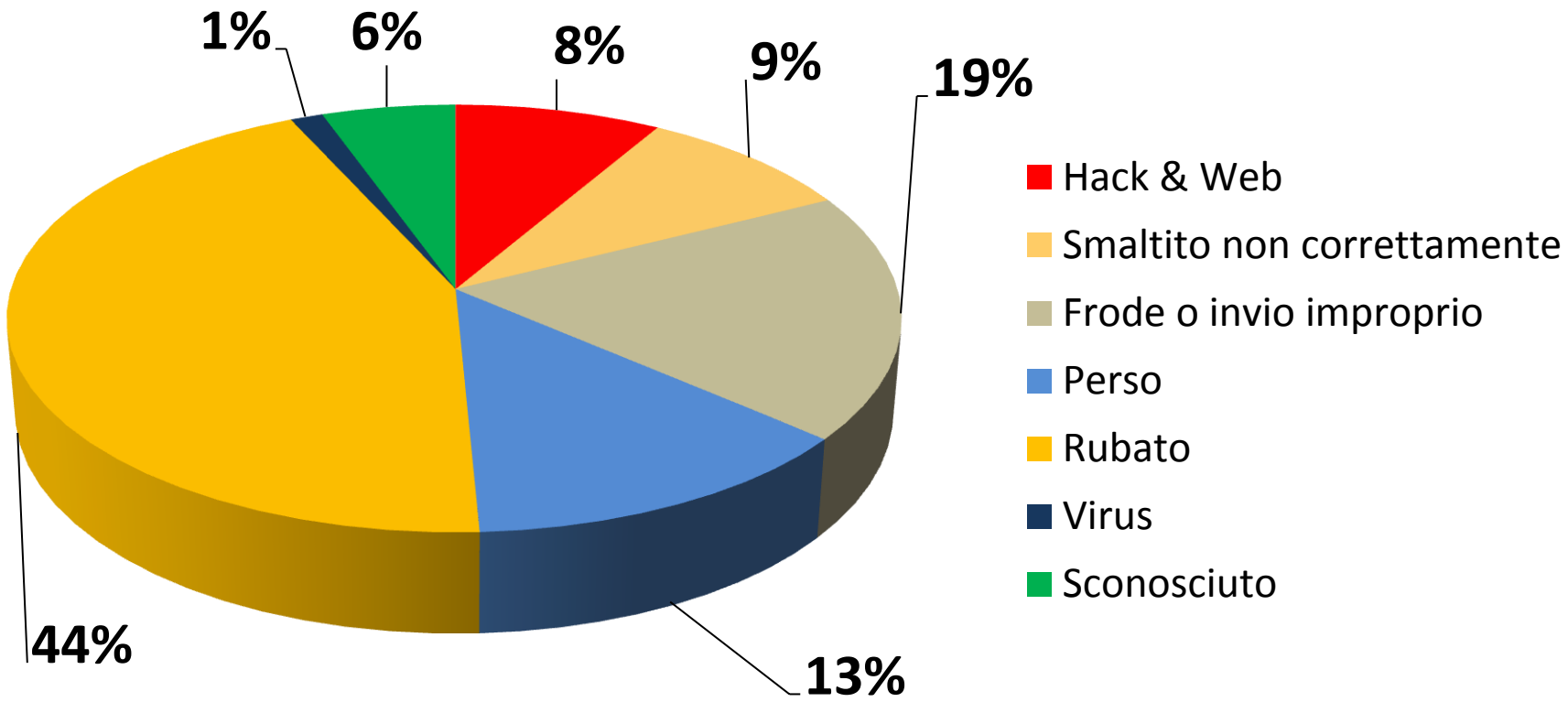
Estrazione 2009-2012 relativa al campo sanitario
Nota: i dati del 2012 sono parziali.

Statistiche Datalossdb.org – Incidenti Web/Hack



Estrazione 2009-2012 relativa al campo sanitario
Nota: i dati del 2012 sono parziali.

Statistiche Datalossdb.org – Tipologia compromissione



Estrazione 2009-2012 relativa al campo sanitario
Nota: i dati del 2012 sono parziali.

Analisi semantica del provvedimento del Garante in tema di Referti on-line

http://www.garanteprivacy.it/garante/doc.jsp?ID=1679033

Modalità di accesso

1) la **ricezione del referto presso la casella di posta elettronica** dell'interessato;

2) il **collegamento al sito *Internet*** della struttura sanitaria ove è stato eseguito l'esame clinico, al fine di **effettuare il *download*** del referto.

Talvolta, **il paziente viene avvisato** della possibilità di visualizzare il referto attraverso una delle modalità sopra descritte mediante **l'invio di uno *short message service* (sms)** sul numero di telefono mobile fornito alla struttura sanitaria dallo stesso paziente all'atto dell'adesione al servizio.

Come interpretare

I referti possono essere inviati tramite email o scaricati dagli utenti via web.

Gli utenti possono dover comunicare il proprio numero cellulare per poter ricevere notifiche inerenti la pubblicazione dei referti.

Funzionalità

In alcune delle iniziative di refertazione *on-line* in essere, è offerto all'interessato anche un servizio aggiuntivo, solitamente gratuito, consistente nella possibilità di archiviare, presso la struttura sanitaria, tutti i referti effettuati nei laboratori della stessa.

Per la consegna degli esiti dell'attività diagnostica e di analisi biomedica si prospettano attualmente i **due** diversi scenari sopra descritti (**email o web**) che pongono problemi di protezione dei dati da affrontare con differenti approcci.

Come interpretare

Il servizio di referti on-line può prevedere il mantenimento dei dati dei pazienti sul server.

Una eventuale compromissione del server permetterebbe, potenzialmente, ad un attaccante di accedere ai referti dei pazienti.

Scenario 1 - Consultazione *on-line*

protocolli di comunicazione sicuri, basati sull'utilizzo di s*tandard* crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (*protocolli https ssl – Secure Socket Layer*);

tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di *caching*, locali o centralizzati, a seguito della sua consultazione *on-line*;

l'utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di *strong authentication*;

disponibilità limitata nel tempo del referto *on-line* (massimo 45 gg.);

possibilità da parte dell'utente di sottrarre alla visibilità in modalità *on-line* o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, **i referti che lo riguardano**.

Come interpretare

Necessario l'uso di SSL.

La cifratura può aiutare nel non lasciare memorizzati dati sensibili in chiaro su sistemi intermedi.

Predilezione per meccanismi di autenticazione forte.

Minimizzazione dell'esposizione al rischio di compromissione di dati sensibili attraverso:
1) una limitazione temporale della permanenza sul server dei referti;
2) la possibilità di del referto rimozione dopo lo scaricamento.

Scenario 2 - Invio via mail

spedizione del referto in forma di allegato a un messaggio *e-mail* e non come testo compreso nella *body part* del Messaggio;
il file contenente il referto dovrà essere protetto con modalità idonee a impedire l'illecita o fortuita acquisizione delle informazioni trasmesse da parte di soggetti diversi da quello cui sono destinati, che potranno consistere in una *password* per l'apertura del file o in una chiave crittografica rese note agli interessati tramite canali di comunicazione differenti da quelli utilizzati per la spedizione dei referti (Cfr. regola 24 del Disciplinare tecnico allegato B) al Codice). Tale cautela può non essere osservata qualora l'interessato ne faccia espressa e consapevole richiesta, in quanto l'invio del referto alla casella di posta elettronica indicata dall'interessato non configura un trasferimento di dati sanitari tra diversi titolari del trattamento, bensì una comunicazione di dati tra la struttura sanitaria e l'interessato effettuata su specifica richiesta di quest'ultimo;
convalida degli indirizzi *e-mail* tramite apposita procedura di verifica *on-line*, in modo da evitare la spedizione di documenti elettronici, pur protetti con tecniche di cifratura, verso soggetti diversi dall'utente richiedente il servizio

Come interpretare

Protezione del referto se spedito via mail con uso di password o crittografia (a meno di altri accordi con il paziente!).

Necessario convalidare gli indirizzi email, nessuna procedura viene suggerita.

Cautele

In ogni caso, per il trattamento dei dati nell'ambito dell'erogazione del servizio *on-line* agli utenti **dovrà essere garantita la disponibilità di**:

idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati), prevedendo il ricorso alla *strong authentication* con utilizzo di caratteristiche biometriche nel caso del trattamento di dati idonei a rivelare l'identità genetica di un individuo;
separazione fisica o logica dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali trattati per scopi amministrativo-contabili.
Il titolare del trattamento dovrebbe, inoltre, **prevedere apposite procedure che rendano immediatamente non disponibili per la consultazione *on-line* o interrompano la procedura di spedizione per posta elettronica dei referti relativi a un interessato che abbia comunicato il furto o lo smarrimento delle proprie credenziali di autenticazione** all'accesso al sistema di consultazione *on-line* o altre condizioni di possibile rischio per la riservatezza dei propri dati personali.

Come interpretare

Data la criticità di un possibile accesso fraudolento che sfrutti le credenziali di accesso di un medico è importante che tutti gli accessi privilegiati siano gestiti con particolati cautele.

I dati medici dei pazienti e le anagrafiche devono essere separate fisicamente o logicamente.

Prevedere procedure di blocco tempestive per impedire la consultazione dei referti a seguito di smarrimento delle credenziali da parte del paziente.

Uhmm controlliamo ?

1. **Ricerca con Google** di sistemi di Referti on-line
2. Presa in esame di **20 siti di Referti on-line**
3. **Analisi blackbox** delle funzionalità:
   - Lettura dei procedure e manuali (se presenti)
   - Analisi delle tecnologie in uso (e.g. SW in uso)
   3. Osservazione di eventuali **discrepanze tra le implementazioni ed i requisiti**

Sicurezza delle comunicazioni

- Richiesto uso di SSL =! Deve funzionare solo in SSL

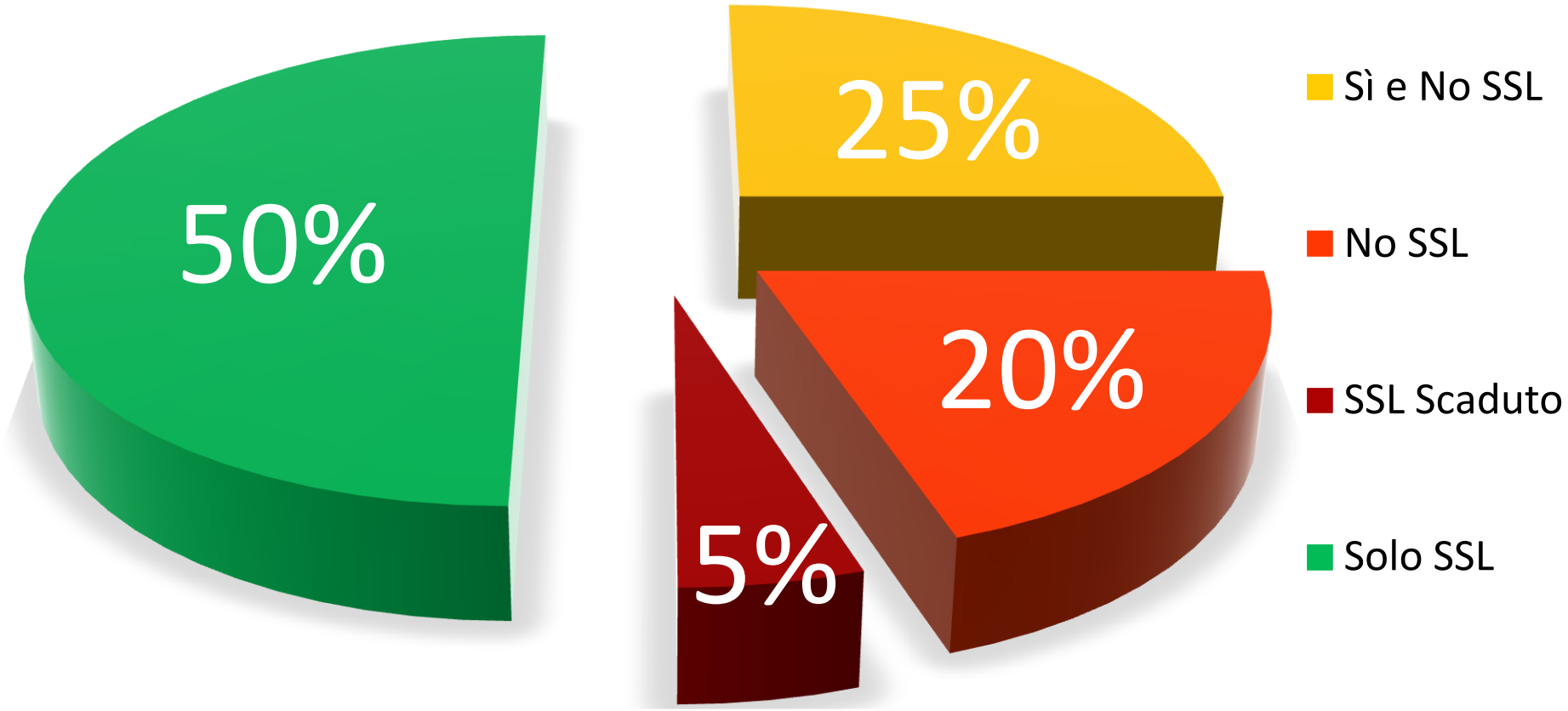
Alcuni **non funzionano in SSL**

- **http://**www.referti[redacted]
- **http://**www.salu[redacted]

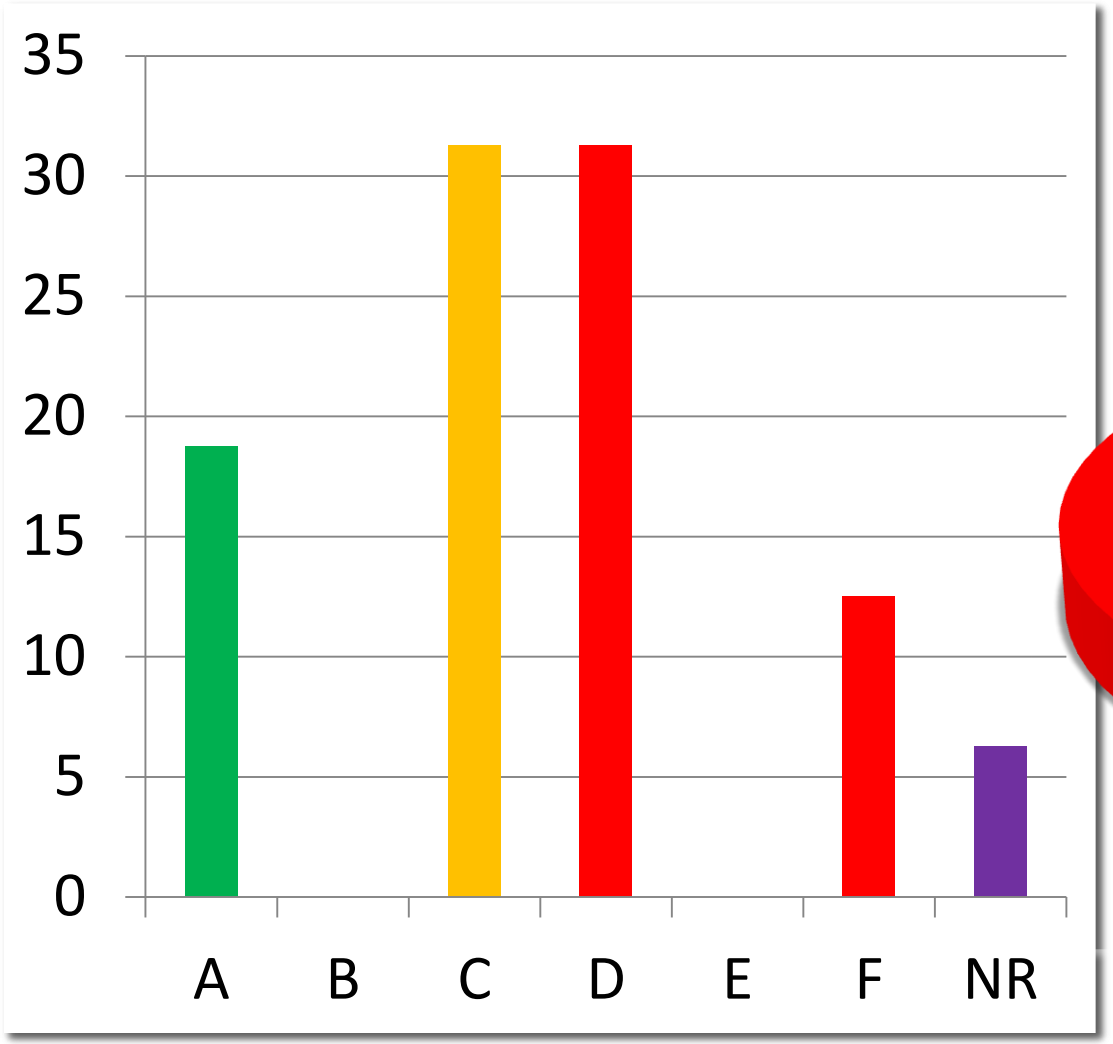
Altri funzionano benissimo **anche senza SSL**:

- **https://**mdb[redacted]/login.jsf
- **http://**mdb[redacted]/login.jsf

Analisi dell'uso di SSL

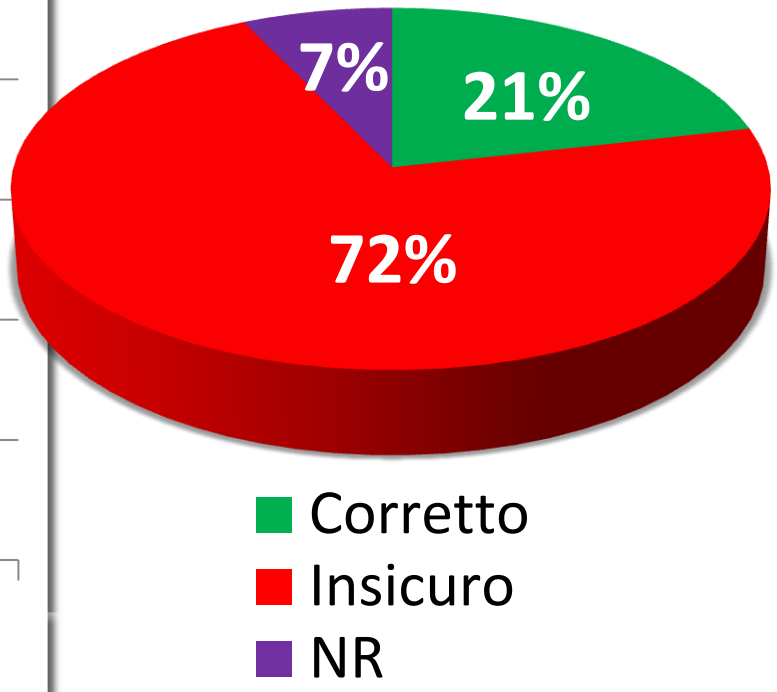


Di quelli che implementavano SSL…



QUALYS® SSL LABS

Riassumendo:



Sembra quasi phishing… in realtà è Hosting!

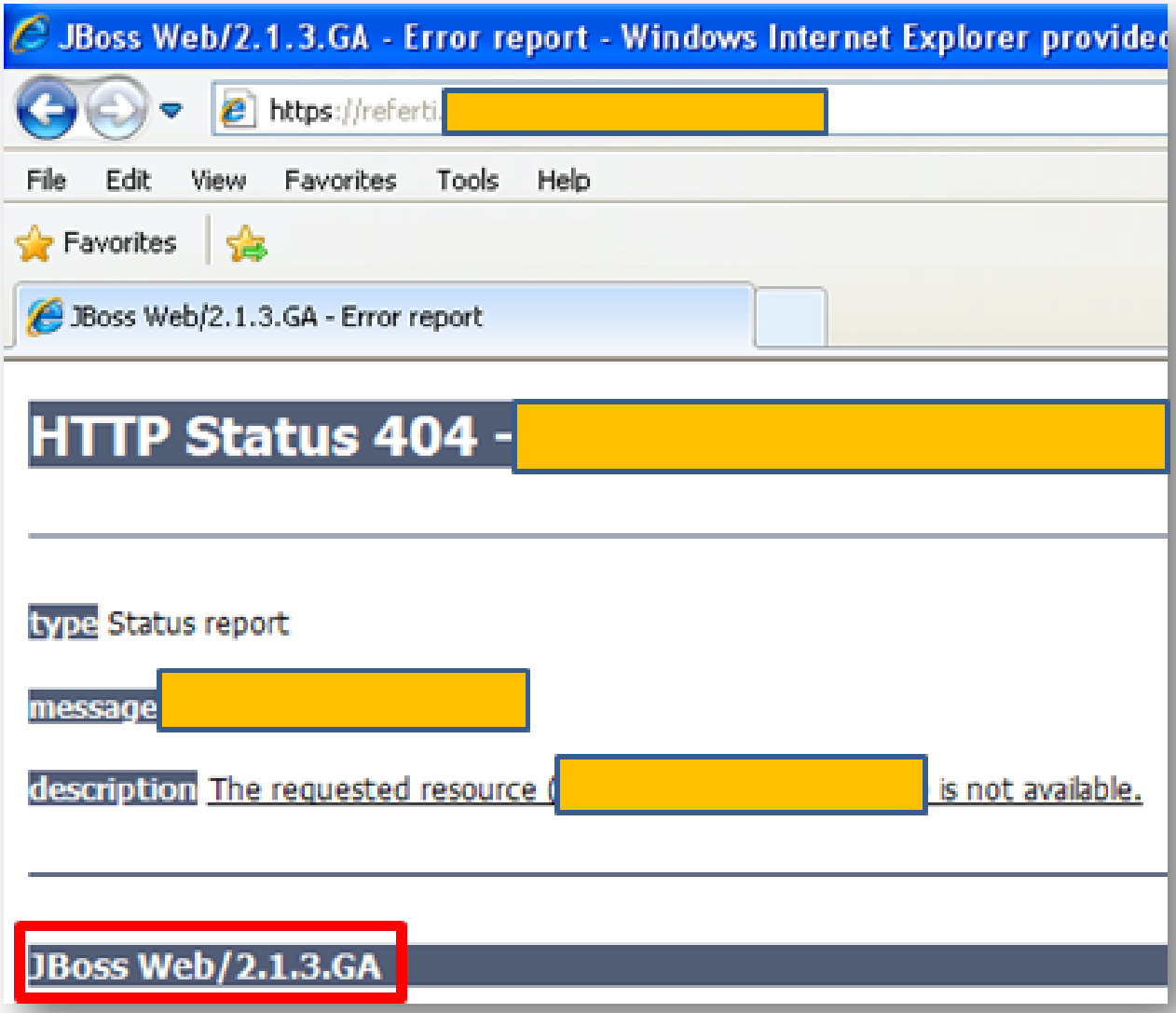
- Spesso i referti sono scaricabili da indirizzi come:
  - https://online[redacted].it
  - https://referti[redacted].it/
- A volte non è un sito riconducibile all'ospedale!
  - I referti della [redacted] della regione [redacted] che ha come sito http://www.[redacted]it sono pubblicati su un sito esterno di una società informatica: http://www.[redacted].mi.it/[redacted]/

Analisi delle tecnologie in uso

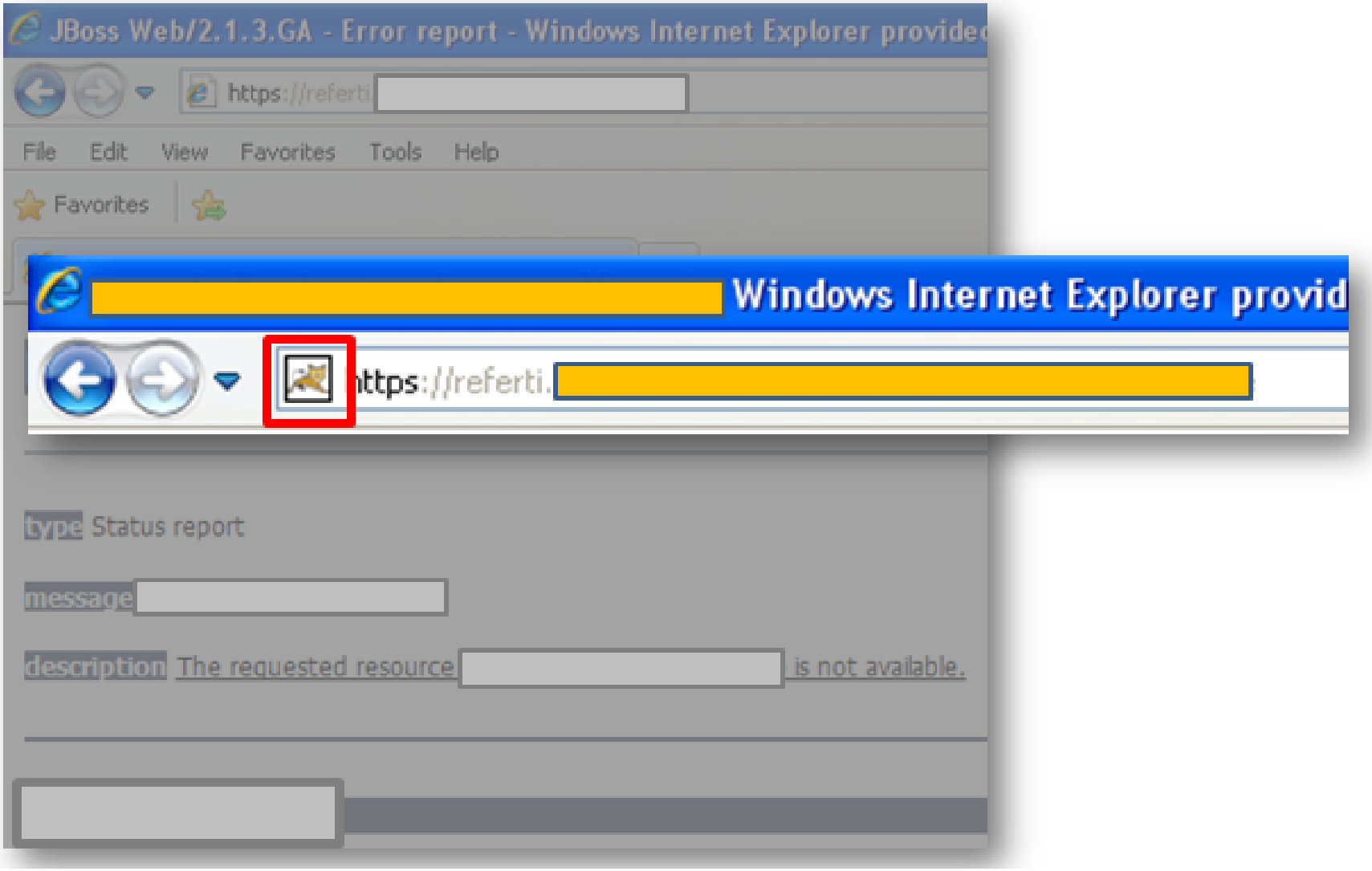
- Web Server
- Application Server
- Web application
- Linguaggio di programmazione
- Framework
- Sistema operativo in uso
- Etc..

Apache

Analisi delle tecnologie in uso: JBoss



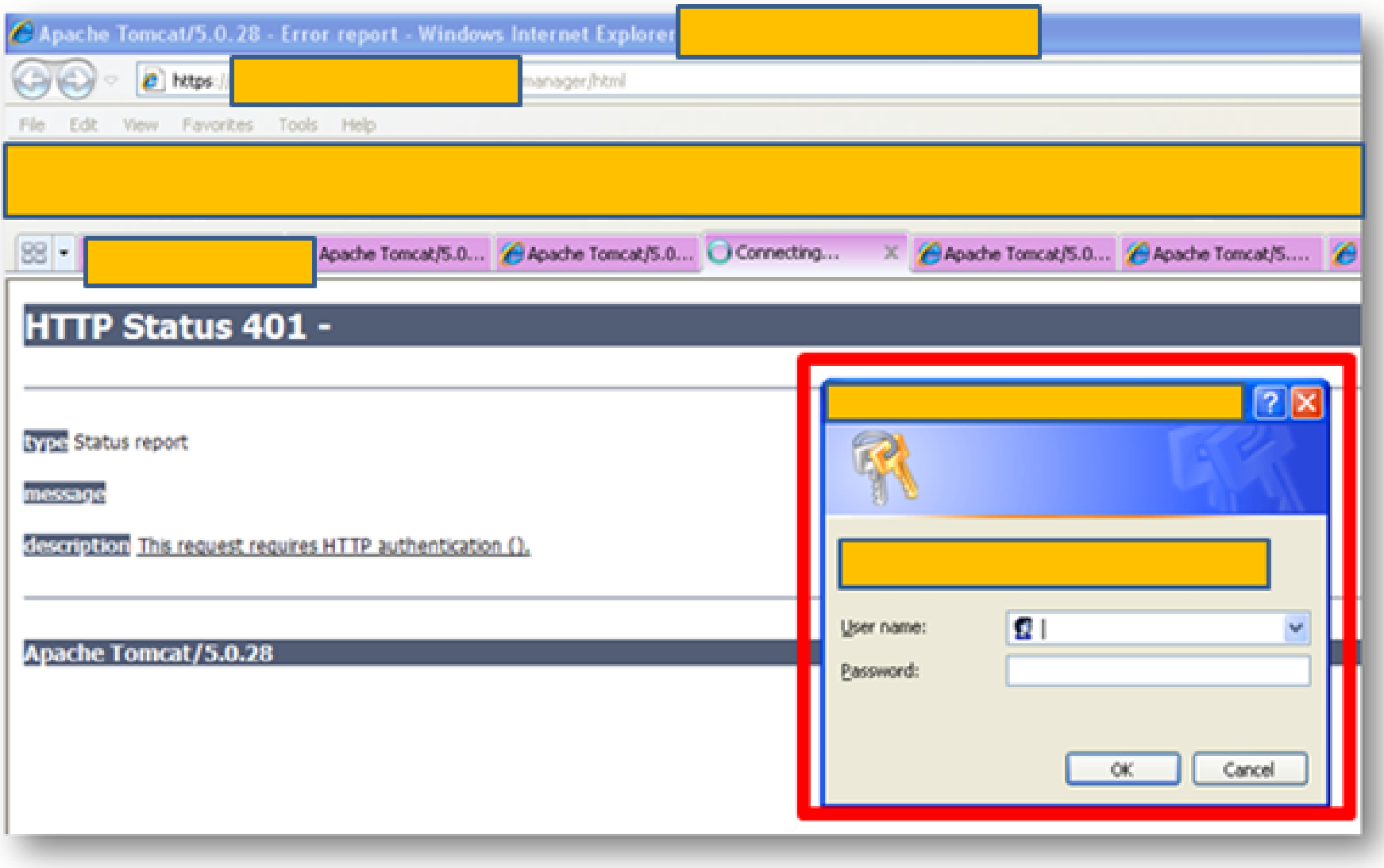
Analisi delle tecnologie in uso: Tomcat



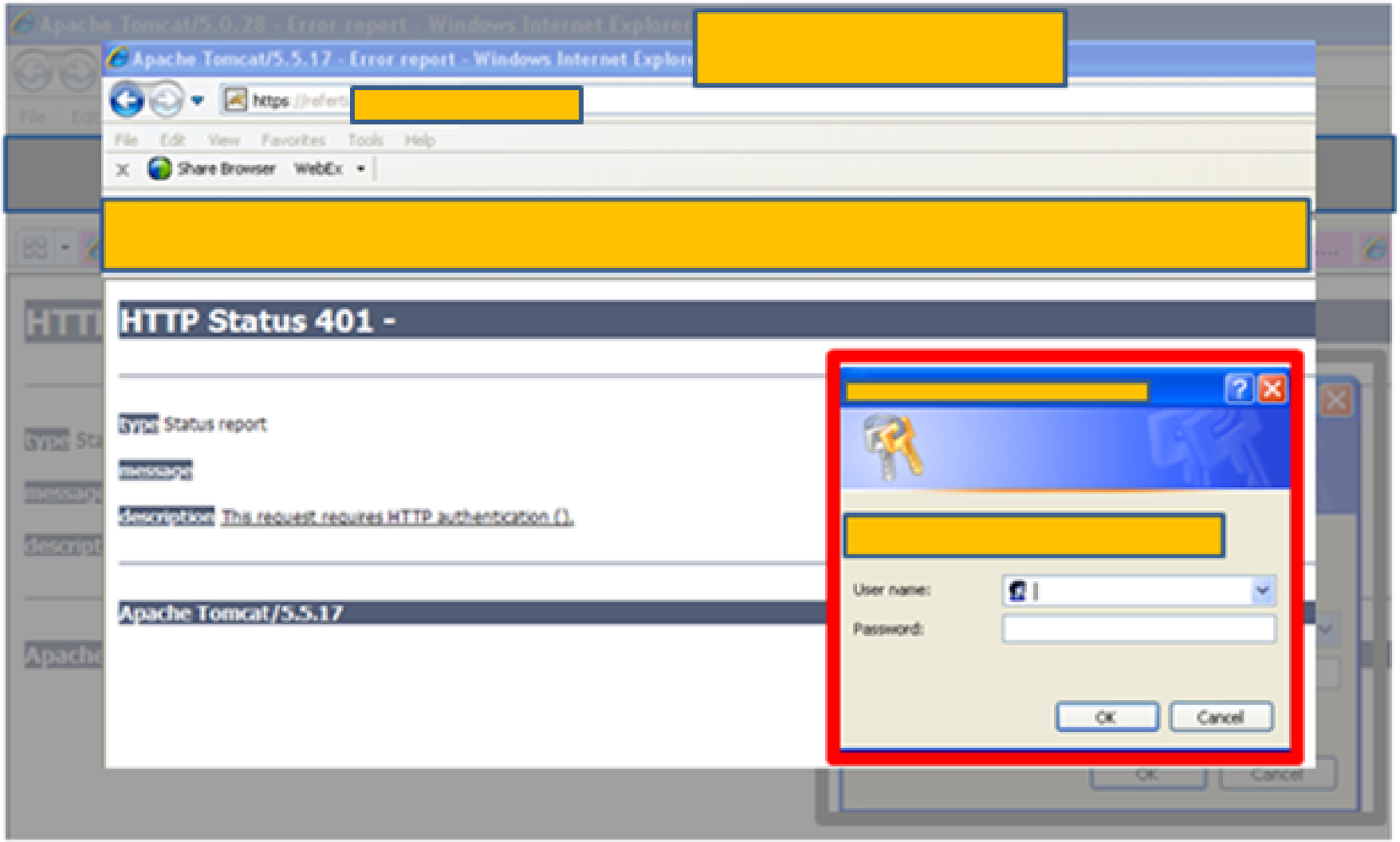
Pannelli di amministrazione esposti / nascosti

- **Login per Applicazione Server**
- **Login per Pannelli di amministrazione dei Framework**
- **Login per Pannelli di amministrazione delle Web Application**
- **Login per Medici e dipendenti**
- **Etc..**

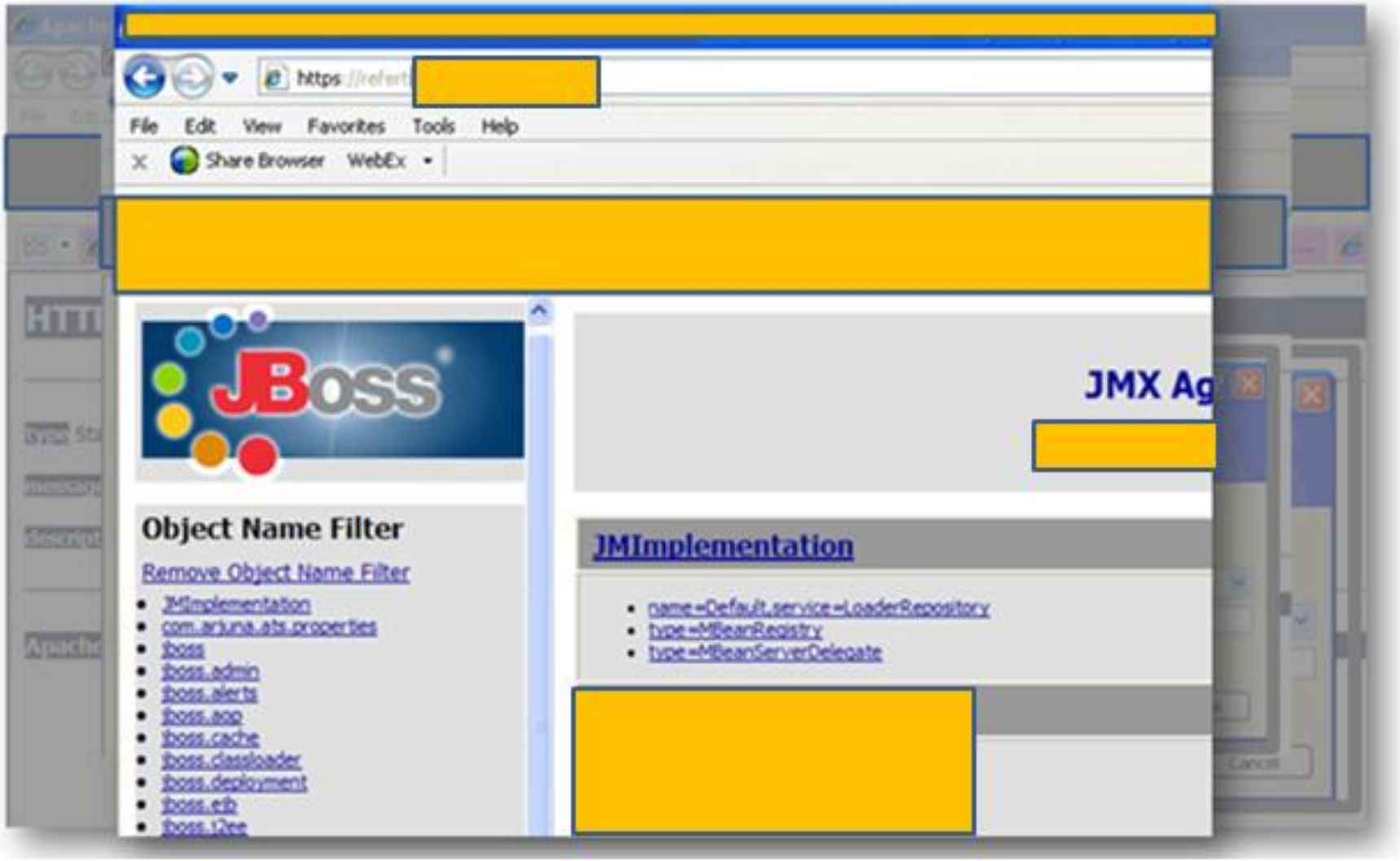
Login per App. Server? Contiamo: Uno…



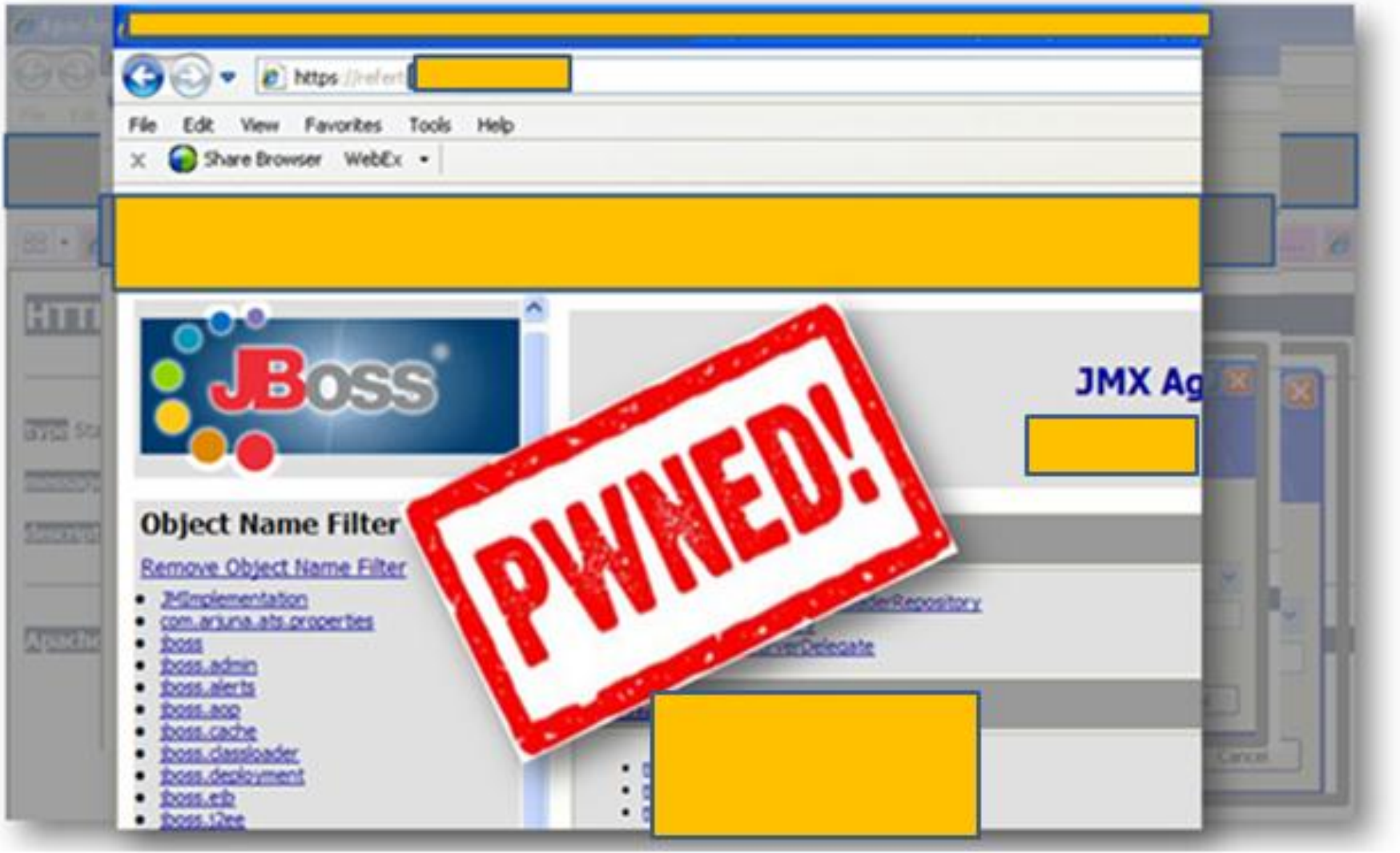
Login per App. Server? Contiamo: Uno… Due…



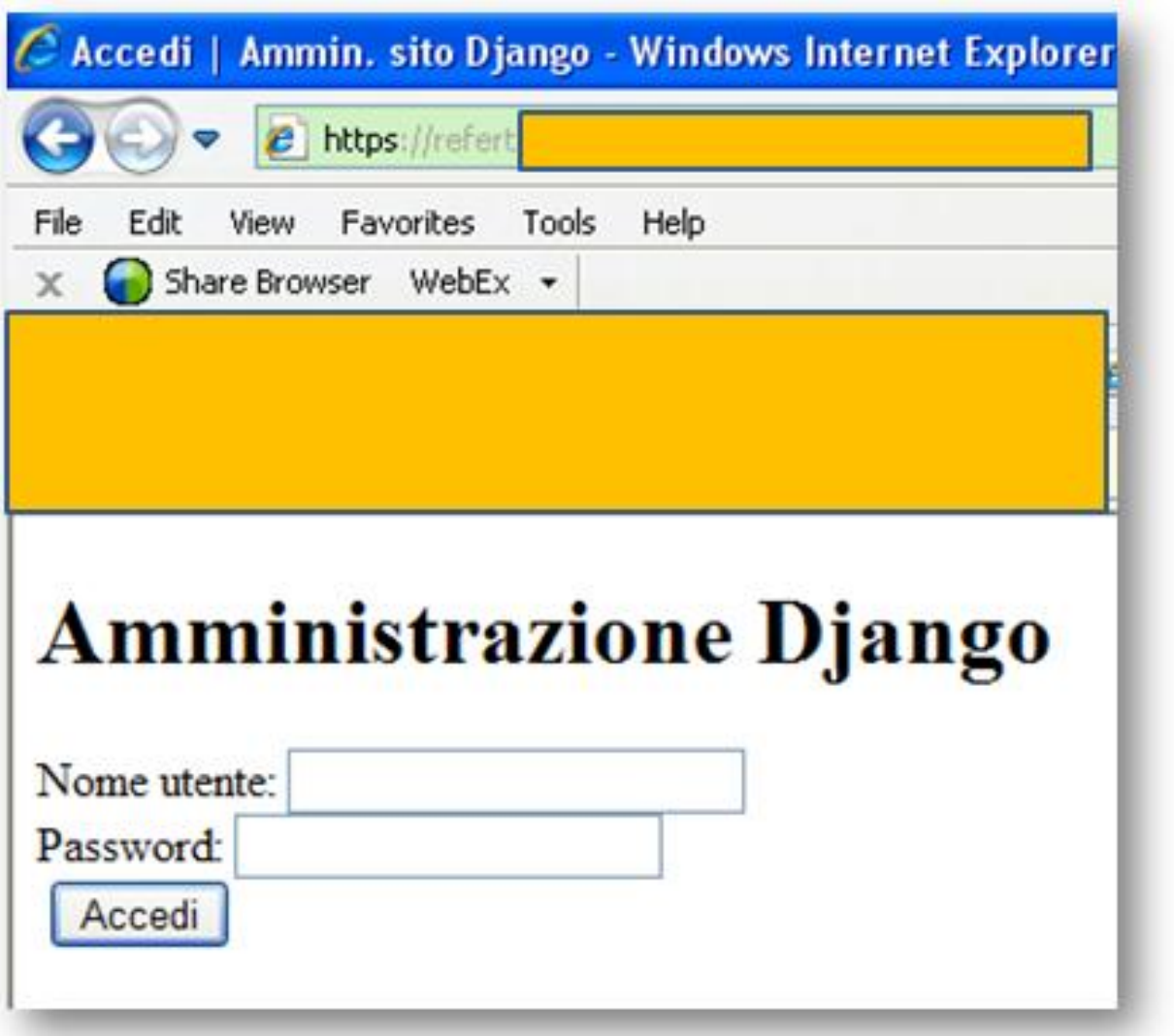
Login per App. Server? Contiamo: Uno… Due..Tre!



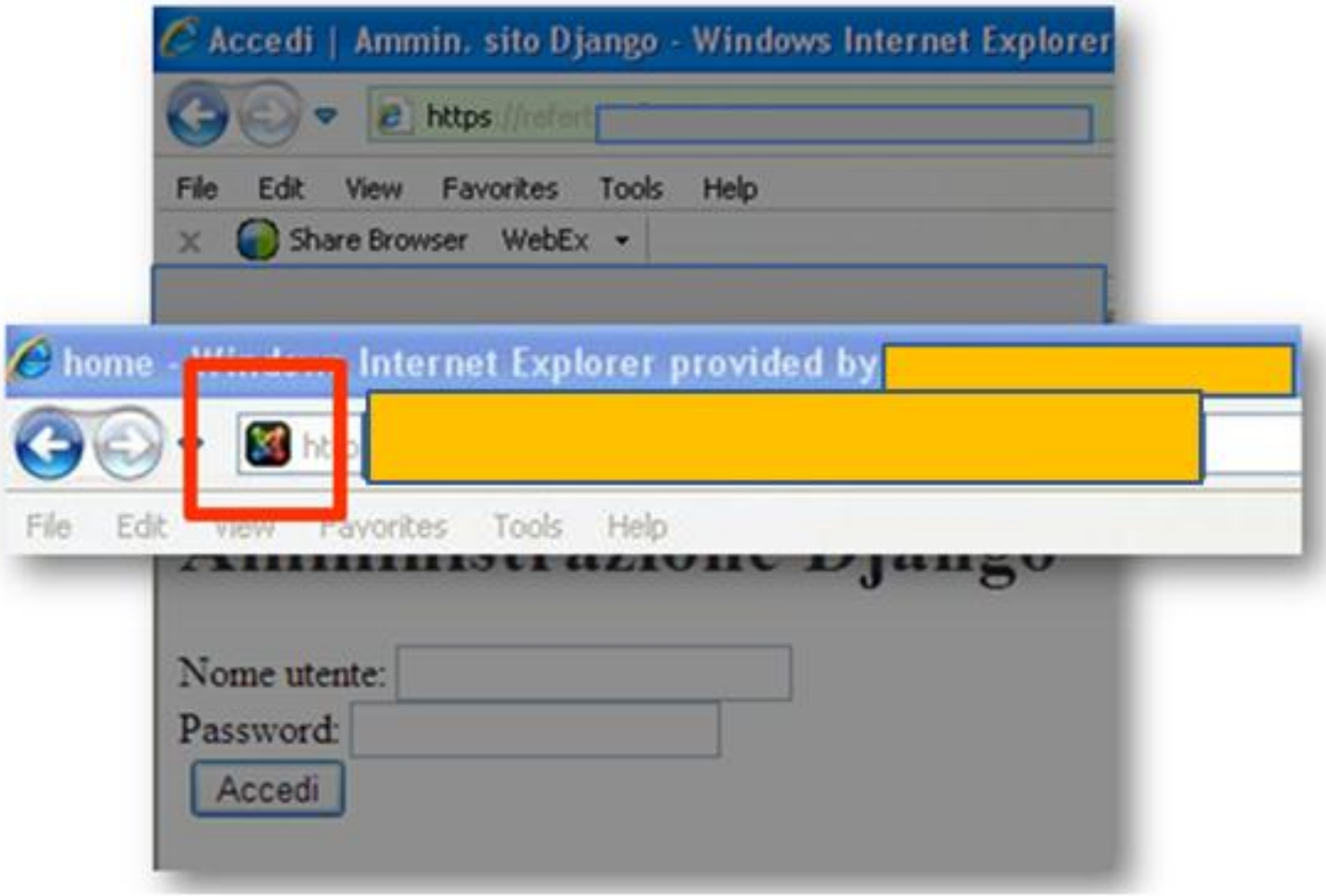
Login per App. Server? Contiamo: Uno… Due..Tre!



Login Amministrazione Framework/Web app ?



Login Amministrazione Framework/Web app ?



Software obsoleti… per dati sensibili

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. **In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.**

Fonte: http://www.garanteprivacy.it/garante/doc.jsp?ID=1557184

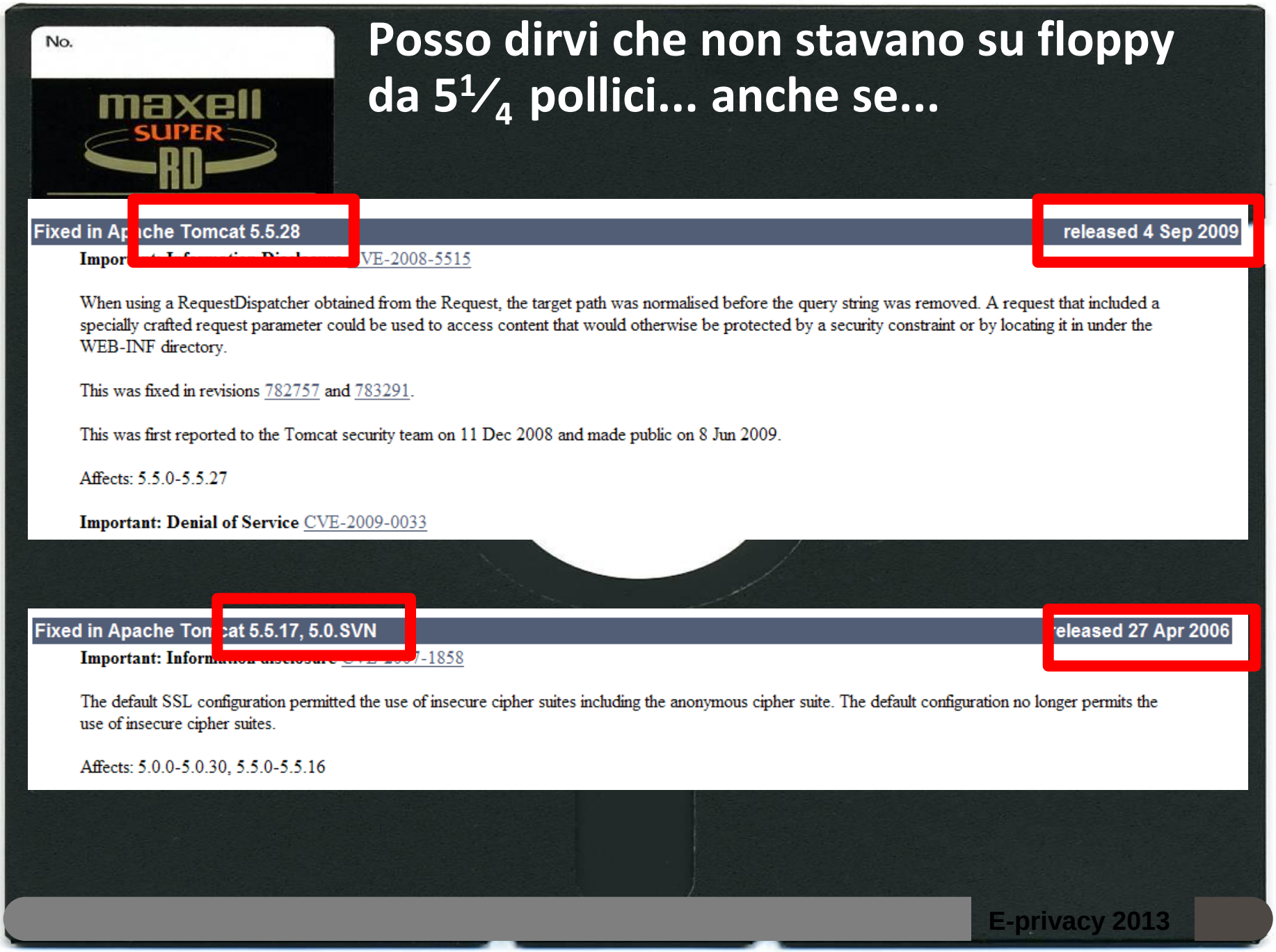
Come interpretare

Applicare ogni sei mesi gli aggiornamenti rilasciati dai produttori dei software in uso, seguire le linee guida per la configurazione sicura dei programmi.

- Vi ricordate le versioni dei due Tomcat visti poco fa?

Posso dirvi che non stavano su floppy da 5¼ pollici... anche se...

Pronti?



Posso dirvi che non stavano su floppy da 5¼ pollici... anche se...

Fixed in Apache Tomcat 5.5.28 — released 4 Sep 2009

Important: Information Disclosure CVE-2008-5515

When using a RequestDispatcher obtained from the Request, the target path was normalised before the query string was removed. A request that included a specially crafted request parameter could be used to access content that would otherwise be protected by a security constraint or by locating it in under the WEB-INF directory.

This was fixed in revisions 782757 and 783291.

This was first reported to the Tomcat security team on 11 Dec 2008 and made public on 8 Jun 2009.

Affects: 5.5.0-5.5.27

Important: Denial of Service CVE-2009-0033

Fixed in Apache Tomcat 5.5.17, 5.0.SVN — released 27 Apr 2006

Important: Information disclosure CVE 2006-1858

The default SSL configuration permitted the use of insecure cipher suites including the anonymous cipher suite. The default configuration no longer permits the use of insecure cipher suites.

Affects: 5.0.0-5.0.30, 5.5.0-5.5.16

Posso dirvi che non stavano su floppy da 5¼ pollici... anche se...

Apache » Tomcat » 5.0.28 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:tomcat:5.0.28*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : Cve Number Descending Cve Number Ascending CVSS Score Descending Number Of Exploits Descending

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type (s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complex ity	Authen tication	Confiden tiality	Integrity	Availa bility
1	CVE-2009-3548	255		+Priv	2009-11-12	2011-07-18	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges.														
2	CVE-2006-3835				2006-07-25	2010-05-12	5.0	None	Remote	Low	Not required	Partial	None	None
Apache Tomcat 5 before 5.5.17 allows remote attackers to list directories via a semicolon (;) preceding a filename with a mapped extension, as demonstrated by URLs ending with /;index.jsp and /;help.do.														
3	CVE-2007-0450	22		Dir. Trav.	2007-03-16	2010-08-21	5.0	None	Remote	Low	Not required	Partial	None	None
Directory traversal vulnerability in Apache HTTP Server and Tomcat 5.x before 5.5.22 and 6.x before 6.0.10, when using certain proxy modules (mod_proxy, mod_rewrite, mod_jk), allows remote attackers to read arbitrary files via a .. (dot dot) sequence with combinations of (1) "/" (slash), (2) "\" (backslash), and (3) URL-encoded backslash (%5C) characters in the URL, which are valid separators in Tomcat but not in Apache.														
4	CVE-2007-5333	200		+Info	2008-02-11	2011-04-20	5.0	None	Remote	Low	Not required	Partial	None	None
Apache Tomcat 6.0.0 through 6.0.14, 5.5.0 through 5.5.25, and 4.1.0 through 4.1.36 does not properly handle (1) double quote (") characters or (2) %5C (encoded backslash) sequences in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks. NOTE: this issue exists because of an incomplete fix for CVE-2007-3385.														
5	CVE-2006-7195			XSS	2007-05-09	2010-08-21	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in implicit-objects.jsp in Apache Tomcat 5.0.0 through 5.0.30 and 5.5.0 through 5.5.17 allows remote attackers to inject arbitrary web script or HTML via certain header values.														
6	CVE-2006-7196	79		XSS	2007-05-09	2009-02-05	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in the calendar application example in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.31, 5.0.0 through 5.0.30, and 5.5.0 through 5.5.15 allows remote attackers to inject arbitrary web script or HTML via the time parameter to cal2.jsp and possibly unspecified other vectors. NOTE: this may be related to CVE-2006-0254.1.														
7	CVE-2007-1355			XSS	2007-05-21	2009-07-01	4.3	None	Remote	Medium	Not required	None	Partial	None

Posso dirvi che non stavano su floppy da 5¼ pollici... anche se...

Apache » Tomcat » 5.0.28 : Security Vulnerabilities

Apache » Tomcat » 5.5.17 : Security Vulnerabilities

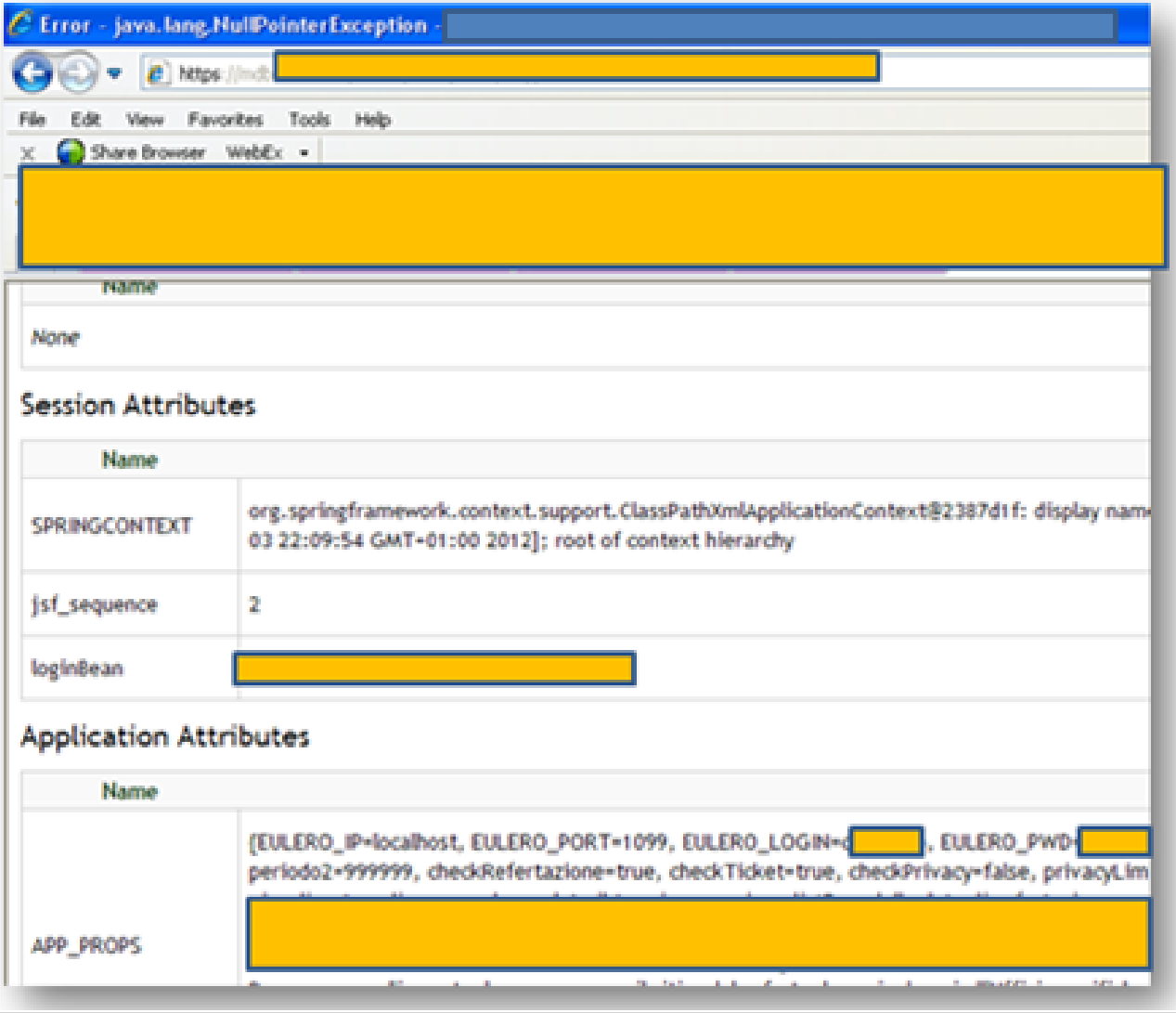
Cpe Name:*cpe:/a:apache:tomcat:5.5.17*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

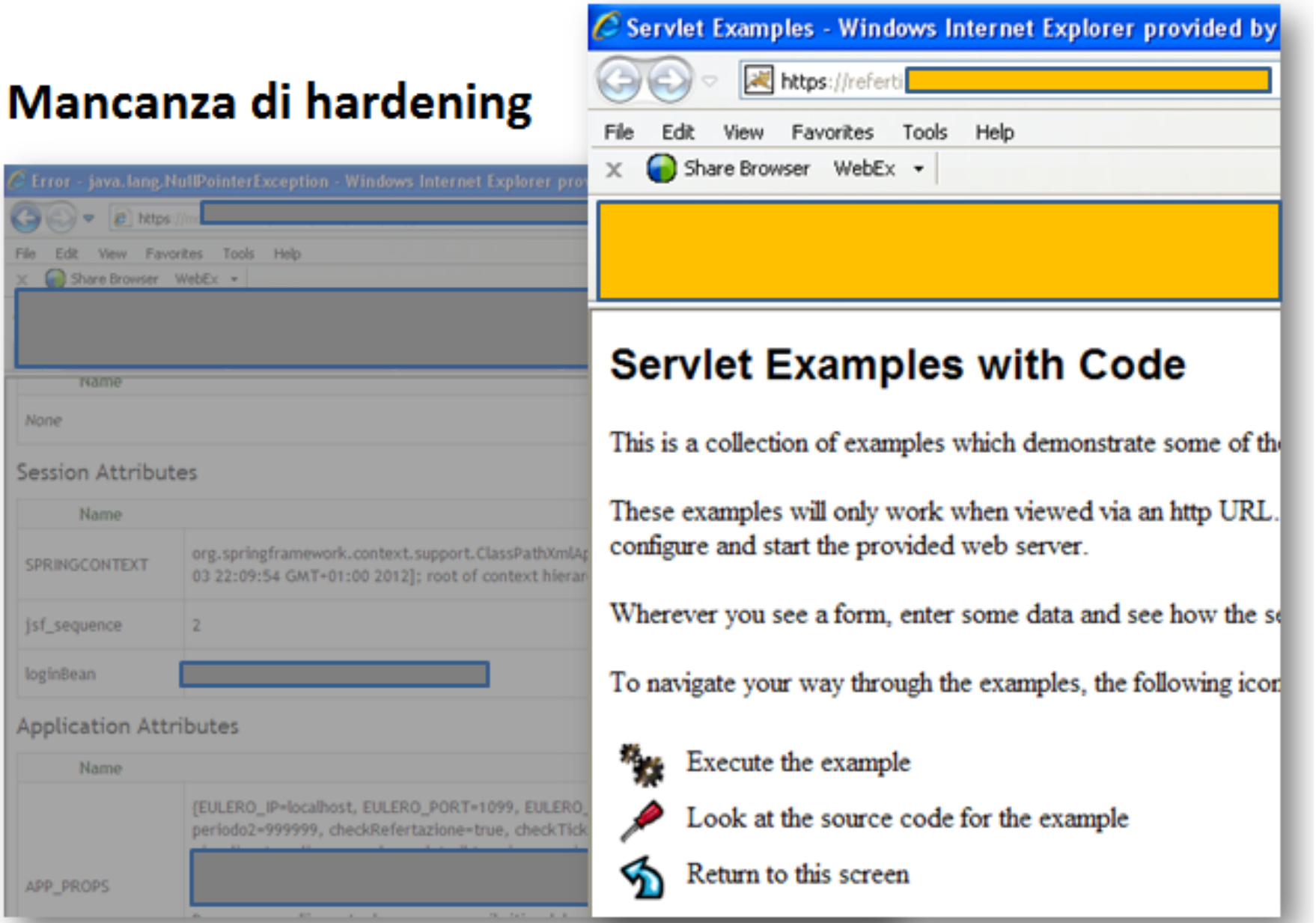
Sort Results By : Cve Number Descending Cve Number Ascending CVSS Score Descending Number Of Exploits Descending

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type (s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complex ity	Authen tication	Confiden tiality	Integrity	Availa bility
1	CVE-2009-3548	255		+Priv	2009-11-12	2011-07-18	7.5	User	Remote	Low	Not required	Partial	Partial	Partial
The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges.														
2	CVE-2011-3190	264		Bypass +Info	2011-08-31	2012-08-13	7.5	None	Remote	Low	Not required	Partial	Partial	Partial
Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.33, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request.														
3	CVE-2007-5342	264			2007-12-27	2010-08-21	6.4	None	Remote	Low	Not required	Partial	Partial	None
The default catalina.policy in the JULI logging component in Apache Tomcat 5.5.9 through 5.5.25 and 6.0.0 through 6.0.15 does not restrict certain permissions for web applications, which allows attackers to modify logging configuration options and overwrite arbitrary files, as demonstrated by changing the (1) level, (2) directory, and (3) prefix attributes in the org.apache.juli.FileHandler handler.														
4	CVE-2010-2227	119		DoS Overflow +Info	2010-07-13	2011-10-20	6.4	None	Remote	Low	Not required	Partial	None	Partial
Apache Tomcat 5.5.0 through 5.5.29, 6.0.0 through 6.0.27, and 7.0.0 beta does not properly handle an invalid Transfer-Encoding header, which allows remote attackers to cause a denial of service (application outage) or obtain sensitive information via a crafted header that interferes with "recycling of a buffer."														
5	CVE-2009-2693	22		Dir. Trav.	2010-01-28	2011-09-06	5.8	None	Remote	Medium	Not required	None	Partial	Partial
Directory traversal vulnerability in Apache Tomcat 5.5.0 through 5.5.28 and 6.0.0 through 6.0.20 allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in an entry in a WAR file, as demonstrated by a ../../bin/catalina.bat entry.														
6	CVE-2007-0450	22		Dir. Trav.	2007-03-16	2010-08-21	5.0	None	Remote	Low	Not required	Partial	None	None
Directory traversal vulnerability in Apache HTTP Server and Tomcat 5.x before 5.5.22 and 6.x before 6.0.10, when using certain proxy modules (mod_proxy, mod_rewrite, mod_jk), allows remote attackers to read arbitrary files via a .. (dot dot) sequence with combinations of (1) "/" (slash), (2) "\" (backslash), and (3) URL-encoded backslash (%5C) characters in the URL, which are valid separators in Tomcat but not in Apache.														

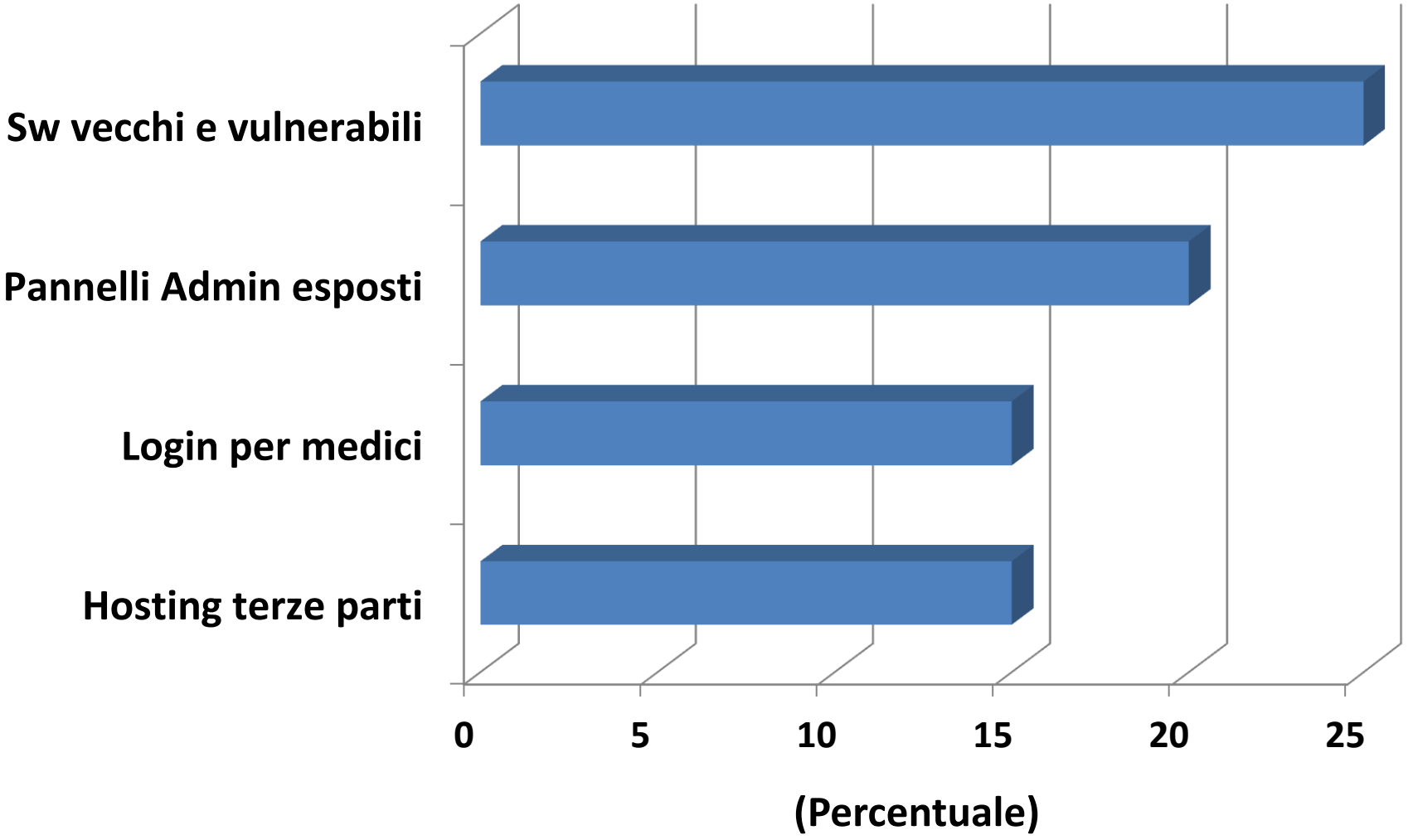
Mancanza di hardening



Mancanza di hardening

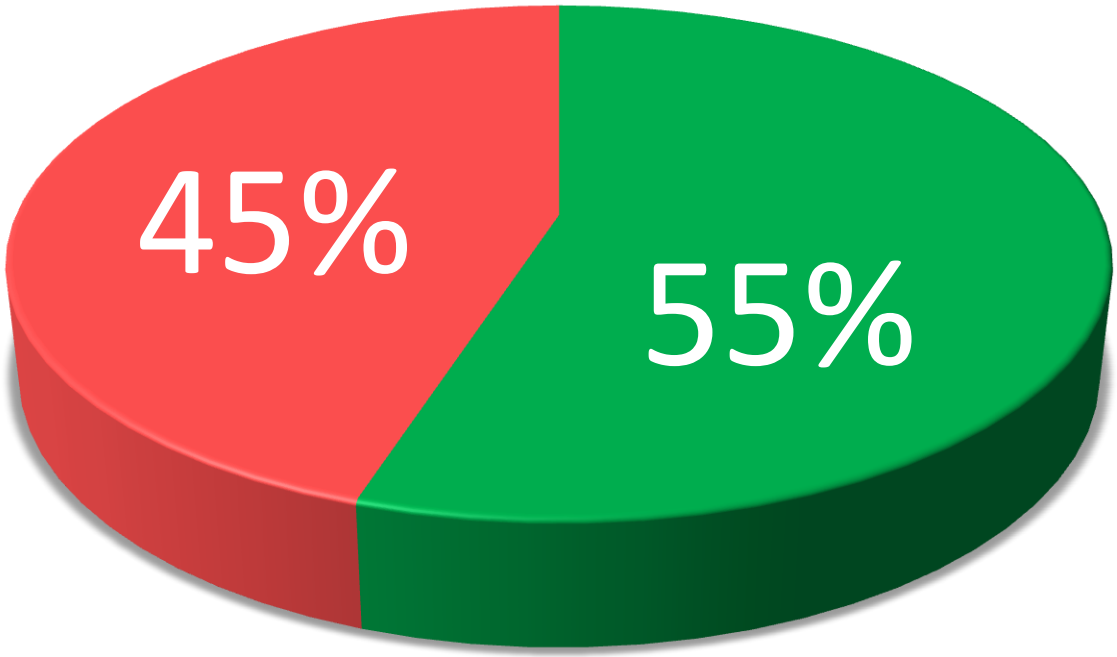


Analisi di alcune delle caratteristiche discusse



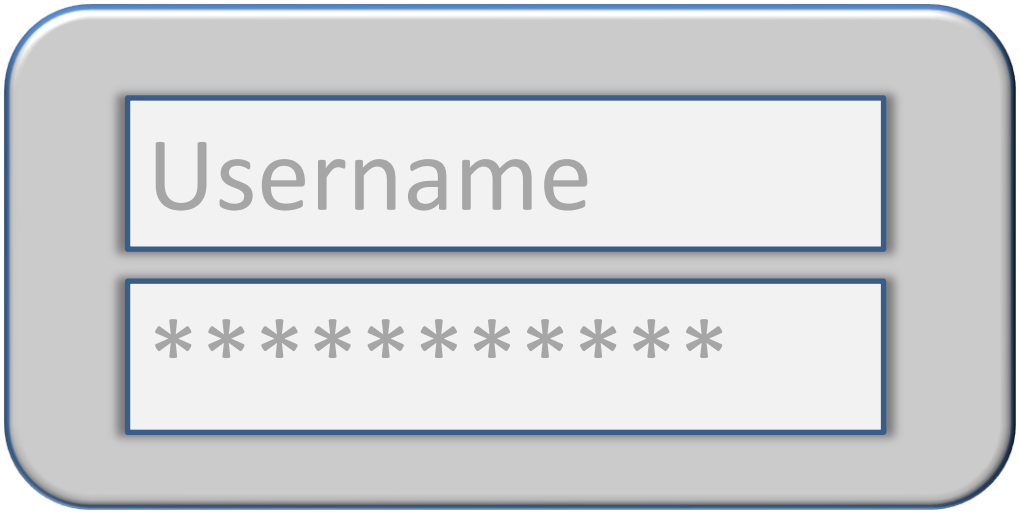
Analisi riassuntiva della rischiosità percepita

- Sistemi non particolarmente rischiosi
- Sistemi particolarmente rischiosi (Pannelli Admin esposti + Sw vulnerabili e non aggiornati)

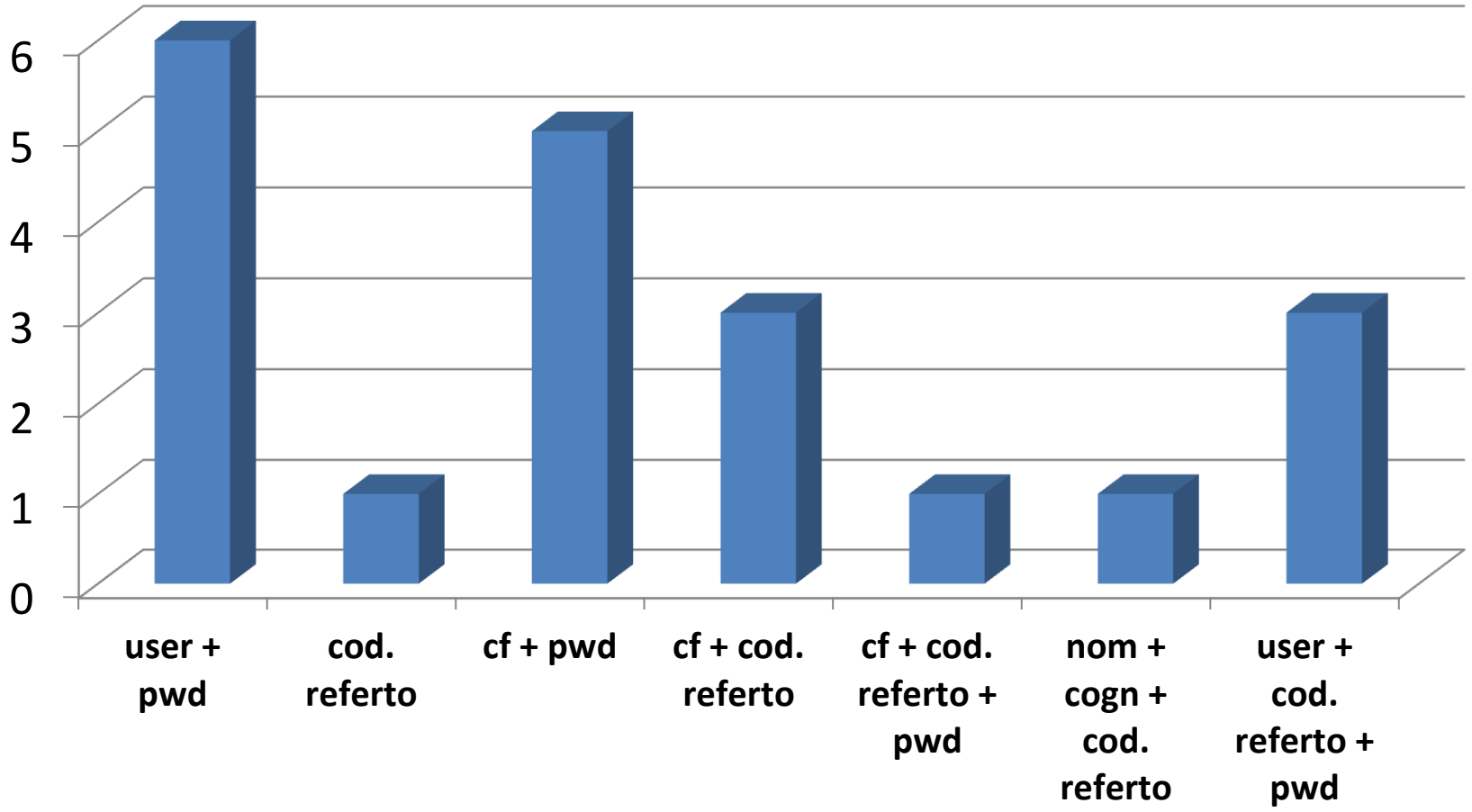


Ma come si fa il login?

- La maggior parte richiede:
  - Username: **codice fiscale**
  - Password: **codice referto/numero richiesta**
  - Alcuni richiedono un “**PIN**” altri hanno anche un **Captcha**
  - In Lombardia si predilige l’uso della **CRS**



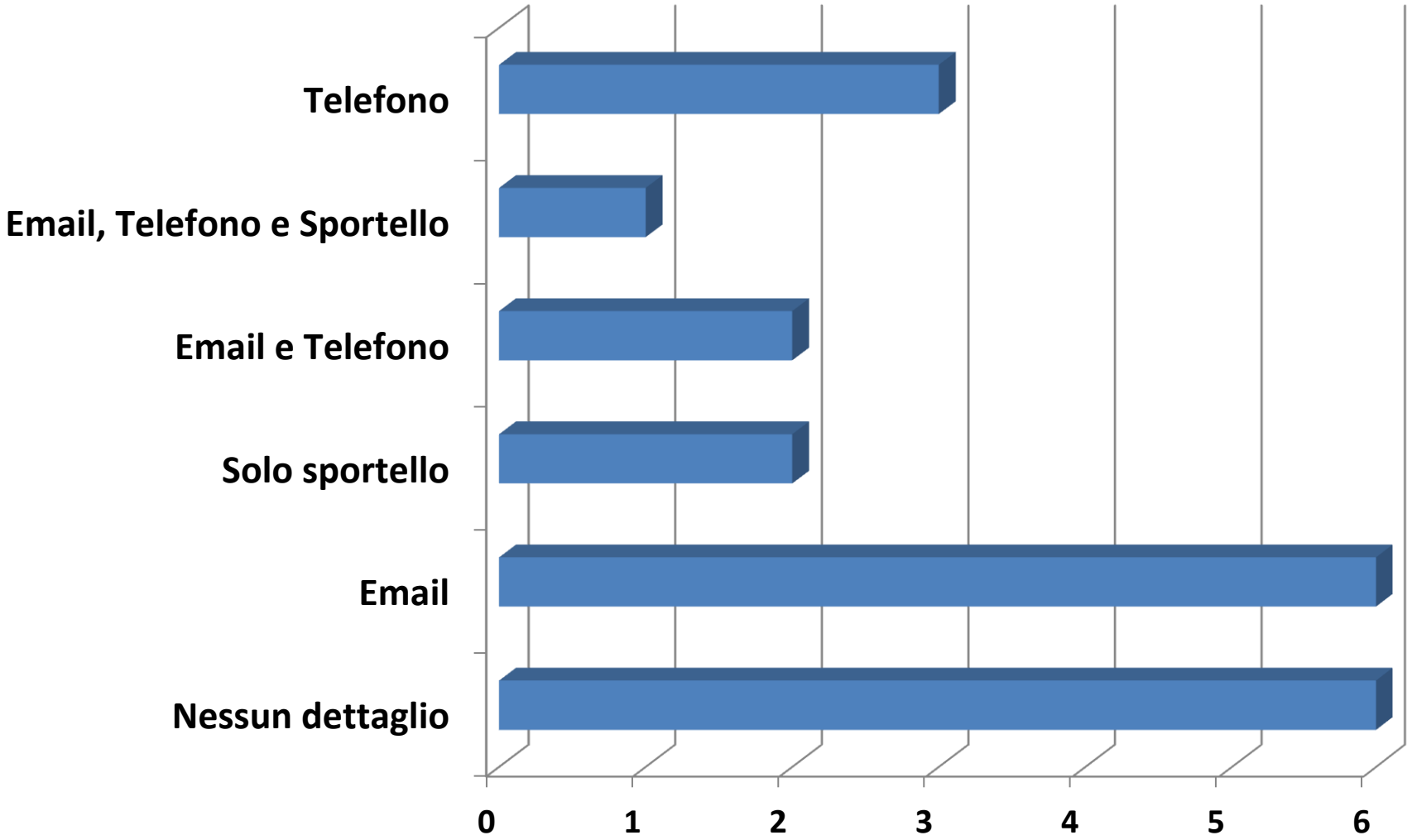
Analisi dei sistemi di login



Smarrimento e blocco delle credenziali di accesso

- Diversi siti non hanno una procedura predefinita e ben comunicata agli utenti per il blocco delle credenziali di accesso o del sistema di invio via mail
- Nella maggior parte dei casi esiste un numero telefonico e/o un indirizzo email di assistenza che in orari “da ufficio” gestisce questo tipo di “pratiche”
- In un paio di casi è necessario andare allo sportello…
- Nessuno sembra adoperare una procedura di blocco in real-time

Statistica sui sistemi di blocco



Riassumendo…

- Abbiamo analizzato il funzionamento del servizio Consultazione Online dei referti e abbiamo trovato le seguenti situazioni:
  - Uso di canali di trasmissione insicuri
  - Uso “discutibile” di sistemi di terze parti
  - Pannelli di amministrazione esposti su Internet
  - Pannelli di amministrazione senza password
  - Software non aggiornati e vulnerabili
  - Mancanza di hardening
  - Fantasia nei sistemi di autenticazione

Nessun sito è stato maltrattato durante queste analisi

- $ Non abbiamo provato nessun attacco volto a sfruttare vulnerabilità nei sistemi di autenticazione, autorizzazione, validazione degli input, logica dell'applicazione, etc..
- $ Non abbiamo avuto modo di agire dopo il login
- $ Non abbiamo avuto modo di analizzare i sistemi di invio referti via email
- $ Non abbiamo avuto modo di validare le soluzioni di richiesta di blocco dell'account

Frequently Asked Questions / Frequently Repeated Answers

Domanda: Cosa succede dopo che l'utente si autentica ?

Risposta: Può scaricare i referti

Domanda: Sì ma …. solo i suoi vero?

Risposta: La sicurezza di sitemi critici come quelli che garantiscono l'accesso a dati sensibili dovrebbero essere progettati con precauzioni e controlli di sicurezza periodici per minimizzare i rischi...

E' solo fantasia?

Vecchie soluzioni per vecchi problemi

- Per tutte le applicazioni esposte su Intenet che trattano dati sensibili si dovrebbero **verificarne gli aggiornamenti e la sicurezza in modo periodico** e applicare le patch rilasciate dai produttori. Esistono soluzioni automatizzate che permettono di avere un inventario degli asset e di gestire i software ed i relativi aggiornamenti.
- Esistono **soluzioni automatizzate** che scansionano i server ed **individuano problematiche di sicurezza.**
- Alcuni sistemi di base come l'uso di canali cifrati HTTP over SSL dovrebbero essere sempre adottati e manutenuti nel tempo (Rinnovare i certificati).
- Se si vogliono mantenere sistemi di login critici come quelle di medici, farmacie e amministratori l'**uso di token** è auspicabile. **Esistono soluzione di token virtuale** su telefono che abbattono notevolmente i costi.

Domande ?

Thank you!

gabriele.zanoni@gmail.com

https://www.twitter.com/infoshaker