- SQL Injection -
Di seguito viene presentato un esempio di come sia possibile sfruttare la vulnerabilita' per eseguire comandi SQL sul database di back-end, tramite una normale richiesta HTTP all'indirizzo

http://www.toroassicurazioni.it. Questi comandi possono essere utilizzati per interagire con il database (creare/cancellare tabelle, leggere i dati, etc.), o anche, grazie
alle extended stored procedure di MS-SQL Server, per eseguire programmi sul server di back-end.
E' importante notare che la vulnerabilita' e' sfruttabile da qualsiasi pagina del sito, e non e' legata ad
una sezione o form particolare.

http://www.toroassicurazioni.it/index.asp?IDCAT=1%3B+EXEC+master.dbo.xp_cmdshell+%27cmd+%2Fc+del+c%3A%5Cfile.txt%27%3B--

http://www.toroassicurazioni.it/index.asp?IDCAT=1%3B+EXEC+master.dbo.xp_cmdshell+%27ping+-n+10+127.0.0.1%27%3B--

I precedenti esempi utilizzano la procedura xp_cmdshell per eseguire comandi sul server. Nella fattispecie, la prima richiesta tenta di cancellare il file C:\file.txt; la seconda richiesta esegue ping.exe verso localhost (10 volte).

- Web Mail vulnerability -
Tutti i dettagli della vulnerabilita' relativa alla webmail di nuovatirrena sono pubblici e reperibili all'indirizzo http://www.securityfocus.com/bid/17292.
Inoltre, all'indirizzo
http://downloads.securityfocus.com/vulnerabilities/exploits/horddy-v2.pl,
e' possibile scaricare l'exploit per eseguire comandi sulla macchina remota.
Inoltre, su questo server sono state trovate tracce di almeno una precedente intrusione che, con tutta probabilita', ha avuto come scopo l'utilizzo della macchina come IRC-BOT e SPAM-SERVER.

- Rete interna -
La struttura della rete visibile dal server nuovatirrena, mancando di sistemi di difesa interni
(es: firewall intranet, DMZ, etc.), ha permesso di avere accesso a tutta una serie di macchine (client e server) assestate sulla intranet (probabilmente roma e torino).
In seguito ad una rapida analisi, e' stato possibile avere accesso ad alcune di queste macchine,
senza sfruttare vulnerabilita' particolari, ma semplicemente riuscendo ad ottenere unalista degli
account di sistema con password deboli (es: DATI-ISVAP, INFORMIX, etc.).
Tuttavia quest'analisi NON e' stata svolta in maniera approfondita, in quanto sara' oggetto della seconda fase dell'attivita' (attacco alla rete interna).
E' quindi possibile ipotizzare che tutti i risultati che saranno ottenuti dall'attacco alla rete interna, possano essere raggiunti anche dall'esterno, utilizzando il server pubblico vulnerabile
come "testa di ponte".