Milano, 14 giugno 2007

Spett.le
Gesi S.p.A.
Viale Brenta, 32
20100 MILANO (MI)

Offerta n. 20070614.02GP

Alla cortese attenzione: Sig. Sergio Insalaco

Oggetto: Offerta per attività di Ethical Hacking - POMS

A seguito dei colloqui intercorsi vi sottoponiamo la nostra migliore proposta per il servizio in oggetto.

In attesa di un vostro gradito riscontro, vi porgiamo i nostri più cordiali saluti.

Hacking Team S.r.l.

Gabriele Parravicini
Responsabile commerciale

Offerta
Attività di Ethical Hacking – POMS

SOMMARIO

1. STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	14 giugno 2007	Emissione

2. RICHIESTA DEL CLIENTE

GESI S.p.A. richiede di formulare una proposta, con relativa offerta economica, relativa ad un intervento di Ethical Hacking atto a rilevare lo stato di sicurezza del portale denominato POMS.

In altre parole, si richiede una consulenza per verificare le attuali condizioni di sicurezza dell'applicativo POMS.

3. DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA

Analisi applicativa

Questa analisi è costituita da una serie di tentativi di attacco che coinvolgono solo i protocolli di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni. Nel caso specifico delle applicazioni web, tali attacchi sono basati su manipolazioni dei pacchetti HTTP che vengono scambiati fra i browser degli utenti ed il web server. Esistono diverse categorie di attacchi verso applicazioni web, che possono portare alla compromissione di uno o più layer dell'intera infrastruttura applicativa: web server, application server, data tier.
Caratteristica comune a tutti gli attacchi applicativi è la completa trasparenza ad ogni sistema di difesa perimetrale (firewall, ids, ecc.): manipolazioni dei protocolli di layer 7 (applicativi) non possono essere rilevate da dispostivi che analizzano il traffico a layer 3 (network).
Il test sarà condotto in modalità anonima. L' attività comprende l'analisi dell'applicazione sia in termini architetturali sia in termini implementativi.
L' attività di security audit dell'applicazione web identifica in modo completo le classi di attacco, in particolare saranno testate:

- Cross-site scripting: attacchi che sfruttano una non corretta validazione dei contenuti restituiti dal server in risposta a richieste HTTP opportunamente modificate.
- Parameter tampering: attacchi che sfruttano una non corretta validazione dei parametric passati dal browser al web server.

- Hidden field manipulation: attacchi che, sfruttando paradigmi di programmazione non sicuri, alterano il valore di parametri applicativi fra due successive richieste HTTP.
- Backdoors e opzioni di debug: attacchi basati su errori di configurazione e/o di programmazioni molto noti e diffusi.
- Stealth commanding: attacchi che mediante tecniche di injection mirano ad eseguire comandi sui server.
- Forceful browsing: attacchi che mirano ad accedere a risorse protette seguendo percorsi di navigazione non previsti.
- Buffer overflow: attacchi che comportano l'esecuzione di codice arbitrario in assenza di opportuna validazione dei parametri in ingresso.
- Cookie poisoning: attacchi basati sulla manipoloazione dei coockie di sessione HTTP.
- Configurazioni errate: attacchi che sfruttano comuni errori di configurazione.
- Vulnerabilità note: attacchi che sfruttano la mancata applicazione di patch.
- SQL injection: attacchi che mirano all'esecuzione di query non previste sui DBMS di backend. Attacchi http: manipolazioni degli Header HTTP.

4. DOCUMENTAZIONE UTENTE

Oltre a ciò specificatamente richiesto nel capitolo 2 (RICHIESTA DEL CLIENTE), al termine dell'attività sarà fornito un report sulla base della documentazione standard concordata con il cliente.

Sarà inoltre allegata una descrizione dei possibili miglioramenti che potrebbero essere apportate all'applicazione, ai sistemi o ai servizi.

5. PIANO DI INTERVENTO

Da valutare assieme al cliente in sede di Kick off meeting

5.1. Attività (tipologie)

Attività
Attività di Ethical Hacking applicativo, vedi tabella seguente.

6. OFFERTA ECONOMICA

6.1. Servizi a corpo

Descrizione	Q.tà	Elapsed*	Totale
• Analisi con metodologia black-box o Test complessivi (verifica campi di input, XSS, SQL INJECTION, ecc) o Forzatura della login o Studio del codice sorgente della pagina di Login • Analisi con metodologia white-box o Test complessivi o Sicurezza delle sessioni o Forzatura della eventuale login dispositiva	**1**	**1 week**	**€ 3.000,00**
		Totale	**€ 3.000,00**

Gli importi indicati s'intendono al netto delle imposte.

6.2. Documentazione Utente

La documentazione e la reportistica, laddove previste, sono comprese nei servizi sopra esposti.

6.3. Piano di manutenzione

In questa offerta non è previsto piano di manutenzione.

6.4. Condizioni di fatturazione e pagamento

La presente offerta ha validità 30 giorni dalla data d'emissione.

La fatturazione dei servizi avverrà come segue:

100% all'ordine

I pagamenti s'intendono a 30gg d.f.