ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI TERAMO

Teramo, 4 dicembre 2014
Ns. Prot. n. 1913

Spett.le
Consiglio Nazionale Ingegneri
Via IV Novembre n. 114
00187 Roma
segreteria@ingpec.eu

Comitato Italiano Ingegneria dell'Informazione CII
c/a Consigliere Delegato CNI Angelo Valsecchi
segreteria@ingpec.eu

Ordini Ingegneri Italia

Commissione Ingegneri Informazione Ordini Ingegneri Italia

Iscritti ordine di Teramo

Oggetto. Segnalazione criticità, errori e riflessioni sito www.formazionecni.it

Con la presente vogliamo segnalare un grave problema di sicurezza relativo alla sezione di autocertificazione rilasciata dal sito del Consiglio Nazionale degli Ingegneri in data 2/12/2014 all'indirizzo http://www.formazionecni.it/html/cnt/autocertificazione.asp

La grave falla risiede proprio nella logica di registrazione necessaria per la compilazione dell'autocertificazione, la quale richiede di fornire Codice Fiscale e N. Iscrizione all'Ordine, dati pubblici e facilmente reperibili nel sito dell'Ordine dell'iscritto.

Nella fase successiva si richiede di confermare l'indirizzo email o di aggiungerne uno nuovo senza controlli di alcun genere.

A questo punto un malintenzionato può, una volta in possesso dei dati di un iscritto qualsiasi, immettere un qualsiasi indirizzo email per confermare la registrazione e compilare un'autocertificazione falsa, il tutto all'oscuro dell'iscritto possessore dei dati.

Riteniamo che il problema segnalato non possa essere classificato come bug, cosa che per versioni di software ai primi rilasci potrebbe essere anche accettabile (anche se riteniamo non plausibile che per sistemi delicati come questo siano presente bug dopo i test dalle versioni

alfa e beta che il sistema avrebbe dovuto superare), ma in questo caso si tratta di un vero e proprio errore grave di progettazione.

In questa maniera l'unico vincolo di sicurezza è affidato alla speranza di non incontrare malintenzionati che possano falsificare le autocertificazioni.

Analizzando ulteriormente il sito, in qualità di Commissione del Terzo Settore, non possiamo non fare delle riflessioni che la nostra professione ci obbliga a fare.

Per primo punto vorremmo far notare che la nuova sezione del sito è stata sviluppata in un linguaggio ASP con Framework 2.0 ormai vecchio di quasi 10 anni (a breve spiegheremo anche come abbiamo ottenuto la versione del framework), ormai datato e superato dalle nuove tecnologie ed anche di difficile manutenzione, ma relativamente a ciò non vogliamo indagare o aprire discussioni poiché potrebbero esserci delle decisioni all'origine di queste scelte che non conosciamo (economiche, di riuso del codice ecc..), le quali possono essere più o meno discutibili.

Quello che vogliamo sottolineare è che un sistema software per prima cosa deve essere progettato seguendo dei criteri atti a garantire la qualità del codice, una facile manutenzione, ecc.

Inoltre devono essere rispettate tutte le fasi di esecuzione del progetto, prevedendo uno sviluppo preliminare in un ambiente di test e successivamente la pubblicazione in versione stabile in un ambiente di produzione sicuro.

Abbiamo inoltre analizzato in modo critico anche la sezione corsi, che dovrebbe essere nella sua versione stabile poiché rilasciata da tempo.

Dopo una consultazione come utenti semplici, oltre ad aver incontrato vari bug nel sistema, ne abbiamo rilevato uno di gravità altissima.

Il sistema ha restituito un'eccezione ed è stato mostrato l'intero sorgente del progetto, che vi alleghiamo nella nota con una piccola immagine.

L'intero sorgente, che non alleghiamo, è disponibile per la consultazione.

Da una veloce visione del sorgente abbiamo notato che non è rispettato nessuno dei criteri esposti in precedenza.

Per primo, il grave errore è rilasciare un software in un ambiente di produzione e mostrare i dettagli di errore agli utenti.

Gli errori devono essere mostrati solamente ai tecnici che stanno sviluppando il sistema o chi lo sta testando in un ambiente di test.

La tecnologia ASP permette di nascondere questi errori negli ambienti di produzione.

In secondo luogo da una veloce visione del sorgente, abbiamo notato come l'intero sistema sia scritto in una sola pagina da 32.799 righe di codice, in cui la logica di layout, la Business Logic Layer, la logica di accesso ai dati ecc, non seguono alcun criterio di progettazione,

rendendo quindi il sistema instabile, come tutti abbiamo visto, e sicuramente di difficile manutenzione.

Inoltre il codice scritto sembra di bassissimo livello e sicuramente molto macchinoso.

Ad esempio con un codice scritto in questa maniera è praticamente impossibile cambiare la grafica del sito, cosa che invece permettono anche sistemi di semplicissimo utilizzo come i CMS open source e commerciali, per il cui utilizzo non sono richiesti particolari professionalità. Considerate che nel sorgente abbiamo anche scorto una password di PayPal in chiaro, speriamo che non sia una vera password, ma non indaghiamo al momento. Inoltre, essendo stati mostrati pubblicamente i sorgenti del software, riteniamo che il sistema non sia più sicuro, in quanto chiunque potrebbe aver in mano il sorgente del codice con tanto di query al database, e quindi studiando il sistema potrebbe scoprire le vulnerabilità ed effettuare un attacco, che vista la superficialità di progettazione e sviluppo del codice, non riteniamo improbabile.

Abbiamo rilevato inoltre ulteriori carenze sul sistema, sebbene di minore entità, rispetto ai gravi errori citati in precedenza (si rimanda agli screenshot allegati).

Tra gli altri l'impossibilità di utilizzo attraverso dispositivi mobili, vincolo oggi irrinunciabile.

L'Ordine degli Ingegneri della provincia di Teramo grazie al supporto della commissione del terzo settore sta lavorando molto al fine di diffondere il ruolo dell'ingegnere dell'informazione sia nel settore della pubblica amministrazione, che nell'industria nel nostro territorio, e vedere che il Consiglio Nazionale degli Ingegneri rilascia un software così scadente, e su cui non vogliamo credere che ci abbia lavorato un ingegnere con le dovute professionalità, ci demoralizza non poco.

Rilasciare un software progettato male e di difficile controllo sicuramente, oltre che avere un costo elevato, significa anche un danno all'immagine della nostra professione e quindi alla comunità.

Ci permettiamo di porre delle riflessioni sugli ingegneri che spesso si spacciano per ingegneri dell'informazione all'interno di organismi quale ad esempio la commissione specifica del CNI.

Chiediamo che i soggetti che ne debbano far parte devono essere ingegneri che si occupano di progettazione di sistemi informatici e dimostrino di sviluppare applicazioni.

Diversamente saremo circondati di ciarlatani che parlano perché forse in qualche occasione hanno ascoltato qualcosa che li ha interessati.

Comunque se da un lato siamo demoralizzati dall'altro siamo ancora più motivati a far meglio ed oltre a inviare questa segnalazione, come Commissione del Terzo Settore dell'Ordine degli Ingegneri di Teramo, ci mettiamo a disposizione per aprire una discussione o un dialogo al fine di migliorare il servizio per tutti quanti.

In attesa di riscontro si porgono cordiali saluti.

ing. Marco Chiesi

Commissione Terzo Settore

Presidente Ordine degli Ingegneri di Teramo

Ing. Alfonso Marcozzi

ing. Matteo Canzari

Coordinatore Commissione Terzo Settore

Server Error in '/' Application.

Compilation Error

Description: An error occurred during the compilation of a resource required to service this request. Please review the following specific error details and modify your source code appropriately.

Compiler Error Message: CS0246: The type or namespace name 'Utente' could not be found (are you missing a using directive or an assembly reference?)

Source Error:

```
Line 42:    public IDVariant HTML1 = new IDVariant(0,IDVariant.STRING);
Line 43:    public IDVariant HTML2 = new IDVariant(0,IDVariant.STRING);
Line 44:    public Utente UTENTE = null;
Line 45:    public IDVariant WEBPATH = new IDVariant(0,IDVariant.STRING);
Line 46:    public IDVariant DEBUGMODE = new IDVariant(0,IDVariant.INTEGER);
```

Source File: e:\inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs **Line:** 44

Show Detailed Compiler Output:

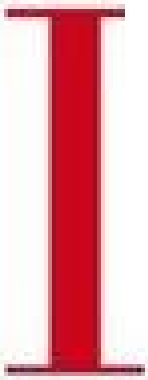
```
C:\Windows\SysWOW64\inetsrv> "C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /t:library /utf8output /R:"C:\Windows\


Microsoft (R) Visual C# 2005 Compiler version 8.00.50727.5483
for Microsoft (R) Windows (R) 2005 Framework version 2.0.50727
Copyright (C) Microsoft Corporation 2001-2005. All rights reserved.

e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(44,10): error CS0246: The type or namespace name
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(7890,47): error CS0234: The type or namespace nam
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(8489,48): error CS0234: The type or namespace nam
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(8508,48): error CS0234: The type or namespace nam
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(8773,48): error CS0234: The type or namespace nam
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(10628,48): error CS0234: The type or namespace na
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(10699,75): error CS0234: The type or namespace na
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(10720,159): error CS0234: The type or namespace r
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(11011,48): error CS0234: The type or namespace na
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(11034,55): error CS0246: The type or namespace na
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(12098,48): error CS0234: The type or namespace na
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(13405,42): error CS0246: The type or namespace na
e:\Inetpub\w3root\formazionecni.it\www\online\App_Code\MyWebEntryPoint.cs(26776,10): error CS0246: The type or namespace na
```

Show Complete Compilation Source:

```
Line 1:     // ***********************************************
Line 2:     // Web Entry Point (session handler)
Line 3:     // Instant WEB Application: www.progamma.com
Line 4:     // Project : CNI
Line 5:     // ***********************************************
Line 6:     using System;
Line 7:     using System.Text;
Line 8:     using System.Collections;
Line 9:     using System.IO;
Line 10:    using System.Web;
Line 11:    using System.IO.Compression;
Line 12:    using Microsoft.Win32;
Line 13:    using com.progamma.ids;
Line 14:    using com.progamma;
Line 15:    using com.progamma.doc;
Line 16:    using CIDREObj = com.progamma.idre.CIDREObj;
Line 17:    using IDREGlb = com.progamma.idre.IDREGlb;
Line 18:
```



Username

Password

Credenziali dimenticate ?

Accedi

via IV Novembre 114, 00187 Roma – Tel.

Home

Registrazione Provider

Normativa

Moduli e manuali

FAQ

Contatti

Crediti Informali

Autocertificazione 15 CFP

26/09/

Titolo

Ragione

Eventi FR

cerca

SCUOLA SUPERIORE DI
FORMAZIONE PROFESSIONALE
PER L'INGEGNERIA
CONSIGLIO NAZIONALE
DEGLI INGEGNERI

via IV Novembre 114, 00187 Roma – Tel. +39066976701 – Fax. +390669767048/49 E-Mail segreteria@cni-online.it PEC segreteria@ingpec.eu

Username
Password

Credenziali dimenticate ?

Accedi

Sono stati trovati 0 eventi

Ricerca

Ordinamento

Tipo: Codice evento | Data inizio | Crediti | Titolo

Verso: Crescente | Decrescente

Errore

Errore imprevisto

Errore: 207

Invalid column name 'idregioneprovincia'.

Effetti: L'operazione non può essere completata.

Cosa fare:
1) Controlla i dati inseriti e riprova.
2) Riprova più tardi.
3) Richiedi supporto tecnico.

Causa: ListaEventi - OnSendMessage

Torna all'applicazione