

## Informačný systém pre komunikáciu s absolventmi

*Posudok prototypu tímu č. 14*



Tím číslo: 12

Školský rok: 2007/2008

Bc. Marián Bán  
Bc. Marián Majan  
Bc. Maroš Majerčík  
Bc. Pavol Michalco  
Bc. Attila Nagy  
Bc. Ľuboš Zelinka

# 1 Úvod

Tento dokument opisuje prototyp *informačného systému na komunikáciu s absolventmi* tímu č. 14. Úlohou tohto projektu je vytvorenie informačného systému, ktorý by udržiaval kontakt fakulty s absolventmi a ponúkol im tak možnosť aktívne sa zapájať do fakultných aktivít. Zároveň by mal poskytovať spätnú väzbu o uplatnení absolventov v praxi.

Tím č. 14 pokračoval v práci minuloročného tímu č. 15. Tvorba prototypu teda spočívala v implementácii nových funkčných modulov do existujúceho systému.

## 2 Prototyp systému

Prototyp systému sme obdržali na inštalačnom optickom médiu spolu s dokumentáciou k prototypu. Pri inštalácii prostredia potrebného pre činnosť prototypu sme postupovali podľa inštrukcií z dokumentácie. Vyskytli sa menšie problémy s právami v databáze, v budúcnosti by bolo vhodné v príručke spresniť postup konfigurácie. Tiež si myslíme, že by bolo dobré spomenúť potrebu inštalácie knižnice gd2, ktorá je nevyhnutná v prípade ukladania fotografií ( túto časť implementoval ešte predošlý tím ).

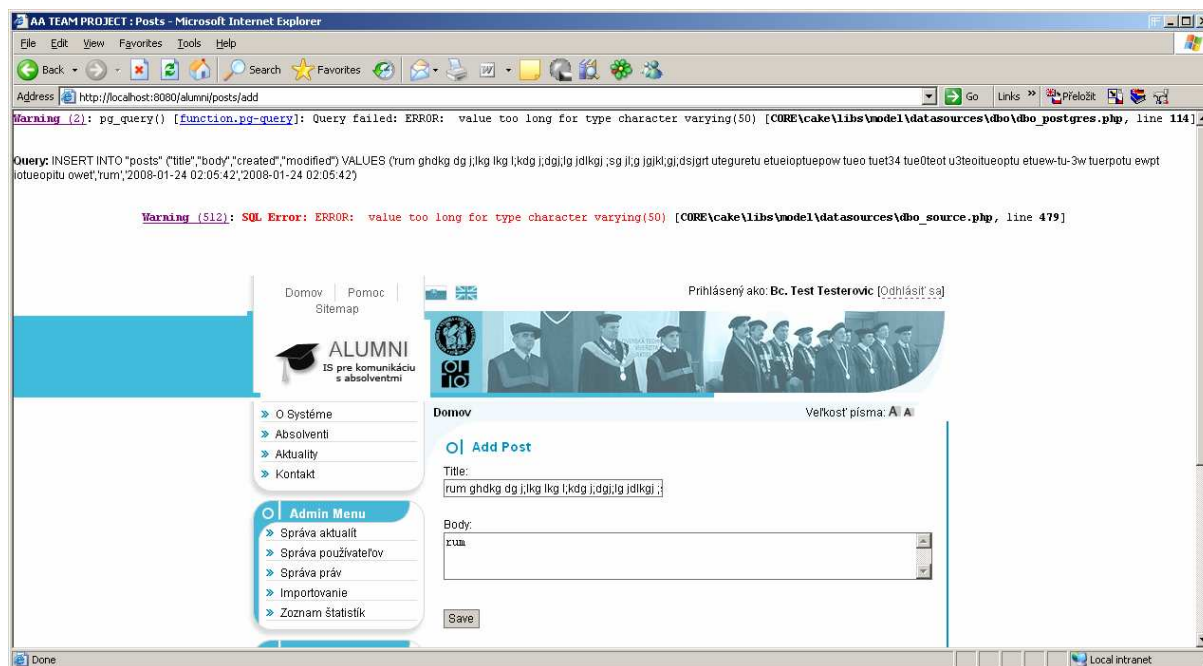
Ako sme spomenuli vyššie, úlohou tímu č. 14 bolo rozšírenie existujúceho systému novými modulmi. V nasledujúcej časti sa preto zameriame len na tie časti systému, ktoré boli vytvorené tímom č. 14 ( uvedené v priloženej dokumentácii ) - aktuality, štatistiky, zväčšovanie a zmenšovanie písmen. Na spoločnom stretnutí bol prezentovaný modul, ktorý umožňuje prihlasovanie sa do systému prostredníctvom hesiel zo servera is.stuba.sk, testovali sme preto aj túto časť.

### 2.1 Aktuality

Modul pre správu aktualít nahradil nástenku minuloročného tímu. Jedná sa o jednoducho spravovateľnú súčasť systému, ktorá zabezpečuje informovanie používateľov o dianí na fakulte a zmenách v systéme.

Modul umožňuje pridávanie, úpravu a odstránenie aktualít, pričom sa definuje nadpis a text aktuality. Pre bežného používateľa modul funguje správne. Pri zadávaní nadpisu aktuality však nie je ošetrená chyba, ktorá sa vyskytne, ak je nadpis dlhší ako 50 písmen. Databáza generuje chybu, ktorá ale nie je programom ošetrená a preto sa zobrazí používateľovi ( Obr. 1 ). Výpis chyby obsahuje aj detailné informácie o štruktúre časti databázy, čo môže potenciálny útočník využiť vo svoj prospech.

Taktiež odporúčame, aby boli aktuality zoradené vzostupne ( najnovšie hore, najstaršie dole ).



Obr. 1 Výpis chyby pri nadpise aktuality dlhšom ako 50 znakov.

## 2.2 Štatistiky

Aj napriek tomu, že v dokumentácii k prototypu systému je uvedené, že modul štatistiky je funkčný, z pohľadu používateľa sa po zaslaní požiadavky nič nestane. Keď sme sa na systém pozreli bližšie, zistili sme, že modul štatistiky vôbec nebol v priloženej verzii systému implementovaný. Tento modul nebol ani odprezentovaný, preto ho nemôžeme bližšie ohodnotiť.

## 2.3 Autentifikácia

Počas prezentácie prototypu bolo uvedené, že v systéme je implementovaný modul umožňujúci prihlasovanie používateľov prostredníctvom údajov získaných zo servera *ldap.stuba.sk* alebo lokálnej databázy.

Prihlásenie menom a heslom z lokálnej databázy je funkčné. Funkčnosť druhej časti systému sme však neboli schopní overiť, respektíve nemôžeme určiť dôvody, pre ktoré nás systém odmietal prihlásiť. Overili sme si však v zdrojových kódach projektu, že táto časť systému je implementovaná a v priestoroch fakulty by mala byť funkčná.

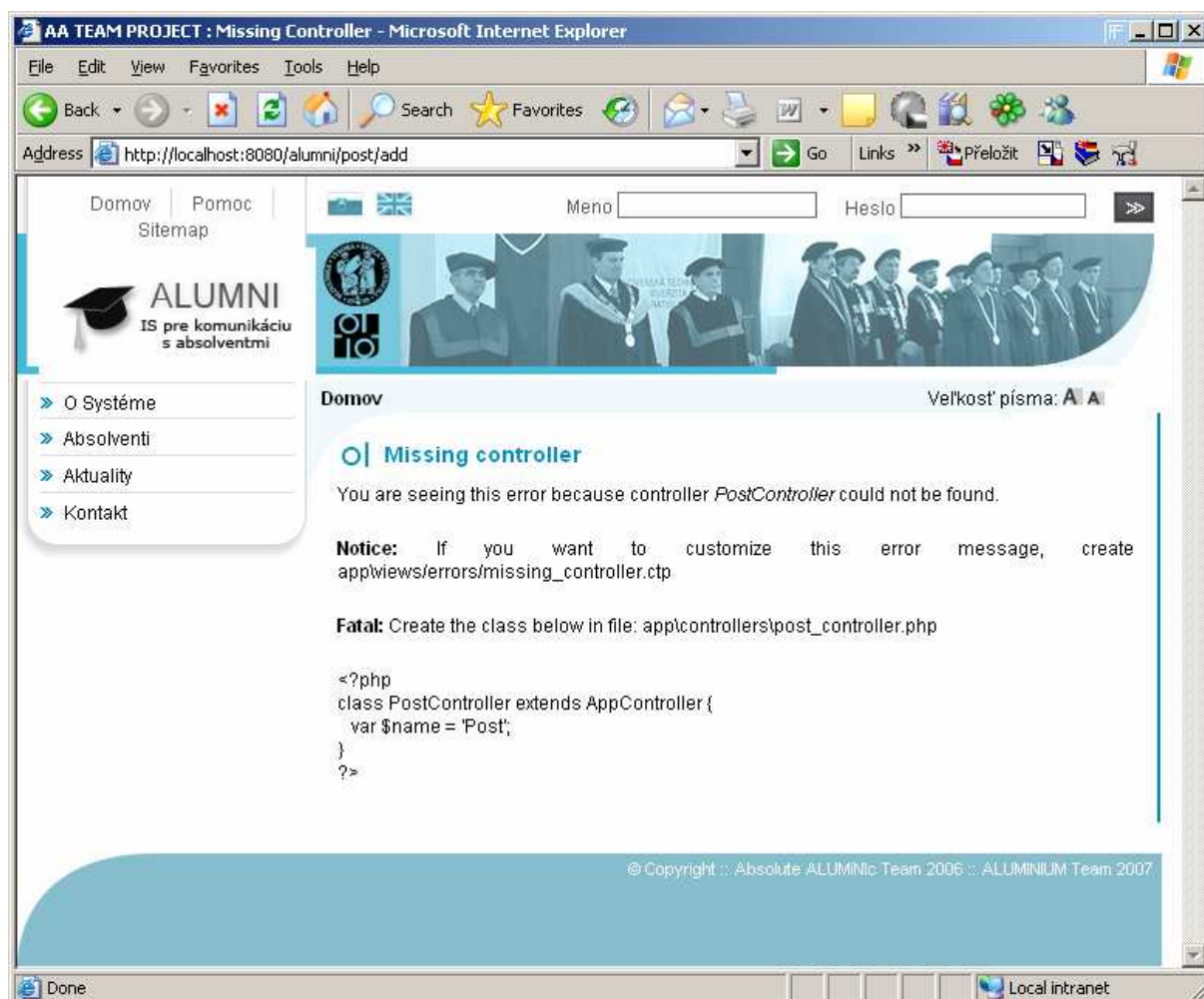
## 2.4 Nástroj na zmenu veľkosti písma

Ďalšou novou súčasťou systému je nástroj, ktorý umožňuje zmenu veľkosti písma zobrazovaného textu. Aj neskúsení používatelia tak môžu využiť štandardnú funkcionality prehliadača, ktorá je inak ťažšie dostupná. Nástroj pracuje správne.

## 2.5 Ďalšie zistené chyby

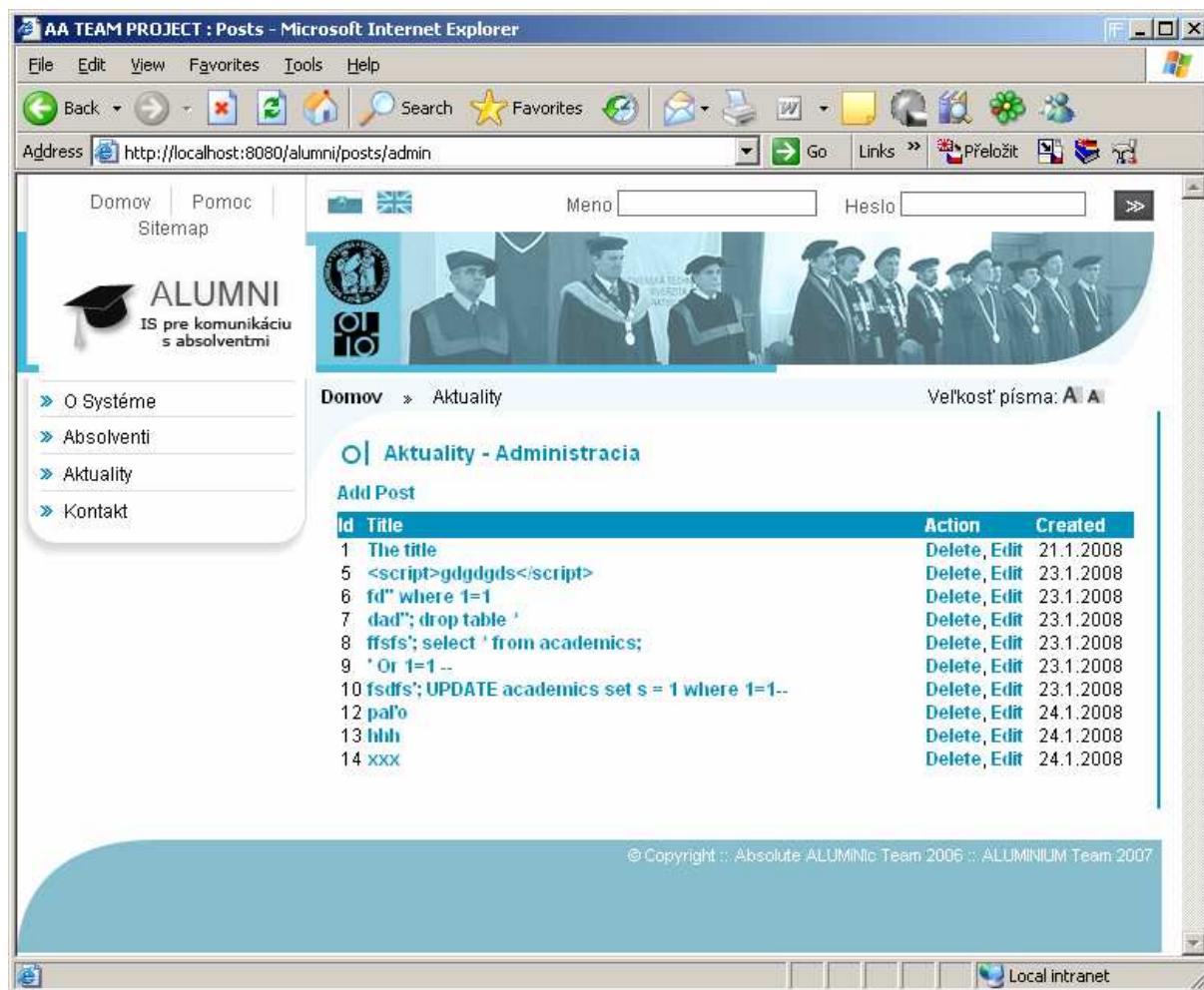
Pri testovaní systému sme odhalili menší bezpečnostný problém, ktorý sa vyskytuje pri zadaní neplatnej adresy ( v danej doméne ) do adresného riadku. Používateľovi sa zobrazí chyba (

Obr. 2 ), ktorá obsahuje detailné informácie, ktoré môže potenciálny útočník využiť vo svoj prospech.

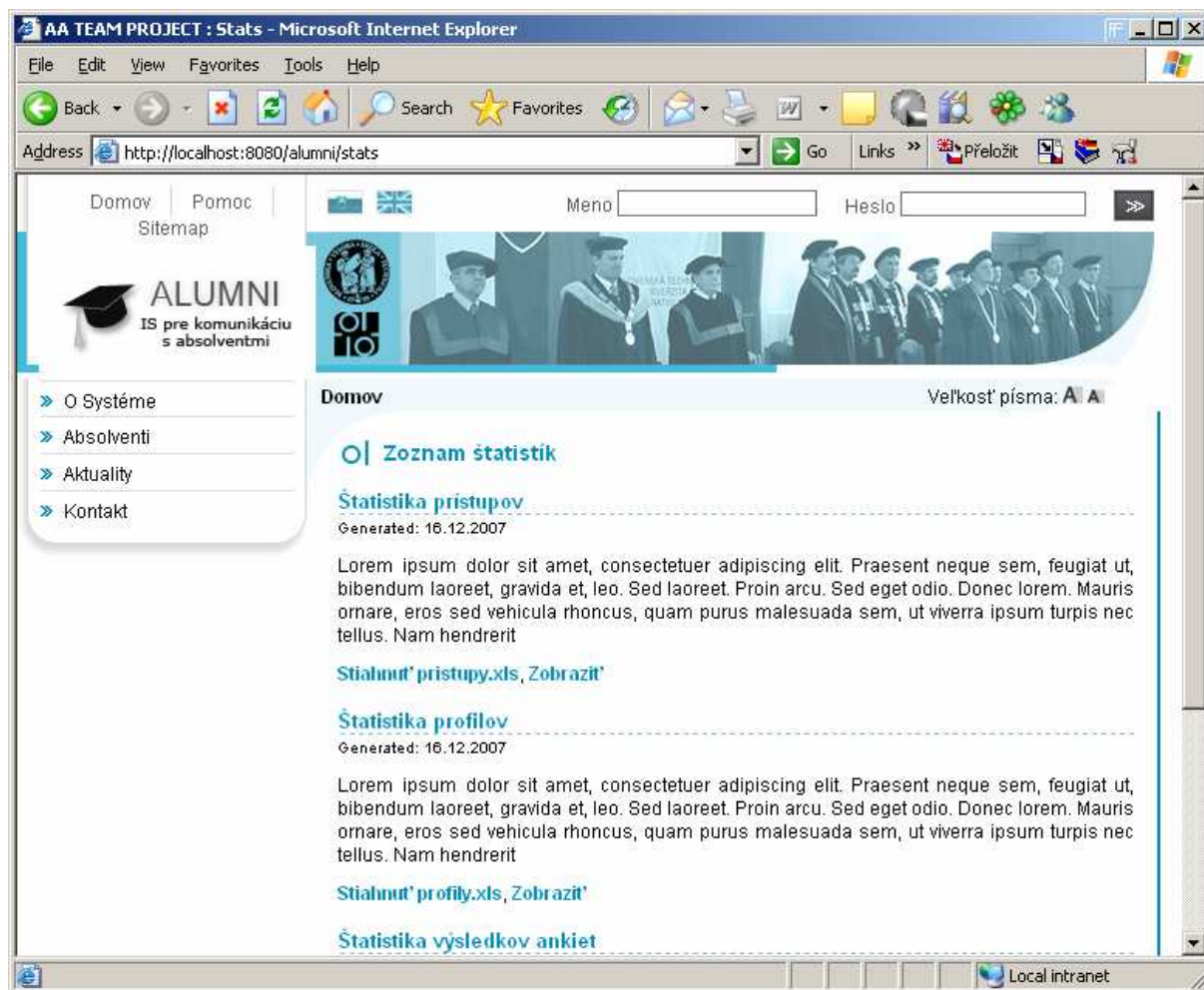


**Obr. 2** Správna adresa má byť `http://localhost:8080/alumni/posts/add`, my sme ju však zmenili na neexistujúcu adresu `http://localhost:8080/alumni/post/add`.

Ďalšia, závažnejšia bezpečnostná diera sa objaví v prípade, ak neprihlásený používateľ pozná adresu k službe spravovania aktualít a štatistík a túto zadá do prehliadača. Získa tak prístup k spravovaniu aktualít a štatistík, na ktoré by však mal mať právo len administrátor. Platí to aj pre prihláseného používateľa bez administrátorských práv. Tento problém sa však vyskytuje len v prípade týchto dvoch služieb ( Obr. 3 a Obr. 4 )



Obr. 3 Používateľ nie je prihlásený, aj tak však môže spravovať aktuality ako administrátor!



**Obr. 4** Používateľ nie je prihlásený, aj tak však môže narábať so štatistikami ako administrátor!

Menším nedostatkom systému je, že po jeho prepnutí do anglického jazyka, služby aktuality a štatistiky ostanú v slovenskom jazyku. Pri prepnutí systému do slovenského jazyka sa horné ľavé menu rozšíri na dva riadky, čím sa všetko pod ním posunie o jeden riadok nižšie, čo naruší dizajn, konkrétne spojenie tela stránky s hlavičkou ( Obr. 5 ). Na operačnom systéme MS Windows sa zobrazovali nesprávne znaky s diakritikou ( na systéme GNU/Linux bolo zobrazovanie bezchybné ).





Obr. 5 Problém so zobrazovaním hlavičky pri prepnutí do slovenského jazyka.

### 3 Záver

Celkový dojem z prototypu je dobrý. Tím č. 14 vychádzal z, podľa nás veľmi vydareného systému, minuloročného tímu. Veľmi pozitívne hodnotíme najmä rozloženie jednotlivých ovládacích prvkov, použitie aplikačného rámca MVC a stabilitu.

Ako menšie negatívum hodnotíme minimálne rozšírenie funkcionality pôvodného systému tímom č. 14, ktorého nie všetky súčasti boli funkčné. Akceptujeme, že rozširovanie existujúceho systému si vyžadovalo pochopenie už cudzích zdrojových kódov a princípov a predpokladáme, že ďalší vývoj už bude prebiehať rýchlejšie, v čom tímu držíme palce.