

# Slovenske spletne aplikacije imajo “TALENT”

Milan Gabor



# 0 nas

- Ni sprememb od lanskega leta
- Isto podjetje, ista služba
- Še vedno iščemo talente na področju informacijske varnosti
- Še vedno nas plačujejo za to, da poskusimo vdreti v sisteme



Tudi take imamo 😊

**SEKTOR ZA INFORMATIKO  
IN IZDAJANJE PODATKOV**

**uradne ure, uradne ure po telefonu:**

**od 9.00 do 12.00  
in sreda od 14.00 do 16.00**



# Teorija?! Praksa

- Veliko teorije – premalo prakse
- Premalo zavedanja
- Veliko zaupanje v zunanje izvajalce
- Hitro lahko pokažemo in dokažemo, da vse v praksi ni tako lepo kot na papirju



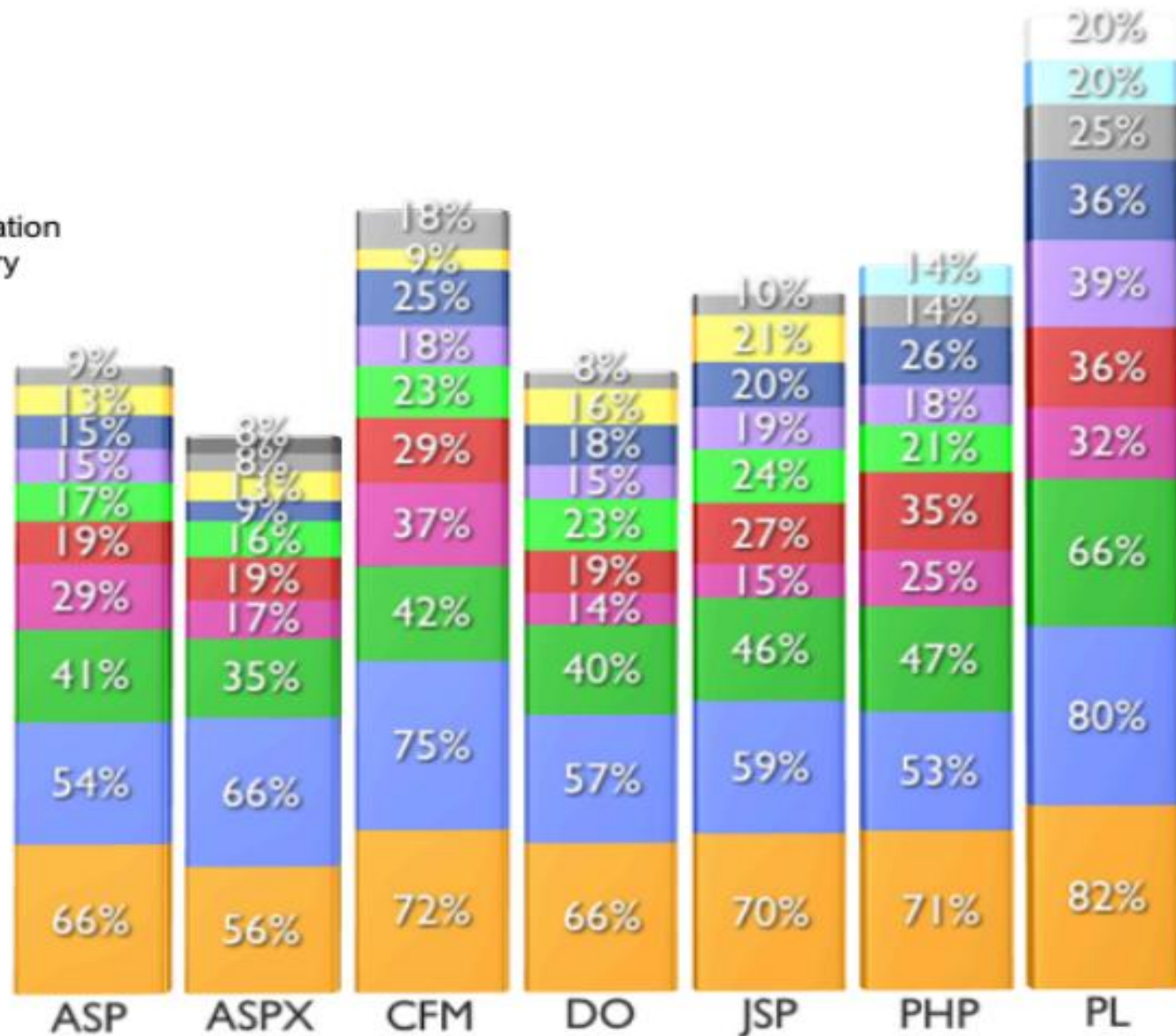
## OWASP Top 10 – 2007 (Previous)

## OWASP Top 10 – 2010 (New)

A2 – Injection Flaws	A1 – Injection
A1 – Cross Site Scripting (XSS)	A2 – Cross-Site Scripting (XSS)
A7 – Broken Authentication and Session Management	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	A5 – Cross-Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	A6 – Security Misconfiguration (NEW)
A8 – Insecure Cryptographic Storage	A7 – Insecure Cryptographic Storage
A10 – Failure to Restrict URL Access	A8 – Failure to Restrict URL Access
A9 – Insecure Communications	A9 – Insufficient Transport Layer Protection
<not in T10 2007>	A10 – Unvalidated Redirects and Forwards (NEW)
A3 – Malicious File Execution	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	<dropped from T10 2010>



- Cross-Site Scripting
- Information Leakage
- Content Spoofing
- Insufficient Authorization
- SQL Injection
- Predictable Resource Location
- Cross-Site Request Forgery
- Session Fixation
- HTTP Response Splitting
- Abuse of Functionality
- Insufficient Authentication
- Directory Traversal
- Directory Indexing





# Kje iskati talente

Time	Notifier	H	M	R	★	Domain	OS	View
2010/03/16	KTN					www.malnaric.si/index.php/kmet...	Linux	mirror
2010/03/16	funky_still	H	M			www.offroadoprema.si	Linux	mirror
2010/03/16	Ghost_Rider		M			skywalker.si/forum/	Linux	mirror
2010/03/16	SQL@Live.se	H	M			psiholog.si	Linux	mirror
2010/03/12	KHG		M			suzuki.panjan.si/sl/predstavit...	FreeBSD	mirror
2010/03/12	KHG		M		★	www.rks.si/docs/	FreeBSD	mirror
2010/03/12	KHG		M		★	www.isuzu.si/f/	FreeBSD	mirror
2010/03/12	KHG		M			linuxdan.si/docs/index.htm	FreeBSD	mirror
2010/03/12	KHG		M			www.antivirus.si/docs/	FreeBSD	mirror
2010/03/12	1923Turk					tvojportal.si/jomtube/sploni-p...	Unknown	mirror
2010/03/11	1923Turk		M	R		www.simbioza.si/index/index.ph...	Linux	mirror
2010/03/10	funky_still	H	M			rozica.si	Linux	mirror
2010/03/10	funky_still	H	M			studio2010.si	Linux	mirror
2010/03/10	KHG		M			www.softnet.si/f/index.htm	FreeBSD	mirror
2010/03/10	KHG		M			www.ro.softnet.si/f/index.htm	FreeBSD	mirror
2010/03/10	KHG		M			www.cn.softnet.si/f/index.htm	FreeBSD	mirror
2010/03/10	KHG		M			www.rcl.si/f/docs/index.htm	FreeBSD	mirror
2010/03/09	KHG		M		★	bayerschering.bayer.si/docs/	FreeBSD	mirror
2010/03/09	khg		M		★	www.bayer-pharma.si/docs/	FreeBSD	mirror
2010/03/09	KHG		M		★	www.healthcare.bayer.si/docs/	FreeBSD	mirror
2010/03/09	Z7FaaN H4Ck3R					dat.si/publikacije	Linux	mirror
2010/03/09	KHG		M		★	www.bayer.si/docs/	FreeBSD	mirror
2010/03/09	KHG		M		★	www.thenorthface-slovenija.si/f/	FreeBSD	mirror
2010/03/09	KHG				★	www.suzuki.si/sl/predstavitev_...	FreeBSD	mirror
2010/03/09	KHG	M	R		★	www.suzuki-odar.si/sl/avtomobi...	FreeBSD	mirror



# Orodja in viri

- Brskalnik
- Google
- Google
- Google

`#/viris[🔍🔍🔍🔍]`







#/viris[📷📺📺📺]



# Talent – 4 mesto

description The server encountered an internal error () that prevented it from fulfilling this request.

## exception

org.apache.jasper.JasperException: An exception occurred processing JSP page /prijava.jsp at line 27

```
24:    aips.connect();  
25:    //int status = 0;  
26:    //PRAVA KODA  
27:    int status = aips.veljaven(user, pass);  
28:    if (user.equals("admin") && pass.equals("admin"))  
29:    {  
30:        session.putValue("student", "admin");
```

## Stacktrace:

```
org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:498)  
org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:411)  
org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:322)  
org.apache.jasper.servlet.JspServlet.service(JspServlet.java:249)  
javax.servlet.http.HttpServlet.service(HttpServlet.java:717)  
org.jboss.web.tomcat.filters.ReplyHeaderFilter.doFilter(ReplyHeaderFilter.java:96)
```



# Talent – 3 mesto

## NAPAKA

Sporocilo:	Pri SQL poizvedbi je prišlo do napake: Unknown column '7a' in 'where clause'		
Datoteka:	/home/sinergija/domains/pejime.si/public_html/admin/classes/MySQL.php		
Vrstica:	88		
Sled napake:	Datoteka:	/home/sinergija/domains/pejime.si/public_html/inc_left_menu.php	
	Vrstica:	33	
	Sprememljivke:	1 => SELECT t1.*, (COUNT(t2.content_id) - 1) AS depth FROM table_content AS t1, table_content AS t2 WHERE t1.lft BETWEEN t2.lft AND t2.rgt AND t1.lang="" AND t1.title!='root' AND t1.section_id=7a AND t1.state=1 GROUP BY t1.content_id ORDER BY t1.section_id, t1.lft	
	Datoteka:	/home/sinergija/domains/pejime.si/public_html/index.php	
	Vrstica:	247	
	Sprememljivke:	1 => /home/sinergija/domains/pejime.si/public_html/inc_left_menu.php	
Datum in čas:	24.05.2010 ob 18:44:24		
Okolje:	PHP 5.2.12 (Linux) na www.pejime.si		



# Talent – 2 mesto

## Server Error in '/esvetovalkaUI' Application.

*String or binary data would be truncated.  
The statement has been terminated.*

**Description:** An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

**Exception Details:** System.Data.SqlClient.SqlException: String or binary data would be truncated.  
The statement has been terminated.

### Source Error:

```
Line 60: //NEPRIMERNA VPRAŠANJA
Line 61: NeprimernaVprasanja.NeprimernaVprasanja neprimernaV = new NeprimernaVprasanja.NeprimernaVprasanja();
Line 62: odgovor = neprimernaV.PreveriVprasanje(osebneBesede);
Line 63: odgovor = odgovor.Trim();
Line 64:
```

**Source File:** c:\AppRoot\ESvetovalkaMariborUIApp\_Code\ESvetovalkaUIFunkcije.cs **Line:** 62

```
System.Web.UI.WebControls.Button.OnClick(EventArgs e) in c:\AppRoot\ESvetovalkaMariborUI\Default.aspx.cs:93
behavior) +573
System.Data.Common.DbDataAdapter.Fill(DataSet dataSet, String srcTable) +161
NeprimernaVprasanja.NeprimernaVprasanjaDL.PreveriPrimernostVprasanja(String stavek) in C:\Documents and Settings\Ines\My Documents\Visual Studio
2005\Projects\ESvetovalkaUI\NeprimernaVprasanja\NeprimernaVprasanjaDL.cs:31
NeprimernaVprasanja.NeprimernaVprasanjaBL.PreveriPrimernostVprasanja(String stavek) in C:\Documents and Settings\Ines\My Documents\Visual Studio
2005\Projects\ESvetovalkaUI\NeprimernaVprasanja\NeprimernaVprasanjaBL.cs:14
NeprimernaVprasanja.NeprimernaVprasanja.PreveriVprasanje(String vprasanje) in C:\Documents and Settings\Ines\My Documents\Visual Studio
2005\Projects\ESvetovalkaUI\NeprimernaVprasanja\NeprimernaVprasanja.cs:16
ESvetovalkaUIFunkcije.OdgovoriNaVprasanje(String vprasanje, Int32 zapStVprasanja) in
c:\AppRoot\ESvetovalkaMariborUIApp_Code\ESvetovalkaUIFunkcije.cs:62
Default.Button1_Click(Object sender, EventArgs e) in c:\AppRoot\ESvetovalkaMariborUI\Default.aspx.cs:93
System.Web.UI.WebControls.Button.OnClick(EventArgs e) +115
System.Web.UI.WebControls.Button.RaisePostBackEvent(String eventArgument) +140
System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +29
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +2981
```





# Talent – 1 mesto

elekrom Slovenije, d.d. | Podjetje | Novinarsko središče | Oglaševanje | Pomoč in podpora | English

**SIOL Moj SiOL**

**Dopust v mobilni hišici!**  
Rezervirajte jo v Istri, Dalmaciji ali Kvarnerju.

**Iščemo poslovne partnerje**  
Ležaji in verige; postani pooblaščen prodajalca!

**Izdelujemo rolete!**  
Po vaši meri in željah. Rolete vam tudi montiramo.

**Rabite nasvet?**  
Uspešni se vedno posvetujejo!

ADpartner

SIOL.net

Iskalnik  slovenski splet siolove strani

- Moj SiOL
- Naročilo
- Prijava v Moj SiOL
- Kaj je Moj SiOL
- Moj profil
- Podnosti za naročnike
- Popust na zvestobo
- Priporočila prijatelja
- Naročanje
- E-pošta
- Uživanje
- Forumi
- Osebnosti

Stran na naslovu http://moj.siol.net pravi:

**Prijava v Moj SiOL**

Moj SiOL je skrbniški vmesnik za registrirane uporabnike portala www.siol.net. Vaš profil vam omogoča enostaven dostop do vseh naročenih storitev pri SiOL-u prek enega vmesnika, z enim samim uporabniškim imenom in geslom.

Uporabniško ime:  (e-naslov)

Geslo:

☐ zapomni se me \*

[pomoč](#)

[Ste pozabili vaše geslo?](#)

PA DODAJMO NEKAJ SVOJEGA TEKSTA NA PORTAL *Tole italic*

## Z enim profilom do vseh storitev!

Moj SiOL je skrbniški vmesnik za registrirane uporabnike portala www.siol.net. Vaš profil vam omogoča enostaven dostop do vseh naročenih storitev pri SiOL-u prek enega vmesnika, z enim samim uporabniškim imenom in geslom.

SIOL.net [Pomoč](#)

radio.siol klub.siol 23.05.2010 08:23

**SIOL - prijava**

Uporabniškim imenom do vseh vaših storitev.

☐ Zapomni si me!

(Označite, če uporabljate javni računalnik!)

tukaj je tekst na spletni strani

[Pozabil sem geslo](#) [Pomoč](#)

#/viris[ ]



# Hall of fame or shame?

## COVL prejel drugo nagrado za najboljši IKT projekt

[objave](#) | [novice](#)

datum: **14.04.2010**  
vir: **Vrhovno sodišče**

*Projekt prenove izvršilnih vpisnikov ter odprave sodnih zaostankov na področju izvršbe, je na tekmovanju za najboljši projekt s področja IKT prejel drugo nagrado kot eden najbolj učinkovitih, uspešnih in kakovostnih projektov na področju informatike v letu 2010.*

V sklopu 17. konference [Dnevi slovenske informatik](#) najboljši projekt s področja IKT za leto 2010, s katero promovira inovativnost, uspešnost, učinkovitost ter k

Letošnjo nagrado je prejelo tudi Vrhovno sodišče RS: vpisnikov ter odprave sodnih zaostankov na področju predsednica Vrhovnega sodišča RS in vodja eviden

## Prenovljene spletne strani

[objave](#) | [novice](#)

datum: **21.05.2010**  
vir: **Vrhovno sodišče**

*V petek, 21. 5. 2010, ob 17.00 uri načrtujemo prehod na prenovljene spletne strani slovenskega sodstva.*

Nova verzija uporabnikom spletnih strani omogoča še večjo preglednost in povezljivost podatkov, pri čemer izhaja tudi iz mnenj in predlogov uporabnikov.

Vabimo vas, da si [ogledate spremembe, novosti in dopolnitve](#).

Dosedanje spletne strani bodo še naprej dostopne na naslovu <http://staro.sodisce.si>.

Če pri uporabi strani naletite na kakšne težave, vas prosimo, da nas o tem obvestite na naslov: [urednistvo.vsr@sodisce.si](mailto:urednistvo.vsr@sodisce.si)



# Wild-card talent

Vhodna stran - Centralni oddelek za verodostojno listino - Mozilla Firefox

Datoteka Urganje Pogled Zgodovina Zaznamki Orodja Pomoč

sodisce.si https://covl-test.sodisce.si/eizvrsbe/eizvrsbe/Inv/mainAction.do

Vhodna stran - Centralni oddelek za v...

Sodstvo Republike Slovenije [sodstvo RS](#)

**Centralni oddelek za verodostojno listino**  
Vrhovno sodišče RS

VRHOVNO SODIŠČE  
REPUBLIKE SLOVENIJE

kontakt pomoč sistemska sporočila

**TESTNI SISTEM 3.2.18**

prijava v sistem  
prijava  
prijava s certifikatom  
pridobitev up. gesla

predlog  
obrazec  
tiskanje obrazcev

navodila  
izpolnjevanje obrazca  
papirni obrazec  
elektronski obrazec

višina sodne takse  
pravna podlaga  
pogosta vprašanja

**Vlaganje predlogov za izvršbo na podlagi verodostojne listine**

Dne 1.1.2008 je začel veljati Pravilnik o obrazcih, vrstah izvršb in poteku avtomatiziranega izvršilnega postopka (Ur. List 121/2007), ki ureja:

- vrste izvršb, v katerih se predlogi za izvršbo in predlogi za nasprotno izvršbo pošljejo na predpisanih obrazcih,
- vrste izvršb, v katerih se predlogi za izvršbo obdelujejo v informacijskem sistemu avtomatizirano in potek tega postopka,
- vsebino in obliko obrazcev predlogov za izvršbo in predlogov za nasprotno izvršbo.

**Načini vlaganja**


Predlog za izvršbo na podlagi verodostojne listine se na predpisanem obrazcu lahko vloži elektronsko ali v papirni obliki na Okrajno sodišče v Ljubljani, Centralni oddelek za verodostojno listino, Zaloška 59, Ljubljana (CoVL).

**1. Elektronsko vlaganje**

a) Upnik lahko vloži predlog za izvršbo z izpolnitvijo pametnega obrazca ali z uvozom podatkov iz datoteke po strukturi, ki jo določi in na svoji spletni strani vsakokrat objavi Vrhovno sodišče Republike Slovenije.

**Pogoji:**

Končano

#/viris[#Q\*]





# Zaključek

- Nekaj talentov smo pokazali
- Namen – dvigovanje zavesti
- Le majhen vzorec
- Premislite, predno dodate aplikacijam različne talente
- Lahko pa vam pomagamo...



# Kaj pa vi?

`#/viris[🔍🔗🌐]`

