SLOVENSKE SPLETNE APLIKACIJE IMAJO »TALENT«

Milan Gabor

ViRIS, Varnost in razvoj informacijskih sistemov
Inštitut za varnost podatkov in informacijskih sistemov
e-pošta: milan@viris.si
URL: http://www.viris.si/

Povzetek

Medtem ko se v Sloveniji iščejo talenti, lahko med spletnimi aplikacijami, ki jih najdemo na tudi na slovenskih straneh, najdemo različne talente. V prispevku bomo izpostavili tako dobre kot slabe prakse iz tega področja. Dotaknili se bomo tipičnih primeov in na njih prikazali, kako je mogoče z uporabo malo drugačnih talentov te aplikacije pripraviti, da nam povedo tisto, kar si avtorji definitivno niso želeli, da nam povedo. Hkrati bomo te naše talente primerjali s svetovno sceno in najbolj pogostimi napakami, ki jih lahko najdemo na OWASP seznamih. V prispevku bodo predstavljeni postopki in mehanizmi, kako se takšnih talentov znebiti.

1. UVOD

OWASP (Open Web Application Security Project) je odprta, globalna, brezplačna in neprofitna skupnost, ki se posveča dvigovanju varnostnega nivoja programske opreme. Poslanstvo OWASP je seznanjanje in osveščanje javnosti o pomembnosti aplikacijske varnosti in primernih načinih zavarovanja. V zadnjem letu se je začela ta skupnost prebujati tudi v Sloveniji in prvi rezultati se že začeli kazati. Glede na velik porast spletnih aplikacij v zadnjih letih, so se hkrati z aplikacijami začele množiti tudi potencialne varnostne pomanjkljivosti v teh aplikacijah. Vedno več aplikacij, ki so se iz intranetnih strani preselile na spletne strani in se s tem odprle širnemu svetu, so s sabo prinesle tudi veliko pomanjkljivosti. Zavedati se moramo, da razvijalci, ki so razvijali intranetne strani niso nikoli pomislili, da bodo te spletne strani kdaj dostopne tudi zunanjemu svetu in zato niso posvečali velike pozornosti varnosti v njih samih.

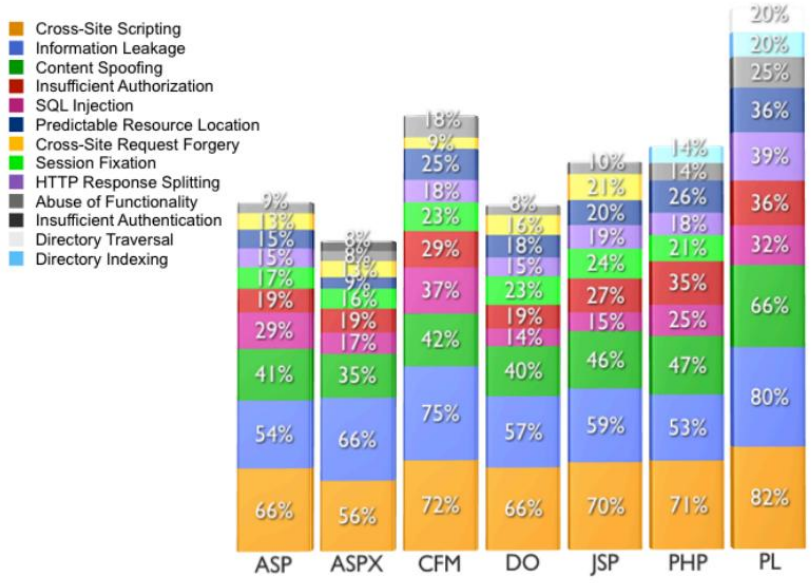
V generalnem za spletne aplikacije obstaja nekaj tipičnih napak in tudi OWASP pripravi vsake toliko časa seznam 10 najpogostejših napak. Takšen seznam je bil sestavljen nazadnje v letu 2007. V letošnjem letu so ga posodobili, tako da imamo čisto nov seznam desetih najpogostejših napak v spletnih aplikacijah. Če primerjamo seznam iz leta 2007 in 2010 lahko ugotovimo, da dejansko ni prišlo do večjih sprememb. Torej to pomeni, da v zadnjih treh letih dejansko ni bilo novih, večjih tipičnih napak, ki bi pristale na tem seznamu. Največja sprememba je na 10 mestu, kjer je pristala nova nevarnost, in sicer nepreverjene preusmeritve in posredovanja. Če pogledamo na hitro seznam napak pri vrhu, lahko ugotovimo, da so nekatere ranljivosti že kar stare, a so še vedno čisto pri vrhu. S tega lahko sklepamo, da tudi razvijalci še vedno delajo približno enake napake.

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>

Slika 1. Primerjava OWASP Top 10 ranljivosti iz leta 2007 in 2010

Poleg naših lastnih izkušenj lahko najdemo tudi zanimive rezultate v raziskavi [2], ki je analizirala preko 1500 spletnih aplikacij v časovnem razmaku od leta 2006 do začetka leta 2010.

Iz rezultatov navedene raziskave lahko vidimo, da so odstotki napak približno enako porazdeljeni po vseh programskih jezikih. Sicer so opažena nekatera odstopanja pri posameznih jezikih, a ta odstopanja niso velika. Iz rezultatov je moč razbrati, da napake, ki jih najdemo v aplikacijah niso odvisne od programskega jezika ali okolja v katerem so nastale, ampak so v veliki meri odvisne od izkušenosti razvijalcev. Če pogledamo širše in zunaj tega kontekstsa, lahko opazimo, da se velika večina teh napak ponavlja in so klasične napake s seznama OWASP Top 10.



Slika 2. Rezultati analize [2] podjetja White Hat Security

2. TALENTIRANA APLIKACIJE V SLOVENIJI

Tudi za aplikacije, ki jih lahko najdemo na slovenskem spletu, lahko rečemo, da včasih pokažejo svoj »talent«. V ožji izbor je prišlo nekaj spletnih aplikacij, ki jih nekateri uporabljamo ali pa smo na njih naleteli naključno in v interakciji z njimi ugotovili, da so »talentirane«. Seveda pa bi jih lahko našteli še veliko več, saj lahko pri vsakodnevnem brskanju po Internetu najdemo veliko pomanjkljivosti v spletnih straneh. Pri odkritjih teh »talentiranih« aplikacij ni izjem glede tega, ali so bile poceni ali so stale malo premoženje in tudi ali so od garažnih podjetjih, ali pa za njimi stojijo močne ekipe razvijalcev. V nadaljevanju bomo na kratko prikazali »talent« nekaj aplikacij. Zaradi občutljivosti nekaterih podatkov pa vseh podrobnosti ne bomo izdali.

2.1 Razobličenja – »talent« nepravilne konfiguracije

Seveda se nam pogosto poraja vprašanje, kje »talente« iskat. Vemo da to ni enostavno delo, saj je potrebno dosti potrpežljivosti in iznajdljivosti, da najdemo res pravi talent. Ena vstopna točka je lahko tudi seznam razobličenih spletnih strani za domeno .si. Hekerji in ostali ki napadajo spletne strani, se radi pohvalijo glede njihovih dosežkov. Glede na to, da se pohvalijo kaj jim je uspelo in na kateri strani, so te spletne strani zelo dobri kandidati za naš izbor. Če pogledamo seznam za mesec marec letošnjega leta, lahko opazimo, da so poleg manjših spletnih strani nekatere označene tudi z zvezdico. Ta razobličenja imajo večjo vrednost kot ostala in če pogledamo so bile na seznamu tudi spletne strani Rdečega križa Slovenije in podjetja Bayer Pharme. Takšna mesta so torej idealen začetek zbiranja talentov. Izkaže se namreč, da poleg ranljivosti, ki so jih že izkoristili za razobličenja vsebujejo še kakšne druge pomanjkljivosti, ki so jih avtomatska orodja, ki jih uporabljajo, izpustila. Nekatera podjetja, ki jih je mogoče zaslediti na teh seznamih, smo tudi opozorili na te pomanjkljivosti, a so se na naš kontakt odzvali le redki.

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

Slika 3. Seznam razobličenih strani za domeno .si

2.2 Spletni portal - talent nepreverjenega vnosa

Opis naslednje napake še ni bil popravljen, zato točnega naslova ne moremo izdati. Je pa zanimiva napaka in zato jo bomo opisali. Spletni portal, ki boleha za to napako, prenaša preko URLja zahtevke za id strani. Pri preverjanju smo opazili, da ta parameter ni problematičen, saj ni reagiral na standardne teste. Po naključju smo poskusili dodati na koncu id parametra še eno ničlo oz smo poskusili odpreti vnesti id, ki ni obstajal in tedaj se je stran začela odzivati precej počasi in nad rezultatom smo bili presenečeni celo sami. Aplikacija nam je namreč vrnila vsebino celotnega CMS sistema in v teh podatkih smo hkrati dobili ne samo vsebino spletne strani, ampak tudi podatke o prijavah vseh uporabnikov in tudi njihova gesla v kriptirani obliki. Tako talentiranih aplikacij, bi si želela večina hekerjev.

2.3 *.uni-mb.si - talent nepravilne konfiguracije

Pri brskanju po spletnih strani različnih organizacij v domeni uni-mb.si je možno naleteti tudi na zanimivo spletno aplikacijo, ki na primer ima že izpolnjene podatke o prijavi, torej uporabniško ime in geslo, saj je to precej olajšalo delo testnemu uporabniku. Po kliku na prijavo smo dobili naslednje sporočilo, ki ga ob pravilni konfiguraciji na noben način ne bi smeli. Še posebej zato ne, ker vsebuje tudi izpis kode in prikazuje privzete vrednosti ob določenem pogoju.

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)
```

Slika 4. Napaka v spletni aplikaciji

2.4 Portal peljime.si - talent SQL vrivanja

Spletna stran www.peljime.si je precej nova in je pristala tudi na seznamu razobličenih strani in tako postala zanimiva za nas. Pri vnosu naslednjega URL naslova spletna stran deluje tako kot mora:

http://www.peljime.si/?lang=&option=content&podrocje=7&id=30.

Če pa le malenkost popravimo parameter področje, pa lahko vidimo, da nam spletna stran postreže z obilico podatkov o sami napaki in še drugih podatkih, ki so lahko še kako zelo koristni napadalcem. Tako smo lahko izvedeli cel SQL stavek, ki je uporabljen za povpraševanje, pot na disku, kjer so shranjene datoteke te spletne strani, dodatne spremenljivke in verzijo uporabljenega PHPja.

http://www.peljime.si/?lang=&option=content&podrocje=7a&id=30

NAPAKA

Sporocilo:	Pri SQL poizvedbi je prišlo do napake: Unknown column '7a' in 'where clause'
Datoteka:	/home/sinergija/domains/peljime.si/public_html/admin/classes/MySQL.php
Vrstica:	88
Sled napake:	

Datoteka:	/home/sinergija/domains/peljime.si/public_html/inc_left_menu.php
Vrstica:	33
Spremeljivke:	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/peljime.si/public_html/index.php
Vrstica:	247
Spremeljivke:	1 => /home/sinergija/domains/peljime.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.peljime.si

Slika 5. Prikaz napake na spletni strani

2.5 Svetovalka – talent nepreverjenega vnosa

Velikokrat naletimo na napake v spletnih aplikacijah, tam kjer dejansko pričakujemo, da jih ne bi smeli najti. Takšen primer je bil tudi primer eSvetovalke, ki so jo imeli na spletni strani občine Maribor. Pri predolgem vnosu se prikaže spodnja napaka, ki dejansko dosti pove o sami aplikaciji in njeni avtorici, ter izda še druge podatke, ki so lahko potencialnim napadalcem koristni.

Tako lahko na spodnjih slikah razberemo iz napake kje dejansko na disku se nahajajo spletne strani. Iz podatkov na drugi sliki pa lahko celo razberemo celo uporabniško ime avtorice eSvetovalke in pot na disku, kjer so bile izvorne datoteke.

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.

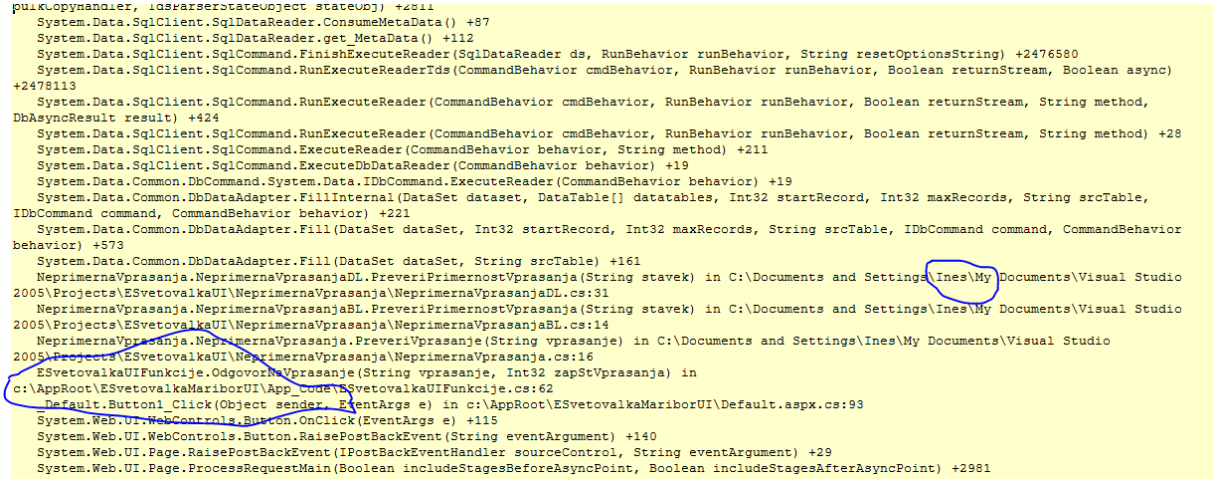
Exception Details: System.Data.SqlClient.SqlException: String or binary data would be truncated.
The statement has been terminated.

Source Error:

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

Source File: c:\AppRoot\ESvetovalkaMariborUI\App_Code\ESvetovalkaUIFunkcije.cs **Line:** 62

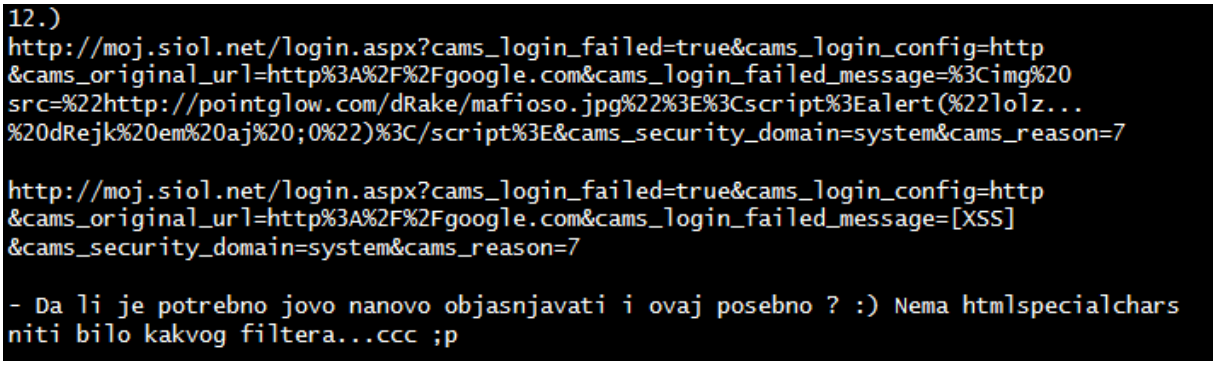
Slika 6. Prikaz napake na spletni strani



Slika 7. Prikaz napake na spletni strani

2.6 SIOL – XSS talent

Kot dokaz, da nimajo težave samo majhne spletne strani, lahko navedemo spletni portal moj.siol.net, ki je služil kot vstopna točka za nastavitve svojega računa. To ranljivost objavljamo zato, ker je bil ta prikaz prikazan že v eni izmed spletnih izdaj navodil za XSS napade. Ta XSS napad je bil objavljen sicer na tej spletni povezavi [3], ampak spletna stran trenutno ni dosegljiva, je pa zato še vedno mogoče priti do vsebine preko Google cache na tej povezavi [4].

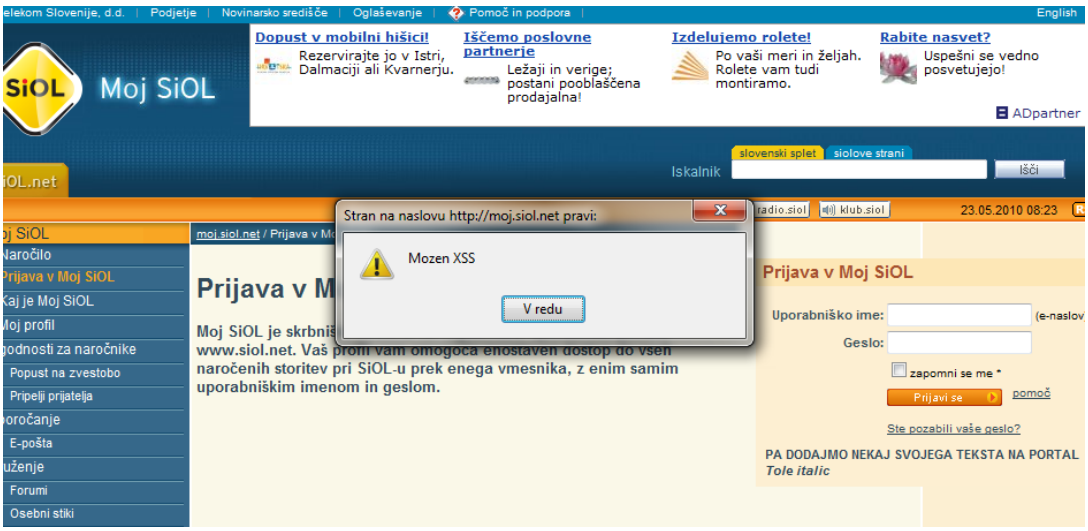


Slika 8. Opis XSS luknje za moj.siol.net na hrvaški spletni strani

Z uporabo namiga z zgornje povezave, lahko v HTML kodo na strežniku vrinemo svoje tekste, HTML kodo ali celo javascript kodo. To smo v nadaljevanju tudi demonstrirali.

http://moj.siol.net/login.aspx?cams_login_failed=true&cams_login_config=http&cams_original_url=http%3A%2F%2Fgoogle.com&cams_login_failed_message=PA%20DODAJMO%20NEKAJ%20SVOJEGA%20TEKSTA%20NA%20PORTAL%3Cbr%3E%3CI%3ETole%20it

alic%3C/i%3E%3Cscript%3Ealert%28%22Mozen%20XSS%22%29%3C/script%3E&cams_security_domain=system&cams_reason=7



Slika 9. Primer XSS, ki s pomočjo javascripta odpre okno

Ker je SiOL spremenil prijavno stran na prijava.siol.net smo preverili, če je tudi na tej strani mogoča enaka napaka. Opaziti je bilo, da je možno po spletni strani pisati, ni pa več možno vpisovati javascripta ali drugih HTML oznak, saj je bila aktivirana zaščita, ki to onemogoča.

https://prijava.siol.net/default.aspx?cams_login_failed=true&cams_login_config=http&cams_original_url=http%3A%2F%2Fwww.siol.net&cams_login_failed_message=Tukaj%20je%20tekst%20na%20spletni%20strani&cams_security_domain=system&cams_reason=7

Slika 10. Dodajanje teksta na spletni strani prijava.siol.net

3. PRIPOROČILA »TALENTOM«

Veliko večino prikaza problemov »talentiranih« aplikacij je možno odpraviti v kratkem času z malo vloženega napora in tudi rešitve so precej enostavne za tiste, ki se s tem ukvarjajo. Predvsem je potrebna pravilna konfiguracija in sicer najprej samega okolja v katerem te spletne aplikacije potem tečejo, torej operacijskega sistema, PHP ali ASP okolja in same podatkovne baze. V velikem številu primerov je tudi opaziti, da je produkcijska aplikacija hkrati tudi razvojna ali testna aplikacija in se na njih dela tudi razvoj, kar lahko vodi do nepričakovanih rezultatov. Če bi nekako morali izbrati najpomembnejši nasvet pa je ta, da je potrebno vsak vnos, ki pride s strani uporabnika, preveriti. Ne moremo se namreč zanašati na to, da so uporabniki zanesljivi ali na primer, da se preverjanje vnosa opravi na strani uporabnika, saj se lahko ta preverjanja vnosov obide na enostaven in lahek način.

Vsa opažanja glede primerov aplikacij lahko strnemo v spodnje tri točke, s katerimi bi lahko »talentirane« aplikacije v veliki meri odpravili:

- opraviti je potrebno pravilno konfiguracijo programskega in sistemskega okolja,
- upoštevati je potrebno priporočila in dobre prakse pri implementaciji aplikacij,
- pred objavo spletne aplikacije je potrebno interno ali eksterno preveriti aplikacijo glede pravilnih nastavitev in varnosti.

4. ZAKLJUČEK

V prispevku smo prikazali, da tudi v Sloveniji obstaja veliko »talentiranih« ljubiteljskih in tudi profesionalnih razvijalcev, ter posledično tudi kar nekaj »talentiranih« aplikacij. Dokler so te aplikacije namenjene samo spletnim predstavitvam ni težav. Težave se lahko pokažejo, ko te aplikacije začnejo prenašati kakšne osebne podatke ali druge občutljive podatke. Veliko neželenih »talentov« lahko tako predstavlja potencialno veliko nevarnost ne samo za podatke, ampak tudi za informacijske sisteme, ki so zgrajeni okrog teh spletnih aplikacij. Kot vemo je Internet dinamična stvar in prav tako tudi napadalci, zato je mogoče včasih priporočljivo poseči tudi po zunanjih izvajalcih, ki lahko pomagajo zmanjšati število »talentiranih« aplikacij.

LITERATURA

1. *http://www.owasp.org/*, OWASP *Top 10 2010*.

2. *WhiteHat Website Security Statistic Report,Spring 2010, 9th Edition, www.whitehatsec.com, 2010.*

3. XSS SIOL http://presszone.org/home.pz?misc=search&subaction=showfull&id=1263128230&archive=&cnshow=news&start_from=&ucat=3

4. Google cache: http://webcache.googleusercontent.com/search?q=cache:E7d-jGzcgusJ:presszone.org/home.pz%3Fmisc%3Dsearch%26subaction%3Dshowfull%26id%3D1263128230%26archive%3D%26cnshow%3Dnews%26start_from%3D%26ucat%3D3+xss+moj.siol.net&cd=7&hl=sl&ct=clnk&gl=si&client=firefox-a