

Sigurnost Joomla CMS-a

doc.dr. Samir Lemeš



templates SEO
SECURITY ACL
design extensions
power SPEED
translation

Doc.dr. Samir Lemeš

- Doktor tehničkih nauka, Univerza u Ljubljani, 2010
- Zaposlen na Univerzitetu u Zenici od 1996
- Rukovodilac odsjeka za veze i kriptozastitu u Centru službi bezbjednosti Zenica (1993-1996)
- Predsjednik BAS/TC I (BH standardi, Tehnički komitet I - Informacione tehnologije)
- Autor zvaničnog prevoda standarda BAS ISO/IEC 17799:2006 "IT - Sigurnosne tehnike - Pravilo dobre prakse za upravljanje sigurnošću informacija"
- Član stručnog savjeta Akademske i istraživačke mreže BiH BIHARNET
- Autor 7 knjiga, 44 naučna rada, 10 članaka u magazinu INFO, 24 web stranice,...

Sigurnost Joomla CMS-a

- Važnost sigurnosti CMS-a
- Pojam sigurnosti (C-I-A)
- Serija standarda ISO/IEC 27000
- Procjena rizika
- Planiranje
- Zaštita
- Oporavak
- Linkovi



Važnost sigurnosti CMS-a

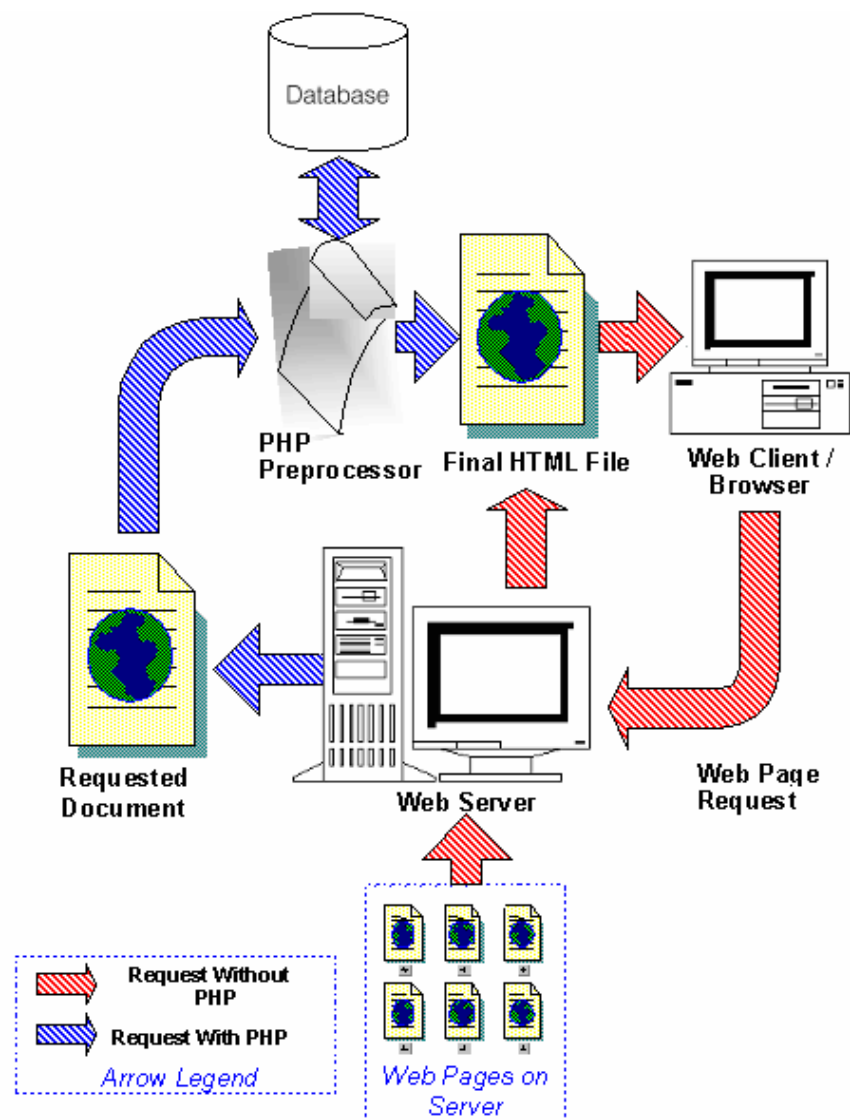
- U XXI vijeku informacije su postale najskuplja imovina
- Sve vrste podataka se digitalizuju kako bi iskoristili prednosti internet povezanosti: tehnička dokumentacija, lični podaci, novac i novčane transakcije, mediji, komunikacije, GIS/GPS, prevozna sredstva, energetika, trgovina, emocije,...
- Radi multiplatformskog pristupa, teži se ka univerzalnom, web-baziranom interfejsu

Važnost sigurnosti CMS-a

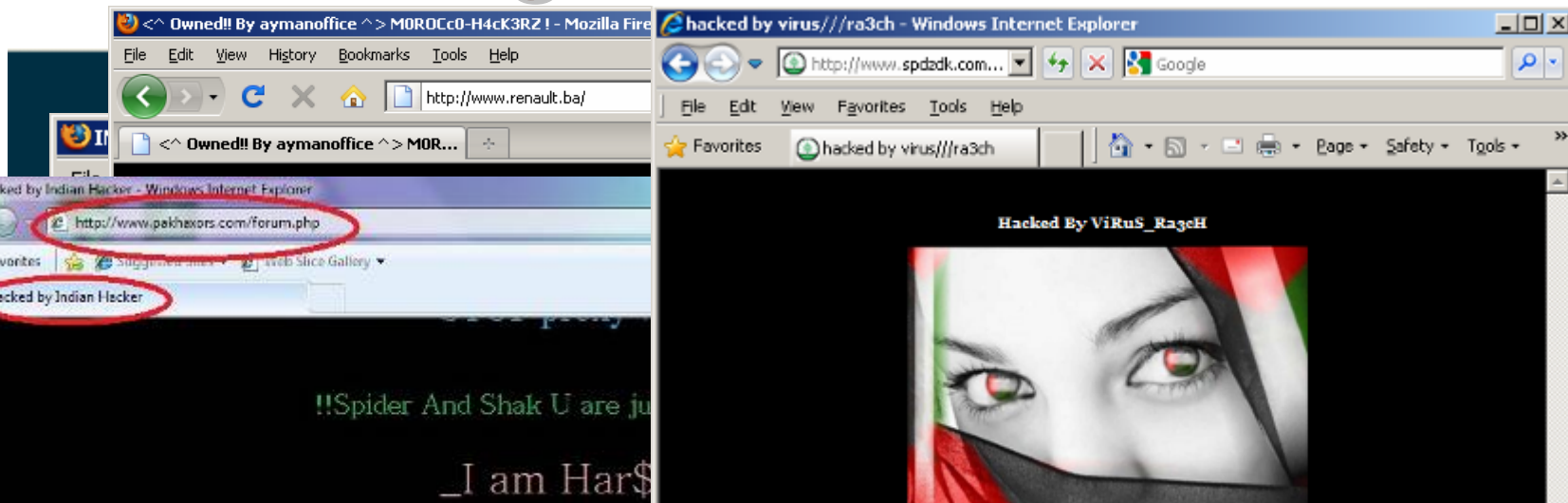
- Umjesto statičkih HTML stranica, sve su prisutniji dinamički web portali (koriste skriptne jezike da generišu HTML u trenutku pristupa stranici)
- Za veću pristupačnost održavanja i ažuriranja dinamičkih web portala koriste se CMS (*Content Management System*)
- Tri trenutno najpopularnija CMS-a: Wordpress, Joomla, Drupal
- Popularnost = veća izloženost prijetnjama

Važnost sigurnosti CMS-a

- Razlika između statičkih HTML i dinamičkih PHP stranica:
- Složeniji sistem = veći broj prijetnji kojima je izložen
- Svaka komponenta predstavlja potencijalnu prijetnju



Važnost sigurnosti CMS-a



HACKED BY SCIENTIST/AYT

AYYILDIZ TEAM



Özgürlük Sembolümüz Bayrak Oldu Vatan'a
Bayrakta ki Rengimiz Gurur Duysak Az Sana
Gece Oldu AYYILDIZ Secde Etti Allah'a
Yükselen Bir Ses Gibi Canım Kurban Vatan'a



HaCkEd By ViRuS_Ra3cH



* لا إله إلا الله محمد رسول الله *

ALGERIAN HACKER IS HIER

Hacked By rageh

Pojam sigurnosti (C-I-A)

- **C-I-A: Confidentiality - Integrity - Availability**
- **Sigurnost informacija** se u standardu ISO/IEC 27001:2005 predstavlja kao očuvanje:
 - a) povjerljivosti (tajnosti):** osiguranje da su informacije dostupne samo onima kojima je dopušten pristup;
 - b) integriteta:** očuvanje tačnosti i kompletnosti informacija i metoda za obradu;
 - c) dostupnosti:** osiguranje da ovlašteni korisnici imaju pristup informacijama i imovini u vezi s njima, kada se to zahtijeva

Pojam sigurnosti (C-I-A)

- Sigurnost informacija se postiže implementacijom odgovarajućih **kontrola**, koje mogu biti načela, prakse, procedure, organizacione strukture i softverske funkcije
- Te kontrole treba uspostaviti da bi se obezbijedilo poštivanje specifičnih sigurnosnih ciljeva te organizacije
- Primjer kontrole:
Implementirati bolju provjeru autentičnosti korisnika i mehanizme pristupa IT sistemima koji sadrže podatke o kupcima

Pojam sigurnosti (C-I-A)

- Informacioni sistemi su izloženi brojnim sigurnosnim prijetnjama: računarske prevare, špijunažu, sabotáže, vandalizam, požare i poplave, zlonamjerni kod, haking, napadi uskraćivanjem usluga
- **ISMS** (*Information Security Management System*) pruža model za uspostavljanje, implementaciju, korištenje, nadzor, reviziju, održavanje i unapređenje zaštite informacija, s ciljem postizanja ciljeva poslovanja, na osnovu procjene rizika i nivoa prihvatljivih rizika u organizaciji

Pojam sigurnosti (C-I-A)

- **Hacker:** Osoba koja proučava tehnologiju kako bi mogao napisati bolji kôd
- **Cracker:** Osoba koja proučava tehnologiju isključivo s kriminalnim namjerama, s ciljem krađe, destrukcije, zaposjedanja ili špijunaže.
- **Owned:** Stanje računara nakon probijanja zaštite i nakon instaliranja kôda za krađu, špijuniranje ili uništavanje podataka
- **Exploit:** Potencijalna sigurnosna prijetnja koja se može iskoristiti za razbijanje zaštite ili napad na internet server preko mreže

Serijski standardi ISO/IEC 27000

- Informacije iz informacijskog sistema organizacije često predstavljaju poslovne tajne od suštinske važnosti za organizaciju
 - Primjer 1: Ako se onemogući protok informacija – koliko dugo će organizacija funkcionirati?
 - Primjer 2: Nesvjesno koristite netačne podatke. Kako možete donositi dobre odluke za poslovanje?
 - Primjer 3: Do vaših poslovnih planova može doći bilo ko, pa i konkurencija. Imate li tako budućnosti?
- Odgovore na ovakva pitanja daje sistem za upravljanje informacijskom sigurnošću (ISMS) zasnovan na seriji standarda ISO/IEC 27000.

Seriya standarda ISO/IEC 27000

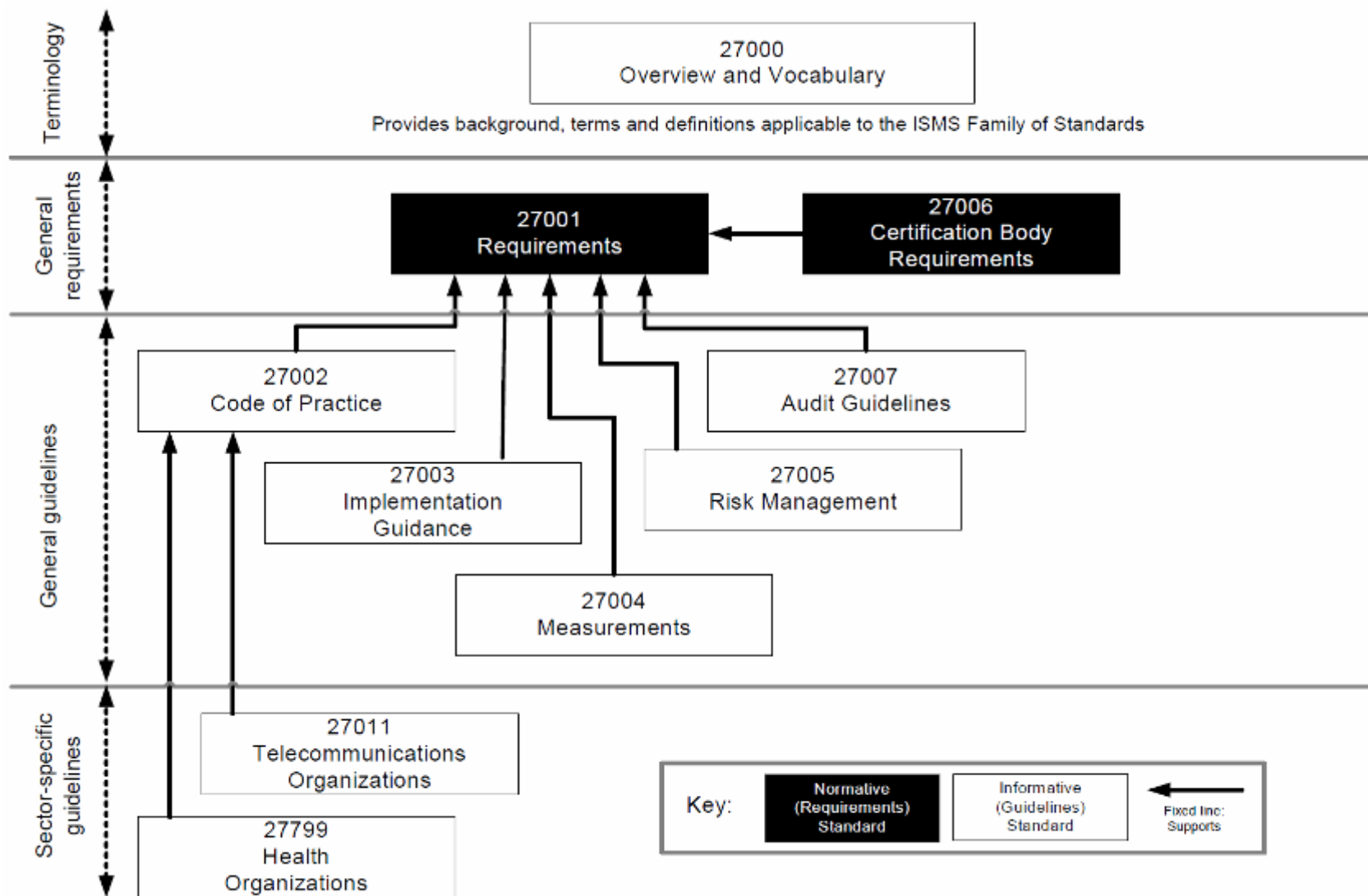
- Seriya standarda ISO/IEC 27000 daje smjernice i dobre prakse za dizajniranje, implementaciju i audit sistema za upravljanje sigurnošću informacija (ISMS) s ciljem zaštite povjerljivosti, integriteta i dostupnosti informacija.
- Standardi su potekli iz Velike Britanije, u DTI (*Department of Trade and Industry*), s ciljem definisanja kriterija za procjenu informacijske sigurnosti i kreiranja pravila dobre prakse (*Code Of Practice*).



Serijski standardi ISO/IEC 27000

- 1995. godine usvojen prvi standard, BS 7799, krajem 2000. godine postaje ISO/IEC 17799. Taj standard je revidiran 2005. godine.
- Nakon toga je ISO komitet JTC1/SC27 pokrenuo razvoj i usvajanje serije standarda 27000.
- 1998. godine BSI je izdao drugi dio standarda, BS7799-2, koji je sadržao specifikacije ISMS, a koji je kasnije postao ISO/IEC 27001
- 2007. godine je ISO/IEC 17799 preimenovan u ISO/IEC 27002

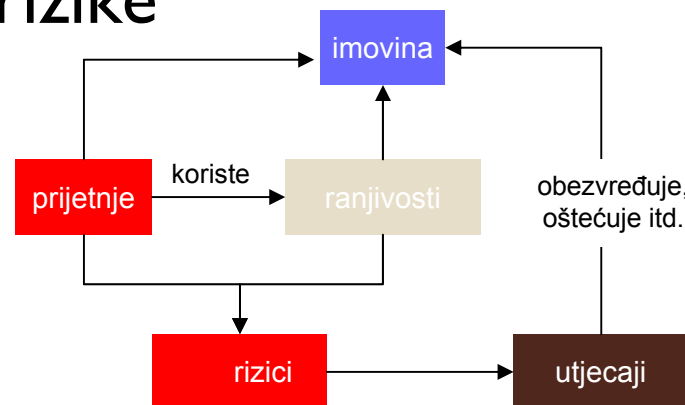
Seriya standarda ISO/IEC 27000



Procjena rizika

1. Definirati pristup
2. Identifikovati i procijeniti rizike

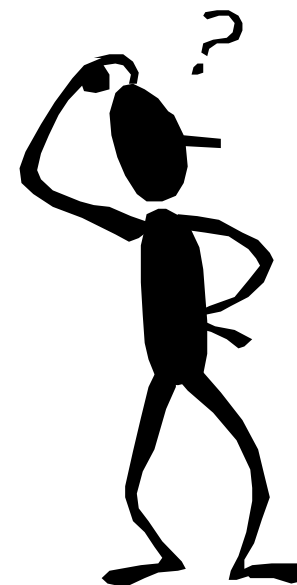
- Imovina i njena vrijednost
- Prijetnje i ranjivosti
- Rizici i utjecaji



- **Primjer:**
 - **Imovina** - podaci o kupcima - osjetljivi i vrijedni
 - **Prijetnje** - neovlašten pristup, curenje, modifikacije
 - **Ranjivosti** - nedostatak ili neodgovarajuća kontrola pristupa, nedostatak provjere autentičnosti korisnika
 - **Rizik** - visok
 - **Utjecaj** - visok

Procjena rizika

- Opcije
 - **Smanjiti rizik** – implementacija kontrola
 - **Prihvatiti rizik** – posljedice koje organizacija može finansijski podnijeti
 - **Transfer rizika** – osiguranje ili kroz ugovore
 - **Izbjeći rizik** – ne planirati tu aktivnost jer ona može dovesti do rizika
- Odluke donosi menadžment
 - Kriteriji za prihvatanje rizika i zaostali rizici
 - Zahtjevi i potrebe s aspekta poslovanja
 - Troškovi i resursi



Procjena rizika

- Šta se može desiti?
 - hardverski/softverski kvar, DNS, hakeri, zemljotres, krađa, nestanak struje, preopterećenost, ...
- Šta se može uraditi da se to spriječi?
 - redundantnost, backup, plan oporavka, pažljivo i detaljno proučavanje dokumentacije, definisanje prava pristupa, implementacija captcha i sličnih mehanizama, komercijalne ekstenzije za zaštitu...
- Procjena prihvatljivosti rizika: da li šteta koja bi mogla nastati opravdava investiciju u sigurnost? (lični blog i eCommerce nemaju isti nivo sigurnosnih zahtjeva)

Planiranje

- Morate poznavati rizike kojima je izložen CMS
- Procijenite troškove: oni koji nastaju ako se rizik ostvari i troškove oporavka
- Plan mora biti jednostavan
- Plan treba testirati prije implementacije
- Mora se znati ko je za šta odgovoran
- Mora se znati kada se plan aktivira
- Plan mora imati odobrenje rukovodstva
- Osoblje mora biti upoznato s planom

Zaštita

- Ključna je priprema servera; treba provjeriti: ekstenzije, hosting, otvorene portove, verziju HTTP servera (Apache)
- Treba ispravno podesiti prava pristupa za datoteke (644) i foldere (755)
- Fino podešavanje konfiguracijskih datoteka: .htaccess, hosts, php.ini
- Instalirati što noviju, stabilnu verziju CMS-a
- Brisanje nepotrebnih i nekorištenih datoteka, modula, ekstenzija, skripti
- Redovan backup

Zaštita

- Najčešće greške:
 - Administrator ima korisničko ime ADMIN
 - Šifre koje je lako kompromitovati: P@ssw0rd
 - Pogrešno podešena prava pristupa datotekama i folderima (777)
 - Nepostojanje datoteka ".htaccess" ili "php.ini"
 - Komponente koje nisu provjerene ili koje dolaze s nesigurnih izvora (warez)
 - Nedovoljno proučene upute
 - Nedostatak dokumentacije
 - Nepostojanje backup-a



Zaštita

- *Default database prefix (jos_)* se može promijeniti, kako bi se spriječili SQL upiti koji mogu preuzeti podatke (username / password) iz tabele "jos_users".
- Prava pristupa 777 ili 707 se koriste samo kad skripta mora snimati u datoteku ili folder. Svi ostali folderi/datoteke trebaju biti:
 - PHP datoteke, .htaccess: 644
 - Config datoteke: 666
 - Svi ostali folderi: 755

Zaštita

- Podsjećanje na prava pristupa (unix/linux):

- `ls -al`
`file.php user group rwx r-x r-x`

- **Owner**, **Group**, **Other**

- **r** = Read, **w** = Write, **x** = Execute

- `rwx r-x r-x = 111 101 101 = 755`

- `rw- r-- r-- = 110 100 100 = 644`

- `rwx rwx rwx = 111 111 111 = 777`

- Ako imate SSH pristup serveru:

- `cd /`

```
find . -type f -exec chmod 644 {} \;
```

```
find . -type d -exec chmod 755 {} \;
```

Zaštita

- Pomoću ".htaccess", osjetljivi folderi (administrator) se mogu zaštititi šifrom, i može im se ograničiti pristup po IP adresi
- Rename "/htaccess.txt" u "/.htaccess"
- Osim povećanja sigurnosti CMS-a, ova datoteka se može koristiti i za:
 - Promjenu stranica s greškama (404)
 - Preusmjeravanje URL-ova
 - Zabranu listinga foldera bez index.php
 - Zaštitu pomoću username/password-a
 - itd.

Zaštita

- Pod pojmom SPAM obično se podrazumijeva neželjena pošta (reklame, pisma, e-mail)
- Ukoliko su na web stranici omogućeni komentari, velika je vjerovatnoća da će u komentarima biti SPAM poruka
- Rješenja: ekstenzije, Captcha, registracija korisnika, komentari vezani za Facebook



Zaštita

- Primjer probijanja zaštite koristeći *SQL injections*:
 - http://www.joomla_server.ba/index.php?option=com_user&view=reset&layout=confirm

Potvrda Registracije

Verifikacijski token je poslan na vašu email adresu. Unesite token u polje ispod da biste dokazali da se zaista radi o vašem korisničkom računu.

Token:

Pošalji

- Ukoliko server nije pravilno konfigurisan, može se pristupiti SQL bazi o korisnicima

Zaštita

- Dobro se informisati i proučiti uputstva
- Zatvoriti sve nepotrebne portove na serveru
- Deinstalirati nepotrebne ekstenzije i module
- Instalirati sve zakrpe za OS, Apache, MySQL, PHP, Joomla
- Strogo kontrolisati prava pristupa (rwx)
- Podesiti .htaccess i php.ini
- Ako je dozvoljen upload, ograničiti veličinu datoteke
- Podijeliti prava pristupa po grupama korisnika

Zaštita

- Promijeniti *default* imena korisnika i foldera, posebno administratora
- Redovno provjeravati log datoteke
- Napraviti plan za oporavak
- Redovan backup: php, SQL, media
- Pripremljen rezervni server
- Blokirati IP adrese s kojih su stizali napadi
- Informisanje o novim prijetnjama
- Informisati hosting providera o svakoj sigurnosnoj prijetnji

Oporavak

- Ukoliko se sigurnosna prijetnja ipak ostvari:
 - Procijenite štetu
 - Napravite kopiju svih logova i sačuvajte je izvan servera (radi eventualnih sudskih procesa)
 - Brisanje datoteka koje su kompromitovane (index.php, index.htm, index.html,...)
 - Restauracija iz rezervnih kopija
 - Informišite hosting providera



Linkovi

- http://docs.joomla.org/Security_Checklist_I_-_Getting_Started
- <http://www.rsjoomla.com/joomla-components/joomla-security.html>
- <http://www.phpera.com/2010/12/joomla-site-optimization-security>
- <http://forum.codecall.net/security-tutorials/4867-joomla-hacking-script.html>
- Tom Canavan: Joomla! Web Security:
<http://www.amazon.com/Joomla-Web-Security-Tom-Canavan/dp/1847194885>