

UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSTDIPLOMSKE STUDIJE

STUDIJSKI PROGRAM
SAVREMENE INFORMACIONE TEHNOLOGIJE



Upravljanje sadržajem na internetu sa osvrtom na sigurnost

-MASTER RAD-

Mentor:

prof. dr Milan Milosavljević

Kandidat:

Nikola Živković, 410257/2012

Beograd, 2013

Sadržaj

1 Uvod.....	1
1.1 Šta znači CMS?	1
1.2 Šta je Content Management System?	1
1.3 Web Content Management System.....	1
1.4 Šta je Content Management System?	2
1.5 Content Management System tipovi	4
1.6 Portali opšte namene.....	5
1.7 Ecommerce CMS.....	5
2 Wordpress.....	6
3 Open Cart.....	9
3.1 Problemi i njihovo rešavanje	9
4 Razlozi za Magento	11
4.1 Struktura Magento aplikacije	11
4.2 Struktura	12
5 CMS bezbednost i operacije.....	14
5.1 Meta.....	14
5.2 Operativna razmatranja	15
5.3 Edukacija zaposlenih i krajnjih korisnika	16
5.4 Podizanje svesti o bezbednosti.....	16
5.5 Obuka o politikama, Bezbednost informacija	17
5.6 Pružanje standardnih protokola za izveštavanje o pretnjama	17
5.7 Obezbeđivanje sigurnosti mejla	17
5.8 Primena zakrpa i updejta	18
5.9 Biti svestan i ostati siguran.....	18
Napomena	18
6 Gledajući sajt „Kroz oči hakera”	18
6.1 Koraci ka dobijanju pristupa sajtu	20
6.2 Istraživanje	20
6.3 Guglovanje.....	22
6.4 Korišćenje Google Hacking Tools (Dorks).....	23
6.5 Footprinting.....	24

6.5 Korišćenje Nmap-a u loše svrhe	27
6.6 Korišćenje traceroute.....	29
7 Primer CMS-a izrađenog na osnovu prethodnih informacija.....	30
7.1 Izgled strane za ubacivanje proizvoda	31
7.2 Izgled strane za menjanje detalja postojećeg proizvoda	32
Zaključak	33
Literatura:	34

1 Uvod

Centralni predmet ovog master rada su savremeni sistemi za upravljanje sadržajima na internetu (Content Management System - CMS).

U prvom delu rada biće analizirane tipične klase ovih sistema, posebno sa stanovišta potreba korisnika i zahteva u pogledu administriranja i održavanja.

Takođe, detaljnije su obrađeni popularniji Content Management System-i, kao što su *Wordpress*, *Drupal*, *Magento* itd., kao i Content Management System-i pravljeni posebno za firme, preduzeća i kompanije koji se prilagođavaju samom korisniku i njihovim zahtevima. Naravno, opisano je i kako se maksimalno mogu iskoristiti besplatni Content Management System-i.

1.1 Šta znači CMS?

Content Management System je termin koji se koristi u mnogim sistemima i mnogim procesima u celom svetu. Postoji više tipova Content Management System-a, ali da ne bi došlo do zabune oko značenja ovog termina, u narednim podnaslovima biće objašnjeno šta Content Management System znači za temu ovog rada.

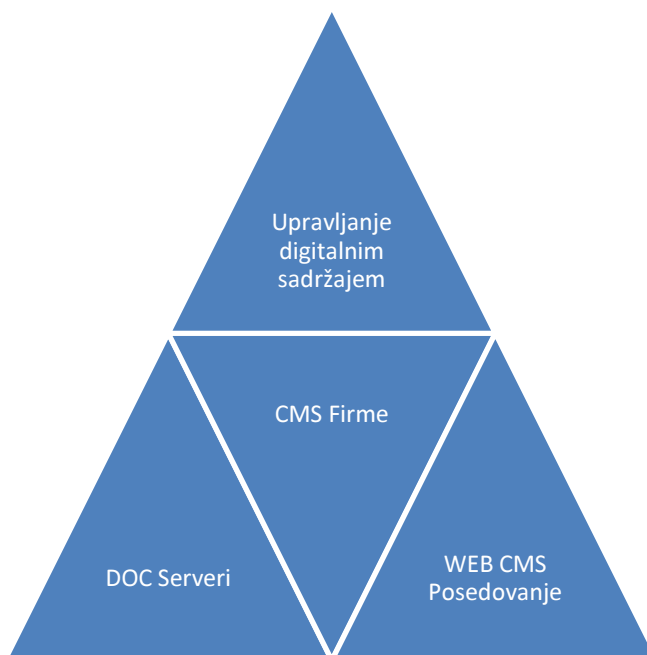
1.2 Šta je Content Management System?

To su bilo koji procesi koji dozvoljavaju pojedincima da unose, menjaju, brišu ili uređuju sadržaj samih stanica ili sistema. Ovi sistemi mogu biti on-lajn ili of-lajn. Neki su besplatni za korišćenje i njihov programski kod je dostupan svima, dok postoje i oni koji se nalaze u vlasništvu proizvođača. Bazirani su uglavnom na jednom ili više tipova sadržava („content type”). Često se dešava da se pomeša terminologija i značenje Content Management System-a sa nekim granama, iako se koristi za različite procese.

1.3 Web Content Management System

Mnogi Content Management System-i su vlasnički i veoma su moćni alati unutar organizacija za upravljanjem sadržajem, različitih tipova medija i distributivnih kanala.

Slika 1



U nastavku u centru pažnje biće besplatni Content Management System-i koji služe za upravljanje veb-sajtovima, njihovim sadržajem i izgledom. Uglavnom se za njih koristi precizniji naziv – Web Content Management System, iako ga dizajneri i veb-programeri ipak zovu samo Content Management System.

1.4 Šta je Content Management System?

Termin Web Content Management System obično se definiše kao softver na server strani koji je dizajniran da pojednostavi kreiranje sajta i njegovo održavanje. Ovi sistemi upravljaju on-lajn sadržajem, kreiranjem veb-strana i dozvoljavaju korisnicima da menjaju i koriste sadržaj bez nekog tehničkog znanja i iskustva.

Dalje će biti reči o nekim od osnovnih funkcionalnosti Content Management System-a.

Sam sadržaj se uglavnom nalazi u nekoj bazi podataka, ovim nam dozvoljava da ga menjamo koristimo gde god želimo, menjamo ili upotrebljavamo u druge svrhe.

Uglavnom Content Management System ima i deo koji je administrativni i koji sliži za ubacivanje, izbacivanje i menjanje sadržaja same baze podataka.

Ovakva vrsta administracije je dostupna preko bilo kog pretraživača, što znači da nije potrebna instalacija nekog klijentskog softvera, tako da gde god da se nalazimo i imamo pristup internetu, imamo i pristup i našim podacima u bazi koja se nalazi na nekom od servera, jednostavnim logovanjem pomoću korisničkog imena i lozinke.

U stvari, Content Management System-i ne služe samo za ubacivanje i brisanje sadržaja, već služe da taj sadržaj prikažu na odgovarajući način na samoj veb-strani.

Content Management System će iskoristiti svoje okruženje da napravi sajt od vašeg sadržaja i korišćenjem predefinisanih šablona ili dizajniranjem šablona prema potrebama i željama korisnika.

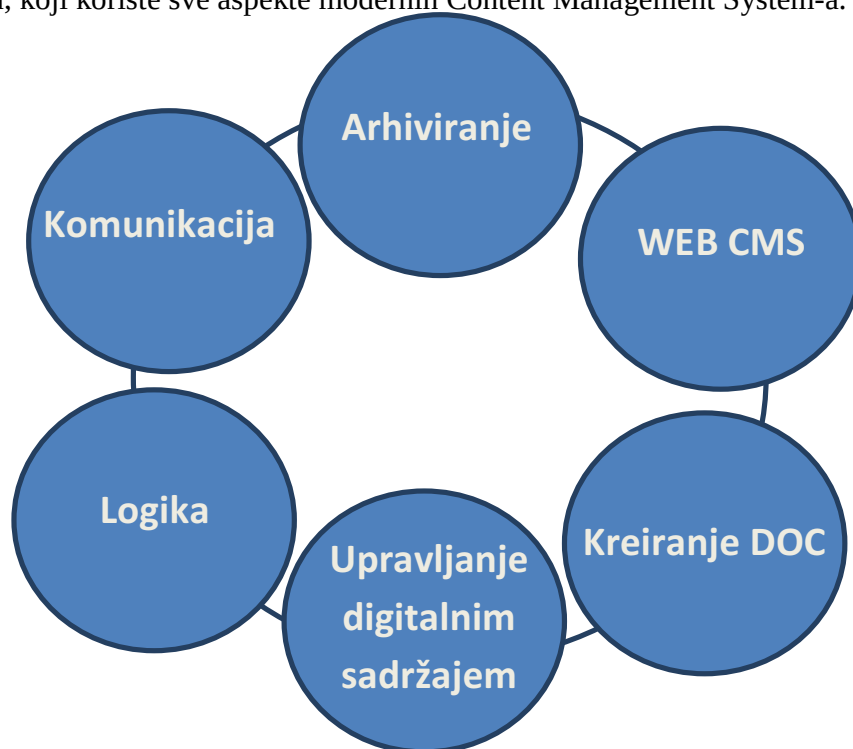
Content Management System nam uglavnom sa svojim templejtima/šablonima daje mogućnost upravljanja celokupnim sadržajem i izgledom sajta, zaglavljima, podglavljima, sajdbarom, blog stranama, galerijom, komentarima, mejlovima, korisnicima itd., čak i upravljanje bazom podataka korišćenjem nekih od alata koji su takođe besplatni.

Content Management System-i drastično mogu da ubrzaju razvijanje veb-sajtova od strane dizajnera i veb-programera, mogu da dizajniraju kompleksnije i veće sajtove za manji vremenski period, čak je i moguće dodavanje naprednijih funkcionalnosti još lakše i, naravno, mogućnost da i lica koja nisu obučena za rukovanje takvim sistemima mogu da ih koriste i unapređuju bez većih problema.

1.5 Content Management System tipovi

Na današnjem tržištu Content Management System tipova postoji doslovno na stotine vrsta iliti tipova Content Management System-a i gotovo je nemoguće suziti ih u jednu kategoriju, ali mogu se kategorizovati po nekim standardima. Content Management System tipovi serverski, bazirani na kodu daju velike mogućnosti korisnicima sistema.

U daljem tekstu CMS tipovi biće kategorisani na osnovu industrije u kojoj se koriste. Uglavnom, potraga za Content Management System-om se može smanjiti tako što se prvo bira tip rešenja a onda treba tražiti Content Management System-e koji se specijalizuju u oblasti kojom se bavite. Jedan od boljih primera je Content Management System u velikim organizacijama, koji koriste sve aspekte modernih Content Management System-a.



Slika2

Ovakvi sistemi se koriste tamo gde su potrebe organizovanja dokumenata velike. U slučaju da nekome treba određena vrsta Content Management System-a, potrebno je angažovati programera koji će izraditi sistem koji odgovara potrebama korisnika.

1.6 Portali opšte namene

Ovi sistemi nisu fokusirani na određene stvari, ali su zato dizajnirani da daju kontrolu nad arhitekturom sajta, objavljivanjem sadržaja i administracijom samog sajta. Većina ovih sistema je nadogradiva, tj. sa određenim dodacima može se unaprediti njihova funkcionalnost. Neki od tih Content Management System-a su: Drupal Joomla Typo3 Modx, Made simple, Wordpress... Neke od ovih sistema biće detaljnije opisane dalje u radu. Iako Wordpress spada među ove sisteme, on je jedan od najpopularniji blogerskih Content Management System-a, kao i movable type, text pattern.

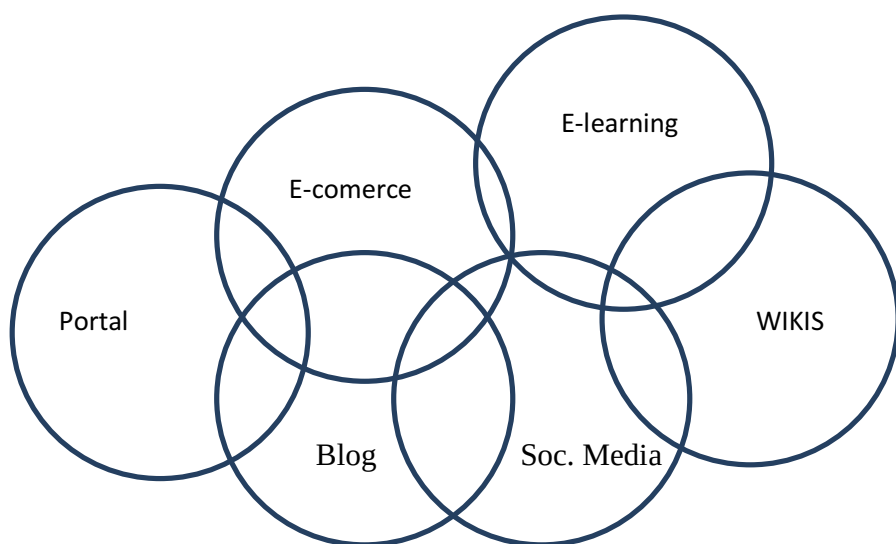
U poslednje vreme dosta Content Management System tipova počinje i da ulazi u oblast e-learning-a, koji su bazirani na blog Content Management System-ima. Pošto se takvi sistemi koriste u obrazovanju, imaju i mogućnost pravljenja kvizova testova i sl. Uglavnom mogu da koriste sve vrste dokumenata od pdf-a, docx-a, htm-a audio, video, sadržaja. Neki od poznatijih e-learning sistema su: .LRN, ATutor, Moddle, Docebo.

1.7 Ecommerce CMS

Content Management System-i su aplikacije za upravljanje on-lajn korpama ili ecommerce sajtovima, proizvodima koje prodaju i daju akcenat sigurnosti i on-lajn plaćanju. Neki najpoznatijih su „Magento”, „Cube cart”, „Opencart”, „Zencart” i „Presta shop”.

Jedan od najpoznatijih Content Management System-a danas je Content Management System koji se koristi za društvene mreže, mogu ga koristiti zajednice za upravljanje profilima i omogućavanje dopisivanja u vidu teksta, a i videa i aploudovanja sadržaja kao što su slike, pesme, linkovi, youtube linkovi, dokumenta...

Najveći broj današnjih Content Management System-a je toliko evoluirao da se mogu koristiti u gotovo svim oblastima, od raznih ministarstava do zdravlja, takoreći svuda. Sa svojim pluginovima poboljšavaju svoju funkcionalnost i šire se na što veće tržište.



Slika3

2 Wordpress

Ako imate posao, profitbilan ili neprofitabiln, i želite da imate on-lajn pristup, moraćete da imate sajt. To je mesto gde se stvari komplikuju vrlo brzo.

Wordpress. Postoje i druge opcije, ali **Wordpress** je veoma dobar i bio je u upotrebi nekoliko godina u velikim i malim poduhvatima. Dakle, tu je testiran.

Wordpress daje dve stvari gotovo momentalno [8],

- 1) Profesionalni izgled, on-lajn pristup i
- 2) Sajt možete sami da uređujete.

„**Wordpress** je open source blog izdavačka aplikacija.”

Šta to znači za korisnika? Ako želite da imate veb-sajt, možete da koristite **Wordpress** da odmah pokrenete sajt koji koristi blogging alate, ali i druge mogućnosti.

Treba razmišljati o korišćenju postojeće tehnologije i raznovrsnosti rešenja i resursa dostupnih preko interneta, besplatno, za podešavanje veb-sajta zasnovanog na motoru ili „blogovanje blogu izdavačke primene” prema potrebama korisnika.

Wordpress

Wordpress dolazi u dve varijante, tri zapravo, tj. dve koje su najvažnije korisnicima – **Wordpress.com** и **Wordpress.org**.

Razlika između COM i ORG verzije **Wordpress-a** jeste da je neko od njih i domaćin drugog. **Wordpress.com** je domaćin sajt na svojim serverima, tako da ne morate učiniti ništa o pronalaženju domaćina ili ISP. Sve što treba da uradite je da se registrujete sa **Wordpress.com** i onda da jednostavno pokrenete blog. Stranice se mogu popunjavati sadržajem koji sami odaberete.

Wordpress.org je samostalna verzija koja mora da se preuzme i zatim instalira na posebnom veb-hostu (ili ISP). Neki domaćin (host) koji preporučuje **Wordpress** na njihovom sajtu, nude jedan klik od automatske instalacije. Proverite sa hostom mogućnost instalacije kod njih. Takođe, uverite se da sami provajderi imaju podršku najnovijeg PHP-a i SQL-a.

[8]. To će omogućiti da instalacija **Wordpress** radi na tom hostu.

Bilo da korisnik želi rešenje domaćina ili da sam pronađe rešenje, tj. host, može biti zanemarljive razlike, ali i velike razlike, u zavisnosti od toga šta mu je potrebno.

Wordpress.com nudi 30–40 gotovih šablona ili tema koje se mogu izabrati za određivanje izgleda sajta, neke od njih deluju profesionalno, reprezentativno i u nekim slučajevima veoma impresivno. Mogu se prilagoditi neki elementi većini tih šablona, kao što su umetnička dela koja stoje u zaglavlju sajta. **Wordpress.org** ima hiljade šablona dostupnih na sajtu **Wordpress.org**, kao i preko interneta. Ovo su šabloni napravljeni od strane stotine različitih dizajnera, neki su dobri, a neki loši, neki se mogu kupiti, ali većina je potpuno besplatna.

Ako je neophodno ili korisnik jednostavno želi da njegov sajt bude jedinstven, onda neko ko zna HTML/CSS, treba da osmisli jedinstven stil da promeni izgled ovih šablona.

Izraz šabloni odnosi se na pojedine delove koda i raspored elemenata koji čine Wordpress sajt. Gde ovo je posebno bitno? Neke teme koriste više ili manje šablona za rukovanje podacima na veb-sajtu. U osnovi, to znači funkcionalnost. Ako korisnik želi najviše funkcionalnosti za svoj sajt, treba da odabere temu koja ispunjava ono što želi, a zatim se može uraditi redizajn, da bi izgledao onako kako želi.

Ako „objavljivanje blogova aplikacija” nije jasno, kako je ovo? **Wordpress** omogućava da se kreiraju veb-stranice (Pages ili poruke) na sajtu korisnika, organizuje ih hijerarhijski i ispuni ih sadržajem kojim želi[8].

Dakle, ako korisnik ima posao i želi da prodajete proizvode (ili usluge), može napisati karakteristike i objaviti na sajtu. Ukoliko ima fotografije proizvoda, može ih jednostavno postaviti. Ako je potrebna funkcionalnost upravljanja transakcijama kreditnih kartica, može se registrovati sa Checkout servis Google i dodati dugme Kupi.

Bingo, eto ga e-commerce sajt!

Wordpress je počeo kao rešenje za pravljenje blogova, to je primarna funkcija – da omogući kreiranje i objavljivanje sadržaja. Dakle, ono što većina ljudi prepoznaje kao blog, (članke napisane od strane vlasnika sajta i postavljene na sajt, organizovane u skladu sa hronologijom), zapravo je poruka u **Wordpress-u**.

Stranice, s druge strane, jesu statične informacije, stranice kopije (i fotografije i slično), koje se ne menjaju često ili uopšte i treba da se organizuju i arhiviraju na osnovu njihovog datuma upisa. Pošto **Wordpress** koristi snagu baze podataka da pruža informacije (stranice i poruke) za posetioce veb-sajta, to je po definiciji dinamičan sajt. Dakle, da budemo precizniji, stranice u **Wordpress** sajtu ne zahtevaju ažuriranje ili upravljanje kao i poruke.

Šta je korisniku potrebno?

Ako gorepomenuta objašnjenja nisu jasna, evo dodatnog pojašnjenja.

Da li znate da je **Wordpress** besplatan?

Wordpress omogućava da se u nekoliko koraka dobije gotov sajt. U slučaju **Wordpress.com** potrebno je se obave sledeći koraci 1) Registracija, 2) Pokretanje bloga, 3) Sadržaj bloga (Pages ili poruka) i 4) Hit „Publish” za svaki novi dodatak. Ako se dodaju stanice ili postovi, kreće se u razvijanje sajta i daje informacija posetiocima zbog kojih bi trebalo ponovo da se vrate i pogledaju dalji tok razvijanja sajta.

Sa sajtom wordpress.org je ista situacija. U osnovi je potrebna ista količina vremena da korisnik i veb-master dovedu sajt u stanje gde će biti spreman za postavljanje na internet, obezbeđivanjem domena, baze i ostalih potrebnih stvari.

Tradicionalni mali biznisi i njihova potreba za sajtom je održala HTML kodere na vrhu jer je njihovo znanje danas iole potrebno. U najboljem slučaju su to ljudi koji su koderi, dizajneri, koriste najnovije softvere i znanja, a u najgorem slučaju su to tako reći deca koja znaju nešto da sastave i to klijentu prodaju za neki manji iznos.

Sa **Wordpress-om** korisnik može svoje vreme, pažnju i budžet poveriti profesionalcima koji mogu da stvore Wordpress Theme koje su specijalno prilagođene potrebama korisnika. Back-end tehničke stvari već obrađuju stotine sjajnih programera i hiljade korisnika i testera.

3 Open Cart

OpenCart je, kako se može naslutiti, skripta za pokretanje on-lajn (e-shop) trgovine na internetu. Ni manje ni više, nego izuzetno lagana i pouzdana ako je potreban pouzdan portal na kome korisnik želi da ponudi proizvode i usluge. Moja korpa, najtraženije, popularno, preporuka, kao i lista želja, 2CheckOut, jesu samo neki od modula koje dobijate uz ovu skriptu. Naravno, pokretanje ovakve skripte nije tako jednostavno i zahteva poznavanje nekih osnovnih pravila kod instalacije i podešavanje PHP skripti i .config.php fajlova [9].

Upravo na ovakvoj skripti su podignuti mnogi sajtovi za prodaju. Svi rade lepo i zarađuju. Ipak, i pored ove lepe i lake strane, postoje i određeni problemi na koje ćemo obratiti pažnju.

Naime, nakon instalacije **OpenCart** skripte, dobijate svoj admin panel pomoću kojeg administrirate svoj sajt za prodaju. Ubacujete artikle, kreirate kategorije, uređujete cene, ubacujete slike artikala i opise itd. Imate mogućnost bekapa baze i vraćanja (restore) baze, što je dobro za one koji vole da stalno nešto eksperimentišu. E-shop poseduje i statistiku, registraciju korisnika, upravljanje članovima i još puno stvari. Takođe, zanimljiv je deo kod narudžbine gde se kupac koji dođe na sajt može odlučiti da artikal stavi u korpu i naruči za nekog drugog uz napomenu (čestitku), nešto kao poklon za rođendan i slično [9]. Definitivno, za većinu klijenata, pravi izbor je upravo Open Cart veb-prodavnica.

3.1 Problemi i njihovo rešavanje

Kad se pokrene OpenCart shop, sve radi lepo, dok radi. Međutim, javlja se i po koji problem koji može biti jako iritantan. Ovde ćemo navesti samo dva problema, a oba su vezana za promenu hostinga ili oštećenje skripte usled napada hakera.

Ukoliko korisnik promeni hosting na kome se nalazio E-Shop OpenCart, vrlo verovatno će morati ponovo da konfiguriše parametre u (config.php) fajlu koji se nalazi unutar skripte. Takođe, ovaj (config.php) fajl se nalazi i u admin folderu u kome se isto mora ponovo konfigurisati. Najčešće je potrebno samo promeniti putanju do skripte [9].

Open Cart, kao i sve ostale skripte koje dozvoljavaju upload slika na server, imaju svoje principe i zavisno od tehnologije koja ih pokreće, zahtevaju održavanje. Recimo, nakon napada hakera, jedna elektronska prodavnica je pretrpela neke promene u svojim php stranicama.

Međutim, nakon što se očiste sve stranice od malicioznog koda, ostao je nerešen problem koji se manifestuje kao poruka kad pristupimo prodavnici i ona izgleda ovako:

**Warning: imagejpeg() [function.imagejpeg]: Unable to open
'/home/mojisajt/domains/mojisajt.com/public_html/image/cache/data/rock/ rock D/Candy
Dulfer - Big girl-40x40.jpg' for writing: Permission denied in
/home/mojisajt/domains/mojisajt.com/public_html/system/library/image.php on line 43
Warning: fopen(/home/mojisajt/domains/mojisajt.com/public_html/system/logs/error.txt)
[function.fopen]: failed to open stream: Permission denied in
/home/mojisajt/domains/mojisajt.com/public_html/system/library/log.php on line 12**

Ukoliko korisnik dobija ovakvu poruku na OpenCart-u, vreme je da obrati pažnju na dozvole (permisije) za foldere u kojima se nalaze slike. Koristeći neki FTP menadžer, recimo Filezilla, za folder „image” postavite CHMOD sa 755 na 777. Permisije moraju da se odnose na sve foldere i podfoldere. Unutar foldera „image” nalazi se folder „cache” koji mora imati dozvole podešavanja na CHMOD 777. Ukoliko se u Filezilli izabere opcija da dozvole budu primenjene na sve foldere i podfoldere, „cache” ne morate odmah menjati, ali proverite za svaki slučaj desnim klikom na folder pa „allow”. Dalje, otvorite sada system/cache, za folder cache postavite takođe CHMOD 777. Dešava se da ove radnje ne pomognu u rešavanju gornje poruke o grešci. Iz greške vidimo da je negde problem u /image/cache/data/rock/ rock D/Candy Dulfer - Big girl-40x40.jpg' for writing što znači da ova slika ili nedostaje u folderu rock D ili je preimenovana. Rešićete ovo jednostavnim ubacivanjem slike Candy Dulfer - Big girl-40x40.jpg .

Ukoliko se javi problem sa podizanjem slika u okviru admin panela, najverovatnije nije dobro podešena dozvola foldera „images”. Kada se bude omogućilo da svi folderi u kojima se smeštaju slike budu čitljivi i otvoreni za upload (CHMOD 777), ovakvi problemi se neće pojavljivati.

4 Razlozi za Magento

Korisnik treba da koristi Magento ukoliko želi da vodi e-komerc (*e-commerce*) veb-sajt koji izgleda i radi upravo onako kako to želi [10]. Magento je tehnologija, nije templejt/šablon. Ovo su neke od njegovih karakteristika:

- Lak za korišćenje Administrativni Sistem
- Jednostrani Checkout
- Slanje pošiljki na više adresa
- Istovremeno upravljanje sa više veb-sajtova
- SEO se obavlja automatski
- Premeštanje podataka preko DataFlow

4.1 Struktura Magento aplikacije

Magento je e-commerce CMS platforma zasnovana na php-u i Zend Frameworku. Uz pomoć njega, korisnici su u mogućnosti da u potpunosti upravljaju svojom on-lajn prodavnicom, prikažu određene proizvode, omoguće kupcima različite metode plaćanja i isporuke, kao i mnoge druge opcije [10].

Dolazi u tri verzije:

- Besplatna osnovna „community” verzija,
- „Enterprise” verzija koja se plaća i pruža dodatne funkcionalnosti kao i tehničku podršku,
- „Go” koji je on-lajn verzija za mala preduzeća i funkcioniše kao servis za čije se korišćenje plaća mesečna pretplata.

Magento je trenutno vodeća open source ecommerce platforma – preko 125 000 sajtova napravljenih uz pomoć Magenta i 386 zvaničnih partner firmi koje se bave Magento razvojem. Takođe, treba napomenuti da postoji program sertifikacije Magento programera kao i veoma snažna zajednica na internetu, okupljena na blogovima i forumima.

Nastao je tako što se 2007. godine okupio tim programera koji je radio na jednom drugom eCommerce rešenju – osCommerce. Rešili su da ga modifikuju, ali su se u toku razvoja odlučili da naprave svoj proizvod. U 2011. godini eBay je u potpunosti kupio Magento, čime je on postao deo eBay x Commerce platforme.

Kao CMS prilagođen potrebama e-Commerce rešenja, Magento podrazumeva administratorski i frontend deo, po ugledu na vodeća CMS rešenja.

4.2 Struktura

Za organizaciju fajlova koristi se princip modularnosti. Čitav kod aplikacije je podeljen u 3 tzv. code pool-a u kojima se nalaze moduli sa fajlovima:

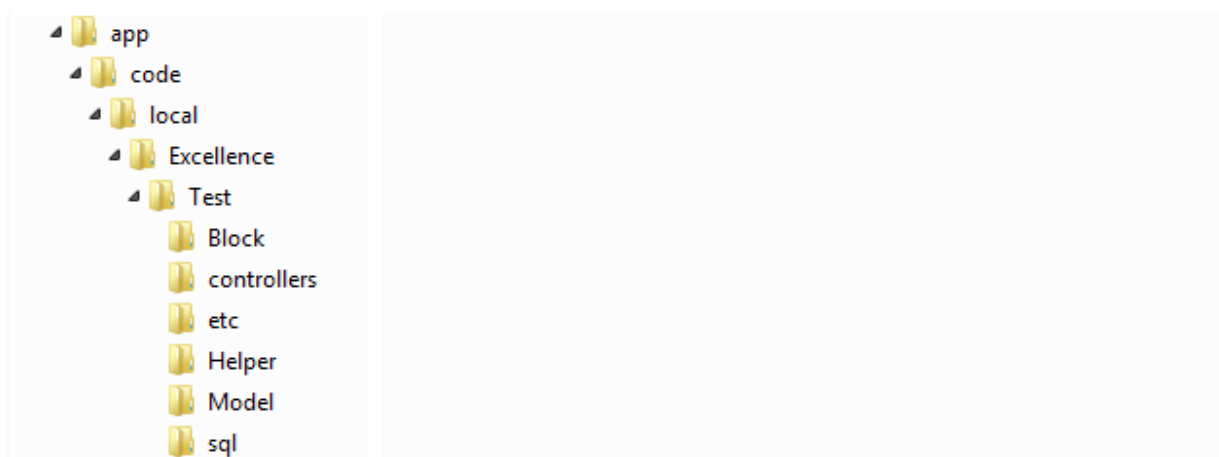
- „core”: sastoji se od fajlova napravljenih od strane Magento razvojnog tima,
- „community”: sadrži module koji su zvanične ekstenzije sa Magento marketa,
- „local”: sadrži module vezane direktno za projekat.

Podrazumevane Magento funkcionalnosti koje su opisane u core code pool-u mogu se promeniti preko modula iz „community” i „local” code pool-a. Ovakav pristup pruža velike mogućnosti za prilagođavanje i nadogradnju osnovnih funkcionalnosti kao i za prilagođavanje osnovne aplikacije konkretnim zahtevima.

Svaki modul sadrži folder „etc” u kojem se nalazi konfiguracija u xml formatu. Fajl „config.xml” definiše sva potrebna podešavanja za funkcionisanje modula. On sadrži informacije o elementima modula kao što su:

- Block
- Helper
- Controllers
- Model
- Sql

Struktura foldera jednog modula izgleda ovako:



Svi moduli se nalaze u folderu „code”, a postoje još neke celine kao što su „template” i „layout” koje se nalaze u folderu „design”.

- ▼ 📁 app
 - ▶ 📁 code
 - ▼ 📁 design
 - ▼ 📁 adminhtml
 - ▼ 📁 default
 - ▶ 📁 default
 - ▼ 📁 frontend
 - ▼ 📁 base
 - ▶ 📁 default
 - ▼ 📁 default
 - ▶ 📁 blank
 - ▶ 📁 default
 - ▶ 📁 iphone
 - ▶ 📁 modern
 - ▼ 📁 install
 - ▼ 📁 default
 - ▶ 📁 default

5 CMS bezbednost i operacije

Kao vlasnik preduzeća, korisnik se može suočiti sa problemom trošenja novca za stvari koje zahteva informaciona tehnologija (IT) i osoblje. Šta bi zahtev za više novca mogao da uraditi za povećanje prodaje? Zašto bi bila potrebna pisana prava?

IT osoba u toj situaciji ne može da razume pritiske sa kojima se suočavaju ljudi iz višeg rukovodstva, posebno ako nije do detalja sve precizirano. Ako korisnik nosi istovremeno obe kape, može balansirati ciljevima vođenja preduzeća, što prodaje, što sređivanja knjiga. Razmišljanje o sajtu i bezbednosti će verovatno biti nisko na listi prioriteta.

U svakom slučaju, moraju se jasno razumeti ciljevi poslovanja. Konkretno, ako postoji neki od open source sistema za upravljanje sadržajem (CMS), kao što su Joomla, Drupal, WordPress, ili! Plon, korisnik može misliti da niske cene ovih sistema znače da ih može dobiti a da pri tome nije neophodno dodatno vreme iskustvo i troškovi, da bi odobrili zahtev osobi iz IT-a[1].

5.1 Meta

Današnji sajt nije samo obična stanica na internetu. To je meta za hakere. Upotreba servera i sajta može da posluži kao početna tačka za napade na druge sajtove. Kompromitovani sajtovi mogu da se koriste za phishing prevare gde su kuće u blizini ogledala – kopije bankarskih sajtova. Oni mogu koristiti zlonamerne programe koji će se naći na računarima korisnika.

Sadašnji medijski izveštaj navodi zauzimanje jednog dela Zevsa bande. Ovaj poznati kriminalni elemenat je uspešno okupio nekoliko stotina hiljada mašina. Ovi „zombiji” (kako ih zovu) su u potpunosti pod kontrolom kriminalca Zevsa. Između ostalog, njihov cilj je krađa novca. I oni su bili veoma uspešni u svom poslu.

Drugo veliko ime izrade prethodnih naslova vesti je poznat kao crv Stuknet. Ovaj visoko sofisticirani crv je našao svoj put u električne sisteme u mnogim zemljama. Prema nekim izveštajima, on je pronađen u Iranu, Kini i SAD. Stuknet je veoma napredan crv (ili virus) i pokazao se kao veoma opasan.

Izazov je to što mnogi sistemi na internetu imaju slabosti i ranjivosti. Ove slabosti često su rezultat podrazumevane lozinke ili slabih lozinki koje čuvaju vrata obezbeđena za ulazak ka sajtovima.

Pored banaka i komunalnih preduzeća, mala i srednja preduzeća i vlasnik sajta je u velikoj opasnosti. Kao jedan od tih vlasnika, korisnik ima pune ruke posla sa sve većim upravljanjem poslovanja. Čuvanje sajta i podataka korisnika nije samo važno. Postoji moralni imperativ da se uradi sve što se može da bi se sprečio gubitak podataka. Gubitak podataka može

nastati zbog lošeg upravljanja poslom, kao na primer kada dođe do oštećenja hard diska ili može doći kroz sajber napada[1].

5.2 Operativna razmatranja

Rad sajta će se u velikoj meri razlikovati u zavisnosti od toga koji model ili tip CMS-a se koristi. Ako je u pitanju manji Wordpress sajt koji ima malo prometa i pad nije mnogo važan, onda, operativno, nema potrebe za brigom. Međutim, ako se radi o velikom Joomla! ili Drupal sajtu koji podržava aktivne i profitabilne baze klijenata, stvari se komplikuju.

Operacije za takav sajt će se sastojati od mnogo stvari, uključujući sledeće:

Disaster Recoveri i Business Continuity Plan – Ovaj postupak predstavlja i plan kako reagovati na različite vrste problema koji mogu zadesiti sajt ili operacije. Ova katastrofa i kontinuitet poslovanja plana treba da sadrži sve elemente potrebne za uspešnu obnovu i oporavak veb-poslovanja i on-lajn sistema[2].

Backup i of-sajt skladištenje podataka – Izrada rezervne kopije je veoma važna. Kada napravite rezervnu kopiju, sledeći korak je da se zaista iskopiraju podaci na lokalnom disku ili medijima kao što su CD-ROM, DVD ili USB disk. Druge vrste operacija mogu zahtevati rezervne trake. U svakom slučaju, sačuvati kopiju podataka sa servera na lokalnoj mašini je veoma važno.

Krpljenje – To je termin koji se koristi u tehnologiji, prostoru primene ažuriranja softvera. Primena zakrpa u malim organizacijama se obično vrši periodično, a zavisi od postavke. Srednja preduzeća će morati da upravljaju procesom krpljenja češće, jer jednostavno neće moći više da održe korak sa ostalima[2].

Uspostavljanje i razvoj test platforme će gotovo uvek biti potreban za razvojnu platformu sajta. „Test i dev” okruženje se koristi za testiranje zakrpe, treba probati novu šifru i dizajn novog sajta, koji bi se mogao iskoristiti kao ogledalo kopije u hitnim slučajevima.

Log kritike – Normalno, sav saobraćaj i aktivnost na sajtu i serveru su zabeleženi u posebnom dosijeu pod nazivom „log fajl”. Redovne administrativne aktivnosti treba da sadrže pregled raznih log fajlova. Ovaj zadatak nije zabavan i često se ignoriše. Ipak, dosledan i detaljan pregled neće dati nikakve znake upozorenja u vezi sa narednim napadima. Pitanja u vezi sa sajtom kao što su propusni opseg potrošnje, niskog prostora na disku, i svim drugim događajima koje treba da privuku pažnju, mogu se brzo rešavati[2].

Preduzimanje akcije na log-podacima – Pronalaženje sporne stavke u log fajlu je dovoljan razlog da se preduzmu dalji koraci u pregledu operacija. To ne znači da neki decino-Scripter u kafani negde u svetu pokušava da se probije bez oglašavanja alarma. To ne znači da jednostavno blok IP adresa nije neophodna ako postane smetnja. Drugi primer je ako se vidi

(preko svojih logova) neovlašćeni pristup FTP sajtu, što ukazuje da korisnik ima šansu da napravi kompromis. Akcije u evidencijama će diktirati i garantovati odgovarajuće radnje.

5.3 Edukacija zaposlenih i krajnjih korisnika

Ako je posao veoma mali, svest o sigurnosti i obuka neće biti tako teški kao što će biti za veći posao. Samo se treba truditi da imate dobru sajber bezbednost, i trebalo bi da bude sve u redu. Ako je posao većeg do srednjeg obima, onda treba da se sprovede program za obuku i da zaposleni budu svesni sajber bezbednosti.

Politika zaštite informacija – Dobar početak je dobro razvijena IT bezbednosna politika koja odražava biznis potrebe i meri rizike poslovanja. Na primer, pretpostavimo da korisnik koristi za razmenu trenutnih poruka (IM) program za komunikaciju sa klijentima. Ako ta IM aplikacija može da prihvati ili pošalje datoteke, rizik je da se nešto može dozvoliti unutar ili nešto poput poverljivih dokumenata može izbaciti.

Učinite da IT bezbednost bude svačija briga – Treba proveriti da li osoblje shvata da je lična sigurnost IT-ja njihova odgovornost. Takođe, treba obezbediti da zaposleni shvate politiku i proceduru i koja je uloga menadžmenta. Često, stvari kao što su etičke obuke ili IT bezbednost se posmatraju sa pasivnim prezirom od strane zaposlenih. Međutim, svest o IT bezbednosti je nešto što mora svaki poslodavac da shvati ozbiljno i da obezbedi da osoblje radi dobro. Sprovođenje disciplinskih postupaka zbog nepoštovanja je jedan metod obezbeđivanje poštovanja.

Nadgledanje – Treba uspostaviti proces za praćenje i pregled informacija bezbednosne politike. Niko ne treba da se izuzme iz treninga svesti o bezbednosti. To znači da bi trebalo da postanu deo korporativne kulture, počev od vrha. Menadžment u bilo kojoj organizaciji daje ton. Dakle, menadžeri treba da pokažu pravilno ponašanje u IT bezbednosti.

5.4 Podizanje svesti o bezbednosti

Prema www.dictionary.com, biti svestan je imati znanje. To takođe može da znači da treba biti informisan, oprezan i obrazovan. Svest potencijalnih bezbednosnih rizika je od vitalnog značaja za uspeh bilo kog veb-orijentisanog poslovanja. To podrazumeva da programi treba da budu dizajnirani da podignu nivo svesti o pretnji i opasnosti od sajber-napada na zaposlene i poslovne partnere.

Obrazovni naponi su konkretniji u prirodi od pukih kampanjama koje promovišu svest zaposlenih. Gde se svest bavi potencijalnim pretnjama, obrazovanje treba da sadrži elemente koji daju zaposlenima sredstva za podršku bezbednosti. Sledećim koracima pogledaćemo nekoliko dokazanih načina za edukaciju zaposlenih o bezbednosti.

5.5 Obuka o politikama, Bezbednost informacija

Obukom svojih zaposlenih o politikama bezbednosti informacija poslodavac daje do znanja šta može i šta ne može da se uradi.

Ova obuka je prilika da se otvoreno diskutuje o on-lajn sigurnosti i kako se to odnosi ka konkretnoj poslovnoj politici (pravima). Tada treba razgovarati o sankcijama za kršenje politike.

5.6 Pružanje standardnih protokola za izveštavanje o pretnjama

U današnje vreme, terorizam može da se pojavi u mnogim oblicima. Sajber-terorizam je verovatno u povoju, ali neće tako ostati još dugo. Zbog „nacije bez državljanstva” i prirode interneta, napad ili pretnja ne moraju da potiču iz mesta odakle se prvo misli da potiču.

Osoblje treba da bude svesno da treba da prijave događaje kao što su virusi koji se nalaze na njihovim računarima. Oni moraju da znaju šta je dokumentovan proces. Tu bi trebalo da bude dokumentovan proces za izgubljenim ili ukradenim računarima koji obuhvata promene lozinke, identifikacije podataka koji su ukradeni, kao i potencijalne opasnosti po kompaniju. Na primer, mnoge veće kompanije imaju procedure za rešavanje katastrofa za vreme požara, poplave, pa čak i za izveštavanje pretnje bombom.

Razmislite o uspostavljanju sličanog proces izveštavanja za sajber pretnje.

5.7 Obezbeđivanje sigurnosti mejla

Do sada, imejl je jedno od najistaknutijih mesta koje predstavlja pretnju po infrastrukturu. U stvari, više od 80 odsto mejlova koji protiču preko interneta danas predstavljaju spam. Veći deo tog spama ima potencijal da napravi štetu.

Spam mejl izgleda veoma važno i zvanično. On upućuje primaoca na link koji onda prikuplja sve njihove informacije, posebno preko procesa plaćanja. Naravno, to je prevara koju koriste hakeri da ukradu lične podatke.

Neverovatno, mnogi ljudi i dalje podležu ovakvom obliku prevare. Poslodavac mora naučiti svoje zaposlene o tome kako da identifikuju vezu u mejlu (na primer, da se desnim tasterom miša kopira URL lokacija i nalepi u uređivaču teksta, kao što je Notepad). Većinu

vremena, zlonamerni mejlovi rade jednu stvar i potpuno preusmeravaju pretraživač na drugu lokaciju (sajt).

5.8 Primena zakrpa i updejta

Ako su zaposleni odgovorni za bilo kakav oblik apdejta, treba obezbediti da oni samo prate uputstva koja su im data ili osigurati da su u stanju da identifikuju odakle apdejtovi dolaze. Obezbedite zaposlenima pouzdan intranet ili verifikaciju programa koji će im omogućiti da primene odgovarajuće zakrpe.

U suštini, program obrazovanja o ovoj temi treba da ojača sve dečje naučene lekcije, npr. „Ne pričaj sa strancem ili ne ulazi u njegova kola!”, „Ne uzimaj slatkiše od stranaca” i tako dalje[2].

5.9 Biti svestan i ostati siguran

Kako program sazreva, treba razviti program za ažuriranje i edukaciju o savremenim pretnjama. Pretnje se menjaju veoma često, a ono što postoji danas, možda neće i sutra. Pretnje imaju tendenciju da prate složenu tehnologiju i nivo rasta.

Zaposleni bi trebalo da prolaze kroz obuku o bezbednosti veoma često [3].

Napomena

Za dobar plan o obuci, pogledajte „Izgradnja informacione tehnologije svesti o bezbednosti i program obuke”, napisao Mark Vilson i Džoan Haš, i proizveden od strane Nacionalnog instituta za standarde i tehnologiju. Možete ga naći u <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>.

6 Gledajući sajt „Kroz oči hakera”

U knjizi The Art of War (New York: Oxford University Press, 1971), Sun Cu piše o planiranju vojnog napada:

„General koji dobije bitku čini mnoge kalkulacije u svom zamku pre nego što se bitka odigra. General koji gubi bitku čini kalkulacije pred samu bitku. Tako da mnoge kalkulacije

dovode do pobeđe, a nekoliko kalkulacija i do poraza. Ovakav način razmišljanja odlučuje ko će pobediti ili izgubiti.”

U suštini, kaže se da što više vojni planer zna o potencijalnoj situaciji, a planirao je pre bitke, to je veća verovatnoća da će pobediti.

Hakovanje veb-sajta ili nelegalno dobijanje pristupa računarskom sistemu planiranja zahteva isti napor. Jači cilj, više planiranja je potrebno, a što je cilj je slabiji, manje napora je potrebno.

Ako sajt nije zaštićen, onda će kiddie-Scripters dobiti i zadržati pristup sajtu sve dok ne bude uklonjen. Međutim, dobro obezbeđen sajt je odličan za odvrćanje prosečnog hakera.

Ako žele ući, i dobri hakeri će imati većih problema da to urade ako je sajt osiguran. Praćenjem umeća ratovanja, što više haker zna pre nego što pokušava da se probije na određeni sajt, veća je njegova šansa za uspehom. Obrnuto, što korisnik više zna o svojoj bezbednosti i sajtu, bolje će šanse imati da se odbranit od hakera.

Odlični hakeri su vrsta za koje nikad nećete znati da su uopšte bili tu. Oni su digitalni ekvivalent magle. Oni mogu da uđu, dobiju ono što im je potrebno, a ne ostavljaju tragove. Prodor ka sajtu znači da prvo moraju da prikupljaju obaveštajne podatke o tom sajtu. Poznavajući odbranu koja je na snazi, slabosti koje postoje, gde su sistemi za praćenje i koji mogu biti, olakšano im je planiranje[4].

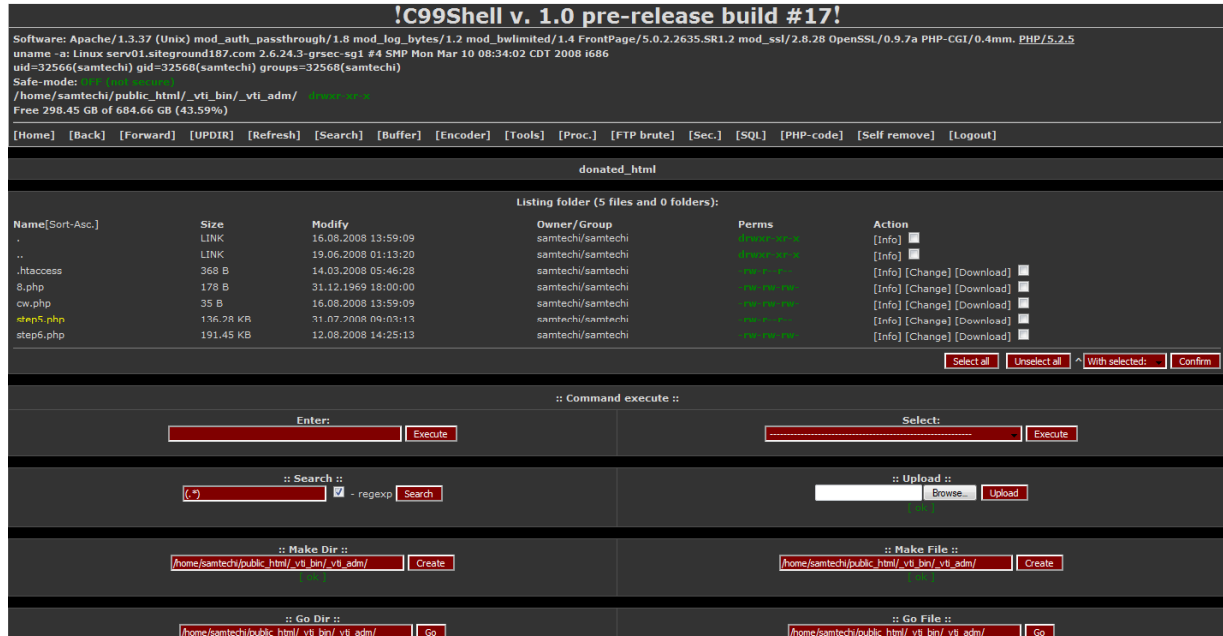
Početak prikupljanja podataka je često pasivna aktivnost. Pasivni koraci mogu da otkriju mnogo informacija o samom upadu u sistem.

Mapiranje elemenata mreže, zaštitni zid, CMS i aplikacija su deo faze spremanja pre napada. Hakeri pronalaze slabost u prethodnoj fazi i onda mogu prodreti kroz odbranu i osiguravaju svoj pristup dodavanjem backdoor-ova i brišući tragove.

U podzemnom svetu interneta, hakeri su poznati kao blackhats. Njihove alatke su moćne i opasne, a njihove veštine su skoro bez premca[4].

Zanimljivo je dobro napisan i opasan program C99 Shell. Pisan u PHP-u, ovaj „blackhat” hakerski alat daje veliku kontrolu nad serverskim okruženjem. Nakon što je ušao na server, haker može da kontroliše datoteke, da promeni dozvole, otvori portove, prisluškuje, prati slanje e-pošte, otpremanje podataka, dodajte IRC aplikaciju, ili jednostavno isključi i obriše sajt. Slika 1.1 pokazuje delimičnu sliku C99.php programa kontrole. Ova veoma moćna aplikacija se lako može koristiti za obavljanje neodređenog broja zlonamernih napada na sajtu[4].

Slika 1.1 Delimična pogled C99 Shell



Najbolje sredstvo odbrane je da se sajt posmatra kroz oči neprijatelja. Ono što korisnik vidi i hakeri će videti.

6.1 Koraci ka dobijanju pristupa sajtu

Dalje je opisano nekoliko osnovnih koraka koje haker može da prati i da stekne potrebna znanja za napad na sajt.

6.2 Istraživanje

Napadači prvo žele da znaju sve o sajtu koji su odabrali kao metu, na kom je serveru, koji operativni sistem koristi, koje aplikacije rade u određenim verzijama i tako dalje. Znanje o odbrambenim sistemima za detekciju upada takođe će pomoći hakerima u izbegavanju i da budu uhvaćeni. Nakon što su sve to odradili, oni mogu da počnu rad na istraživanju ranjivosti.

Na primer, ako se koristi osetljivi softver, oni će ciljati upravo taj softver da bi ušli.

Napad poznat kao „SQL injection” bi koristio dobro izrađenu SQL naredbu koja bi mogla otkriti administratorovo korisničko ime i lozinku, dajući napadaču administrativni pristup sajtu.

Kao primer istraživanja, trebalo bi imati sajt sa dobrim hostingom i pokrenuti neku vrstu CMS sajta na Linuks serveru.

Napadač prvo proverava na kom serveru se nalazi određeni sajt. To se može uraditi pasivno ili aktivno na više načina, uključujući i sledeće:

Pogledati izvornu stranicu pomoću pregledača na sajtu. To će pomoći da saznate koji je njen sistem – da li je u pitanju Joomla, WordPress, Drupal, ili Plon (ili bilo koji drugi veb-sistem)...

Dalje treba pokrenuti skener alat „Blind Elephant” na sajtu, da bi se odredila vrsta i verzija CMS-a.

Pokušati da se dobije pristup administratorskom delu CMS.

Pitate se kako je neki sajt napravljen i zato želite da imate tako lep sajt! Ovo je primer socijalnog inženjeringa.

Koristi se Google pretraga kao što je „allinurl Pokreće Joomla!”.

Mnogi CMS-ovi će pokazati Favicon sa svojim logom. To čini identifikaciju veoma jednostavnom.

Možete videti da je broj metoda o saznanju koji je sajt u pitanju veliki.

Dalje, napadači bi želeli da nauče o firmi čiji sajt će napasti, čime se bavi i gde se nalazi, da bi u suštini izgradili profil o meti. Za ovaj zadatak, napadač može da koristi sledeće alatke:

Google – Ovaj alat može reći napadaču dosta o kompaniji, jer Google pretraga može da se prikaže saopštenja, vesti i druge informacije.

Sistem imena domena (DNS) – napadač bi mogao da preispita DNS zapise da vidi ko je tehnički kontakt, brojeve telefona (u nekim slučajevima), fizičku adresu. Napadač takođe može koristiti alatke kao što su nslookup, da se upoznaju sa DNS informacijama sajta koje hoće da napadne.

Fizička lokacija – Ako postoji fizički objekat, napadači mogu da kopaju u kanti za đubre za Tossed-out znanja. Ovo može uključivati i listu kupaca, internih informatora, „Media” (kao što je CD) i još mnogo toga. Ako napadač želi da dobije pristup operacijama, on se može predstavljati kao insajder preko telefona.

Imajući pristup svim ovim i drugim sitnicama informacijama, kao što su imena zaposlenih, proizvodi koji se prave ili prodaju, i još mnogo toga, može da omogući napadaču da prevari nekoga.

6.3 Guglovanje

Google je odličan alat za svakodnevnu upotrebu za pronalaženje potrebnih informacija. To je jednako dobro za izgradnju profila o potencijalnim metama. Hajde da radimo na tome i da vidimo šta može da se otkrije.

Pretpostavimo da je haker odlučio da provali na sajt korisnika. Prvo, napadač mora da prikupi neke informacije o meti. Šta bi Google rekao hakeru?

Adresa zgrade – Ovo je odličan način da se uradi neko lov-level izviđanje zaposlenih, okolina, straža, i još mnogo toga. Posvećen napadač može iskoristiti ovu priliku za prikupljanje nekih važnih informacija, što znači da haker ispituje spoljašnji objekat za bežične pristupne tačke.

Službenici ili menadžeri kompanija ovih zaposlenih su omiljena meta socijalnih inženjera. Kroz ove radnike, napadač može da nauči sve o gornjoj upravi. Zauzvrat, hakeri mogu da koriste ove informacije da prevare druge zaposlene na jedan bezazlen način.

Pozicije za zapošljavanje – Kroz oglas za posao, napadač može da nauči mnogo o infrastrukturi, mestu, jeziku, hardveru, sistemu i serverima u upotrebi. Najbolji pravac delovanja je da se što manje informacija oda u samom oglasu a da on pritom privuče prave talente. Treba proveriti da li su telefonski razgovori pažljivo rukovani tako da ne otkrivaju unutrašnje delovanje kancelarije i IT-a[5].

Potencijalno postavljanje lozinke na podršci bloga – Iako ova tačka može izgledati očigledno, iznenađuje koliko često se lozinke otkriju na taj način. Ono što je još šokantnije je da, ako znate kako da koristite Google, možete povremeno naći liste lozinki u upotrebi. Naravno, najbolje je privremeno sredstvo koje neće objavljivati ili davati lozinke i korisnički ID. Sledeća najbolja odbrana je da se pokrene politika koja zahteva promene lozinke na redovnoj osnovi i češće. Ovo obezbeđuje da ukoliko lozinka pobegne u divljinu, da će se to uskoro promeniti[5].

Oglasi za zapošljavanje za firme su posebno ranjiva zona. Na primer, pretpostavimo da haker želi da nauči više o fiktivnoj firma koja se zove Centar velikog znanja. Pretraga oglasne table može sadržati sledeće:

Centar velikog znanja, neprofitni izdavača, traži Drupal

Programera da radi u svom sedištu u Čikagu, Ill

Veb Developer će pomoći da vodi razvija sajtove na Drupal platformi. Održavanje postojećih sajtova na drugim platformama, kao što su Oracle, će takođe biti potrebni. Ovo pozicija izveštava CIO kompanije.

Potrebne kvalifikacije:

- * Minimum 2 godine iskustva u razvoju Drupal-a.
- * Jaka PHP znanja.
- * KHTML, CSS i Web Standards iskustvo i znanje
- * Pokazala sposobnost da proizvede kod

Napadač bi mogao da podnese lažnu biografiju ovoj firmi i imao bi priliku za razgovor za posao telefonom sa poslodavcem. Napadač može čak da ide na intervju za posao lično.

Ova informacija će omogućiti napadaču da na lak način locira slabosti koje postoje u Drupal sajtovima. Do sada, ništa što je urađeno nije protivzakonito. To je jednostavno čin prikupljanja obaveštajnih podataka.

6.4 Korišćenje Google Hacking Tools (Dorks)

Pre nekoliko godina, bezbednosni istraživač Džoni Long je postavio on-lajn bazu podataka cut-and-paste Google pretrage da otkrije do tada nepoznate informacije. Prema njegovom sajtu, „Hakeri u dobrotvorne svrhe” (www.hackersforcharity.org/ghdb/), ove pretrage se zovu „googledorks” ili „kreteni” kratko značenje „nesposobnost ili glupost ljudi kao što je otkriveno od strane Google-a”.

Mnogi od ovih pretraživanja mogu da otkriju podatke kao što su lozinke. Iako je namera bila da se verovatno neće dozvoliti da takve liste lutaju otvorenim internetom, zabrinjava činjenica je da su one tu. Dorkovi na sajtu su veoma zastareli, ali, iznenađujuće, mnogi još uvek daju rezultate. Drugi sajtovi i dorkovi su sada nikli.

Budite oprezni u vezi sa ovom vrstom pretraživanja. Možda ćete naći neprijatan ili uvredljiv sadržaj.

Treba vremena za pregledanje dorkove i proveru da li će se sajt pojaviti tu kako bi se osiguralo da se ne otkrivaju osetljive informacije[5].

6.5 Footprinting

Nakon što je haker okupio mnoštvo detalja i razvio profil sajta, on će se premestiti na footprinting fazu. Ovo je faza u kojoj napadač pokušava da razvije kartu sajta, server i mrežu.

Kao što je pomenuto ranije, fiktivna kompanija, Centar za svo znanje, radi u Drupal sajtu ili sajtovima. Mapiranje kompanije Drupal modula i verzija je prvi korak u footprintingu.

Identifikovati CMS je prilično lako, a danas je nekoliko alata na raspolaganju za pomaganje napadaču da odredi CMS sajta.

Blind Elephant (pomenuto) iz Qualsys čini ovu vrstu rada veoma lakom. Ovaj Python-baziran alat je poznat kao fingerprinter veb-aplikacija. Slepí slon pokušava da otkrije verziju (poznatu) veb-aplikacija kao što su CMS-ovi. Kroz poređenja statičkih datoteka koje postoje na poznatim lokacijama, i da na osnovu tih informacija dođe do informaciji o CMS-u[5].

Ova alatka otkriva verzije sledeće:

Drupal

Joomla!

Liferay

MediaWiki

Moodle

MovableType

Joshua

phpBB

phpMiAdmin

PHPnuke

SPiP

WordPress

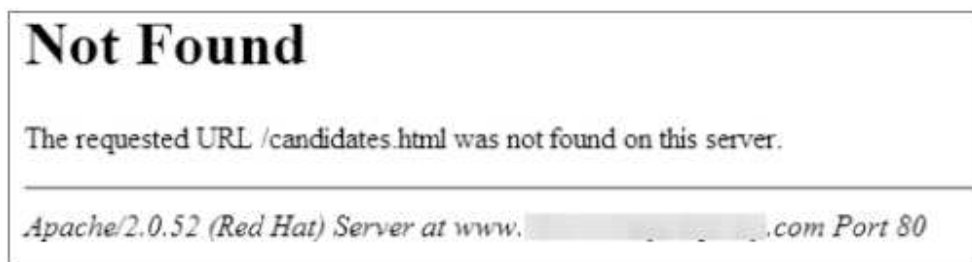
Pored toga, ona otkriva više od deset dodatka za Drupal i dvadesetak za Wordpress. Očigledna implikacija dovodi do lake identifikacije CMS-a.

Dalje, hakeru je potreban veb-server verzija. S obzirom na to da je Apache uveliko najpopularniji veb-server današnjice, verovatno postoji šansa da se sajt vodi pod Apache. Međutim, napadač mora da potvrdi da li je to slučaj i da identifikuje verziju.

Jedan brzi način da to uradite je da pošaljete na veb-server zahtev za lažne stranice. Napadač bi mogao da ukuca nepostojeću veb-stranicu na sajtu da vidi šta je greška rezultata. Na primer, pretpostavimo da je, na pretraživaču, napadač je ušao u sledeće za politički sajt:

<http://www.domen.com/candidates.html>.

Tada izlazi sledeća poruka 1.2.



Slika 1.2 prikazuje Greška veb-verziju servera

Sa stanovišta veb-servera , takav zahtev nije velika stvar, a to je svakako validan zahtev. Pretraživač je tražio Candidates.html stranu, i zato što ne postoji, server ne može da proizvede stranicu. To je podrazumevana greška koja nije pronašla druge informacije.

Obratite pažnju da haker nije bio usmeren na stranu „404“, stranica nudi i druge podatke, na primer, druge strane mogu da sadrže korisne informacije kao što su linkovi na sajtu.

Razlog je poruka o grešci koja pokazuje verziju Apache veb-sajta. U tom slučaju, ovaj sajt je pokrenut Apache/2.0.52 (Red Hat).

Pretraživanjem Apache 2.0 grane (trenutno do 2.0.63) changelog napadač sada može videti da su 19 bezbednosne zakrpe između ove verzije sajta i trenutno aktuelne verziji. To je 19 metoda koje može haker da koristiti za upad na sajt, koji obuhvata sledeće:

Four Cross Site Scripting (XSS) vulnerabilities

Two buffer-related issues (potential buffer overflow)

Two Secure Socket Layer (SSL) vulnerabilities

Three specific memory-related errors

Various other security fixes

Kao što se može videti, brza pretraga izmena je sve što je bilo potrebno da se otkrije ova informacija.

Napadačima su takođe na raspolaganju dijagnostički alati operativnih sistema. Nekoliko postoji, a sledeći imaju tendenciju da budu univerzalni:

AngriIP – Ovo je jednostavan IP skener alata. Možete saznati više na www.angriip.org.

DIG (Linuk) – Ova alatka pomaže oko upita na DNS zapise. Može se saznati više na www.linuk.com/archive/feature/113992.

hPING-hPING su komandne linije orijentisane na TCP / IP paket monter / analizator
Više na www.hping.org.

NMAP – To je alat za mapiranje mreže. Možete saznati više na www.insecure.org.

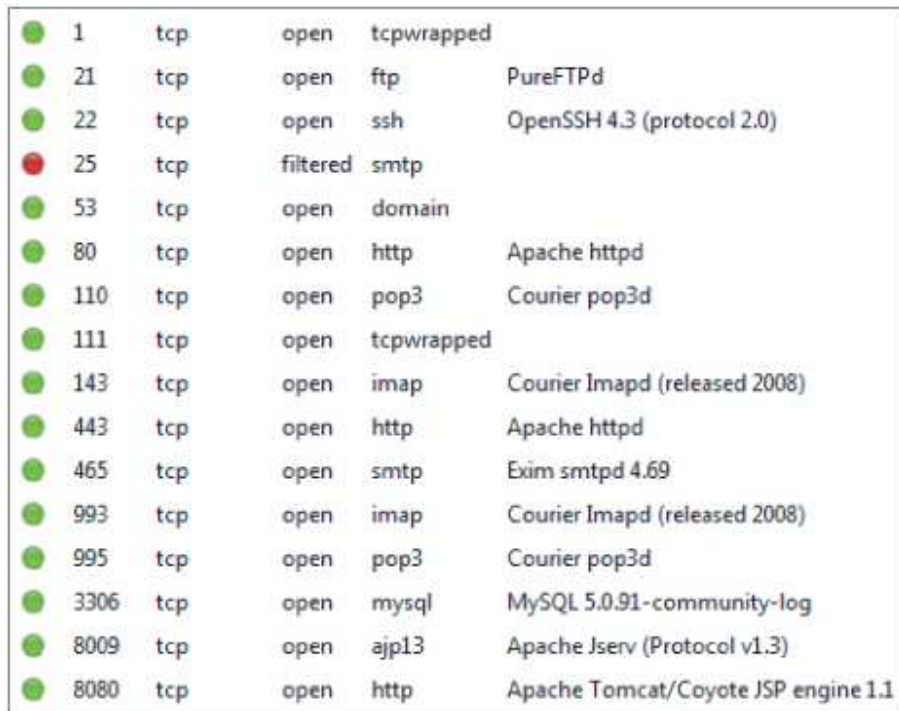
Nslookup (windows, Linuks) – Ovo je još jedan u vezi sa DNS-alatom. Možete saznati više na www.kloth.net/services/nslookup.php.

Traceroute (ili Tracert) – Ovaj alat omogućava da pratite broj hopova do odredišta. Korišćenje ovog alata može da omogući mapiranje mreže. Ovaj alat je ugrađen u operativnim sistemima današnjice. Windows korisnici mogu da ga koriste pomoću Start ⇒ ⇒ Run CMD opcije.

Nekoliko alata za skeniranje ranjivosti su takođe dostupni, kao što su Nessus iz Tennable (www.nessus.org/nessus/).

6.5 Korišćenje Nmap-a u loše svrhe

Pogledajte korišćenja nmap alata. Pretpostavimo rezultate skeniranog sajta prikazanog na slici 1.3



1	tcp	open	tcpwrapped	
21	tcp	open	ftp	PureFTPd
22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
25	tcp	filtered	smtp	
53	tcp	open	domain	
80	tcp	open	http	Apache httpd
110	tcp	open	pop3	Courier pop3d
111	tcp	open	tcpwrapped	
143	tcp	open	imap	Courier Imapd (released 2008)
443	tcp	open	http	Apache httpd
465	tcp	open	smtp	Exim smtpd 4.69
993	tcp	open	imap	Courier Imapd (released 2008)
995	tcp	open	pop3	Courier pop3d
3306	tcp	open	mysql	MySQL 5.0.91-community-log
8009	tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8080	tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Slika 1.3 portovi na serveru nađeni pomoću Nmap-a

Ova informacija je dragocena napadaču. Naravno, vrednost će varirati na šta hacker nalazi i šta može biti planirani napad. U najmanju ruku, napadač zna sledeće iz ovog pregleda na serveru:

Apache web server

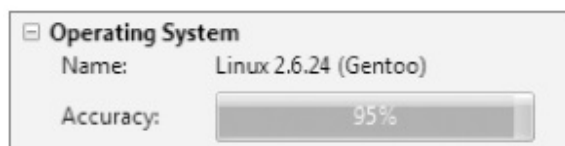
MySQL (verzija 5.0.91)

Apache Tomcat i Jserv

FTP i SSH, Razni mail serveri

Otvoreni port 53, što može biti problem ako je to DNS iako je omogućen transfer.

Kao što je prikazano na slici 1.4, NMAP je identifikovao ovaj server kao da imaju 95 odsto šanse da bude Linux 2.6.24, Gentoo distribucije. Kao što je prikazano na slici 1.5, alat otkrio nekoliko novih uređaja[6].



Slika 1.4 O / S identifikacija koristi Nmap

OS Class					
Type	Vendor	OS Family	OS Generation	Accuracy	
general purpose	Linux	Linux	2.6.X	95%	
firewall	IPCop	Linux	2.4.X	95%	
WAP	Linux	Linux	2.4.X	93%	
WAP	Linksys	Linux	2.4.X	91%	
WAP	Linux	Linux	2.6.X	90%	
broadband router	Linux	Linux	2.6.X	90%	
telecom-misc	Avaya	Linux	2.6.X	88%	
firewall	Check Point	Linux	2.4.X	88%	
WAP	AVM	embedded		88%	
general purpose	Linksys	Linux	2.4.X	88%	
specialized	Linux	Linux	2.4.X	88%	
proxy server	Riverbed	embedded		88%	
storage-misc	D-Link	embedded		87%	
WAP	Linksys	embedded		87%	
remote management	Dell	embedded		87%	
switch	HP	embedded		87%	

Slika 1.5 Uređaji otkrivene Nmap na IP adresi

Kao što možete da vidite, napadač može reći mnogo o ovom okruženju, uključujući i verovatnoće Voice over IP (VoIP) telefonskog sistema koji Avaya (88 odsto šanse), verovatnoća Linksys Wireless Access Point (više od 90 odsto verovatnoća), i uključivanje Dell i Hewlett-Packard prekidača. Sve u svemu, to ne bi bilo loše plen informacija[6].

6.6 Korišćenje traceroute

Jedan zajednički alat koji se koristi u fazi otisak, zove se traceroute (na Vindovs mašinama, to se zove tracert). Internet stranica može da odredi putanju od izvora (kao, na primer) do odredišta u sistemu. Sa traceroute, napadač može da dobije dovoljno informacija da sastavi pristojan dijagram mreže. (Međutim, ovaj rezultat bi potrebno nekoliko prolaza na traceroute alata i neke druge alate.)

Pored traceroute (Linuksa) ili tracert (Windows), postoji nekoliko alata za prikupljanje ove vrste informacija:

DnsStuff (www.dnsstuff.com)

3D Internet stranica (www.d3tr.de)

GEOSpider (www.orevare.com)

Napadač će verovatno pokušati da skenira mrežu koristeći jedan od ovih alata, mnogi od kojih su slobodno dostupni. Svrha ovog aktivnog skeniranja je da se prikupe informacije o sistemu. Koristeći alate kao što su AngriIP, Nmap, i drugi (svi kreirani za razne potrebe), gde napadač može da efikasno isplanira svoju mrežu.

Treba imati na umu da skeniranje ovakvim alatom kao sto je nmap može izazvati razne alarme na serveru i odbrambenoj mreži.

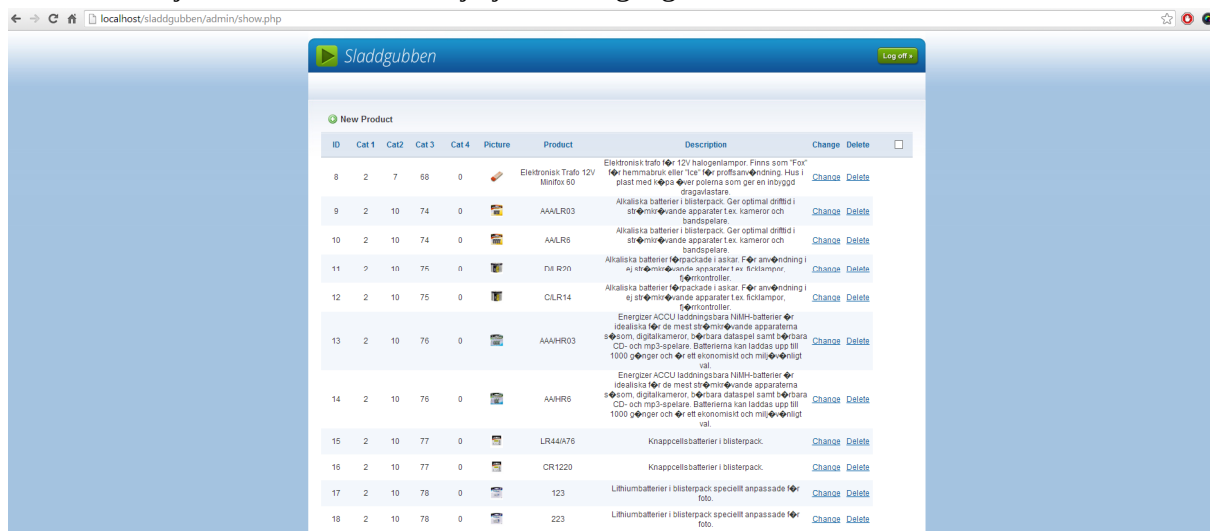
7 Primer CMS-a izrađenog na osnovu prethodnih informacija

Sama administracija sajta je veoma lako realizovana sa početnom stranom admin login,



Zahteva korisničko ime i lozinku koji se nalaze u samoj bazi podataka u tabeli korisnici, dakle kucanjem korisničkog imena i lozinke šalje se zahtev bazi da se provere sami podaci. Ukoliko su tačni, korisnik tog portala će nastaviti na drugu stranu i počće administracija, ukoliko se desi da su podaci pogrešni, pristup će i dalje biti zabranjen.

Strana koja služi za administraciju je ovakvog izgleda:

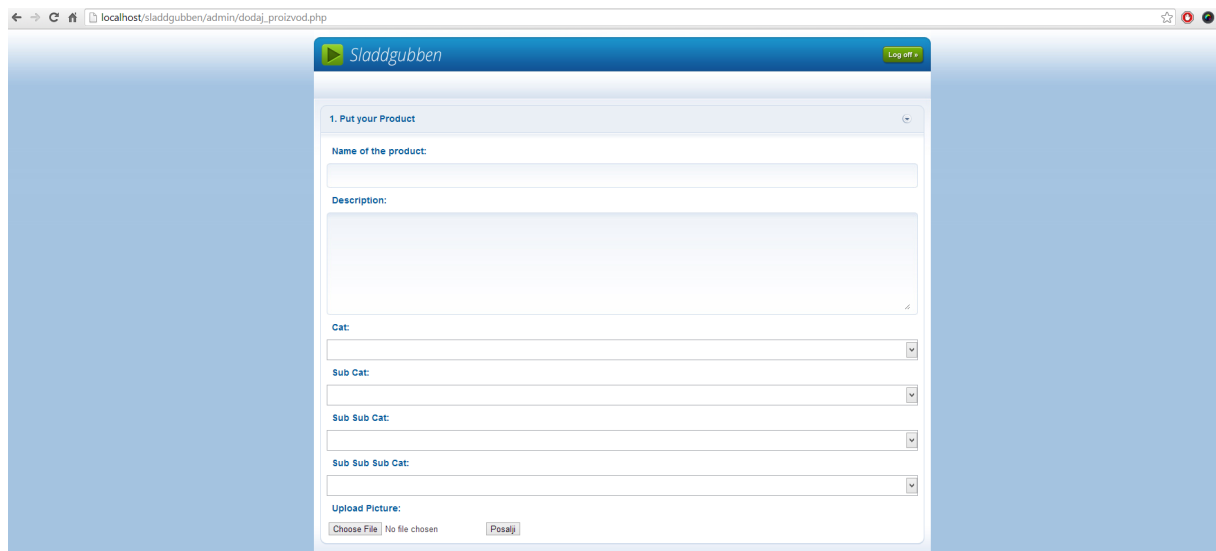


Dakle, na samom portalu možemo videti koji ID ima proizvod, sliku, cenu, količinu, šiping, opis i naravno dva dugmeta, jedno služi da se podaci o samom proizvodu menjaju a jedno da se taj proizvod izbriše. Ima dakle i dugme u gornjem levom uglu – dodaj novi proizvod – u kome se upisuju svi podaci novog proizvoda i ubacuje se slika, samim tim automatski se dodaje

ID svakom proizvodu koji se sledeći ubacuje. Postoji još i dugme – izadi – i uz pomoć njega se briše sesija i izlazi sa portala vraćajući na index.php tj. na početnu stranu.

7.1 Izgled strane za ubacivanje proizvoda

Sam izgled strane je dizajniran tako da bude lak za korišćenje samom korisniku, pruža mu mogućnosti da daje naziv proizvodu koji ubacuje, daje opis proizvoda, daje putanju tj. lokaciju gde će se listati na samom sajtu odabiranjem kategorija koje su na slici prikazane i koje se listaju kao padajući meni. Cela funkcionalnost ove strane je odrađena uz pomoć HTML-a koji mu daje jedinstven izgled i uz pomoć PHP-a koji radi pozadinski posao i sve sto je ubačeno u datim poljima čuva na određenim pozicijama u samoj data bazi.



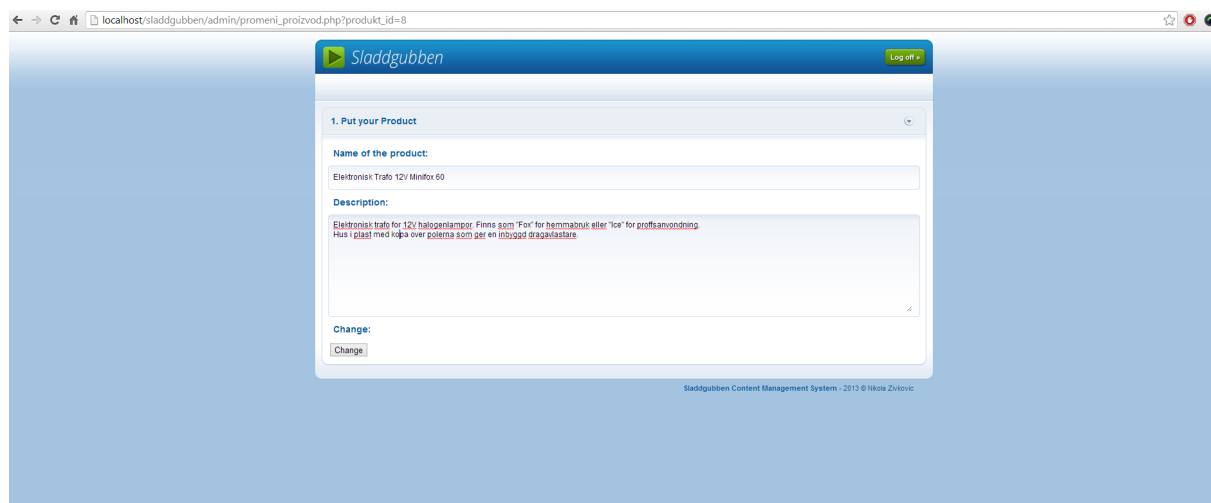
The screenshot shows a web browser window with the URL `localhost/sladdgubben/admin/dodaj_proizvod.php`. The page has a blue header with the 'Sladdgubben' logo and a 'Log off' button. The main content area is titled '1. Put your Product' and contains the following form fields:

- Name of the product:** A text input field.
- Description:** A large text area with a 'Go' button at the bottom right.
- Cat:** A dropdown menu.
- Sub Cat:** A dropdown menu.
- Sub Sub Cat:** A dropdown menu.
- Sub Sub Sub Cat:** A dropdown menu.
- Upload Picture:** A section with a 'Choose File' button, the text 'No file chosen', and a 'Postaj' button.

7.2 Izgled strane za menjanje detalja postojećeg proizvoda

Ista je situacija i ovde, dakle, postojeći proizvod koji se nalazi u bazi dakle na osnovu njegovih ID-jeva, kategorija, podkategorija, naziva itd. Povlače se informacije koje su za njega ubačene, dakle samim povlačenjem informacija dobija se ceo proizvod koji je onda na nama ostavljen da li želimo da ga menjamo ili ne.

Izmena samih informacija je veoma laka i za svakog laika i nekog ko nije nikad to radio veoma jednostavna, dakle prostim klikom na polje koje želite da menjate selektuje se tekst korišćenjem backspace opcije briše se postojeći tekst i dodaje novi. I tako za sva polja za koja je potrebna izmena ili ne.



Zaključak

Samim tim što su objašnjene osnove Wordpress-a, Joomla i drugih CMS-ova, njihove zaštite i mane, pojedinci koji žele da bolje shvate ovu oblast moraju da budu dosta aktivni i da prate dalja dešavanja na IT sceni i izmene u samim bezbednosnim aspektima CMS sistema, jer na osnovu iskustva tako će obezbediti sebe i druge za koje rade, a i biće u toku sa samom tehnologijom CMS-a, što im za dalje ostavlja bolje izgleda za njihovu budućnost.

Literatura:

- [1] <http://www.cms-security.org/>
- [2] <http://www.namecheap.com/support/knowledgebase/article.aspx/9156/12/>
- [3] <http://sparktrust.com/capabilities/cmsprotection>
- [4] http://www.slideshare.net/impresscms_de/cms-and-security-privacy-8205328
- [5] <http://forums.phpfreaks.com/>
- [6] <http://www.secureworks.com/resources/whitepapers-shortcut/27147/>
- [7] <http://www.cmsgeeks.com/articles/Security-and-your-site-73.html>
- [8] <http://www.miracletutorials.com/wordpress-vs-joomla-review/>
- [9] <http://forum.opencart.com/viewtopic.php?t=5792>
- [10] <http://boagworld.com/reviews/why-magento-is-worth-it-for-some/>
- [11] Lynda - CMS Fundamentals <http://www.lynda.com>