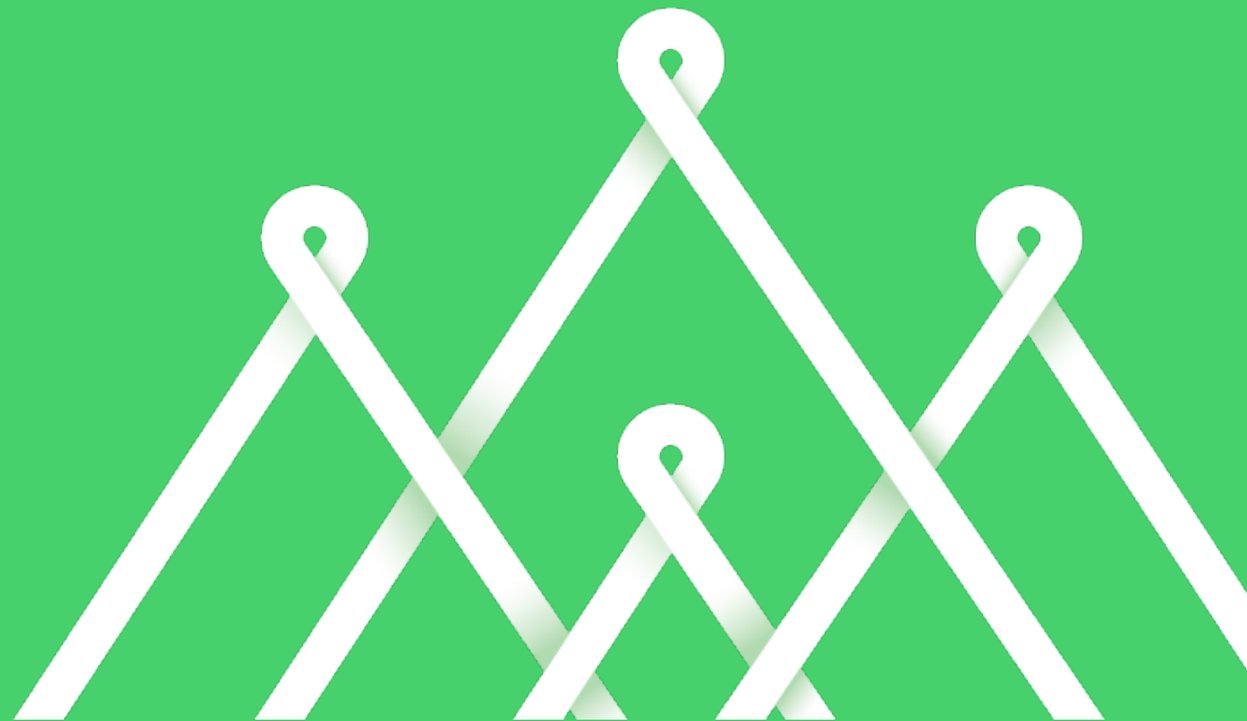
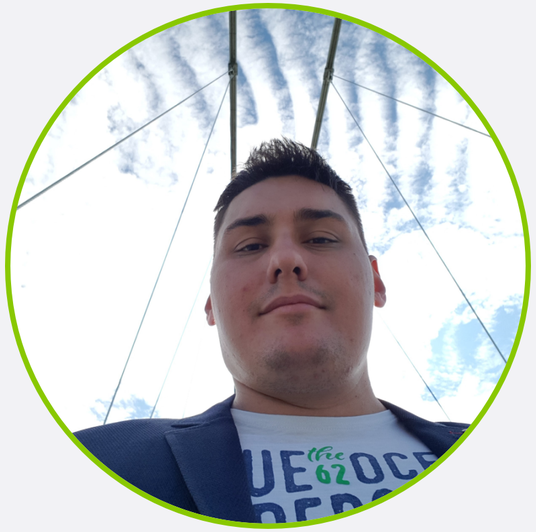
Kako preživeti katastrofu

Svi želimo da radimo na savršenim projektima, ali šta da radimo i kako da se postavimo u stanju haosa?

MINT





Igor Hrček, CTO

Započeo sam svoje preduzetničko putovanje sa 24 godina i osnovao hosting kompaniju Mint Hosting. Otkako znam za sebe bavim se programiranjem i stvaranjem visokokvalitetnih bagova. Zaljubljenik u rokenrol i kafu. Bogatu karijeru sam započeo kao 8bit Padawan, sad sam 64bit Jedi :)

agenda
prezentacije

Priča o jednoj katastrofi

Zatečeno stanje, Sodoma i Gomora

Kako smo preživeli katastrofu

Kako da učinite svoj WordPress bezbednijim?

Projekat danas

Kako ceo projekat izgleda danas?

o čemu
se radi (2016)?

Statistička analiza, kompleksni biznis proračuni

Osnovna uloga servisa su kompleksni proračuni zasnovani na unosu velike količine podataka na nedeljnom i mesečnom nivou uz pomoć komplikovane biznis logike.

Enterprise grade biznis platforma

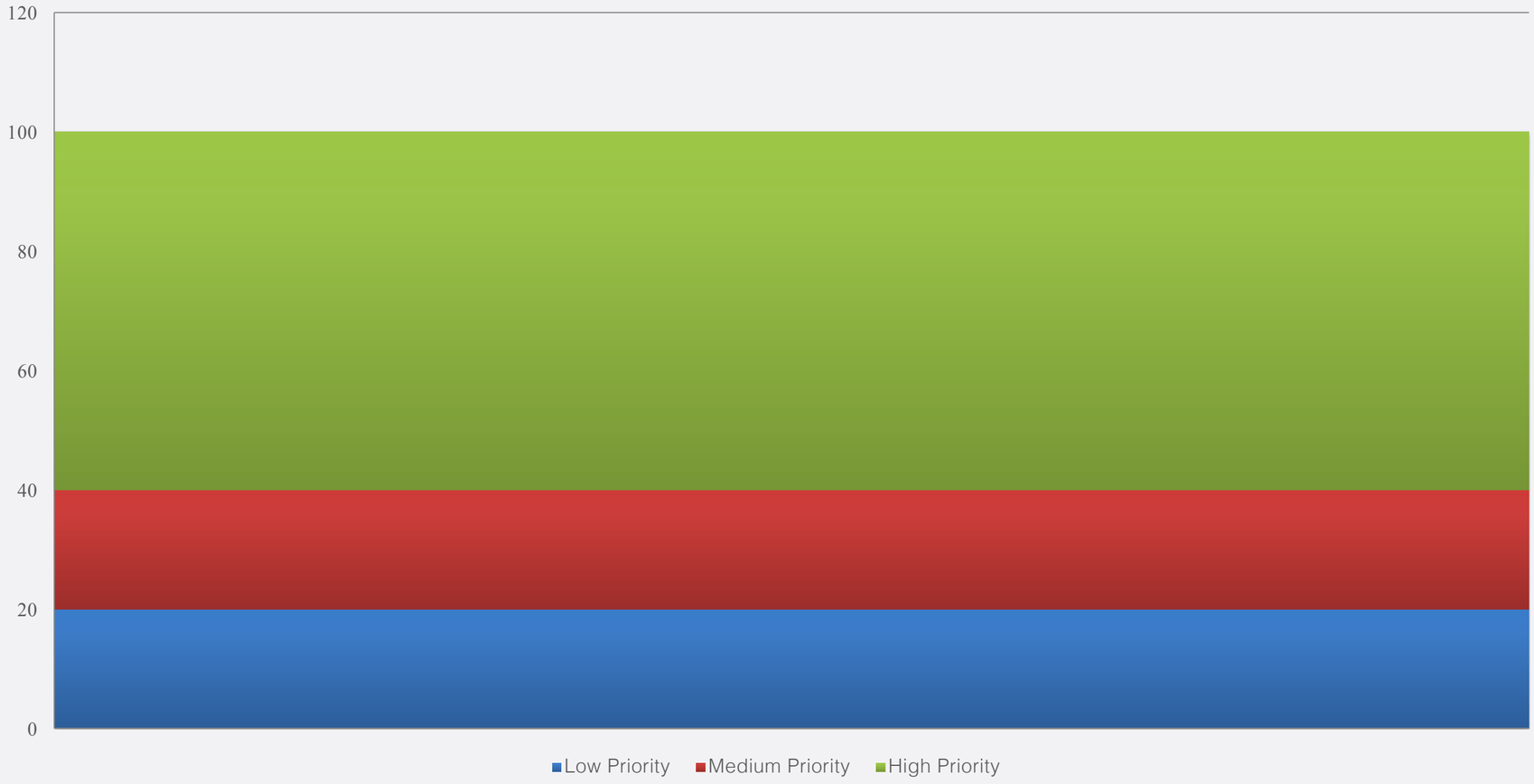
Platformu koriste velike kompanije u svakodnevnom poslovanju za analizu uspešnosti poslovanja, a na osnovu čijih proračuna vrše dalju optimizaciju poslovanja i planiranje

WordPress

Kao osnova platforme odabran je WordPress v4.2 (PHP 5.2, MYSQL 5.1, Apache 2.2)

... ali razvoj je radila outsource kompanija iz Indije...

penetration testing



Rezultati Penetration testa

- Izveštaj od 74 strane
- 167 bezbednosnih propusta iz svih OWASP Top 10 kategorija

zatečeno stanje
WordPress

- Kompletno paralelan sistem korisnika
- Paralelan sistem za upravljanje fajlovima
- Izmišljen Session menadžment umesto WordPress sistema za upravljanje autentifikacijom
- WPDB zamenjen sa ručnim upitima kroz mysql_query
- Modifikovano WordPress jezgro
- Besmislen pokušaj sakrivanja informacije o WordPress-u
- Razbacani fajlovi po disku
- Isprepletana biznis logika između tema i dodataka

zatečeno stanje
kod

```
71          if ($value) {
72            $value = $value;
73          } else {
74            $value = 0;
75          }
```

zatečeno stanje
kod

```php
foreach ($query as $hh2) {
    $fe2 = json_decode($hh2->formula_value);

    foreach ($fe2 as $keyepi2 => $nf2) {

        if ($nf2->epikey == $qq->id) {
            $dated = date("m", strtotime($hh2->date));

            if(!isset($oor_values_epis[$nf2->epikey][$hh2->userid]) || !in_array($dated, $oor_values_epis[$nf2->epikey][$hh2->userid])) {
                $hn24[$nf2->epikey][$hh2->userid][$dated] = $nf2->total;
                $hn27[$nf2->epikey][$dated][$hh2->userid] = $nf2->total;
            }

            if($hh2->userid == $Logged_ID) $hn24[$nf2->epikey][$hh2->userid][$dated] = $nf2->total;

        }
    }

}
```

zatečeno stanje
kod

- Malo nekog PHP-a...
- ... zatim jedan kompletno besmislen SQL upit ipresecan sa 4 funkcije...
- ... pa onda malo JavaScript koda koji je direktno ubačen u PHP kod...
- ... i čisto da stvar bude zanimljivija, i po koji CSS stil...
- ... a HTML? Pa naravno i malo njega...
- ... praćeno sa tri nove PHP funkcije kriptičnih imena...
- ... kao uvertira za 500 linija JavaScript koda kopiranog sa StackOverflow-a...
- ... i na kraju (ako je to kraj) po koji include drugih fajlova
- GOTO 1

zatečeno stanje
kod

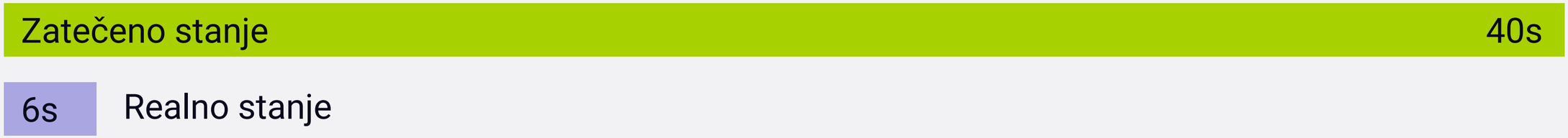
- WordPress template model implementiran na najpogrešniji mogući način. U stvari ovde WordPress ne postoji.
- PHP fajlovi na koje se direktno šalje POST kako bi se izvršio neki upit i vratio rezultat
- 72% SQL upita generiše MYSQL Query greške
- Nijedna jedina PHP klasa! Kompletan kod je proceduralan!
- Do 8 ugnježdenih for i foreach petlji
- Promenljive kriptičnih imena

zatečeno stanje
dokumentacija

zatečeno stanje
hosting infrastruktura

- Root pristup preko FTP-a, user root, lozinka !rootroot!
- PHP 5.2 u vreme kada je PHP 7 odavno dostupan
- Ne postoji firewall
- Ne postoji aplikativni firewall
- 82% SQL upita su deklarisani kao Slow Queries (10+ sekundi)
- PHP max_execution_time = -1
- PHP Memory Limit 1GB
- Često pucanje konekcije ka server, Error 500 svaki drugi zahtev, nedostatak memorije...
- Bekap? Nema.

zatečeno stanje
performanse



zatečeno stanje
istorijat, procesi...

- Dokumentacija? Nema.
- Git? Nema ni toga.
- Dokumentovana biznis logika? Nope.
- Roadmap? Ne.
- Database model? Ni toga.
- Bilo kakav pisani trag koji bi objasnio zatečeno stanje? Nope.

zatečeno stanje
najozbiljniji problemi

- **Aplikacija daje kompletno neispravne podatke**
- **Aplikacija je veći deo dana nedostupna, na šta se korisnici svaki dan žale**
- **Industrijska špijunaža konkurencije je moguća kroz jednostavnu manipulaciju DOM stablom iz browsera!**
- Ne postoji dobro definisan standard za ulaz i izlaz podataka
- Interfejs aplikacije je izuzetno loš, nefunkcionalan i bagovit
- **Kompletan biznis je skoro kompletno izgubio poverenje od strane krajnjih korisnika**
- Klijent u tom momentu ne razume pojam kvalitetnog koda, pravilnog procesa rada i zašto je dokumentacija neophodna

šta dalje?

- **Kako objasniti klijentu stanje stvari?**
- **Koju preporuku dati i kako ga savetovati?**
- **Da li odustati od projekta?**
- Čak i da ga zakrpimo, ima li to sve smisla?
- Odakle početi?

zavođenje reda
bezbednost

Kako smo se organizovali?

- Definisali smo tri kategorije – Low, Medium i High Risk
- Redosled od lakšeg ka težem
- Rešili smo pitanje bezbednosti servera
- Uveli smo ModSecurity, monitoring, redovan bekap na udaljenu lokaciju

Koje smo probleme imali?

- Često nije bilo moguće utvrditi u kom momentu se neki kod poziva
- Izuzetno otežani uslovi testiranja
- Više verzija jednog te istog fajla
- Zbog načina na koji je kod pisan, PHP je limitiran na 5.4.42

zavođenje reda
biznis

Kako smo se organizovali?

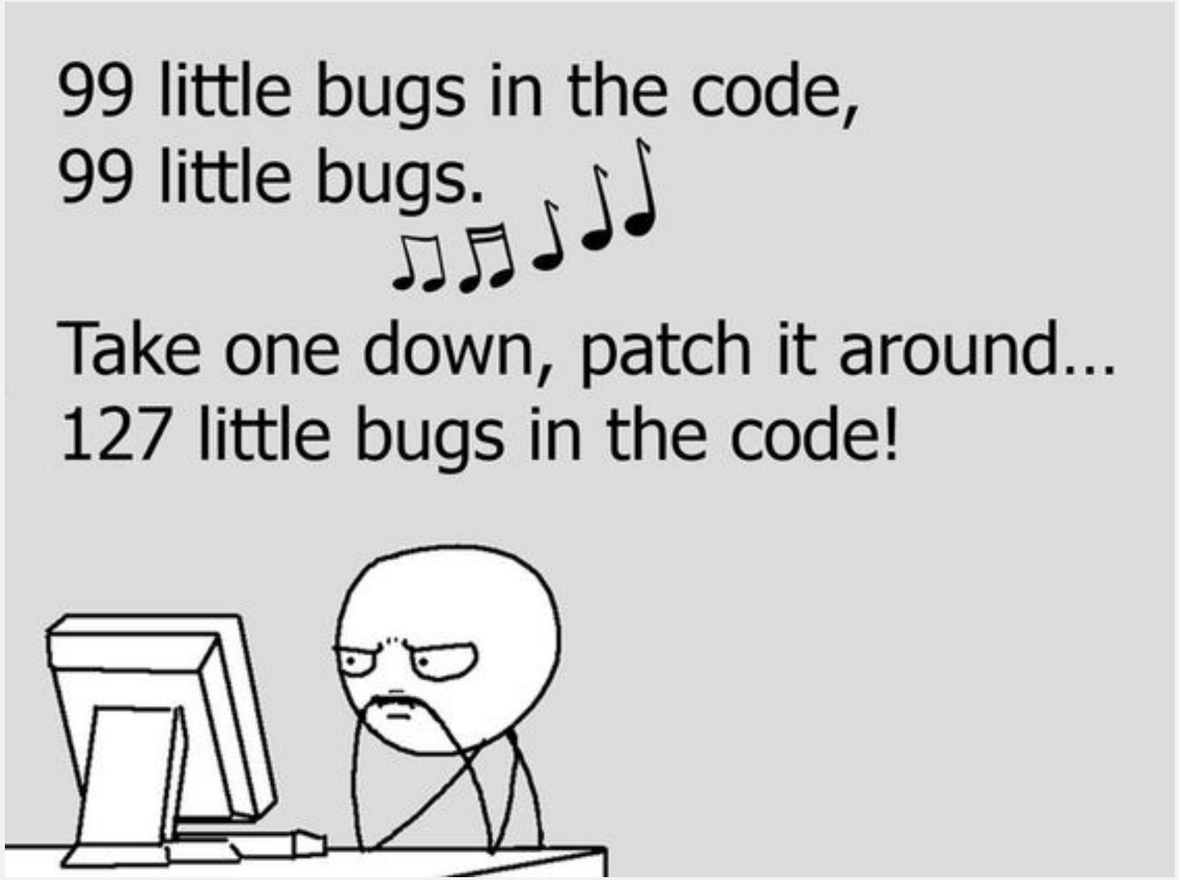
- Prepoznali smo najkritičnije probleme koji su zahtevali momentalnu pažnju i rešenje
- Otvorili smo poseban kanal za feedback i bug report korisnika kako bi smanjili tenzije
- Otvorena komunikacija o ispravljenim bagovima na nedeljnom nivou

Koje smo probleme imali?

- Tabanje u mraku
- Nedostatak bilo kakve dokumentacije pomešan sa izuzetno lošim kodom je u nekim momentima činio posao nemogućim

zavođenje reda
biznis

U realnosti?



zavođenje reda
performanse

Kako smo se organizovali?

- Promenili smo hosting provajdera
- Zamenili smo zastareli Apache sa nginx app serverom, prebacili bazu na MariaDB 10.1
- Izmenili smo 140 modela i dodali indekse
- Implementirano FastCGI static keširanje za **ulogovane** korisnike što je dovelo do ubrzanja kompletnog servisa za 96%, uz smanjenje opterećenja za preko 70%

Koje smo probleme imali?

- Standardni pristup keširanju je bio nemoguć
- Static HTML keširanje se nikada ne koristi na mestima gde postoji razdvajanje prikaza po korisnicima
- Prevencija curenja podataka
- Automatizovano odžavanje keša za svakog pojedinačnog korisnika

zavođenje reda
nakon prvih 6 meseci

Kako smo se organizovali?

- Krenuli smo od najjednostavnijih stvari ka težim
- Izbegavali smo modifikaciju postojećeg sistema
- Delovi koji su zahtevali modifikaciju su pisani iz početka (ukoliko je bilo moguće)
- Veliki deo interfejsa je kompletno razvijen od nule

Koje smo probleme imali?

- Kod koji smo nasledili je bio napisan tako da može da radi samo jednu stvar
- Izuzetno težak proces integracije ili modifikacije
- Jako česti bagovi u nekim delovima servisa koji nemaju nikakve direktne veze sa modifikovanim kodom

zavođenje reda
najgori momenti

- Prva tri meseca nismo imali pojma gde se nalazimo niti šta radimo
- Nešto je puklo, situacija je gadna i ne možemo da reagujemo momentalno
- Osećaj da nismo dorasli zadatku
- Zašto nam je ovo trebalo u životu?

nakon
dve godine

- Izašli smo iz faze stabilizacije
- Servis je sada potpuno operativan, sve informacije koje se prezentuju su ispravne
- Poverenje krajnjih korisnika se značajno uvećalo
- Povećan broj novih korisnika
- Rešeni (maskirani) osnovni problemi sa performansama i hostingom
- Fokus na razvoj novih mogućnosti

nakon
tri godine

- Kompletan biznis je prepoznat kao unikatan zahvaljujući realizovanim rešenjima
- Audit izvršen od strane treće kompanije opisao je kompletnu aplikaciju kao pouzdanu
- Prvi javni API!
- Migracija od monolitne aplikacije ka mikroservisima
- Kompletan servis je izazvao veliko interesovanje od strane drugih kompanija koje se bave agregacijom biznis podataka, nakon čega je konačno u maju prodat jednoj od najvećih kompanije tog tipa u USA

bitne lekcije

- Dobro pazite sa kime radite jer to direktno utiče na vaš biznis
- Novac može da se vrati, vreme ne
- Nismo dovoljno bogati da bi kupovali jeftine stvari
- Otovreno priznajte kada niste u stanju da izvedete nešto i potražite pomoć
- Pravite realne i ostvarive planove
- Otvoreno, transparentno i smireno komunicirajte u svim situacijama
- Pišite dokumentaciju
- Brinite o bezbednosti, redovno testirajte svoj kod
- Obratite pažnju kod odabira platforme

to je to, nema više

pitanja & odgovori

kutija

igor.hrcek

mint.rs

hvala ☺