

KDAJ STE NAZADNJE SERVISIRALI VAŠE APLIKACIJE?

Milan Gabor

Inštitut za varnost podatkov in informacijskih sistemov, ViRIS d.o.o.,
Šmartinska cesta 130, 1000 Ljubljana
e-pošta: milan@viris.si
URL: <http://www.viris.si/>

Povzetek

Verjetno primerjava spletnih aplikacij z avtomobili ni primerna, vendar pa lahko vseeno potegnemo kakšno vzporednico predvsem z življenjskim ciklom obeh produktov. Tako kot imamo pri avtomobilu redne servisne cikle, bi pri življenjskemu ciklu spletnih aplikacij moralo biti vsaj podobno če ne že enako. Redni servisni posegi so tisti, ki naše jeklene konjičke ohranjajo v formi, skrbijo za našo varno vožnjo in hkrati podaljšujejo življenjsko dobo naših prevoznih sredstev. Enaki servisni cikli bi morali veljati tudi za naše aplikacije, ki jih daje v uporabo, pa naj bodo to interne aplikacije ali aplikacije, ki jih objavljamo na spletu. Vendar pri našem delu opažamo, da so takšni servisni posegi redki, sploh če aplikacija izpolnjuje naročnikove zahteve.

1. UVOD

V realnosti je v velikem številu primerov tako, da je potrebno spraviti aplikacije čim hitreje v produkcijsko okolje, kljub temu, da mogoče niso bile dovolj preizkušene ali pa manjka še kakšna funkcionalnost. Poleg vsega pa lovljenje rokov povzroči med drugim tudi to, da aplikacijam manjka podrobna dokumentacija in najbrž še kaj drugega. Pri sami vzpostavitvi delovanja aplikacije seveda ne moremo mimo pravilne konfiguracije okolja v katerem bo aplikacija tekla. Velikokrat se namreč zgodi, da kljub dobro zasnovani in tudi preverjeni aplikaciji, ostajajo šibki členi okolje in sistemi na katerih teče ta aplikacija. In v tem sistemu je najšibkejši člen tisti, ki se ga bodo potencialni napadalci lotili prvega.

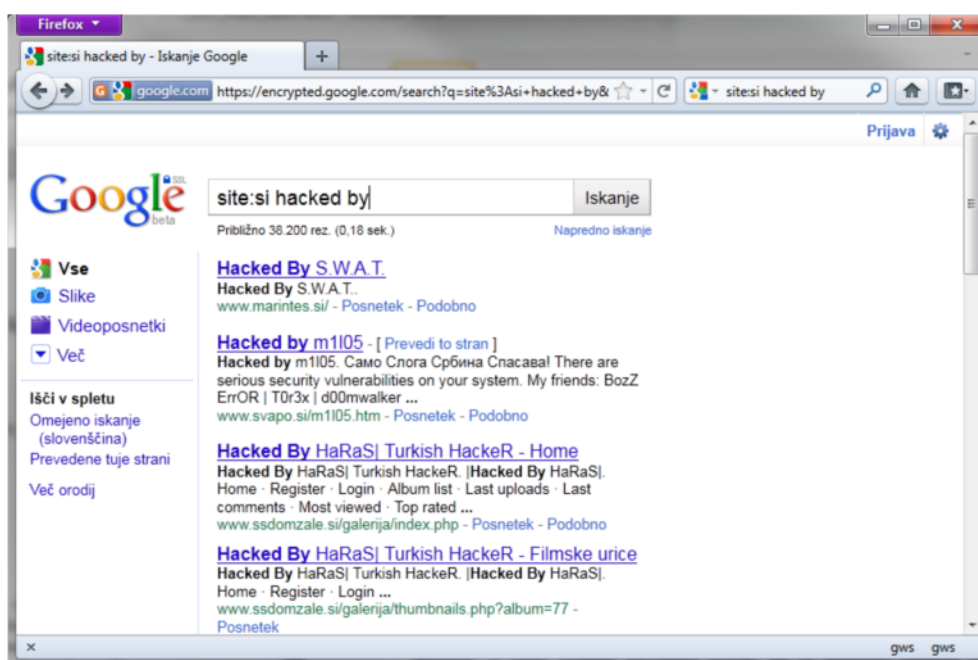
Poleg podrobnega preverjanja aplikacij preden gredo v produkcijsko okolje, je mogoče opaziti, da se po tej fazi življenjskega cikla aplikacije dejansko proces upočasni ali celo zaustavi. Aplikacija gre v produkcijo, napak ni opaziti in stranke so zadovoljne. Zelo pomembno pa je tudi nadaljnje dogajanje v življenjskem ciklu aplikacije. V veliki večini se vršijo le popravki pomanjkljivosti in dodajanje funkcionalnosti, ki jih opazijo in zahtevajo končni uporabniki.. Pravega servisiranja aplikacije v tej fazi življenjskega cikla pa ni. Prav tako velikokrat ostane nedotaknjeno tudi okolje v katerem te aplikacije tečejo oz. druge pomožne knjižnice in drugi elementi od katerih so aplikacije odvisne. Ker pa se tudi v teh knjižnicah in okoljih najdejo kakšne pomanjkljivosti, je potrebno skrbeti tudi za te elemente. Resničnost pa kaže, da velikokrat na te elemente enostavno pozabimo ali pa se jih zaradi določenih razlogov nočemo dotikati ali spreminjati, kaj šele nadgrajevati in servisirati. In ti elementi so lahko ključni, da nekega lepega dne ugotovimo, da je bila naša aplikacija ali

produksijsko okolje kompromitirano, naša aplikacija izrabljena, podatki, ki pa jih je hranila pa so odtekli neznano kam.

2. APLIKACIJSKE TEŽAVE

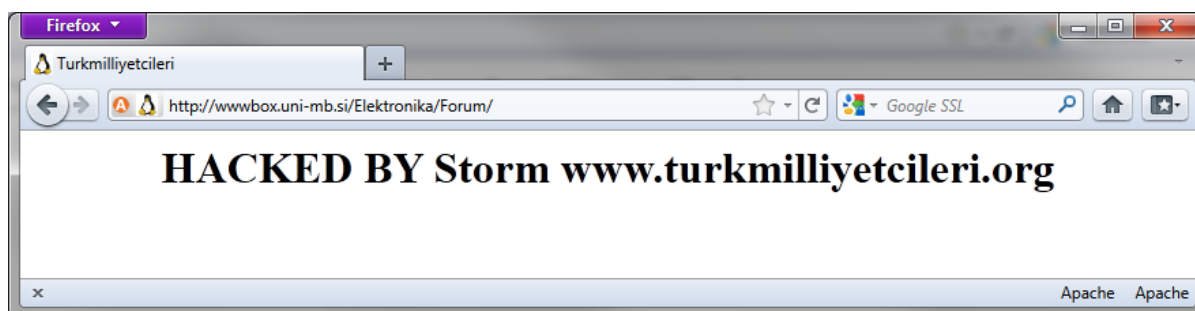
Če si na začetku zastavimo vprašanje, katere aplikacije so sploh primerne za servisiranje, lahko ugotovimo, da je mnogo takšnih. In kako težko jih je najti? Niti ne preveč, saj lahko z uporabo iskalnika Google ali Bing dobimo hitro zelo dobre zadetke, ki so zelo aktualni. Za iskanje so primerni recimo naslednji iskalni nizi:

- site:si hacked by
- site:si turkish hacker
- site:si x-turk was here
- site:si defaced by.



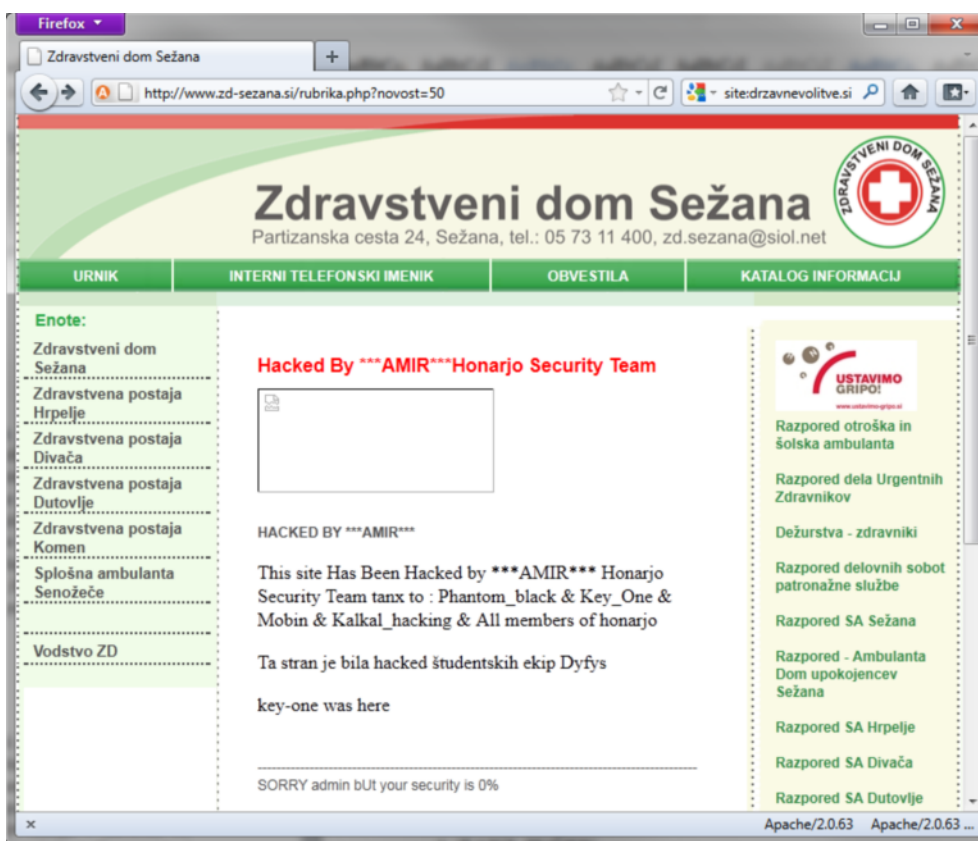
Slika 1. Iskalnik Google je dober začetek

Rezultati takšnih iskanj so dober znanilec tistih spletnih strani in aplikacij, ki zadnje čase niso bile na nobenem servisnem posegu. Iz teh rezultatov lahko tudi hitro opazimo, katere strani kdo sploh uporablja. Opažamo, da skrbniki nekaterih strani, kljub temu, da so bile spremenjene nihče ne opazi in so lahko takšne »popravljenе« na spletu tudi več časa. Včasih celo tedne ali mesece.



Slika 2. Primer že dolgo spremenjene strani

Večina teh spremenjenih strani, so strani manjših podjetij ali drugih ustanov, ki se mogoče ne zdijo pomembna in niso vredne pozornosti. Vendar tudi te manj pomembne strani so lahko problematične, sploh če smo preko njih posredovali kakšne naše podatke. Med rezultati napadenih strani, ki jih je mogoče najti s pomočjo iskalnika je tudi spletna stran Zdravstvenega doma Sežana. Kot kaže vzdrževalci spletne strani niso pozorni na to, da imajo na njihovih straneh vsebino, ki tja ne sodi. Dokler so strani na strežniku, kjer je samo predstavitev ne bi smelo biti težav. Ampak kaj če bi pa na tem strežniku bili še podatki o pacientih, njihovi urniki obiskov pri zdravnikih in mogoče še namen obiska? Potem pa ne bi bila ta sprememba na spletni strani tako nedolžna, sploh za tiste ljudi, ki obiskujejo ta zdravstveni dom. Edina sreča v nesreči je ta, da so takšni napadi večinoma avtomatski in tudi napadalci ne razumejo točno kakšno tarčo so napadli in kakšne podatke lahko s takšnih tarč pridobijo. Če bi imeli te dodatne podatke, potem se najbrž ne bi zadovoljili samo z vstavljanjem te vsebine, ampak bi aplikacije huje zlorabili.



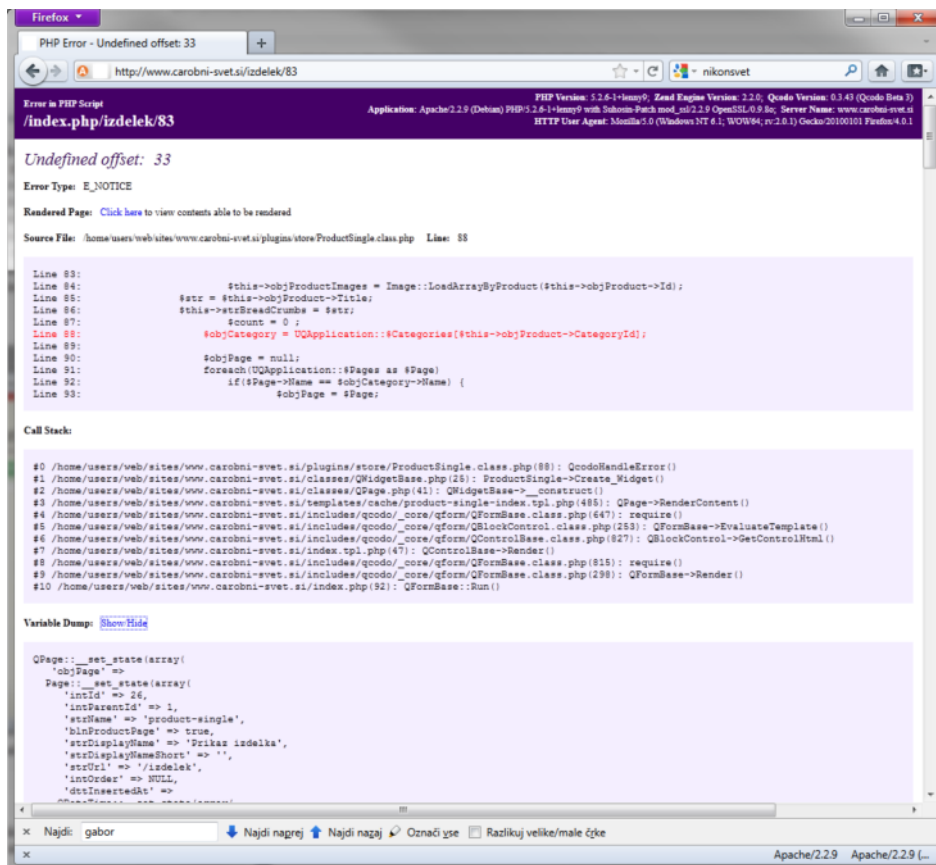
Slika 3. Tudi zdravstvo ni imuno pred napadi

3. SISTEMSKE TEŽAVE

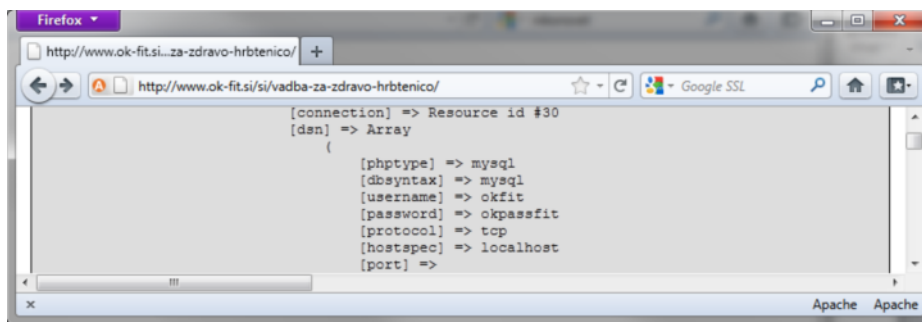
Podobno kot pri aplikacijskih težavah, ki smo jih opisali zgoraj, lahko opazimo tudi več nepravilnosti pri konfiguraciji okolja ali sistemov. Tudi pri tem so iskalniki v veliko pomoč. Naslednji iskalni nizi so idealni za začetek iskanja:

- php warning site:si
- php error site:si
- SQL error site:si
- Stack trace site:si.

V teh primerih nam aplikacije postrežejo z veliko podatki, ki potencialnim napadalcem lahko zelo koristijo s tem, da kot stranski produkt izpišejo podatke, ki jih praviloma ne bi smele. Tako so napadalci oboroženi z dodatnimi podatki, ki jih lahko s pridom izkoristijo in bodisi povzročijo škodo na straneh ali pa ukradejo kakšne osebne podatke. Na naslednjih slikah je mogoče opaziti, da bi bilo mogoče takšne napake zelo enostavno odkriti, če bi se v preizkus vložilo le malo napora. Hkrati bi se s tem bistveno izboljšala kakovost same aplikacije.



Slika 4. Aplikacije lahko izpišejo kopico podatkov



Slika 5. Aplikacije lahko izpišejo tudi druge podatke

4. KDAJ IN ZAKAJ NA SERVIS?

Glede na naše lastne izkušnje pri analizah aplikacij opazamo, da se cikel pri razvoju aplikacije konča s tem, ko se aplikacija postavi v produkcijsko okolje, preveri osnovno delovanje,

namesti še kakšen popravek, potem pa se zgodba konča. Potem so aplikacije prepuščene samemu sebi in konfiguraciji ki je bila narejena. Zaradi določenih razlogov in včasih tudi pomanjkanja dokumentacije, se potem teh aplikacij nihče več ne upa dotikati. Sploh do takrat ko delajo v skladu s pričakovanji so velikokrat pozabljene in zapuščene. Šele ko se pojavi kakšna težava v zvezi z njihovim delovanjem, se spomni kdo na njih in šele takrat se sproži proces iskanja napak in testiranja. V tem vmesnem času, ko se ta proces izvaja, pa lahko naročniku nastaja dodatna škoda, ki bi se lahko minimizirala ob rednem servisu aplikacij.

V določenih časovnih intervalih bi bilo potrebno preveriti naslednje parametre in nastavitve okolja:

- nove verzije aplikacije, posebej v primeru če smo uporabili kakšno odprtokodno,
- preveriti osnovne nastavitve okolja,
- preveriti popravke za sistem in okolje v katerem teče aplikacija,
- narediti hitre teste za znanimi pomanjkljivostmi,
- preveriti za kakšnimi ostanki datotek na produkcijskih strežnikih.

Intervali, v katerih bi se naj aplikacije servisirale, so odvisne od procesov, ki jih ima naročnik vpeljane ali od dobrih praks s tega področja. Vsekakor pa se priporoča, da se vsaj dvakrat letno naj preverijo osnovne stvari glede aplikacij. V kolikor pa se je izbrala za programsko rešitev kakšna odprtokodna aplikacija, je priporočljivo redno spremljati kakšne pošne sezname, kjer se redno objavljajo pomanjkljivosti najdene v teh aplikacijah in aplikacije redno posodabljati.

5. ZAKLJUČEK

Če potegnemo črto pod naš prispevek, lahko tako hitro že na palec ocenimo, da se splača tudi kdaj pa kdaj poslati spletne aplikacije na servis. Kot se izkaže so najboljši zunanji servisi, ki jih opravijo usposobljeni strokovnjaki, ki bodo na spletne aplikacije pogledali na drugačen način, kot na njih gledajo bodisi vzdrževalci aplikacij ali celo njihovi avtorji. Pogled etičnih hekerjev je velikokrat najboljši, saj razmišljajo na drugačen način kot ostali uporabniki aplikacij. S termi rednimi servisnimi posegi, pa se drastično zmanjša verjetnost, da bo aplikacija imela kakšno kritičnost ranljivost, ki bi jo lahko morebitni napadalci izkoristili.