DIGITALNI IZZIV – KO NE VIDIMO OČITNEGA

Milan Gabor

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

Povzetek: *Že Mali princ nas uči, da je bistvo očem skrito in to preprosto resnico lahko uporabimo tudi v našem digitalnem svetu, ki prinaša veliko digitalnih izzivov. Aplikacije, sistemi, storitve in ne nazadnje tudi oblaki skrivajo veliko informacij, ki jih drugi lahko vidijo in izkoristijo. Včasih je potrebno pogledati le malo bližje in že se odkrijejo stvari, ki so skrite pod lepo zloščeno površino. In prav te stvari velikokrat krojijo naša digitalna in tudi resnična življenja. Na našem digitalnem sprehodu se jih bomo nekaj dotaknili in predstavili svoje izkušnje.*

1. UVOD

V zadnjem času nam različni varnostni incidenti dajo resno misliti in nas silijo v to, da se začnemo spraševati, koliko so naši sistemi sploh varni. Če le malo spremljamo incidente s tega področja, lahko opazimo, da ne mine dan, da ne bi bilo novic o kraji ali izgubi podatkov, o varnostnih pomanjkljivostih v aplikacijah in sistemih. Skupina Anonymous je poskrbela za to, da so te novice prišle na prve strani vseh časopisov in glavnih spletnih strani. Videli smo, da tudi Slovenija ni imuna na takšne tipe napadov, saj smo lahko bili priča DDOS napadu na NLB in nekatere politične stranke. Priča smo bili tudi pridobitvi seznamov nekaterih elektronskih naslovov ljudi in drugi manjši izgubi podatkov, ki pa na srečo ni bila kritična. Takšne aktivistične, ali če rečemo hektivistične, akcije kažejo na to, da Internet nima meja in da je v globalnem omrežju lahko tarča vsak, ki je priklopljen v omrežje. In tudi velikokrat mala Slovenija v tem pogledu ni nobena izjema več.

Kot je že v povzetku napisano, pa se resnica skriva v tem, da so velikokrat pomembne stvari skrite očem in če jih hočemo res videti, je potrebno pogledati pod lepo površino, ki velikokrat prekrije prave izzive. Tako lahko ugotovimo, da različnim napadalcem v veliko primerih ni potrebno veliko hekerskih aktivnosti. Velikokrat se namreč zgodi, da so napake v aplikaciji, aplikacijski logiki ali v sami konfiguraciji okolja tako očitne, da ni potrebno direktno napasti aplikacijo, ampak samo pozorno spremljati odzive ob različnih robnih primerih. In v teh robnih primerih aplikacije izdajajo veliko koristnih informacij napadalcem, ki jih le-ti zlahka izkoristijo.

Poleg direktnih napadov pa so napadalcem v veliko pomoč tudi iskalniki. Iskalniki hranijo v svojih shrambah verzije spletnih strani, ki so jih obiskali v trenutkih, ko so se aplikacije nadgrajevale ali so imele kakšne druge pomanjkljivosti. S pomočjo iskalnikov lahko napadalci te strani izbrskajo ali pridobijo druge koristne informacije, ki jih s pridom izkoristijo v samem napadu na spletno stran ali njene obiskovalce. Tako se lahko osnovna funkcionalnost spletnih iskalnikov uporabi na način, na katerega morda pri snovanju niti niso pomislili.

2. DIGITALNI IZZIV

Glede na našo primarno dejavnost in naše poslanstvo smo se v letu 2011 odločili in zasnovali idejo o digitalnem izzivu, s katerim bi lahko tematiko s področja informacijske varnosti približali širšemu krogu ljudi. Hkrati bi lahko s tem izpostavili tudi ponavljajoče se pomanjkljivosti in tako prispevali k večji vlogi informacijske vloge pri samem razvoju in pri vpeljavi informacijskih tehnologij.

Digitalni izziv predstavlja idejo o tekmovanju v uporabi informacijske tehnologije, računalniške varnosti in iznajdljivosti. Prvotni namen tekmovanja je ponuditi privlačno, informacijsko varnostno obarvano aktivnost oz. izzive v sklopu različnih dogodkov na tem področju.

Slika 1. Spletni prikaz rezultatov

Namen tekmovanja je torej soočenje tekmovalcev z raznolikimi izzivi, jih spodbuditi h kreativni in iznajdljivi uporabi računalnikov, informacijske tehnologije in varnosti ter jim na zabaven način predstaviti koncepte računalniške varnosti in informacijske tehnologije nasploh.

Tekmovanje je zasnovano kot vrsta različno težavnih izzivov v obliki nalog, ki jih lahko hkrati rešuje večje število udeležencev s pomočjo svojih prenosnih računalnikov. Sodelovanje v tekmovanju primarno poteka preko spletnega portala, prijava pa je brezplačna za vse udeležence konference. Na spletnem portalu, kot tudi na zaslonu v prostorih konference, se lahko v živo spremlja napredek različnih skupin, število rešenih nalog in točk.

S takšnim digitalnim izzivom povečujemo zavest s področja informacijske varnosti in pripomoremo k varni uporabi storitev in spletnih aplikacij.

Slika 2. Prikaz primera naloge na tekmovanju

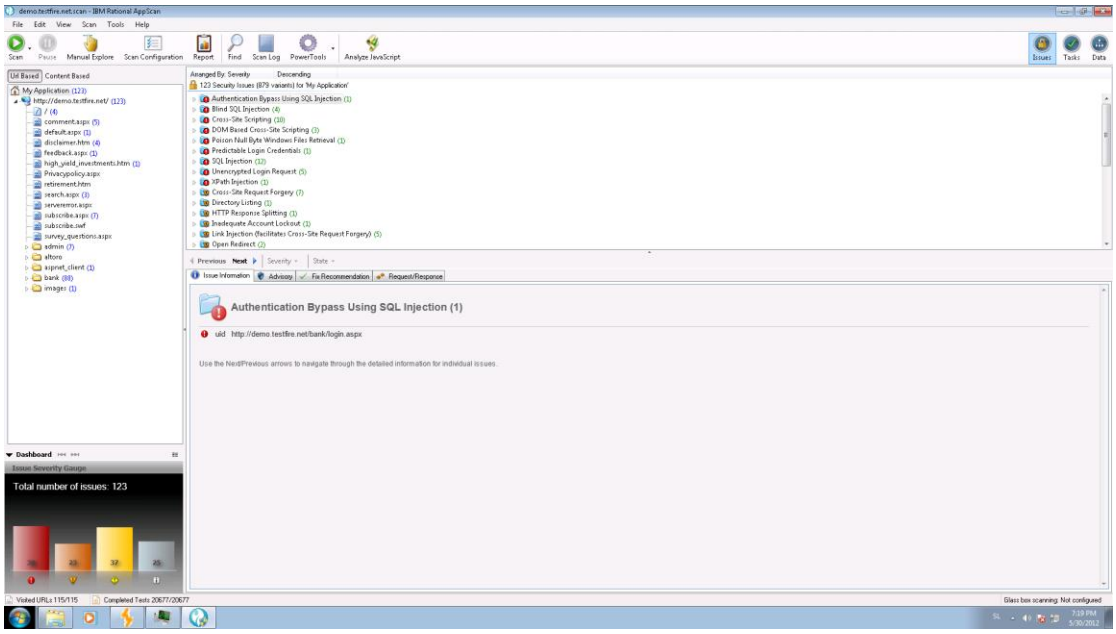
3. APLIKACIJSKI IZZIV

Glede na poplavo aplikacij, pa naj si bodo klasične ali spletne aplikacije, je na tem področju veliko izzivov. Sploh glede na to, da precej teh aplikacij hrani naše podatke, pa naj bodo to splošni ali osebni podatki, ki jih je treba hraniti v skladu z zakonodajo ali drugimi dobrimi praksami.

Za izvedbo analize varnosti na aplikativni ravni danes v večini primerov ne gre brez aplikativne podpore. Veliko izvajalcev se zanaša na avtomatska orodja, ki odkrijejo večino varnostnih pomanjkljivosti in napak v aplikaciji. Tako jih večina analizira ranljivosti po OWASP TOP 10 ali preverja skladnost s kakšnim standardom, na primer PCI ali HIPAA.

Seznam trenutno najboljše ocenjenih komercialnih orodij, ki jih večina uporabnikov uporablja pri svojem delu:

- IBM Rational AppScan,
- HP WebInspect,
- Rapid7 Nexpose.



Slika 3. Rezultati pregleda z orodjem IBM Rational AppScan

Seveda obstaja na tem področju tudi kopica prosto dostopnih ali odprtokodnih orodij, kot na primer naslednja:

- Netsparker,
- ZAP proxy,
- OWASP Mantra.

Glede na izkušnje pa je zmotno prepričanje, da lahko aplikacije v celoti nadomestijo ročno ali delno ročno preverjanje. Avtomatsko preverjanje aplikacij je lahko v veliko pomoč in lahko poda smernice, v katerih je treba izvesti še dodatno testiranje. Poleg tega so poročila avtomatskih testiranj precej podrobna in dolga, iz katerih je včasih kar težko izluščiti prave pomanjkljivosti, saj se pogosto zgodi, da dobimo kopico lažnih napak in je treba te še enkrat ročno preveriti in se prepričati, da so pomanjkljivosti res prisotne. Najboljša kombinacija za dosego optimalnih rezultatov testiranja je torej kombinacija ročnega testiranja in pametne uporabe avtomatskih orodij. Seveda se je potrebno prej prepričati, katero orodje je najbolj primerno za uporabo v določenem scenariju in tipu aplikacije.

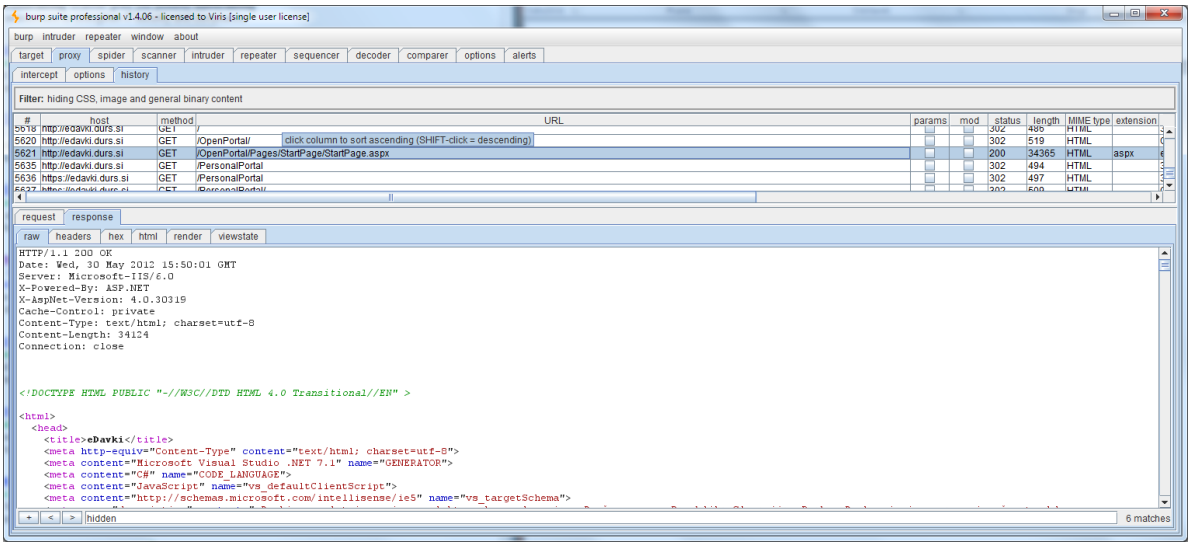
4. ROČNI IZZIV

Ročno testiranje je poseben način analize, kjer je potrebno precej znanja z različnih področij, da se lahko analiza uspešno izvede. Za uspešno analizo je potrebno predvsem dobro poznavanje različnih protokolov in tehnologij (HTTP, FTP, WS, XML). Pri tem seveda ne gre brez vmesnega strežnika (proxy server), ki nam omogoča naslednje aktivnosti:

- prestrezanje klicev na strežnik,
- zamenjava vrednosti,
- hranjenja in podtikanja sej,
- različno hitre načine dekriptiranja nizov (BASE64, različna kodiranja),
- simuliranje klicev z različnimi parametri in analiza dobljenih rezultatov,
- shranjevanje vseh klicev in ponovljivost testa.

Pri ročnem testiranju je seveda mogoče naleteti tudi na težave, ki jih v določenih primerih lahko rešimo na enostaven način, nekatere pa zahtevajo malo več iznajdljivosti in dodatnih aktivnosti. Naj naštejemo nekatere:

- SSL povezave,
- avtentikacija s certifikati,
- kriptiranje,
- zahtevna analiza pri velikem številu parametrov,
- težave s časovnimi zakasnitvami pri večji analizi prenesenih podatkov.



Slika 4. Ročna analiza HTTP prometa z orodjem Burp

Takšen način analize lahko ugotovi določene skrite funkcionalnosti v samem delovanju in logiki aplikacije, ki ji avtomatska orodja ne morejo ugotoviti, na primer, če se določeni podatki prenašajo v skritih poljih ali preko GET zahtevkov. Orodja testirajo različne tipe?, ne morejo pa ugotoviti pomena prenesenih podatkov in za kaj točno se uporabljajo. In v takšnih primerih dajejo ročna testiranja bistveno boljše rezultate. Za primerjavo – v nekaterih primerih najprej zaženemo avtomatske teste in potem opravimo testiranje še ročno. Rezultati testiranja so v nekaterih primerih presenetljivi v prid ročnega testiranja, tudi v primeru, da se testira z različnimi orodji za avtomatsko preverjanje. Človeški faktor na tem področju torej še ni nadomestljiv.

5. KONKRETNI IZZIV

Trditev, da so včasih stvari očem skrite in da se zaradi drevesa ne vidi gozda, je mogoče podkrepiti z naslednjim primerom. Pri izvajanju seminarja na temo etičnega hekinga, ki je potekal nepretrgoma 5 dni, so udeleženci odkrivali načine, kako se lotiti preverjanja sistemov. Tako so bila pokrita vsa področja in tehnike, ki jih uporabljajo tudi hekerji. Podana je bila tudi možnost sprotnega preverjanja naučenih tehnik in simuliranje/simulacija različnih napadov na aplikacije.

Za zaključek je bilo predvideno tekmovanje, kjer bi lahko tekmovalci preverili svojo uspešnost spoznavanja različnih tehnik preverjanja varnosti. Takšno vrsto tekmovanja CTF (Capture The Flag) poznajo skoraj vse konference in se jih računalniški navdušenci z veseljem udeležujejo. Za ta namen je bil posebej postavljen sistem, ki je imel dve tipični ranljivosti. Ti dve ranljivosti sta omogočali napadalcem, da so lahko uspešno prevzeli sistem in poiskali manjkajočo datoteko, ki je bila ključ do uspeha. Ranljivosti sta bili različne zahtevnosti. Pri preprosti ranljivosti je bila mogoče dano nalogo uspešno končati precej hitro in ni bilo potrebnega veliko tehničnega znanja, potrebno pa je bilo malo iznajdljivosti in širšega pogleda. Druga ranljivost je terjala več tehničnega znanja in povezovanja stvari med seboj ter bistveno več časa za njeno odkritje in nato tudi izkoriščanje. Zanimivo je bilo, da nihče od tekmovalcev ni ubral lažje in preprostejše poti. Sicer so nekateri tekmovalci videli to možnost, a so raje izbrali težjo pot, kjer so se morali bistveno bolj potruditi, da so lahko prišli do želenega cilja.

Seveda tudi pri izvedbi Digitalnega izziva opažamo, da kljub začetni vnemi in lahkim začetnim nalogam, nekateri tekmovalci hitro obupajo. Še posebej velja to za naloge, kjer se je treba poglobiti v tematiko in jo preučiti, da jih lahko uspešno rešimo. Eno takšnih področij je kriptografija, kjer je potrebno tudi precej drugega znanja in ne samo računalniških izkušenj. Pri teh nalogah poznavanje matematike pride še kako prav. Seveda pa je včasih potrebno tudi kanček sreče in iznajdljivosti. Te pa tudi pravim hekerjem ne manjka, kar nam dokazujejo na dnevni bazi.

6. ZAKLJUČNI IZZIV

Če potegnemo črto pod različne izzive, ki smo jih nanizali, lahko sklenemo, da je informacijska varnost pomemben del vsake aplikacije ali celotnega informacijskega sistema. Velikokrat se zaradi preprostih napak, ki so nastale zaradi slabega načrtovanja, slabe implementacije ali preprosto človeškega faktorja, izkaže, da imajo aplikacije ali sistemi veliko pomanjkljivosti, ki jih je včasih zelo težko na prvi pogled odkriti. Včasih res zaradi drevesa ne vidimo gozda ali ne vidimo očitnega. Definitivno so zunaj obiskovalci, ki bodo naše aplikacije pogledali drugače ali se spustili tudi v njihovo drobovje in potegnili kakšne zanimive zaključke in na koncu prišli tudi do tistih podatkov, ki smo se jih odločili varovati.

Zaradi takšnih razlogov se splača pomembne aplikacije podvreči zunanjemu testiranju in tudi mogoče kakšnemu pregledu izvorne kode. Naše analize namreč kažejo, da so aplikacije, pri katerih je že ob samem snovanju na začetku razvoja znano, da bodo podvržene pregledu, njihova kvaliteta bistveno boljša in je pri testiranju mogoče najti bistveno manj napak.

Glede na samo naravo testiranja aplikacij pa lahko iz izkušenj zaključimo, da se človeškega ročnega preverjanja ne bomo mogli skoraj nikoli rešiti.

Po drugi strani pa lahko mirno trdimo, da so najboljše rešitve najenostavnejše.