SIGURNOSNI ASPEKTI I ZAŠTITA WEB STRANICA KOD VISOKOŠKOLSKIH USTANOVA NA PRIMJERU SOFTVERA ZA SKENIRANJE RANJIVOSTI

HIGHER EDUCATION INSTITUTIONS SECURITY ASPECTS VULNERBABILITY

dr. sc. MUHAREM KOZIĆ, vanredni profesor
Ekonomski fakultet Univerziteta „Džemal Bijedić“ u Mostaru
prof. dr. MLADEN RADIVOJEVIĆ, redovni profesor
dr. sc. ALEM KOZAR

***Sažetak**: Web stranice ili aplikacije sadrže važne informacije, sigurnost softvera kod obrazovnih institucija je jednako važna kao i sigurnost softvera u bankarskom sektoru. Postoji mnogo akademskih institucija koje nisu u potpunosti implementirale sigurnosne i zaštitne mehanizme svog postojećeg informacionog sistema kako se nebi desio neki napad na ranjive sisteme koji su razvijeni kroz web tehnologije. Web aplikacije su danas ključan faktor da bi se neka usluga prezentovala ili promovisala ciljanoj klijenteli ili da bi neki proizvod došao do potencijalnog kupca. Najveća prednost ove vrste aplikacije je njena nezavisnost od vrste računara, operativnog sistema ili platforme. Rezultati su pokazali da postoje različite vrste ranjivosti na web stranicama univerziteta, a anketom se došlo do zaključka da ½ ispitanih univerziteta u BIH raspolaže sa dovoljno novčanih sredstava za ulaganje u IT sektor, dok ½ ne raspolaže sa dovoljno novca što utiče na sigurnost informacionih sistema, zbog nedostatka stručnog kadra.*

***Ključne riječi:** Web aplikacije, Informacioni sistemi, Akademske institucije, Ranjivosti, Sigurnost web stranice.*

***Abstract:** Websites or applications contain important information, software security with educational institutions is just as important as software security in the banking sector. Many academic institutions have not fully implemented the security and safeguard mechanisms of their existing information system to prevent any attack on vulnerable systems developed through web technologies. Web applications are a key factor for a service to be presented or promoted to a targeted clientele or for a product to reach a potential customer. The biggest advantage of this type of application is its independence from the type of computer,*

operating system or platform. The results showed that there are different types of vulnerabilities on university web sites, and the survey concluded that ½ BiH universities surveyed have enough money to invest in the IT sector, while ½ does not have enough money, which affects the security of information systems. due to lack of professional staff.

Key words: *Web Aplications, Information Systems, Academic Institutions, Vulnerabilities, Web Site Security.*

UVOD

Određena poglavlja u radu su usmjerena na 9 visokoškolskih, akademskih institucija u BiH. Oni su podijeljeni u tri kategorije: državni, privatni univerziteti i visoke škole. Od državnih univerziteta su odabrana 4 univerziteta (Univerzitet u Sarajevu, Univerzitet u Tuzli, Univerzitet u Bihaću i Sveučilište u Mostaru). A od privatnih univerziteta su odabrana dva (Internacionalni univerzitet Travnik, Univerzitet Sinergija Bijeljina. Što se tiće visokih škola odabrano je ukupno tri među kojima su: Visoka škola CEPS - "Centar za poslovne studije" Kiseljak, ITEP - Visoka škola Banja Luka i Visoka škola "Logos centar" Mostar.

Softverski stručnjak za pronalaženje sigurnosnih rupa ili ranjivosti na web stranicama naziva se web skener. Web skeneri pokreću automatsku sigurnosnu reviziju web stranice. Sastoje se od dvije faze: prva je otkrivanje sadržaja, postupak izgradnje strukture mjesta. Nabraja sve datoteke i od vitalnog značaja je da se osigura da se sve datoteke na web stranici skeniraju. Drugo je skeniranje, proces inspekcije intenzivno pronalazeći sigurnosne ranjivosti. Po defaultu, postupak skeniranja uključuje otkrivanje sadržaja. Skeneri se koriste za pronalaženje pukotina i mogućih problema u aplikacijama. Prvo prikupljaju bitne podatke o web aplikaciji kao što su web server, vrsta operativnog sistema, njihova verzija i bilo koje instalirane zakrpe; ove se informacije obično pojavljuju u sistemskom natpisu i korisne su za otkrivanje poznatih ranjivosti na serveru. Pa je mudro sakriti takve informacije od neovlaštenih pojedinaca. U ovom radu korišten je alat za skeniranje web ranjivosti pod nazivom Acunetix.[1] Ovaj softver se koristi za provjeru širokog spektra ranjivosti na web platformi, a uključuje mnoge inovativne funkcije kao što su:

1) Automatski analizator JavaScript,

3) Vizualni makro snimač olakšava testiranje web formi i područja

1 Acunetix Web Vulnerability Scanner, 2008,http://www.acunetix.com/vulnerability-scanner/

koja su zaštićena šifrom,

4) Obimni izvještaji koji uključuju OWASP Top 10 ranjivosti,

5) Inteligentni alat za indeksiranje otkriva vrste web servera i jezik aplikacije,

6) Pregledava i analizira web stranice uključujući flash sadržaj,

Acunetix[2] skener ranjivosti interneta na napade hakera je automatizovana internet aplikacija za testiranje sigurnosti koja kontroliše internet aplikacije provjeravajući ih na osjetljivost na hakerske napade, kao što su SQL injekcije[3], Cross Site Ccripting i druge. Generalno, Acunetix skener ranjivosti interneta na napade hakera skenira bilo koji internet sajt, ili internetsku aplikaciju koja je dostupna preko internetskog pretraživača i koristi HTTP/HTTPS protokol. Acunetix skener ranjivosti interneta na hakerske napade nudi snažno i jedinstveno rješenje za analiziranje internet aplikacija (i softvera koji se individualno pravi za klijente i onog generalno dostupnog u radnjama), uključujući aplikacije koje koriste JavaScript, AJAX i Web 2.0 aplikacije.[4] Sljedeća metodologija, u ovom istraživanju, za određivanje stepena sigurnosti na web aplikaciji uključivala je sljedeće korake. Prvo skeniranje kroz web stranice svakog uzorka i popis svih pronađenih ranjivosti. Zatim dijeljenje pronađene ranjivosti u četiri vrste prema stepenu ozbiljnosti, i to: visoka, srednja, niska i informativna. Kasnije su identifikovane ranjivosti svakog tipa i nabrojane su u posebnim kategorijama prema njihovoj ozbiljnosti i kreirana je tabela za svaki tip.

Analiza

Alat za skeniranje Acunetix otkriva informacije o ciljanom odredištu koje se ispituje i može otkriti vrijedne informacije kao što je korištenje web tehnologija u hostu, operativni sistem koji pokreće web server, verzije softvera sistemskog sistema itd. Ostale informacije o dijagnostici uključuju: distribuciju ukupnih upozorenja za svaku vrstu razine prijetnje (Visoka, Srednja, Niska i Informativna)[5], popis pronađenih ekstenzija file-ova i broj file-ova po ekstenziji (proširenja file-ova mogu pružiti informacije o tome koje se tehnologije koriste na napadnutim web aplikacijama), distribucija

2 Acunetix Web Vulnerability Scanner, 2008,http://www.acunetix.com/vulnerability-scanner/

3 WASC, Classes of attacks, Retrieved from website:http://www.webappsec.org/projects/threat/classes_of_attacks.ht ml

4 National Vulnerability Database, http://nvd.nist.gov

5 Web Application Security Consortium, “Threat Classification”,http://www.webappsec.org/projects/threat/

deset najboljih file-ova koji sadrže najniže vrijeme odziva izmjereno tokom postupka otkrivanja sadržaja (prosječno vrijeme odziva za svaki host izračunava se u milisekundama), distribucija popisa klijentskih skripti koje sadrže Javascript kôd na koji se navodi web stranica (Javascript[6] je potencijalna prijetnja za mnoge vrste napada), popis vanjskih hostova koji su povezani sa web stranicom institucije, i na kraju, lista adresa e-pošte koja se nalazi na ciljanom hostu.

Tabela 1. Prikaz ranjivosti u obrazovnim institucijama BIH

Institucija/Razina	Visoka	Srednja	Niska	Informativna	Ukupan broj upozorenja
Univerzitet u Sarajevu	0	0	0	1	**1**
Univerzitet u Tuzli	1	46	117	31	**195**
Univerzitet u Bihaću	0	0	0	0	**0**
Sveučilište u Mostaru	0	0	9	11	**20**
Internacionalni univerzitet Travnik	1	64	103	247	**415**
Univerzitet Sinergija Bijeljina	1	41	7	44	**93**
Visoka škola CEPS – "Centar za poslovne studije" Kiseljak	2	18	10	13	**43**
ITEP – Visoka škola Banja Luka	0	4	66	758	**828**
Visoka škola "Logos centar" Mostar	0	16	8	6	**30**

Nakon što je alat za skeniranje analizirao ciljane institucije, ogromna količina podataka je prikupljena. Ukupan broj različitih prijetnji pronađenih u svim uzorcima za svaku razinu ranjivosti bio je sljedeći: Visoka 4, Srednja 8, Niska 8 i 13 informativnih prijetnji. Tabela 1 sadrži statistički sažetak o broju ranjivosti pronađenih za svaku vrstu na web stranicama svake institucije ciljanog odredišta. Iz grafikona je lako uočiti zajedničke ranjivosti koje su se uglavnom pojavile na skeniranoj web aplikaciji i njihove procente prema ukupnom broju pronađenih ranjivosti svake razine.

Visoka ranjivost

Ova vrsta ranjivosti je najopasnija vrsta prijetnji koja web aplikaciju stavlja na maksimalni rizik od hakiranja i krađe podataka. Direktno utiče na sigurnost, integritet, privatnost informacija web stranica. Zlonamjerni

6 WebGoat Project. OWASP. http://www.owasp.org/index.php/Category:OWASP WebGoat Project

korisnik može iskoristiti ove ranjivosti i ugroziti rezervnu bazu podataka ili uništiti web aplikaciju. Ukupan broj ranjivosti svih web aplikacija koje su skenirane bio je ograničen na 4. U tabeli 2 je definisan uži popis najozbiljnijih napada koji su otkriveni u aplikacijama obrazovnih institucija a to su *Security Vulnerability in MySQL/MariaDB sql/password.c* sa 25% pojavljivanja, zatim *HTTP Parameter Pollution* sa 25%, *Weak Password* sa 25% i *Cross Site Scripting*[7] također sa 25% pojavljivanja i ove 4 ranjivosti zauzimaju 100% najtežih ozbiljnih napada.

Grafikon 1. Učestalost pojavljivanja ranjivosti visokog rizika

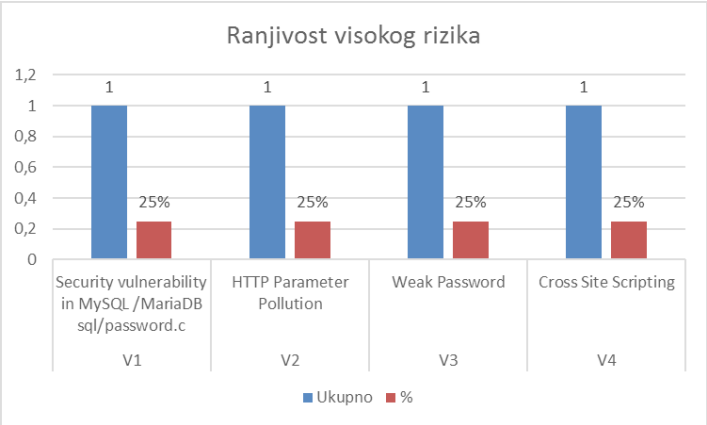


Tabela 2. Ranjivost visokog rizika

Oznaka	Visoka ranjivost	Ukupno	%
V1	Security vulnerability in MySQL /MariaDB sql/ password.c	1	25%
V2	HTTP Parameter Pollution	1	25%
V3	Weak Password	1	25%
V4	Cross Site Scripting	1	25%

Srednja ranjivost

Ranjivosti ove vrste uzrokovane su pogrešnim konfiguracijama servera i nedostacima kodiranja programa koji olakšavaju prekid i propadanje servera. Poruke sa greškom ove vrste mogu otkriti osjetljive informacije. Tabela 3 prikazuje pronađene ranjivosti u srednjoj razini gdje prijetnja *Application error message* zauzima 27,77% pojavljivanja, zatim prijetnja *HTML form without CSRF protection* sa 22,77%, *PHP open_basedir* sa 5,56%, *PHPinfo page found* sa 5,56%, *Source code disclosure* sa 5,56%,

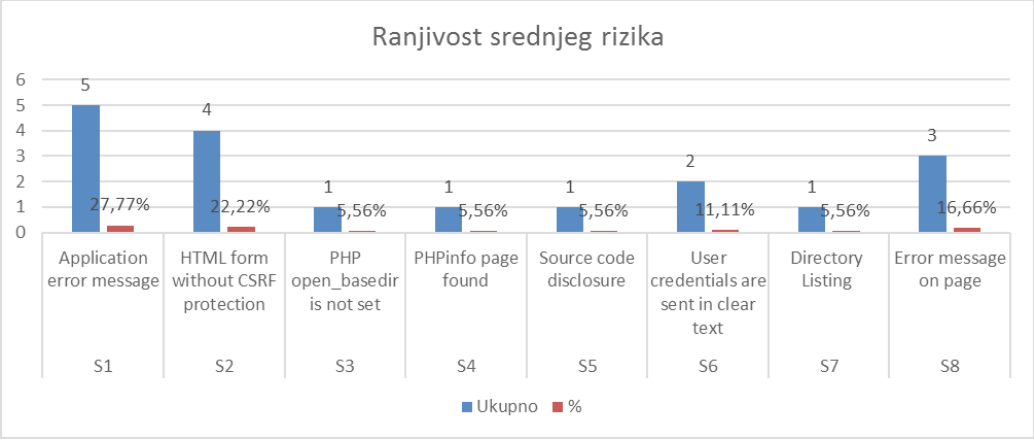
7 Shar, L.K. and Tan, H.B.K. (2012) Automated Removal of Cross Site Scripting Vulnerabilities in Web Applications. Information and Software Technology, 54, 467-478. http://dx.doi.org/10.1016/j.infsof.2011.12.006

User credentials are sent in clear text sa 11,11%, *Directory Listing* sa 5,56% i *Error message on page* sa 16,66%.

Tabela 3. Ranjivost srednjeg rizika

Oznaka	Srednja ranjivost	Ukupno	%
S1	Application error message	5	27,77%
S2	HTML form without CSRF protection	4	22,22%
S3	PHP open_basedir	1	5,56%
S4	PHPinfo page found	1	5,56%
S5	Source code disclosure	1	5,56%
S6	User credentials are sent in clear text	2	11,11%
S7	Directory Listing	1	5,56%
S8	Error message on page	3	16,66%

Grafikon 2. Učestalost pojavljivanja ranjivosti srednjeg rizika



Niska ranjivost

Ove ranjivosti proizilaze iz nedostatka šifriranja prenosa podataka ili otkrivanja putem foldera. Neke od prijetnji koje su otkrivene prilikom skeniranja web aplikacija obrazovnih institucija za nisku ranjivost prikazane su na sljedećem grafikonu 3 i tabeli 4 gdje su otkrivene prijetnje poput *Login page password-guessing attack* koji zauzima 14,81% pojavljivanja, zatim *Possible sensitive directories* sa 14,81%, *Possible sensitive files* sa 14,81, *Session token in URL* sa 3,70%, *Slow response time* sa 11,12%, *Session Cookie without HttpOnly flag test* sa 14,81%, *Session Cookie without Secure flag set* sa 18,53% i *OPTIONS method is enabled* sa 7,41%. Ovih osam predhodno navedenih ranjivosti zauzimaju 100% prijetnji niskog rizika.

Grafikon 3. Učestalost pojavljivanja ranjivosti niskog rizika

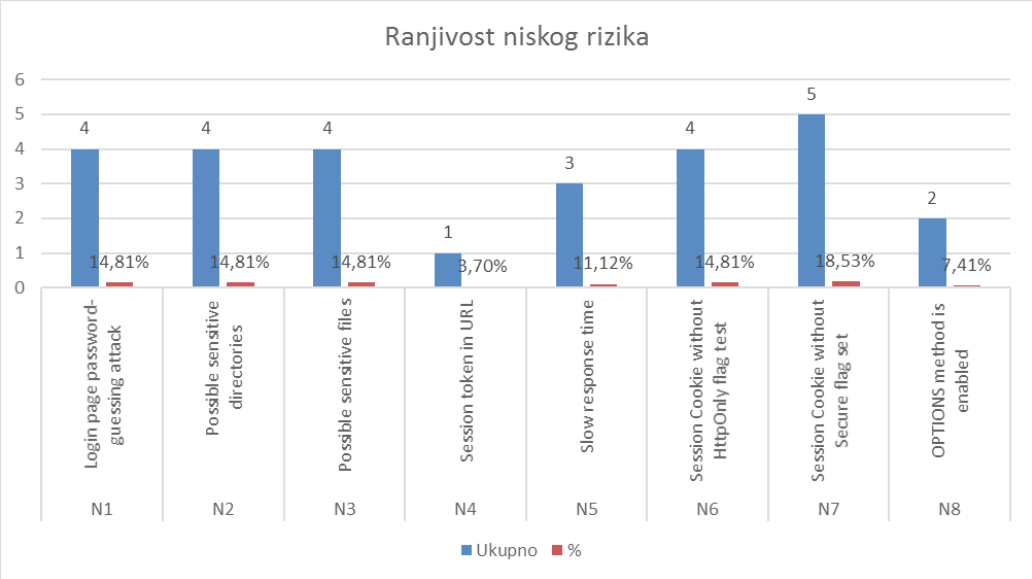


Tabela 4. Ranjivost niskog rizika

Oznaka	Niska ranjivost	Ukupno	%
N1	Login page password-guessing attack	4	14,81%
N2	Possible sensitive directories	4	14,81%
N3	Possible sensitive files	4	14,81%
N4	Session token in URL	1	3,70%
N5	Slow response time	3	11,12%
N6	Session Cookie without HttpOnly flag test	4	14,81%
N7	Session Cookie without Secure flag set	5	18,53%
N8	OPTIONS method is enabled	2	7,41%

Informativna ranjivost

Ova vrsta prijetnji otkriva informacije putem hakerskih nizova pretraživanja ili otkrivanja adresa e-pošte, otkriveno je 13 ranjivosti koje su prikazane na grafikonu 6 i u tabeli 5 iI one čine 100% prijetnji informativnog rizika, dakle softver je otkrio sljedeće prijetnje *Error page web server version disclosure* sa 7,41%, *Broken links* sa 18,52%, *Email address found* sa 22,22%, *GHDB: Administrative login page* sa 3,70%, GHDB: *Possible login page* sa 3,70%, *GHDB: Possible temporary file/directory* sa 3,70%, *Password type input with auto-complete enabled* sa 3,70%, *Possible server path disclosure (Unix)* sa 3,70%, *Possible uername or password disclosure* sa 11,11%, *Content type is not specified* sa 7,41, *Possible Internal IP address disclosure* sa

3,70%, GHDB: *Typical login page* sa 7,41, *Files listed in robots.txt but not linked* sa 3,70%.

Grafikon 4. Učestalost pojavljivanja ranjivosti informativnog rizika

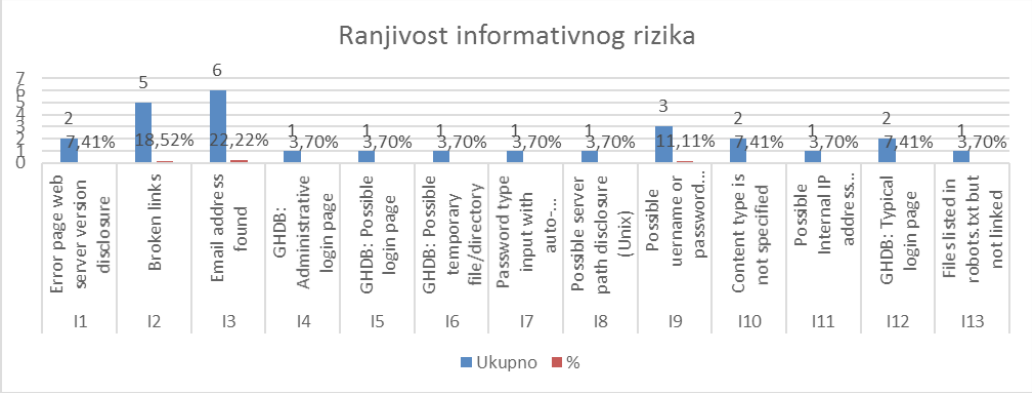


Tabela 5. Ranjivost informativnog rizika

Oznaka	Informativna ranjivost	Ukupno	%
I1	Error page web server version disclosure	2	7,41%
I2	Broken links	5	18,52%
I3	Email address found	6	22,22%
14	GHDB: Administrative login page	1	3,70%
I5	GHDB: Possible login page	1	3,70%
I6	GHDB: Possible temporary file/directory	1	3,70%
I7	Password type input with auto-complete enabled	1	3,70%
I8	Possible server path disclosure (Unix)	1	3,70%
I9	Possible uername or password disclosure	3	11,11%
I10	Content type is not specified	2	7,41%
I11	Possible Internal IP address disclosure	1	3,70%
I12	GHDB: Typical login page	2	7,41%
I13	Files listed in robots.txt but not linked	1	3,70%

ZAKLJUČAK I PREPORUKA

Testiranje web aplikacija koje se radi zbog sigurnosnih ranjivosti je nešto šta treba shvatiti ozbiljno.[8] Rezultati ovog rada otkrivaju skup ranjivosti u web aplikacijama obrazovnih ustanova. Te ranjivosti se kreću u riziku od visoke, srednje, niske do informativne. Proučavani su mnogi razlozi koji stoje iza slabe sigurnosti web aplikacija akademskih organizacija. Predložene su neke od tehnika odbrane kao kontranapada. Glavna lekcija je da sistemi obrazovnih institucija sadrže osjetljive digitalne podatke i informacije koje privlače napadače i prema tome akademske institucije trebaju napraviti reviziju svojih web aplikacija protiv određenih ranjivosti i potencijalnih rizika.

Poželjno je da univerziteti posjeduju jedan od alata (Sniffer ili Acunetix) kako bi skenirali ranjivosti web stranica i time doprinijeli boljoj zaštiti. Mnogi sigurnosni problemi mogu se riješiti iz korijena ako je odgovarajući sigurnosni mehanizam ugrađen u web aplikacije kako bi se osiguralo da u aplikaciji ne postoje potencijalne ranjivosti.

LITERATURA

1. Black, P. E., Fong, E., Okun, V., & Gaucher, R. National Institute of Standards and Technology (NIST). “Software Assurance Tools: Web Application Security Scanner Functional Specification”
2. Acunetix Web Vulnerability Scanner, 2008,http://www.acunetix.com/vulnerability-scanner/
3. National Vulnerability Database, http://nvd.nist.gov
4. WebGoat Project. OWASP. http://www.owasp.org/index.php/Category:OWASP WebGoat Project
5. The OWASP Foundation, “OWASP Top Ten Web Application Security Risks”, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
6. WASC, Classes of attacks, Retrieved from website:http://www.webappsec.org/projects/threat/classes_of_attacks.ht ml
7. Web Application Security Consortium, “Threat Classification”,http://www.webappsec.org/projects/threat/

8 Black, P. E., Fong, E., Okun, V., & Gaucher, R. National Institute of Standards and Technology (NIST). “Software Assurance Tools: Web Application Security Scanner Functional Specification”

8. Shar, L.K. and Tan, H.B.K. (2012) Automated Removal of Cross Site Scripting Vulnerabilities in Web Applications. Information and Software Technology, 54, 467-478. http://dx.doi.org/10.1016/j.infsof.2011.12.006