Summer 8-2020

CYBER SECURITY – PENETRATION TEST

Veton Bejtullahu
University for Business and Technology - UBT

Programi për Shkenca Kompjuterike dhe Inxhinieri

CYBER SECURITY – PENETRATION TEST

Bachelor

Veton Bejtullahu

Gusht / 2020

Prishtinë

Programi për Shkenca Kompjuterike dhe Inxhinieri

Punim Diplome
Viti akademik 2012 – 2013

Veton Bejtullahu

CYBER SECURITY – PENETRATION TEST

Mentori: Prof. Dr. Gazmend Krasniqi

Gusht / 2020

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesshme për Shkallën Bachelor

ABSTRAKT

Si pjesë e rritjes së vazhdueshme të një bote të ndërlidhur mes veti në internet, shteti, infrastrukturat, bizneset dhe të gjithë njerëzit varen nga funksionimi i besueshëm i teknologjisë së informacionit dhe komunikimit. Liria dhe vlera e njerëzve në botën kibernetike duhet mbrojtur ashtu sikur në botën e jashtme. Me numrin e përdoruesve në internet gjithmonë në rritje dhe me teknologjitë e reja, numri i mundësive për sulm së bashku me kompleksitetin e sulmit, po rritet gjithashtu. Rreziku kryesor mbetet krimi kibernetik dhe rritja e tij reflektohet nga zhvillimi i shkathtësive të kriminelëve kibernetik dhe aftësia e tyre për të bërë sulme të organizuara.

Çdo hap i juaji në internet po gjurmohet dhe ruhet, dhe identiteti yt është vjedhur. Privatësia është një luks që pak persona mund ta përballojnë ose kuptojnë (Mitnick, 2017).

Vjedhja e informacionit konfidencial shpesh bëhet për përfitime materiale ose për dëmtime të qëllimshme. Disponueshmëria e lehtë e mjeteve të piraterisë në internet, pajisjet USB dhe lidhjet me Wi-Fi sigurojnë thyerje të lehta. Rezultati është humbje me vlerë prej miliona dollarësh në terma të vjedhjes së IP, rrjedhjes së informacionit të klientit apo individit, etj.

Ky material paraqet një kuptim të kërcënimeve të brendshme, sulmuesve dhe motivit të tyre, si dhe sugjeron teknika parandaluese ndaj sulmeve kibernetike.

MIRËNJOHJE DHE FALËNDERIME

Së pari falënderoj Kolegjin UBT që me programet e veta më mundësoi të studioj Shkencat Kompjuterike që i kam pasion të përjetshëm. Familjen time, që më mbështeti gjatë gjithë kohës dhe investoi jashtëzakonisht shumë në mua. Kolegët dhe miqtë e mi, me të cilët kalova pjesën më të rëndësishme të këtyre viteve të studimeve.

U jam shumë mirënjohës profesorëve dhe asistentëve në fakultet, për punën dhe rolin e tyre në aftësimin tim. Falënderoj veçanërisht mentorin Prof. Gazmend Krasniqi dhe co-mentorin Prof. Atdhe Buja që më ndihmuan dhe sugjeruan gjatë punimit të kësaj teme të diplomës. Ata gëzojnë nderimin tim të thellë.

PËRMBAJTJA

LISTA E FIGURAVE

LISTA E TABELAVE

FJALORI I TERMAVE

Wi-Fi – Wireless Fidelity

LAN –Local Area Network

WAN –Wide Area Network

HTTP – HyperText Transfer Protocol

URL – Uniform Resource Locator

DNS – Domain Name System

URL – Uniform Resource Locator

WLAN –Wireless Local Area Network

DHCP – Dynamic Host Configuration Protocol

HTML –Hypertext Markup Language

UI – User Interface

TLS – Transport Layer Security

SSL – Secure Sockets Layer

SQL – Structured Query Language

DOS – Disk Operating System

CSRF – Cross-Site Request Forgery

DDoS – Distributed Denial of Service

VPN – Virtual Private Network

VM – Virtual Machine

1. HYRJE

Në këtë temë do të flasim për Sigurinë Kibernetike, rëndësinë që ka informacioni dhe privatësia në ditët e sotme, si dhe mënyrat e mbrojtjes në internet.

Qeveritë dhe udhëheqësit e industrisë nga çdo sektor i madh njohin gjerësisht rëndësinë e forcimit të fushës së sigurisë kibernetike. Shkalla e zhvillimit teknologjik po prodhon një sfidë të madhe me ndryshim të shpejtë. Zhvillimet transformuese në fuqinë kompjuterike, cloud computing, celularë, inteligjencën artificiale, ndërlidhshmërinë e kudogjendur dhe sistemet e automatizuara në shkallë të gjerë po sjellin shqetësime të reja dhe të fuqishme për sigurinë kibernetike dhe privatësinë. Implikimet për kërcënimet e ardhshme për privatësinë dhe sigurinë janë të dëmshme dhe mund të jenë ndërlikim për dekadat që do të vijnë. Besimi i publikut në integritetin e sistemeve financiare globale, rrjeteve të informacionit dhe sistemeve të tjera të infrastrukturës kritike është thelbësor për rritjen e vazhdueshme ekonomike, sigurinë publike dhe inovacionin. Ruajtja dhe sigurimi i ekosistemeve digjitale të përmirësuara, të sigurta dhe të besueshme është jetik për të mbrojtur të dhënat organizative dhe personale kundër një vargu gjithnjë e më të madh të kërcënimeve (R. Jashari, 2018).

Si pjesë e ruajtjes dhe mirëmbajtjes së këtyre sistemeve është Penetration Test, që shërben për njohjen dhe shfrytëzimin e nivelit të sigurisë së sistemeve në botën kibernetike.

Rasti i studimit në këtë temë do t'i kushtohet Web Application Penetration Testing, i cili na ndihmon të gjejmë dobësitë e webfaqeve të targetuara.

2. DEKLARIMI I PROBLEMIT

Rrethanat e shtjellimit të kësaj teme janë problemet aktuale të shoqërisë tonë të cilat kanë të bëjnë direkt me keqpërdorimin e të dhënave dhe sigurinë e njerëzve në internet. Përfitimi i madh që vjen nga teknologjia, sjell gjithashtu rreziqet e mëdha që bëhen nga automatizimi i saj duke cënuar kështu privatësinë e çdo njërit prej nesh. Mungesa e njohurive nga shumica e njerëzve për Sigurinë Kibernetike paraqet problem të madh për ta dhe njëkohësisht ua lehtëson punën hakerëve të ndryshëm.

Sipas CISCO, mbi 30% e organizatave kanë përjetuar sulme kibernetike në infrastrukturën teknologjike të operimit. 100 mijë grupe në 150 shtete dhe më shumë se 400 mijë kompjuterë janë infektuar vetëm nga virusi WannaCry Ransomware në vitin 2017, i cili pastaj pësoi rënie të dukshme në vitin 2018. Megjithatë, në vitin paraprak kishte shkaktuar dëm prej 4 bilion dollarësh. Ky virus, së bashku me 90% e Malware-ve shpërndahet përmes e-mail.

Kosto e krimit kibernetik ka shtyrë organizatat që në vitin 2017 të shpenzojnë 23% më shumë se sa në vitin paraprak, një mesatare prej rreth 11 milion dollarë. Ndërsa kosto kohore për një sulm është 50 ditë. Më shumë se 53 mijë incidente të sigurisë kibernetike kanë ndodhur në vitin 2018. Deri në vitin 2021, parashihet që dëmi i shkaktuar të arrijë në 6 trilion dollarë. Komponenti më i shtrenjtë i një sulmi kibernetik është humbja e informacionit, që përfaqëson 43% të kostove. 41% e kompanive kanë mbi 1 mijë fajlla të ndjeshme duke përfshirë numra të kredit kartelave dhe të dhëna shëndetësore të cilat qëndrojnë të pambrojtura (Sobers, 2018).

Pra, problemi dhe sfida kryesore sot në botën e internetit është mbrojtja e të dhënave dhe parandalimi i hakimeve të tilla.

3. SHQYRTIMI I LITERATURËS

3.1 Çka është Penetration Testing?

Penetration Testing apo Pen Test është procesi i përpjekjes për të fituar qasje në burime pa dijeninë e emrit të përdoruesve, fjalëkalimeve dhe mjeteve të tjera normale të qasjes. Nëse fokusi është në burimet kompjuterike, atëherë shembujt e një depërtimi të suksesshëm do të ishin marrja ose shkatërrimi i dokumenteve konfidenciale, çmimeve, bazave të të dhënave dhe informatave të tjera të mbrojtura. Gjëja kryesore që e dallon një Penetration Tester nga një sulmues është autorizimi. Penetration Tester do të ketë leje nga pronari i atyre burimeve informatike që janë duke u testuar dhe do të jetë përgjegjës për të dhënë një raport.

3.2 Pse Penetration Testing?

Përkundër faktit që sulmet kibernetike janë rritur ndjeshëm, shumë kompani apo organizata sot ende nuk e monitorojnë sigurinë e infrastrukturës së tyre në mënyrë aktive dhe kështu mbesin një pre e lehtë për keqbërësit apo hakerët. Sapo të lidhen në internet, sistemet e kompanive mund të kontrollohen, skanohen apo edhe të sulmohen.

Qëllimi i testit të penetrimit është njohja e nivelit të sigurisë dhe rritja e sigurisë së burimeve informatike që testohen. Pra, një ndër hapat e parë drejt parandalimit të sulmeve kibernetike është pikërisht Penetration Test.

3.3 Benefitet e Penetration Testing?

Penetration testing lejon testuesit që të shikojnë sistemin e klientit përmes syve të hakerëve keqdashës. Një proces i tillë mund të sjellë një numër të madh zbulimesh dhe të i'a sigurojë klientit kohën e nevojshme që të riparojë sistemin para se të ndodhë sulmi në të vërtetë. Si shtesë, penetration testing mund të ndihmojë organizatat dhe kompanitë që të vërtetojnë efektivitetin apo mosefektivitetin e masave të sigurisë që janë implementuar, duke demonstruar në mënyrë eksplicite dobësitë e sigurisë në sistem. Për më me rëndësi, ky testim siguron evidencë për të alarmuar menaxhmentin për nevojën që ta marrë më seriozisht sigurinë e informacionit (Hardy, 1997).

3.4 Vulnerability Assessment dhe Penetration Test – Si bëhet një testim?

Vulnerability Assessment apo vlerësimi i cenueshmërisë dhe testimi i penetrimit është një proces total i 9 hapave, të cilët tregohen në figurën 1.

Para së gjithash, testuesi duhet të vendosë fushëveprimin e detyrës (black / grey / white box). Pas vendosjes së fushës, testuesi merr informacione për sistemin operativ, rrjetin dhe IP adresën në hapin e zbulimit. Pas kësaj, ai përdor teknika të ndryshme të vlerësimit të cenueshmërisë në objektin e testimit për të gjetur dobësi. Pastaj testuesi analizon dobësinë e gjetur dhe bën planin për testin e penetrimit. Testuesi përdor këtë plan për të depërtuar në sistemin e viktimës. Pas depërtimit në sistem, ai rrit privilegjin në sistem. Në hapin e analizës së rezultateve, testuesi analizon të gjitha rezultatet dhe përpilon rekomandime për të zgjidhur dobësitë që ka sistemi.

Të gjitha këto aktivitete dokumentohen dhe dërgohen tek menaxhmenti për të ndërmarrë veprimet e përshtatshme. Pas gjithë këtyre hapave, sistemi i viktimës dhe programi i tij preken dhe ndryshohen. Në hapin e pastrimit sistemi rivendoset në gjendjen e mëparshme ashtu siç ishte para fillimit të procesit (Goel, 2015).

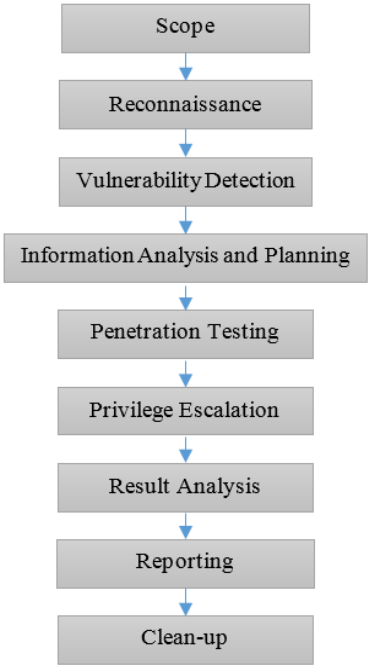

Figura 1 – Cikli i Vulnerability Assessment dhe Penetration Testing

3.5 Metodologjitë dhe teknikat

3.5.1 Metodologjitë e penetration testing

Pasi që shumica e testeve të penetrimit të rrjetit apo sistemit ndajnë disa faza kryesore, shumë profesionistë të sigurisë kanë prezantuar metodologji të ndryshme për të kryer një test penetrimi duke filluar nga ato të thjeshta në proceset më të sofistikuara dhe formale.

Në përgjithësi, pen test përfshin tre faza kryesore që imitojnë hapat që do të përdoreshin nga hakerët e vërtetë për të kryer një sulm (Vacca, 2010). Tri fazat përkatëse janë: para-sulmi, sulmi dhe post-sulmi. Faza e para-sulmit tenton të hetojë ose të eksplorojë objektivin. Faza e sulmit përfshin thyerjen aktuale të objektivit. Së fundmi, faza e pas-sulmit, e cila është unike për ekipin e testimit të penetrimit, tenton të kthejë çdo sistem të modifikuar në fazën e mëparshme para fillimit të testeve (Phong, 2014).

Një metodologji bazike e Penetration testing përfshin 3 hapat e paraqitur në figurën 2.

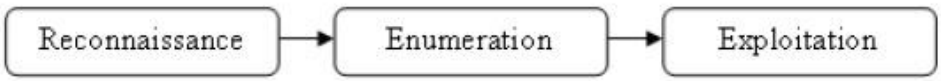

Figura 2 – Metodologjia bazike e penetration testing

Reconnaissance (Zbulimi)

E njohur edhe si Mbledhja e Informacioneve, ky është procesi i kërkimit të informacionit në dispozicion që përdoret në penetration test. Varësisht nga fusha e testimit, aktivitetet e zbulimit mund të përfshijnë mbledhje të ping-ut për të zbuluar IP adresa në rrjet, marrje të informacionit të dobishëm nga punëtorët e kompanisë, hulumtim në mbeturinat e kompanisë për të gjetur fatura të telekomunikimit, e deri tek vjedhja, gënjimi i njerëzve, ndërhyrja në telefonata dhe rrjet. Kërkimi i informacionit është i limituar nga vullneti dhe sjelljet etike të dakorduara ndërmjet klientit dhe ekipit të penetrimit (Osborne, 2006).

Enumeration (Numërimi)

Ky është procesi ku informacioni fitohet direkt nga sistemi i targetuar, aplikacionet, dhe rrjetet me ndihmën e mjeteve (tools) dhe teknikave në mënyrë që të ndërtohet pamja e mjedisit të kompanisë. Numërimi i rrjetit krijon një pamje të konfigurimit të rrjetit që testohet, ndërsa numërimi pritës identifikon shërbimet në dispozicion në pajisje të ndryshme si firewalls, routerë dhe web server, dhe zbulon funksionet e tyre së bashku me hapjen e porteve që mund të përdoren për të depërtuar në sistem. Me anë të këtij procesi identifikohen dhe renditen edhe dobësitë potenciale (Shewmaker, 2008).

Exploitation (Shfrytëzimi)

Faza e shfrytëzimit përdor mjete të ndryshme të automatizuara, teknika dhe hapa manuale të rregulluara në mënyrë specifike për të kompromet uar sistemin përmes dobësive të identifikuara ose kanaleve të tjera që janë gjetur të hapura (Tiller, 2001). Qëllimi përfundimtar i këtij procesi është të sigurojë qasje administrative në sistem.

Ndërsa metodologjia më formale e penetration testing e ndërtuar rreth këtyre 3 hapave, zakonisht përfshin më shumë nën-aktivitete, të paraqitura në figurën 3.

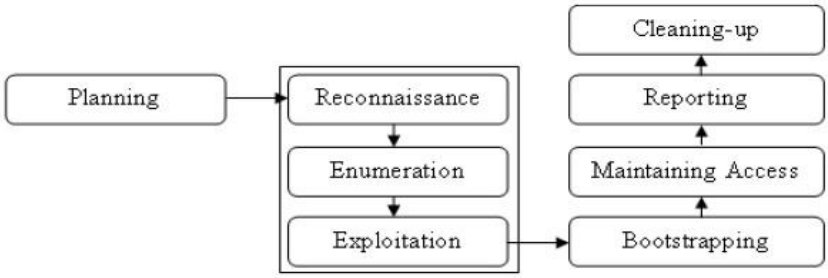

Figura 3 – Metodologjia formale e penetration testing

Planning apo planifikimi është hapi i parë i cili ndikon në rezultatin e testimit. *Bootstrapping* është aktiviteti që starton procesin përsëri për të shikuar nëse ka dobësi të reja. Hapi më i rëndësishëm është *Reporting*, ku një raport i mirë duhet të përbëhet nga përshkrime të qarta të problemeve së bashku me ndikimet e tyre të mundshme, vlerësimi i nivelit të sigurisë, së bashku me numrin e rekomandimeve praktike për klientët për të zvogëluar apo mënjanuar në tërësi dobësitë e tilla.

3.5.2 Teknikat e penetration testing

Black box testing

Në këtë teknikë, testuesi nuk ka ndonjë njohuri paraprake të arkitekturës së rrjetit ose sistemeve të rrjetit të testimit. Zakonisht testimi black box kryhet nga rrjeti i jashtëm në rrjetin e brendshëm. Testuesi duhet të përdorë ekspertizën dhe aftësitë e tij për të kryer këtë testim.

Grey box testing

Në këtë teknikë, testuesi ka disa njohuri të pjesshme të rrjetit të testimit. Testuesi nuk ka njohuri për arkitekturën e plotë të rrjetit, por ai njeh disa informacione themelore për testimin e rrjetit dhe konfigurimin e sistemit. Në të vërtetë, testimi Grey box është kombinimi i dy teknikave të tjera. Ky mund të kryhet nga rrjeti i brendshëm ose i jashtëm.

White box testing

Testeri ka njohuri të plota mbi konfigurimin e rrjetit të testimit. Zakonisht ky testim kryhet nga brenda. White box kërkon një kuptim të thellë të rrjetit apo sistemit dhe jep rezultatet më të mira. Sfida kryesore me këtë lloj testimi është analizimi i sasisë masive të të dhënave në dispozicion për të identifikuar pikat e mundshme të dobësisë, duke e bërë atë llojin e testimit që konsumon kohë më së shumti.

3.6 Web Application Penetration Test

Web Application Penetration Test është procesi që teston një webfaqe apo web aplikacion duke përdorur teste manuale ose automatike të penetrimit për të identifikuar ndonjë dobësi, të meta të sigurisë ose kërcënim. Testimi përfshin përdorimin apo implementimin e ndonjë sulmi të njohur në aplikacion. Testeri fabrikon sulme dhe mjedis prej perspektivës së sulmuesit, sikur përdorimin e testimeve me SQL Injection. Qëllimi kyq i web application penetration testing është të identifikojë dobësi të sigurisë përgjatë gjithë rrjetit të web aplikacionit the komponenteve të tij (source code, databazë, dhe rrjetin back-end). Poashtu ndihmon që të prioritizohen dobësitë e identifikuara, dhe mënyrat për t'i mënjanuar ato. Pra, dobësinë më të madhe që ekziston, testimi do ta shfaq në fillim të raportit.

3.7 Web vulnerabilities

Një dobësi e webfaqes (web vulnerability) është një dobësi apo keq-konfigurim në një kod të webfaqes ose web aplikacionit që lejon sulmuesin të përfitojë kontroll mbi faqen dhe ndoshta host serverin. Shumica e dobësive shfrytëzohen përmes mjeteve të automatizuara, si vulnerability scanners apo botnets. Kriminelët kibernetik krijojnë mjete të specializuara për kërkim në internet të platformave të caktuara, duke shikuar për dobësi të zakonshme dhe të publikuara. Pasi të gjenden, këto dobësi shfrytëzohen më pas për të vjedhur të dhëna, për të shpërndarë përmbajtje me qëllim të keq ose për të injektuar dëmtime dhe përmbajtje spam në faqen e dobët.

3.7.1 Tipet e Web vulnerabilities

Sipas OWASP - Open Web Application Security Project, ekzistojnë dhjetë lloje të zakonshme të dobësive në websajte dhe internet, të cilat shfrytëzohen nga sulmuesit. Përderisa këto nuk janë të gjitha dobësitë e mundshme që një sulmues mund të gjejë në një aplikacion, por përfshihen më të shpeshtat që gjenden sot në internet. Disa prej tyre janë:

1. **SQL Injection:**

   Kjo është një dobësi e sigurisë që lejon një sulmues të ndryshojë deklaratat e backend SQL duke manipuluar të dhënat e plotësuara nga përdoruesi.

   - Një sulmues mund të injektojë përmbajtje me qëllim të keq në fushat e rrezikuara.
   - Të dhënat e ndjeshme si Emrat e Përdoruesit, Fjalëkalimet etj. mund të lexohen nga baza e të dhënave.
   - Të dhënat e bazës së të dhënave mund të modifikohen (Insert / Update / Delete).
   - Operacionet e Administratës mund të ekzekutohen në bazën e të dhënave

2. **Cross Site Scripting (XSS):**

   Dobësitë e XSS synojnë skriptet e futura në një faqe që ekzekutohen në anën e klientit, përkatësisht në shfletuesin e përdoruesit dhe jo në anën e serverit. Këto defekte mund të ndodhin kur aplikacioni merr të dhëna të pasigurta dhe i dërgon në shfletuesin e internetit pa miratimin e duhur.

- Duke përdorur këtë dobësi të sigurisë, një sulmues mund të injektojë skripta në aplikacion, mund të vjedhë cookies të sesionit, të fshijë faqet e internetit dhe mund të shkarkojë programe malware në makinat e viktimave.

3. **Cross Site Request Forgery**

   Sulmi CSRF është një sulm që ndodh kur një faqe interneti me qëllim të keq, një email ose një program i shkakton një shfletuesi të përdoruesit për të kryer një veprim të padëshiruar në një vend të besuar për të cilin përdoruesi aktualisht është i vërtetuar. Një lidhje do të dërgohet nga sulmuesi tek viktima kur përdoruesi klikon në URL dhe pasi të futet në faqen origjinale të internetit, të dhënat do të vidhen nga aty.

   - Duke përdorur këtë dobësi si një sulmues mund të ndryshohet informacioni i profilit të përdoruesit, ndryshohet statusi, krijohet një përdorues i ri për emrin e administratorit, etj.

3.8 Vulnerability scanners

Një vulnerability scanner apo skaneri i dobësive është një program kompjuterik i dizajnuar për të testuar dhe vlerësuar kompjuterët, sistemet kompjuterike, rrjetet ose aplikacionet për dobësi të njohura. Nëse vrimat e sigurisë zbulohen nga skaneri i dobësive, mund të kërkohet zbulimi i nivelit të cenueshmërisë. Personi ose organizata që zbulon dobësitë ose një organ përgjegjës si Ekipi i Gatishmërisë për Emergjenca Kompjuterike (CERT), mund të bëjë zbulimin, nganjëherë pas njoftimit të klientit dhe i lejon atyre një kohë të caktuar për të korrigjuar ose zbutur problemin. Ekziston një numër i madh i këtyre programeve komerciale dhe open source, dhe të gjitha këto kanë përparësitë apo dobësitë e veta, varësisht nga lloji dhe sistemi që punojnë. Disa prej programeve më të njohura për skanim janë:

- Acunetix, Nessus, Nmap, Burp Suite, Netsparker, N-Stealth, Nikto, Vega etj.

3.9 Krahasimi i mjeteve dhe metodave ekzistuese

Pasi që kemi shumë lloje të mjeteve për të bërë një testim, natyrisht se ato dallojnë mes vete për mënyrën se si bëhet testimi dhe njëkohësisht rezultatin apo sasinë e informatave që tregojnë në fund. Me një kërkim të thjeshtë në internet mund të gjejmë open source tools (mjete që janë të lira për këdo), por shumica prej tyre vijnë me një periudhë të caktuar kohore që mund të punojnë pa pagesë. Kjo do të ndikojë që testimi jonë të jetë më i thjeshtë dhe pa ndërlikime, por gjithsesi se do t'i tregojë dobësitë kryesore që ka sistemi apo aplikacioni.
Pra, një open source tool do të mjaftonte për një testim personal të sistemit apo faqes tuaj.
Në anën tjetër, programet komerciale që vijnë me pagesë ofrojnë shumë më tepër opsione dhe shërbime rreth testimit dhe rezultateve finale. Këto përdoren nga testuesit profesional që angazhohen për gjetjen e dobësive në organizata dhe kompani të mëdha.

3.9.1 Windows vs. Linux vs. MacOS

Disa mjete punojnë në mënyrë të barabartë në të dyja sistemet, derisa ka mjete tjera që janë lansuar vetëm për njërën nga këto platforma. Në qoftë se vendosni të punoni në vetëm një OS (Sistem Operativ) p.sh. në Windows, do të humbni shumë nga mjetet dhe teknikat tepër të dobishme që gjenden në Linux. Për të rritur efikasitetin dhe për të përmirësuar rezultatin, sugjerohet që të virtualizohet një nga këto dy OS. Duke përdorur VMware (Virtual Machine), e cila aktivizon një OS brenda sistemit aktual, dhe duke drejtuar të dyja në të njëjtën kohë në të njëjtin harduer ju mundëson që të kaloni shpejt nga Windows në Linux dhe anasjelltas.
Në anën tjetër, MacOS është një platformë shumë stabile nga aspekti i sigurisë dhe lehtë e përdorueshme. Mjetet si Nmap dhe Nikto mund të përdoren edhe në produktet e Apple. Megjithatë, ekzistojnë disa mjete për Linux dhe Windows që nuk mund të funksionojnë në MacOS. Përsëri edhe në këtë rast, mund të aplikoni formën e virtualizimit të një OS tjetër brenda në Mac duke përdorur VMware Fusion e cila mundëson lansimin e Windows apo Linux mbi sistemin MacOS.
Pra, jo medoemos duhet të zgjidhni vetëm njërin sistem apo paketë mjetesh, kur keni mundësi t'i kombinoni ato mes vete dhe të siguroni një performancë më të mirë të testimit dhe rezultat final sa më të detajuar.

3.9.2 Lloji i duhur i testimit

Qëllimi, rezultati, shkathtësia e nevojitur dhe kosto dallojnë mes vete në testime të ndryshme. Kompania IT Governance Ltd në Angli që kryen shërbimin e penetration test ka ofruar spjegim për llojin e duhur të testimit. Në tabelën 1 janë të paraqitura nivelet e testimit që ju përshtaten sipas buxhetit dhe nevojave teknike.

Tabela 1 – Cili nivel i Penetration Testing është i duhur për ju?

	Level 1	**Level 2**
Qëllimi	Për të përcaktuar dobësitë e mundshme dhe mënyrën se si të përmirësohen ato në rend të prioritetit.	Për të identifikuar shtrirjen e plotë të ekspozimit tuaj ndaj një hakeri, të dhënat që mund të ketë akses ose dëmtimet që mund të shkaktojë.
Rezultati	Identifikimi dhe analizimi i dobësive në mënyrë që të bëhet një përgjigje proporcionale drejt rehabilitimit.	Ky vlerësim më i plotë i sigurisë tuaj mundëson të merrni vendime më të informuara rreth investimit në sigurimin e sistemeve kritike të biznesit tuaj.
Organizata e targetuar	Ju keni një ekspozim ndaj sulmuesve oportunistë që kërkojnë webin për targete të lehta dhe dëshironi të siguroheni përtej një vulnerability scan.	Aplikacioni juaj bartë të dhëna të ndjeshme ose personale dhe kryen një rol kritik për misionin në biznesin tuaj dhe mund të ekspozohet ndaj një sulmi.
Niveli i shkathtësisë	Lartë	Avancuar
Imiton një sulm real	Rikrijon fazat e hershme të një sulmi, duke ju ndihmuar që të rrini jashtë radarëve të hakerëve.	Emulim i plotë i një sulmi në web aplikacionin tuaj për nxjerrjen e të dhënave ose dëmtimin e besimit të përdoruesit.
Objektivi	Marrëveshje në fillim	Marrëveshje në fillim
Paketë me çmim fiks	Po	Jo
Thirrja e zbulumit me këshillues	Në dispozicion	Po
Metodologjia e testimit	Qasje e drejtuar nga kërcënimet	Qasje e drejtuar nga kërcënimet
Skanimi i dobësive	Po	Po
Mund të kryhet në vend	Po	Po
Mund të kryhet nga distanca	Po	Po
Identifikimi i false positive	Po	Po
Shfrytëzimi i dobësive	Jo	Po
Raport i detajuar	Po	Po
Vlerësimi manual i rrezikut dhe ndikimit	Po	Po

3.10 Vulnerability Assessment and Penetration Testing Tools

Secili mjet ka përparësitë e veta, por pasi gjendet një numër i madh i tyre në dispozicion, gjithsesi se duhet të veçohen disa mjete që funksionojnë më mirë apo më shpejtë se të tjerat. Në tabelën 2 kemi të paraqitura programet dhe mjetet më të sofistikuara që gjenden në tregun e sotëm, përshkrimet për llojin e licensës që nevojitet, përdorimin e tyre si dhe sistemin operativ mbi të cilin mund të funksionojnë ato. Cross-platform do të thotë që programi në fjalë funksionon në të gjitha sistemet operative që janë cekur më lart.

Tabela 2 – Mjetet e Vulnerability Assessment dhe Penetration Testing

Nr.	Emri	Licensa	Tipi	Sistemi Operativ
1.	Metasploit	Commercial	Vulnerability scanner and exploit	Cross-platform
2.	Nessus	Commercial	Vulnerability scanner	Cross-platform
3.	Kali Linux	Open Source	Collection of various tools	Linux
4.	Acunetix	Commercial/Free (limited)	Web application vulnerability scanner	Windows
5.	Burp Suite	Commercial/Free (limited)	Web application vulnerability scanner	Cross-platform
6.	Nmap	Open Source	Vulnerability scanner and exploit	Cross-platform
7.	N-Stealth	Commercial	Web application vulnerability scanner	Windows
8.	Netsparker	Commercial/Free (limited)	Web application vulnerability scanner	Windows
9.	OpenVAS	Open Source	Vulnerability scanner	Windows, Linux
10.	Vega	Open Source	Web application vulnerability scanner	Cross-platform
11.	Nikto	Open Source	Web application vulnerability scanner	Unix, Linux
12.	Wireshark	Open Source	Network scanner	Cross-platform
13.	Sqlmap	Open Source	Database vulnerab. scanner and exploit	Cross-platform
14.	OWASP ZAP	Open Source	Web application vulnerability scanner	Cross-platform
15.	Aircrack-ng	Open Source	Wi-Fi network security scanner	Cross-platform

4. RASTI I STUDIMIT – Web Application Penetration Testing

4.1 Procesi i Web Penetration Testing

Pasi që kemi marrur programin dhe jemi regjistruar, në këtë rast me programin Acunetix fillojmë procesin e testimit të webfaqes së dëshiruar. Në anën e majtë të menu, zgjedhim **Targets** e cila përmban listën e faqeve të testuara më herët dhe mundësinë e shtimit të targeteve të reja. Klikojmë butonin **Add Target** dhe fillimisht shkruajmë URL e webfaqes, pastaj zgjedhim llojin e Skanimit, opsionet e të cilit shihen në Figurën 6.

Vazhdojmë me llojin e Raportit që dëshirojmë të shohim në fund (Affected Items, Developer, Executive Summary, Quick). Klikojmë butonin **Create Scan** dhe kështu kemi filluar skanimin apo testimin e faqes së caktuar.

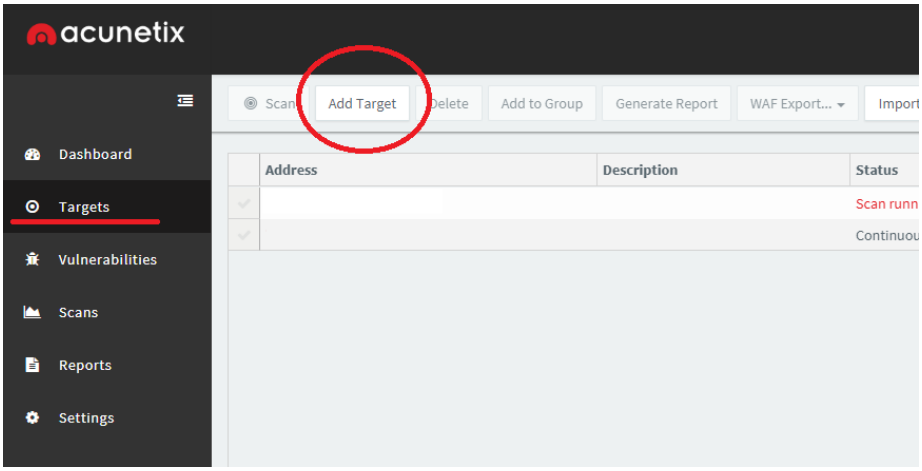

Figura 4 – Add Target

Figura 5 – Vendosja e URL të webfaqes

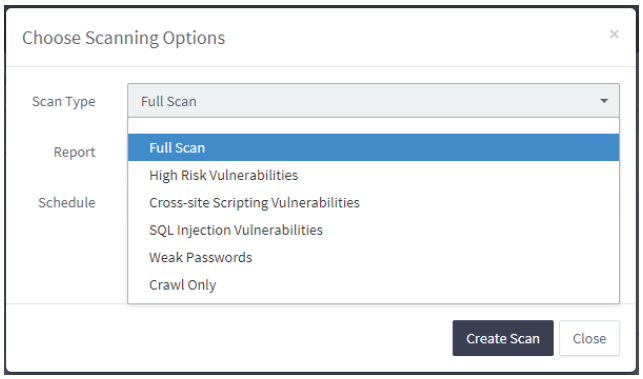

Figura 6 – Zgjedhja e llojit të Skanimit dhe Raportit

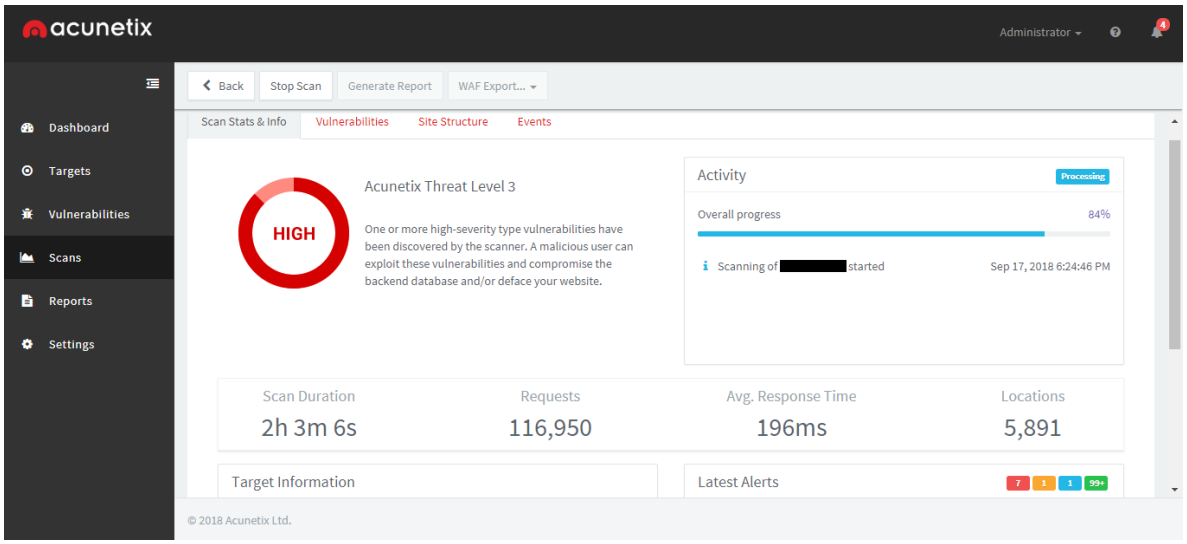

Figura 7 – Penetration Testing në progres

Procesi i testimit nuk ka kohëzgjatje të caktuar. Varësisht nga përmbajtja e faqes ai mund të jetë disa minutësh apo disa orësh. Gjatë procesit, mund të shikojmë Requests që dërgohen në server dhe kohën mesatare të përgjigjeve që mirren.

Butonat **Vulnerabilities** dhe **Site Structure** tregojnë listën e dobësive në kohë reale sapo të zbulohen si dhe strukturën apo formën që ato kanë brenda në webfaqe.

Butoni **Events** përmban informata shtesë rreth kohës kur ka nisur skanimi.

Target Information jep të dhëna si: emri i webfaqes, lloji i serverit që mban faqen, sistemi operativ dhe a është webfaqja responsive apo jo.

Latest alerts tregon numrin e dobësive për nivelet High, Medium, Low dhe Informational.

Tashmë në skanim të thellë, në figurën 7 shohim se testimi ka dërguar mbi 100 mijë requests dhe ka gjetur 7 dobësi të nivelit të lartë (High), 1 mesatare (Medium), 1 të ulët (Low), dhe mbi 200 Informational, ku këto të fundit nuk paraqesin ndonjë rrezik të theksuar.

Pasi të ketë përfunduar skanimi, klikojmë butonin **Generate Report** dhe programi përgatit raportin të cilin mund ta shkarkojmë në formatin PDF.

Edhe nëse gjatë procesit kemi klikuar butonin **Stop Scan**, prap kemi mundësi që të gjenerojmë raport i cili paraqet të gjitha që janë gjetur deri në momentin e ndaljes. Megjithatë, kjo metodë nuk rekomandohet pasi mund të humbasim ndonjë informacion të vlefshëm.

4.2 Përmbledhje e targeteve të testuara

Me lejen e pronarëve të tyre, për këtë rast të studimit janë testuar disa webfaqe për dobësi (vulnerabilities) përmes programit NetSparker dhe Acunetix.
Me gjetjen e këtyre dobësive mund të kemi njohuri se a është faqja e caktuar në rrezik nga sulmuesit, për çasje në informata sensitive apo bllokimin e saj.
Raporti përbëhet nga gjetjet e dobësive në këto faqe, rreziku potencial që ato përmbajnë, si dhe sugjerime për t'i zvogëluar e mënjanuar ato probleme në mënyrë që të parandalojmë sulmet potenciale. Në fund, raporti do të dorëzohet tek pronarët e webfaqeve dhe zhvilluesit e tyre, që të vazhdojë procesi i përmirësimit të dobësive dhe vrimave të sigurisë në ato webfaqe, duke u mbrojtur kështu nga rreziku i hakimit.

Për shkak të sigurisë dhe konfidencialitetit në mes të testuesit dhe klientit, emrat e webfaqeve të testuara nuk do të tregohen por do të shënohen me numra:

1. Targeti 1
2. Targeti 2
3. Targeti 3

4.3 Gjetjet e dobësive - Vulnerabilities

4.3.1 Targeti 1:

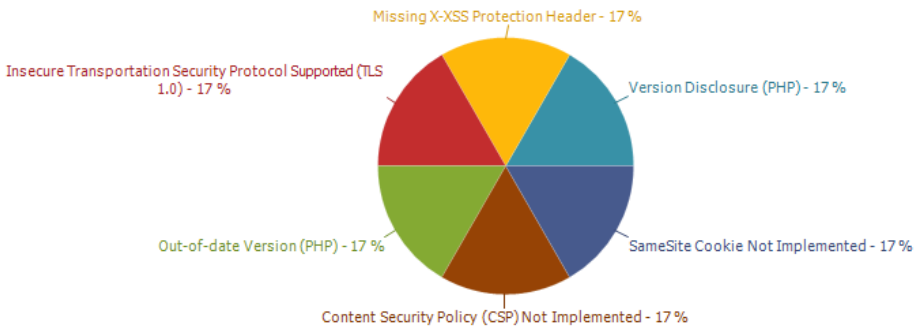

Figura 8 – Rezultatet e testimit të Targetit 1

Emri i dobësisë:

1.1 Cookie Not Marked as Secure – High Risk

Përshkrimi i dobësisë:

This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of PHP.

Rreziku:

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (*such as a session cookie*), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Sugjerim:

1. See the remedy for solution.
2. Mark all cookies used within the application as secure. If the cookie is not related to authentication or does not carry any personal information, you do not have to mark it as secure.
3. Mark all cookies used within the application as secure.

Emri i dobësisë:

1.2 Version Disclosure (PHP) – Low Risk

Përshkrimi i dobësisë:

We have identified a cookie not marked as secure, and transmitted over HTTPS.

This means the cookie could potentially be stolen by an attacker who can successfully intercept and decrypt the traffic, or following a successful man-in-the-middle attack.

This cookie will be transmitted over a HTTP connection, therefore if this cookie is important (such as a session cookie), an attacker might intercept it and hijack a victim's session. If the attacker can carry out a man-in-the-middle attack, he/she can force the victim to make an HTTP request to steal the cookie.

Rreziku:

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Sugjerim:

Configure your web server to prevent information leakage from the SERVER header of its HTTP response.

Emri i dobësisë:

1.3 Insecure Transportation Security Protocol Supported – Low Risk

Përshkrimi i dobësisë:

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.

Rreziku:

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Sugjerim:

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

SSLProtocol +TLSv1.1 +TLSv1.2

- For Nginx, locate any use of the directive ssl_protocols in the nginx.conf file and remove TLSv1.

ssl_protocols TLSv1.1 TLSv1.2;

- For Microsoft IIS, you should make some changes on the system registry.

1. Click on Start and then Run, type regedt32 or regedit, and then click OK.
2. In Registry Editor, locate the following registry key or create if it does not exist:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\

3. Locate a key named Server or create if it doesn't exist.
4. Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".

4.3.2 Targeti 2:

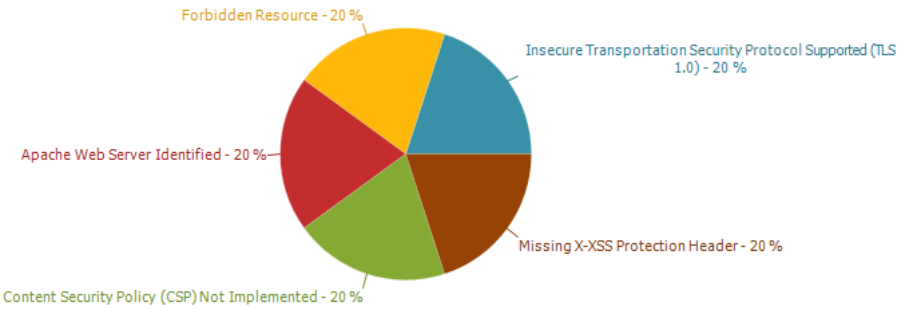

Figura 9 – Rezultatet e testimit të Targetit 2

Emri i dobësisë:

1.1 Insecure Transportation Security Protocol Supported – Low Risk

Përshkrimi i dobësisë:

Netsparker detected that insecure transportation security protocol (TLS 1.0) is supported by your web server.

TLS 1.0 has several flaws. An attacker can cause connection failures and they can trigger the use of TLS 1.0 to exploit vulnerabilities like BEAST (Browser Exploit Against SSL/TLS).

Websites using TLS 1.0 will be considered non-compliant by PCI after 30 June 2018.

Rreziku:

Attackers can perform man-in-the-middle attacks and observe the encryption traffic between your website and its visitors.

Sugjerim:

Configure your web server to disallow using weak ciphers. You need to restart the web server to enable changes.

- For Apache, adjust the SSLProtocol directive provided by the mod_ssl module. This directive can be set either at the server level or in a virtual host configuration.

SSLProtocol +TLSv1.1 +TLSv1.2

- For Nginx, locate any use of the directive ssl_protocols in the nginx.conf file and remove TLSv1.

ssl_protocols TLSv1.1 TLSv1.2;

- For Microsoft IIS, you should make some changes on the system registry.

1. Click on Start and then Run, type regedt32 or regedit, and then click OK.

2. In Registry Editor, locate the following registry key or create if it does not exist: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\

3. Locate a key named Server or create if it doesn't exist.

4. Under the Server key, locate a DWORD value named Enabled or create if it doesn't exist and set its value to "0".

4.3.3 Targeti 3:

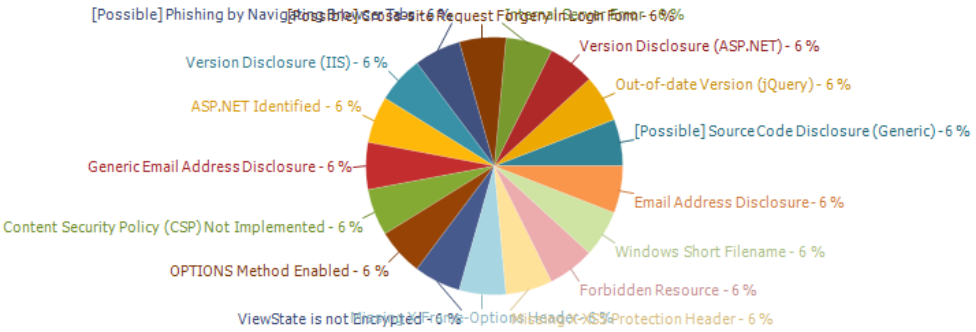

Figura 10 – Rezultatet e testimit të Targetit 3

Emri i dobësisë:

1.1 Out-Of-Date Version (jQuery) – Medium Risk

Përshkrimi i dobësisë:

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Rreziku:

Since this is an old version of the software, it may be vulnerable to attacks.

Sugjerim:

Please upgrade your installation of jQuery to the latest stable version.

Exploit

https://bugs.jquery.com/ticket/11290

Emri i dobësisë:

1.2 [Possible] Source Code Disclosure – Medium Risk

Përshkrimi i dobësisë:

Netsparker identified a possible source code disclosure (Generic).

An attacker can obtain server-side source code of the web application, which can contain sensitive data - such as database connection strings, usernames and passwords - along with the technical and business logic of the application.

Rreziku:

Depending on the source code, database connection strings, username and passwords, the internal workings and business logic of the application might be revealed. With such information, an attacker can mount the following types of attacks:

- Access the database or other data resources. Depending on the privileges of the account obtained from the source code, it may be possible to read,
update or delete arbitrary data from the database.

- Gain access to password protected administrative mechanisms such as dashboards, management consoles and admin panels, hence gaining full
control of the application.

- Develop further attacks by investigating the source code for input validation errors and logic vulnerabilities.

Sugjerim:

1. Confirm exactly what aspects of the source code are actually disclosed; due to the limitations of these types of vulnerability, it might not be possible to confirm this in all instances. Confirm this is not an intended functionality.
2. If it is a file required by the application, change its permissions to prevent public users from accessing it. If it is not, then remove it from the web server.
3. Ensure that the server has all the current security patches applied.
4. Remove all temporary and backup files from the web server.

Required Skills for Successful Exploitation

This is dependent on the information obtained from the source code. Uncovering these forms of vulnerabilities does not require high levels of skills.

However, a highly skilled attacker could leverage this form of vulnerability to obtain account information from databases or administrative panels, ultimately leading to the control of the application or even the host the application resides on.

Emri i dobësisë:

1.3 Internal Server Error – Low Risk

Përshkrimi i dobësisë:

Netsparker identified an internal server error.

The server responded with an HTTP status 500, indicating there is a server-side error. Reasons may vary, and the behavior should be analyzed carefully. If Netsparker is able to find a security issue in the same resource, it will report this as a separate vulnerability.

Rreziku:

The impact may vary depending on the condition. Generally this indicates poor coding practices, not enough error checking, sanitization and whitelisting.

However, there might be a bigger issue, such as SQL injection. If that's the case, Netsparker will check for other possible issues and report them separately.

Sugjerim:

Analyze this issue and review the application code in order to handle unexpected errors; this should be a generic practice, which does not disclose further information upon an error.

All errors should be handled server-side only.

Emri i dobësisë:

1.4 Version Disclosure (ASP.NET) – Low Risk

Përshkrimi i dobësisë:

Netsparker identified a version disclosure (ASP.NET) in target web server's HTTP response. This information can help an attacker gain a greater understanding of the systems in use and potentially develop further attacks targeted at the specific version of ASP.NET.

Rreziku:

An attacker might use the disclosed information to harvest specific security vulnerabilities for the version identified.

Sugjerim:

Apply the following changes to your web.config file to prevent information leakage by using custom error pages and removing X-AspNet-Version from
HTTP responses.

```
<System.Web>
        <httpRuntime enableVersionHeader="false" />
        <customErrors mode="On" defaultRedirect="~/error/GeneralError.aspx">
                <error statusCode="403" redirect="~/error/Forbidden.aspx" />
                <error statusCode="404" redirect="~/error/PageNotFound.aspx" />
                <error statusCode="500" redirect="~/error/InternalError.aspx" />
        </customErrors>
</System.Web>
```

Emri i dobësisë:

1.5 ViewState is not Encrypted – Low Risk

Përshkrimi i dobësisë:

Netsparker detected that ViewState encryption is disabled.

Rreziku:

An attacker can study the application's state management logic for possible vulnerabilities; if your application stores application-critical information in the
ViewState, it will also be revealed.

Sugjerim:

ASP.NET provides encryption for ViewState parameters.
For page based protection, place the following directive at the top of affected page.

```
<%@Page ViewStateEncryptionMode="Always" %>
```

You can also set this option for the whole application by using web.config files. Apply the following configuration for your application's web.config file.

```
<System.Web>
        <pages viewStateEncryptionMode="Always">
</System.Web>
```

Emri i dobësisë:

1.6 Missing X-Frame-Options Header – Low Risk

Përshkrimi i dobësisë:

Netsparker detected a missing X-Frame-Options header which means that this website could be at risk of a clickjacking attack.

The X-Frame-Options HTTP header field indicates a policy that specifies whether the browser should render the transmitted resource within a frame or an iframe. Servers can declare this policy in the header of their HTTP responses to prevent clickjacking attacks, which ensures that their content is not embedded into other pages or frames.

Rreziku:

Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account but are instead typing into an invisible frame controlled by the attacker.

Sugjerim:

- Sending the proper X-Frame-Options in HTTP response headers that instruct the browser to not allow framing from other domains.
- Employing defensive code in the UI to ensure that the current frame is the most top level window.

Emri i dobësisë:

1.7 Windows Short Filename – Low Risk

Përshkrimi i dobësisë:

Netsparker identified a Windows short file/folder name disclosure.

The vulnerability is caused by the tilde character (~) with the old DOS 8.3 name convention in an HTTP request. It allows a remote attacker to disclose file and folder names that is not supposed to be accessible.

Rreziku:

Attackers could find important files that are normally not accessible from the outside and gain intelligence about the application infrastructure. This may cause the leakage of files containing sensitive information such as credentials, configuration files and maintenance scripts.

Sugjerim:

In order to disable short names creation, add a registry key named
NtfsDisable8dot3NameCreation
to HKLM\SYSTEM\CurrentControlSet\Control\FileSystem and set its value to "1".

Emri i dobësisë:

1.8 [Possible] Cross Site Request Forgery in Login Form – Low Risk

Përshkrimi i dobësisë:

Netsparker identified a possible Cross-Site Request Forgery in login form.

In a login CSRF attack, the attacker forges a login request to an honest site using the attacker's user name and password at that site. If the forgery succeeds, the honest server responds with a Set-Cookie header that instructs the browser to mutate its state by storing a session cookie, logging the user into the honest site as the attacker. This session cookie is used to bind subsequent requests to the user's session and hence to the attacker's authentication credentials. The attacker can later log into the site with his legitimate credentials and view private information like activity history that has been saved in the account.

Rreziku:

Attackers could find important files that are normally not accessible from the outside and gain intelligence about the application infrastructure. This may cause the leakage of files containing sensitive information such as credentials, configuration files and maintenance scripts.

Sugjerim:

In order to disable short names creation, add a registry key named
NtfsDisable8dot3NameCreation
to HKLM\SYSTEM\CurrentControlSet\Control\FileSystem and set its value to "1".

Emri i dobësisë:

1.9 [Possible] Phishing by Navigating Browser Tabs – Low Risk

Përshkrimi i dobësisë:

Opened windows through normal hrefs with target="_blank" can modify window.opener.location and replace the parent webpage with something else, even on a different origin.

While this doesn't allow script execution, it does allow phishing attacks that silently replace the parent tab.

Rreziku:

If the links lack of rel="noopener noreferrer" attribute, third party site can change the URL of source tab using window.opener.location.assign and trick the user as if he is still in a trusted page and lead him to enter his secret information or credentials to this malicious copy.

Sugjerim:

To prevent pages from abusing window.opener, use *rel=noopener*. This ensures window.opener is null in Chrome 49 and Opera 36.

For older browsers and in Firefox, you could use *rel=noreferrer* which also disables the Referer HTTP header.

...

5. DISKUTIME DHE REKOMANDIME

5.1 Diskutim

Sigurimi i një kompjuteri, sistemi, rrjeti apo aplikacioni të mirë është përgjegjësi e secilit që bën pjesë në konfigurimin e tij dhe atyre që e përdorin. Duke filluar nga arkitektët e sistemit, zhvilluesit, testerët e deri tek ekipi i sigurimit të cilësisë së një produkti dhe ekipi i menaxhimit të një projekti (Sans, 2004). Pra, jo vetëm ekipi i Sigurisë Kibernetike duhet të merret me rrezikun që sjellin hakerët. Organizatat apo kompanitë duhet të sigurohen që t'ua mësojnë punonjësve të tyre rregullat bazë të mbrojtjes në internet, dhe hapat që duhet ndjekur për ta parandaluar sulmin e mundshëm. Testimi i vazhdueshëm i sistemit apo aplikacionit dhe forcimi i mekanizmave mbrojtës me përditësime, i kursen kompanisë dëme në vlera të paimagjinueshme. Përmirësimi i kohë pas kohshëm i paisjeve teknologjike apo ndërrimi i tyre me paisjet e reja gjithsesi se është hap shumë i rëndësishëm në mirëmbajtjen e sigurisë në përgjithësi.

Jashta kompanive, të gjithë ne që posedojmë mjete teknologjike personale si smartphone, kompjuter, laptop apo çfarëdo paisje tjetër smart (TV, frigorifer, speaker) jemi gjithashtu në rrezik të vazhdueshëm për t'u përgjuar dhe sulmuar. Tashmë dihet që ekzistojnë shumë aplikacione që kanë qasje në të dhënat tona posa të instalohen në paisje. Ato mund të përdoren për të përgjuar lëvizjet dhe gjithçka që ne bëjmë kur kemi një smartphone me vete. Informacionet që rrjedhin më së shpeshti janë numrat e telefonit dhe vendndodhja e paisjes.

Edhe pse një qytetar i thjeshtë mund të mos ketë fshehtësi dhe të dhëna që rrezikojnë shuma të mëdha parash apo dokumente konfidenciale, privatësia dhe mbajtja e të dhënave personale sekrete është e drejtë e secilit.

Mbrojtja në internet fillon me vetëdijësimin dhe njohjen e paisjeve apo programeve që përballemi çdo ditë. Në vazhdim kemi disa rekomandime për të qenë më të sigurtë në hapësirën kibernetike.

5.2 Mënyrat për të siguruar hapësirën tuaj kibernetike

Rrjeti i Wi-Fi në shtëpinë tuaj:

Pasi dikush të ketë qasje në rrjetin tuaj Wi-Fi, ata mund të bëjnë gjithçka nga shkarkimi i të dhënave pa fund, kopje të piratuara të videolojërave, filmave dhe të gjitha këto do të llogariten në shkarkimin tuaj dhe do të regjistrohen si të qasshme nga një pajisje në adresën tuaj të shtëpisë, për të përdorur software përgjimi për të kapur trafikun në rrjetin tuaj - dhe kjo mund të nënkuptojë marrjen e kredencialeve të identifikimit për faqet e internetit.

Filloni me sigurimin që routerit tuaj t'i vendoset një emër dhe një fjalëkalim. Ka shumë njerëz që e lënë routerin me parametrat e parazgjedhura nga prodhuesi (default: admin admin), gjë që vetëm i bën gjërat shumë të lehta për këdo që dëshiron të fitojë akses. Ç'aktivizoni opsionin e hyrjes në router nga jashtë, dhe bëni konfigurimet vetëm me kabllo.

Kontrolloni për të parë nëse ka përditësime të firmware. Kur kompanitë lëshojnë përditësime, ato bëhen për shkak se po i përgjigjen një çështjeje të sigurisë.

Pasi që enkriptimi i zakonshëm i parazgjedhur për routerin është WEP, e cila përbën rrezik dhe mund të hakohet shumë lehtë, vendosim enkriptimin WPA2 PSK. Në fund, jepni një fjalëkalim të fortë për rrjetin tuaj të Wi-Fi, sipas rekomandimeve (Moon 2015).

Kompjuteri juaj:

Një prej metodave primare që t'u qasur në internet është kompjuteri apo laptopi juaj. Këto gjithashtu janë një vatër e problemeve të sigurisë kibernetike. Për të mbrojtur veten tuaj, siguroni paisjen me një fjalëkalim. Enkriptoni të dhënat në hard disk, kështu që edhe nëse dikush fiton çasje në kompjuterin tuaj, do ta ketë të vështirë të shohë dhe lexojë të dhënat. Instaloni softuerë të sigurisë për t'u mbrojtur nga virusët dhe përditësoni ato vazhdimisht. Instaloni vetëm softuerë nga faqe të besueshme. Përdorni versionin më të fundit të web browserit dhe vizitoni vetëm faqe të sigurta, ku shumica prej tyre sot kanë parashtesën http**s** (S qëndron për Secure). Mos klikoni në e-maila nga persona apo organizata të pa njohura, aq më pak nëse kanë ndonjë fajll ose link të bashkangjitur.

Mbani një kopje rezervë të të gjitha të dhënave tuaja me vlerë në një USB apo Hard Disk të jashtëm, dhe në rast që kompjuteri bëhet viktimë e një sulmi të llojit Ransomware, mund të fshihet lehtësisht dhe të ri-konfigurohet nga e para në vend se të mirreni me shantazhuesit.

Smartphone i juaj:

Tabletat dhe smartfonët janë të shkëlqyera për qasje në internet, kudo që jeni. Megjithatë, ato janë gjithashtu të pa mbrojtura ndaj problemeve të sigurisë kibernetike. Ashtu si në PC dhe laptop, qëndroni në websajte të sigurta, mos jepni fjalëkalimet aty ku nuk është e nevojshme dhe gjithsesi sigurohuni që paisja të jetë e mbyllur me password apo sigurim biometrik.

Në të gjithë telefonat e viteve të fundit, keni mundësinë që përveq fjalëkalimit, ta mbroni telefonin tuaj me sigurim biometrik. Kjo përfshin zërin tuaj, shenjat e gishtërinjve apo skanimin e retinës së syrit tuaj. Përdoreni këtë opsion pasi është më i sigurti dhe në rast të humbjes së telefonit tuaj keqbërësit do ta kenë shumë të vështirë çasjen në të. Krahas fjalëkalimit dhe sigurimit biometrik, aktivizoni remote data wiping. Kjo do të thotë që nëse telefoni juaj bie në duar të gabuara, ju mund të fshini nga distanca të gjitha të dhënat që gjenden në të, por edhe në këtë rast duhet që fillimisht të mbani kopje rezervë të të dhënave. Shkarkoni aplikacione vetëm nga dyqanet e besueshme si Play Store dhe App Store. Mos bëni Root (Android) apo Jailbreak (iOS), sepse liria për të instaluar çkado që doni e shkatërron edhe më tej sigurinë e telefonit tuaj. Evitoni çasjen në Wi-Fi publike pa fjalëkalim, përdorni internetin 3G apo 4G nga sim card-a juaj, por nëse nuk keni zgjidhje tjetër dhe duhet të kyçeni në atë Wi-Fi, përdorni shërbimin VPN për të enkriptuar trafikun në internet që ta bëni përgjimin shumë më të vështirë.

Përditësoni aplikacionet, sepse hakerët shpesh shfrytëzojnë dobësitë në versionet e vjetra.

Fjalëkalimet (Passwords)

Për të gjitha paisjet e lart cekura dhe të tjerat, për profilet tuaja në rrjete sociale, punë apo shërbime bankare, vendosni fjalëkalime të vështira që kombinojnë një minimum prej 8 karaktereve të rastësishme (shkronja të mëdha dhe të vogla, numra dhe simbole) – dhe sa më të rastësishme karakteret, aq më i fortë është fjalëkalimi. Mos përdorni informata personale dhe evitoni përdorimin e fjalëve të zakonshme, apo fjalëkalimeve të njejta në disa platforma. Aty ku ofrohet, përdorni verifikimin me 2 hapa, një shërbim që ofrohet nga Apple, Google dhe të tjerë që kërkojnë njëkohësisht një fjalëkalim dhe një pajisje të besuar për t'u identifikuar (telefoni apo kompjuteri personal).

Sikurse brusha e dhëmbëve, fjalëkalimi rekomandohet që të ndryshohet çdo 3 muaj!

6. REFERENCAT

[1] K. Mitnick “The Art Of Invisibility”, 2017

[2] R. Jashari “Mbrojtja e Të Dhënave Personale”, 2018

[3] R. Sobers “60 Must-Know Cyber Security Statistics for 2018” article, 2018
URL: <https://blog.varonis.com/cybersecurity-statistics/>

[4] Ch. Phong “A Study Of Penetration Tools And Approaches” MA Thesis, 2014

[5] J.N. Goel “Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology” Conference Paper, 2015

[5] IT Governance Ltd “Data Sheet Penetration Testing” article, 2018
URL: <https://www.itgovernance.co.uk/download/Data-Sheet-PenTesting_v1.pdf>

[6] G. Weidman “Penetration Testing”, 2014

[7] SANS Inst. “Security Testing of web applications: Best Practices and Tools” GIAC paper, 2004

[8] OWASP “10 Most Common Web Security Vulnerabilities” article, 2018
URL: <https://www.guru99.com/web-security-vulnerabilities.html#3>

[9] B. Moon “7 Ways to Secure Your Cyberspace” article, 2015
URL: <https://investorplace.com/2015/02/cyberspace-security/>