

Universiteti i Prishtinës “Hasan Prishtina”

Fakulteti i Inxhinierisë Elektrike dhe Kompjuterike



Dokumentim teknik i projektit

Lënda: Siguria në Internet

Titulli i projektit: Burp Suite

Emri profesorit/Asistentit

Emri&mbiemri studentëve/ email adresa

Prof. Dr. Blerim REXHA PhD.c Mërgim H. HOTI	1. Diana Zymberi	diana.zymberi@studenti.uni-pr.edu
	2. Diare Daqi	diare.daqi@studenti.uni-pr.edu
	3. Elona Paçarizi	elona.pacarizi@studenti.uni-pr.edu
	4. Veronë Krasniqi	verone.krasniqi@studenti.uni-pr.edu

Prishtinë, 2021

Përmbajtja

Abstrakti	3
Hyrje	4
Çka është Burp Suite?	4
Proxy	4
Scanner	4
Intruder	5
Repeater.....	5
Decoder	5
Comparer	6
Extender	6
Sequencer	7
Qëllimi i punimit	8
Pjesa kryesore	9
Përgjimi i HTTP dhe HTTPS kërkesave	9
Vulnerabilities	13
Cross-Site Scripting.....	14
Cookie Hijacking	18
OTP Bypass.....	22
Konkluzioni	27
Referencat	28

Abstrakti

Në kuadër të projektit të dytë në lëndën “Siguria e të dhënave” përfshihet analizimi dhe shfrytëzimi i opsioneve që i ofron Burp Suite.

Burp Suite është një Java Application i cili përdoret për testim dhe sigurim të web aplikacioneve. Burp Suite përbëhet nga një set i gjerë opsionesh si Server Proxy, Web Spider, Intruder dhe Repeater.

Me anë të Burp Suite Proxy Server, përdoruesit i ofrohet mundësia që të manipulojë trafikun që kalon përmes browser-it të klientit dhe serverit të web-it. Kjo zakonisht njihet si sulm i tipit MITM(Man-in-the-Middle). Për të bërë ndryshimet në trafikun ndërmjet klientit dhe serverit, Burp Suite ofron tabelat, të cilat janë më lehtë të përdorshme, në krahasim me veglat e tjera të cilat shërbejnë për testim dhe siguri të web aplikacioneve.

Me anë të Burp Suite Intruder, përdoruesit i ofrohet mundësia të performojë sulme të automatizuara në aplikacionet në web. Për kryerjen e këtij sulmi përdoruesi duhet të ketë njohuri paraprake për aplikacionin të cilin e sulmon dhe protokollin HTTP. Burp Suite ofron një algoritëm që është i konfigurueshëm dhe që mund të gjenerojë kërkesa të dëmshme HTTP. Me anë të Intruder mund të testohen dhe të zbulohen dobësi të llojit SQL Injection, Cross-Site Scripting (XSS), manipulim i parametrave dhe sulmet brute force.

Me anë të Burp Suite Repeater, përdoruesit i ofrohet mundësia e modifikimit të kërkesave në server dhe ridërgimi i tyre, duke i vëzhguar edhe rezultatet e kthyer nga serveri. Kjo përdoret për testim manual të një aplikacioni.

Hyrje

Çka është Burp Suite?

Burp Suite është një nga mjetet më të njohura të penetration testing dhe gjetjes së cenueshmërisë, shpesh përdoret për të kontrolluar sigurinë e aplikacionit në web. "Burp", siç njihet zakonisht, është një mjet i bazuar në proxy që përdoret për të vlerësuar sigurinë e aplikacioneve të bazuara në web dhe për të bërë testime praktike.

Përveç funksionalitetit bazë, si një server Proxy, një Scanner, një Intruder, mjeti gjithashtu përmban opsione më të avancuara një Repeater, një Decoder, një Comparer, një Extender dhe një Sequencer.

Mjetet kryesore që përdoren në paketën Burp Suite:

Proxy

Proxy

Ai funksionon si një server proxy në internet dhe qëndron si një njeri në mes shfletuesit dhe serverëve të webit të destinacionit. Kjo lejon përgjimin, inspektimin dhe modifikimin e trafikut të papërpunuar që kalon në të dy drejtimet.

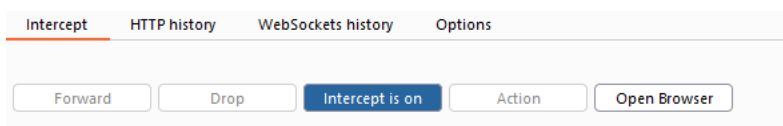


Figura 1: Menyja e Proxy-it

Scanner



New scan



New live task

Një skaner sigurie për aplikacione në web, i përdorur për kryerjen e skanimeve të automatizuara të cenueshmërisë së aplikacioneve në web.



Figura 2: Menyja e Scanner-it

Intruder

Intruder

Ky mjet mund të kryejë sulme të automatizuara në aplikacionet në internet. Mjeti ofron një algoritëm të konfigurueshëm që mund të gjenerojë kërkesa me qëllim të keq HTTP. Mjeti i ndërhyrës mund të testojë dhe zbulojë injeksione SQL, skriptime në vend, manipulim të parametrave dhe dobësi të ndjeshme ndaj sulmeve me brute force .

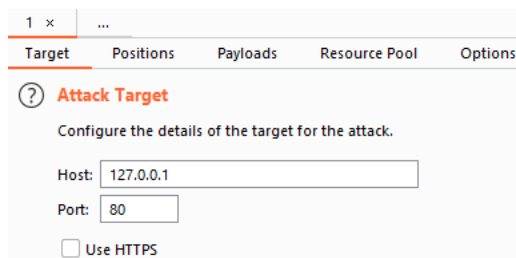


Figura 3: Menyja e Intruder-it

Repeater

Repeater

Një mjet i thjeshtë që mund të përdoret për të testuar manualisht një aplikacion. Mund të përdoret për të modifikuar kërkesat në server, për t'i ridërguar ato dhe për të vëzhguar rezultatet.

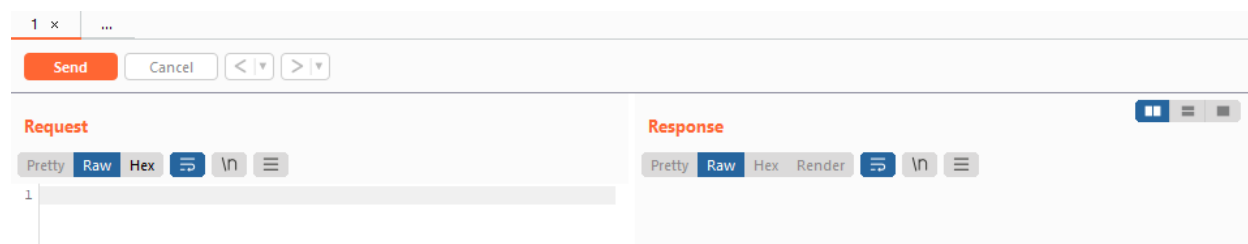


Figura 4: Menyja e Repeater-it

Decoder

Decoder

Një mjet për transformimin e të dhënave të enkriptuara në formën e tyre të kuptueshme, ose për transformimin e të dhënave të papërpunuara në forma të ndryshme të enkoduara dhe të hashuara. Ai është i aftë të njohë në mënyrë inteligjente disa formate kodimi.

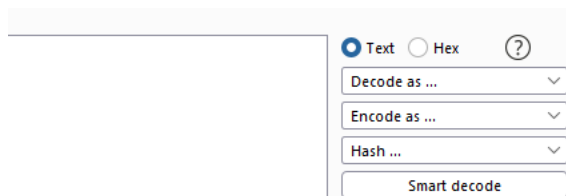


Figura 5: Menyja e Decoder-it

Comparer

Comparer

Një mjet për kryerjen e një krahasimi midis çdo dy të dhënave.

Comparer ⓘ

This function lets you do a word- or byte-level comparison between different data. You can load, paste, or send data here from other tools and then select the comparison you want to perform.

Select item 1:

#	Length	Data
---	--------	------

Paste
Load
Remove
Clear

Select item 2:

#	Length	Data
---	--------	------

Compare ...
Words
Bytes

Figura 6: Menyja e Comparer-it

Extender

Extender

Ai lejon testuesin e sigurisë të ngarkojë shtesat Burp, të zgjerojë funksionalitetin e Burp duke përdorur testuesit e sigurisë së tij ose kodin e palës së tretë.

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger **Extender** Project options User options Learn

Extensions BApp Store APIs Options

Burp Extensions ⓘ

Extensions let you customize Burp's behavior using your own or third-party code. ⓘ

Search...

Add	Remove	Up	Down	Loaded	Type	Name
-----	--------	----	------	--------	------	------

Details Output Errors

☐ Extension loaded ⓘ

Name:

Item	Detail
------	--------

Figura 7: Menyja e Extender-it

Sequencer

Sequencer

Një mjet për të analizuar cilësinë e rastësisë në një mostër të të dhënave. Mund të përdoret për të testuar shenjat e sesionit të një aplikacioni ose elementë të tjerë të rëndësishëm të të dhënave që synohen të jenë të paparashikueshëm, si p.sh. argumentet anti-CSRF, argumentet e rivendosjes së fjalëkalimit etj.

The screenshot shows the 'Sequencer' tool in Burp Suite, specifically the 'Live capture' tab. The interface is divided into three main sections:

- Select Live Capture Request:** This section allows users to select requests from other tools to configure a live capture. It includes a table with columns for '#', 'Host', and 'Request'. There are 'Remove' and 'Clear' buttons on the left, and a 'Start live capture' button at the bottom.
- Token Location Within Response:** This section allows users to select the location in the response where the token appears. It includes three radio buttons: 'Cookie:', 'Form field:', and 'Custom location:'. The 'Custom location:' option is selected, and there is a 'Configure' button.
- Live Capture Options:** This section contains settings that control the engine used for making HTTP requests and harvesting tokens. It includes three input fields: 'Number of threads:' (set to 5), 'Throttle between requests (milliseconds):' (set to 0), and 'Ignore tokens whose length deviates by:' (set to 5 characters). The 'Ignore tokens whose length deviates by:' option is checked.

Figura 8: Menyja e Sequencer-it

Arsyeja kryesore e testimit të sigorisë është të identifikojë kërcënimet në sistem dhe të masë dobësitë e tij të mundshme, në mënyrë që kërcënimet të mund të hasen dhe sistemi të mos ndalojë së funksionuari ose të mos mund të shfrytëzohet.

Sfidë e këtij projekti ka qenë fillimisht konfigurimi i Burp Suite me foxyproxy, pastaj mënyra sesi duhet të përdoret kjo vegël, si implementohen sulmet e ndryshme si dhe mundësitë e pakta që ti ofron community edition i Burp Suite.

Kontributi ynë në këtë fushë është se gjatë testimeve që do të shtjellohen më detajisht në vijim të raportit ne kemi hasur në një dobsi të ashtuquajtur high severity (ashpërsia e lartë) në sistemin e menaxhimit të studentëve në Universitetin e Prizrenit(smu). Çdo testim është kryer për qëllime edukative dhe nuk është cënuar integriteti i askujt.

Qëllimi i punimit

Qëllimi i këtij projekti në lëndën Siguria në Internet është analiza dhe trajtimi i veglës Burp Suite. Qëllimi i çdo penetration test është të identifikojë pikat e dobëta të mundshme në aplikacione, serverë, ose rrjeta ,pika të dobëta që mund të jenë mundësi për të fituar informacion të ndjeshëm ose të privilegjuar akses për një sulmues. Arsyeja për të zbuluar dobësi të tilla nuk është vetëm të dimë se ato ekzistojnë dhe llogaritin rrezikun që i bashkëngjitet, por për të bërë përpjekje për t'i zbutur ose zvogëluar ato në minimum.

Të veçantat e Burp Suite janë:

- Testimi manual i depërtimit dhe rregullimet e konfigurimit
- Përgjimi i kërkesave
- Extensions të shkëlqyera përmes dyqanit që zgjerojnë funksionalitetin

Përparësitë e Burp Suite janë:

- Para së gjithash, është e mundur të kryhen teste manuale të sigurisë së aplikacioneve në internet dhe aplikacioneve celularë duke përdorur këtë mjet. Përparësi është se ju gjithashtu mund të testoni në mënyrë të sigurt dobësitë që lidhen me logjikën e biznesit të këtyre aplikacioneve.
- Burp Suite përdor një përfaqësues lokal, kështu që ju lejon të përgjoni trafikun e aplikacioneve për të gjetur dobësi.
- Vepron si një shërbim i mrekullueshëm proxy: Burp Suite ju ndihmon të plotësoni të gjitha kërkesat e bazuara në web, të cilat madje mund të modifikohen kur dërgohen ose merren. Ndryshe nga përfaqësuesit e tjerë, ky përfaqësues funksionon pa dështuar. Pra, është shumë i besueshëm.
- Burp Suite është mjaft i shpejtë për të kryer një sulm në një faqe interneti.
- Burp Suite ju lejon të identifikoheni me lehtësi në një faqe interneti si hapi i parë në spidering dhe attacking. Kjo është e dobishme për ne pasi shumica e faqeve tona të internetit kërkojnë një hyrje përpara se të mund të skanojmë faqet e brendshme të një faqe interneti.

Të metat e Burp Suite janë:

- Nuk përshkruan se si të testoni dobësi të ndryshme, të cilat mund të jenë sfiduese nëse jeni përdorues i ri i këtij mjeti.
- Edicioni i falas (community edition) ofron një numër të kufizuar funksionesh në krahasim me edicionin profesional. Megjithatë shumë studiues përdorin botimin e komunitetit për testimin e sigurisë, Burp Suite duhet të ofrojë më shumë veçori që do të ishin të dobishme.
- Lehtë për t'u përdorur, por e vështirë për t'u zotëruar.

Pjesa kryesore

Përgjimi i HTTP dhe HTTPS kërkesave

Një kërkesë HTTP bëhet nga një klient, në një host të caktuar, i cili ndodhet diku në një server. Qëllimi i kërkesës është të marrim qasje në burim në server.

Webfaqet e testuara : <https://studenti-uni-pr.edu>,
<https://www.gmail.com>,
<https://www.facebook.com/>

Përshkrimi i dobësisë:

Burp Suite pozicionohet si Man in the Middle mes browserit dhe website-it të cilin e testojmë. Kjo ia mundëson vëlgës Burp Suite që të përgjojë dhe modifikojë të gjithë trafikun që zhvillohet në të dy drejtimet, duke depërtuar edhe në lidhjet e enkriptura me anë të TLS/SSL. Gjatë përgjimit të trafikut në dy websitet e para të lartëcekura, ndër shumë të dhëna tjera, janë përgjuar edhe username dhe password i përdoruesit, të cilat janë shfaqur si tekst i qartë. Mirëpo kjo nuk konsiderohet si dobësi për shkak se Burp arrin të thyej çdo lidhje SSL dhe SSL çertifikata e Burp Suite është e instaluar në browserin tonë. Çdo kush tjetër do të shohë vetëm trafikun e enkriptuar dhe nuk do të jetë në gjendje të tregojë nëse një fjalëkalim po transmetohet.

Shfrytëzimi i dobësisë:

Përgjimi i HTTPS requestes dhe HTTPS responses për testuesit manual është themeli i rrjedhës së punës të testimit. Gjatë përdorimit të browserit, përdoruesi përgjon trafikun dhe e analizon atë, dhe kjo të çon në detyra të tjera dhe opsione të tjera të Burp për veprime më specifike varësisht nga detektimet që mund të bëhen përgjatë përgjimit.

Hapat e zhvillimit të sulmit:

Pas konfigurimit të Mozilla Firefox në mënyrë që të punojë me Burp Suite, hapim <https://studenti-uni-pr.edu>. Në Burp Suite shfaqet kërkesa e cila duhet të dërgohet te serveri. Tek Intercept tab ngecin të gjitha kërkesat për t'u analizuar nga ne si përdorues. Këto kërkesa kemi mundësinë t'i shikojmë, modifikojmë, t'i bëjmë drop që të mos procesohet kërkesa më tutje, t'i forwardojmë tutje tek serveri apo të kryejmë tjera operacione duke e dërguar kërkesën në veglat tjera të Burp Suite si Repeater, Intruder apo ndojnë tab tjetër.

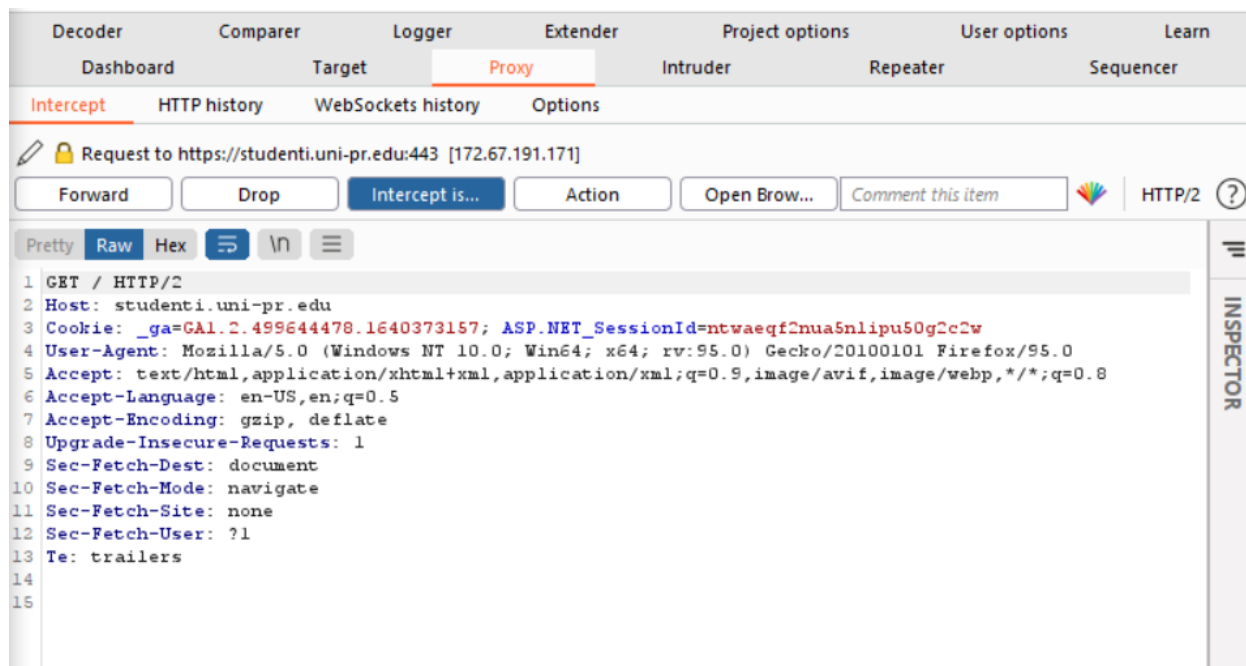


Figura 9. SEMS HTTPS Request

Pas shfaqjes së kërkeses në Burp Suite, klikojmë forward dhe në browser tonë ngarkohet faqja kryesore e SEMS.



Figura 10. Ngarkimi i SEMS pas forwardimit te kërkesës

Pas klikimit në butonin “Qasja”, përsëri kërkesa shfaqet në Burp dhe duhet të forwardojmë tutje për dërgim të kërkesës tek serveri, për shkak se kërkesa ngec tek ne. Pas forwardimit shfaqet faqja për shënimin e kredencialeve si ID e studentit dhe fjalëkalimi.

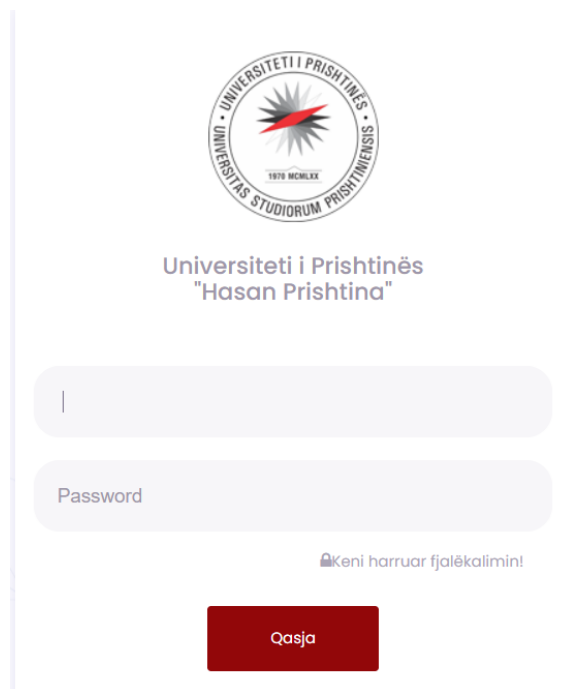


Figura 11: Ngarkimi i Log In page ne SEMS

Kur jepen të dhënat e studentit, në momentin që klikohet tek butoni “Qasja”, në Burp Suite në opsionin Intercept shfaqen të dhënat e shënuara nga studenti, në plaintext.

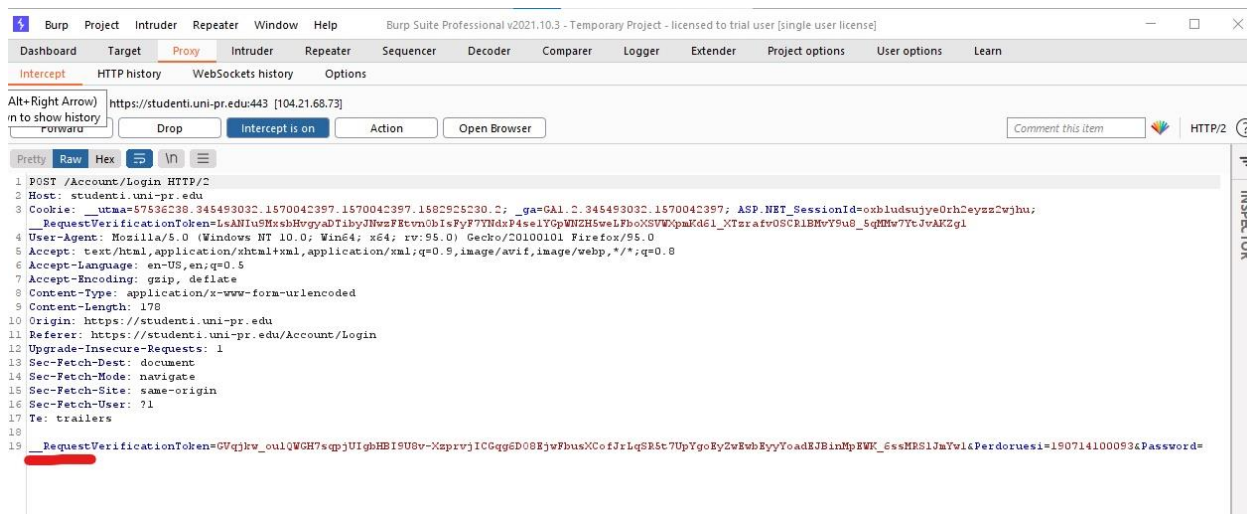


Figura 12: Paraqitja e numrit te ID dhe passwordit te përdoruesit

Ngjashëm kemi përgjuar edhe Gmail HTTPS request, ku poashtu fjalëkalimi shfaqet në plaintext si në rastin e SEMS.

Për shkak se Burp Suite është një vegël shumë e fortë përgjuese dhe çertifikatën që e nënshkruan e besojnë të gjithë browser-ët të dhënat na shfaqen si plaintext.

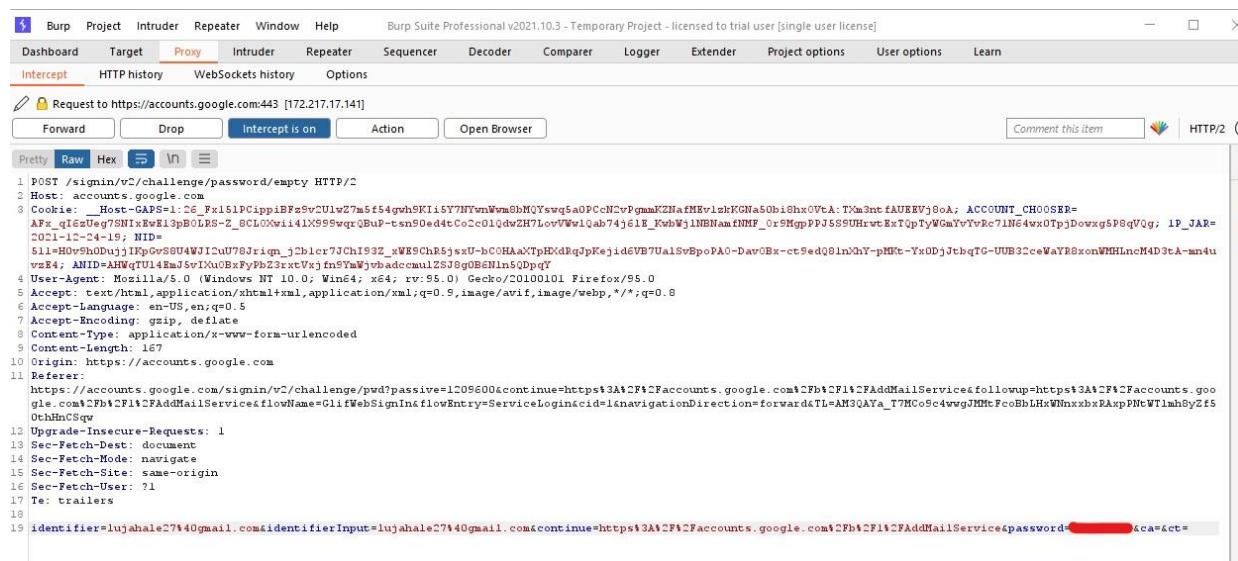


Figura 13. Plaintext kredencialet e përgjuara nga HTTPS Gmail Request

E njëjta ndodhë me kredencialet e përdoruesëve që kyçen në <https://facebook.com>.

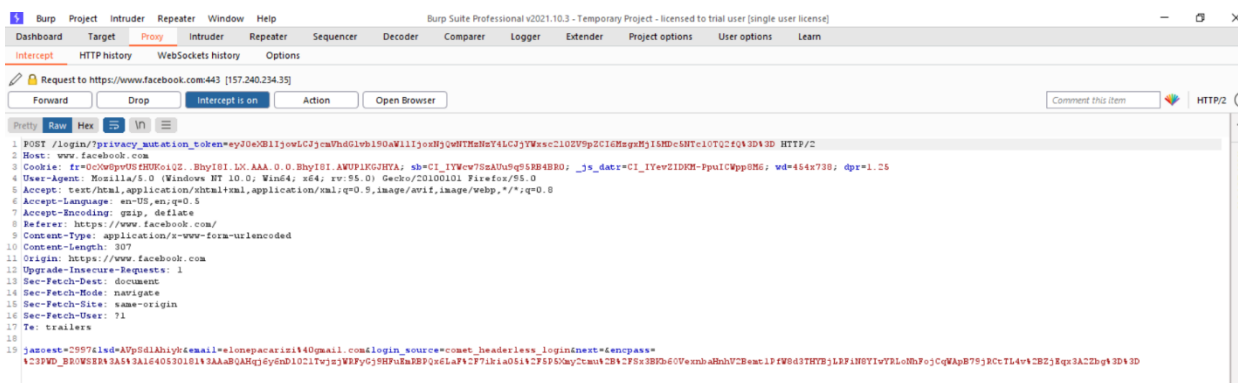


Figura 14. Password-i i enkriptuar nga përgjimi i HTTPS Facebook Request

Sipas parazgjedhjes, Burp Suite përgjon vetëm kërkesat dhe disa file extensions në URL anashkalohen për shkak se gjatë testimit janë kërkesat ato që na interesojnë më shumë. Tek Options mund të bëjmë konfigurime në mënyrë të atillë që i përgjojmë kërkesat bazuar në karakteristika specifike të cilat ato i kanë, dhe e njëjta mund të konfigurohet edhe për përgjigjet nga serveri.

Në mënyrë të ngjajshme arrijmë t'i përgjojmë edhe kërkesat në HTTP.

Vulnerabilities

Webfaqja e testuar: <http://smu.uni-prizren.com/Account/Login>

Dobësia: Clear submission of password

Përshkrimi i dobësisë:

Disa aplikacione transmetojnë fjalëkalime përmes lidhjeve të pa enkriptuara, duke i bërë ato të prekshme ndaj përgjimit. Dobësitë që rezultojnë në zbulimin e fjalëkalimeve të përdoruesve mund të rezultojnë në kompromise që janë jashtëzakonisht të vështira për t'u hetuar për shkak të gjurmëve të errësura të auditimit. Edhe nëse vetë aplikacioni trajton vetëm informacione jo të ndjeshme, ekspozimi i fjalëkalimeve i vë në rrezik përdoruesit që kanë ripërdorur fjalëkalimin e tyre diku tjetër.

Shrytëzimi i dobësisë:

Për të shfrytëzuar këtë dobësi, një sulmues duhet të pozicionohet në mënyrë të përshtatshme për të përgjuar trafikun e rrjetit të viktimës. Ky skenar zakonisht ndodh kur një klient komunikon me serverin përmes një lidhjeje të pasigurt si Wi-Fi publik, ose një rrjet korporate ose shtëpie që ndahet me një kompjuter të komprometuar. Mbrojtjet e zakonshme si rrjetet komutuese nuk janë të mjaftueshme për ta parandaluar këtë. Një sulmues i vendosur në ISP-në e përdoruesit ose në infrastrukturën e pritjes së aplikacionit mund të kryejë gjithashtu këtë sulm. Vini re se një kundërshtar i avancuar mund të synojë potencialisht çdo lidhje të krijuar mbi infrastrukturën bazë të internetit.

Për ta parë këtë dobësi mjafton që ta skanojmë këtë webfaqe dhe na paraqitet pamja si në figurën në vijim.

The screenshot displays the Burp Suite interface with the 'Issue activity' tab selected. It shows a list of vulnerabilities found during a scan of the target website. The 'Event log' at the bottom provides details about the network traffic captured during the scan.

#	Task	Time	Action	Issue type	Host
23	2	16:03:21 26 Dec 2021	Issue found	Vulnerable JavaScript dependency	http://smu.uni-prizren.com
22	2	16:03:21 26 Dec 2021	Issue found	Password field with autocomplete enabled	http://smu.uni-prizren.com
21	2	16:03:21 26 Dec 2021	Issue found	Cleartext submission of password	http://smu.uni-prizren.com
20	2	16:03:19 26 Dec 2021	Issue found	Browser cross-site scripting filter disabled	https://www.facebook.com
19	2	16:03:19 26 Dec 2021	Issue found	Browser cross-site scripting filter disabled	https://www.facebook.com
18	2	16:03:19 26 Dec 2021	Issue found	Strict transport security not enforced	https://content.fpm
17	2	16:03:19 26 Dec 2021	Issue found	Credit card numbers disclosed	https://www.facebook.com
16	2	16:03:19 26 Dec 2021	Issue found	Email addresses disclosed	https://www.facebook.com
15	2	16:03:19 26 Dec 2021	Issue found	Strict transport security not enforced	https://www.facebook.com
14	2	16:03:15 26 Dec 2021	Issue found	Strict transport security not enforced	https://www.facebook.com
13	2	16:03:15 26 Dec 2021	Issue found	Strict transport security not enforced	https://www.facebook.com
12	2	16:03:15 26 Dec 2021	Issue found	Frameable response (potential Clickjacking)	https://www.facebook.com
11	2	16:03:15 26 Dec 2021	Issue found	Browser cross-site scripting filter disabled	https://www.facebook.com

Time	Type	Source	Message
16:03:16 26 Dec 2021	Info	Proxy	scontent.fpm3-1.fna.fbcdn.net is using HTTP/2
16:03:15 26 Dec 2021	Info	Proxy	www.facebook.com is using HTTP/2
16:02:34 26 Dec 2021	Info	Proxy	connect.facebook.net is using HTTP/2
16:02:34 26 Dec 2021	Info	Proxy	w.bookcdn.com is using HTTP/2
16:02:34 26 Dec 2021	Info	Proxy	fonts.googleapis.com is using HTTP/2
16:01:55 26 Dec 2021	Info	Proxy	Proxy service started on 127.0.0.1:8080

Figura 15: Pamje pas skanimit të webfaqes së Sistemit të Menaxhimit të Studentëve të Universitetit të Prizrenit(smu)

Mbrojtja:

Aplikacionet duhet të përdorin enkriptim të nivelit të transportit (SSL ose TLS) për të mbrojtur të gjitha komunikimet e ndjeshme që kalojnë midis klientit dhe serverit. Komunikimet që duhet të mbrohen përfshijnë mekanizmin e hyrjes dhe funksionalitetin përkatës, dhe çdo funksion ku mund të aksesohen të dhënat e ndjeshme ose mund të kryhen veprime të privileguara. Këto zona duhet të përdorin mekanizmin e tyre të trajtimit të sesioneve dhe shenjat e sesionit të përdorur nuk duhet të transmetohen kurrë përmes komunikimeve të pa enkriptuara. Nëse skedarët HTTP përdoren për transmetimin e shenjave të sesionit, atëherë duhet të vendoset flamuri i sigurt për të parandaluar transmetimin përmes HTTP me tekst të qartë.

Cross-Site Scripting

Webfaqja e testuar: <https://xss-game.appspot.com/level1/frame>

Përshkrimi i dobësisë: Browser cross-site scripting filter disable

Shfrytëzimi i dobësisë:

Skriptimi në faqe është një lloj dobësie sigurie që mund të gjendet në disa aplikacione në web. Sulmet XSS u mundësojnë sulmuesve të injektojnë skriptet e klientit në faqet e internetit të shikuara nga përdorues të tjerë.

Hapat për zhvillimin e sulmit Cross-Site Script brenda kësaj webfaqe:

Fillimisht hapim këtë webfaqe në browserin që e kemi të konfiguruar foxyprox-in dhe e skanojmë.

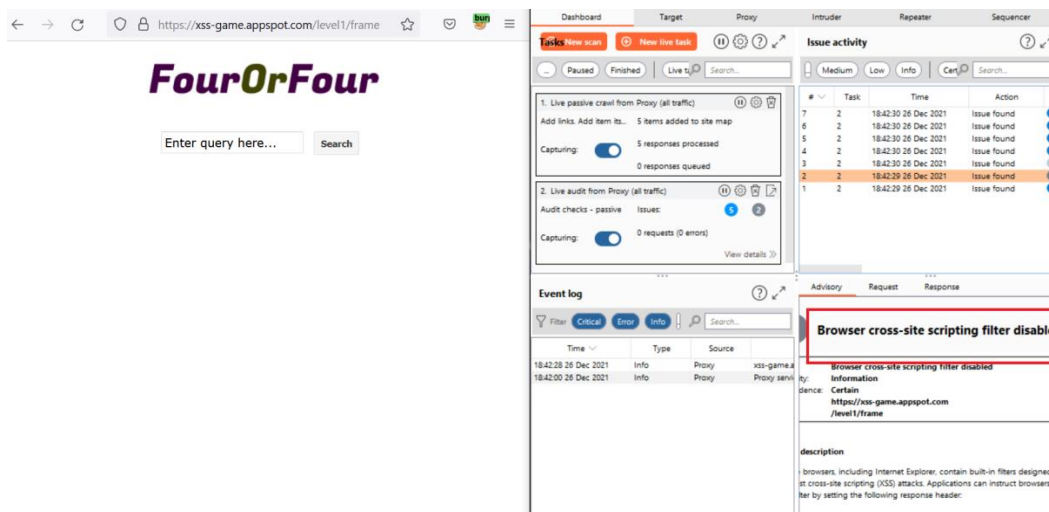


Figura 16: Pamja pas skanimit të webfaqes së lartëcekur

Kërkojmë diqka në fushën e kërkimit të kësaj webfaqe.

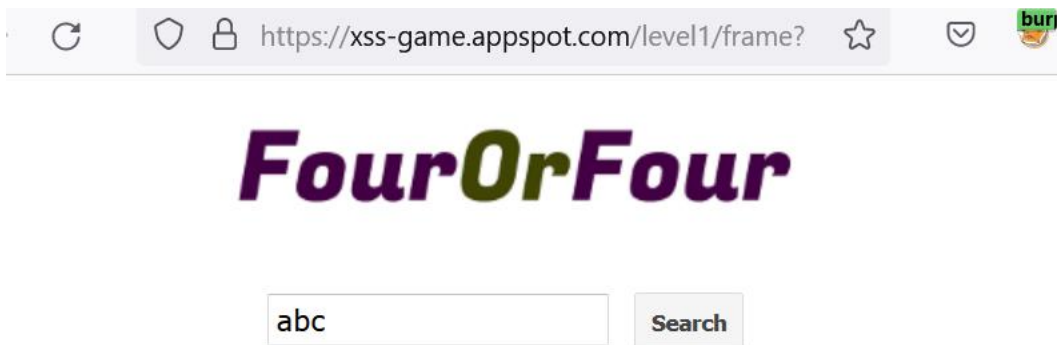


Figura 17: Pamja pas një kërkimi në webfaqen e lartëcekur

Më pas duhet te Burp Suite të shkojmë tek pjesa e Request-it si në figurën e mëposhtme:

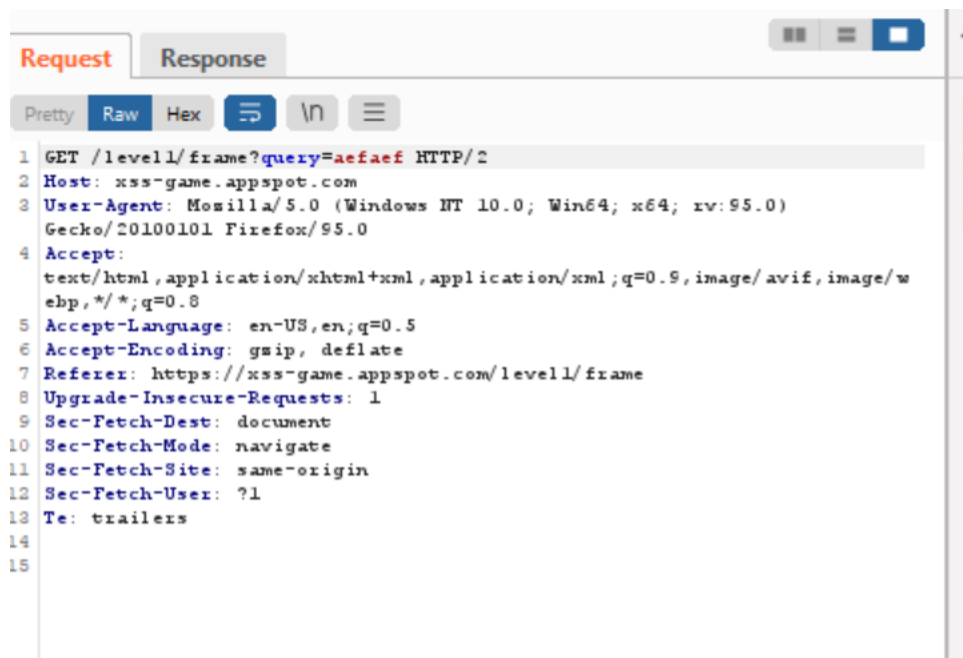


Figura 18: Pjesa e Request-it sa i përket kësaj webfaqe

Më pas klikojmë me tastin e djathtë të miut dhe zgjedhim opsionin send to Repeater dhe më pas shkojmë tek pjesa e repeater nga menyja kryesore e Burp Suite-it.

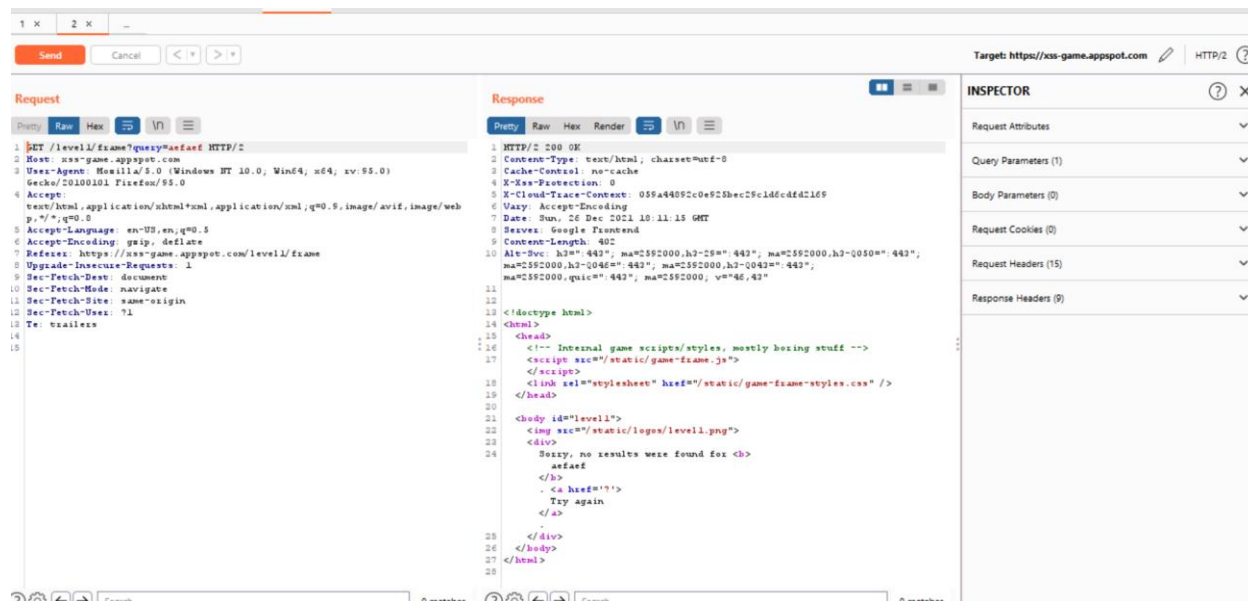


Figura 19: Pamja në pjesën e Repeater

Më pas e shkruajmë një kod brenda një skripte që na mundëson shfaqjen e një alerti.

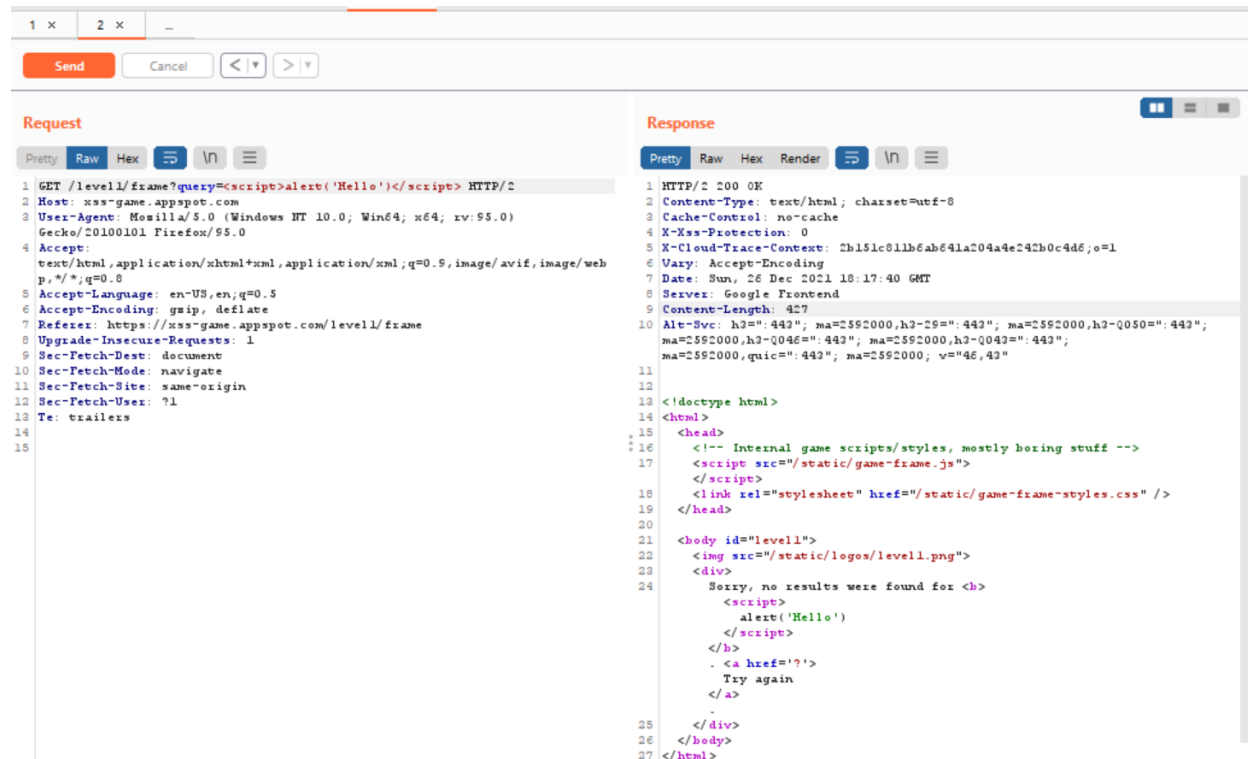


Figura 20: Pamja pas shkruarjes së një alerti në pjesën e query-it

Më pas me tastin e djathtë të miut klikojmë dhe i zgjedhim opsionet si në figurën e mëposhtme:

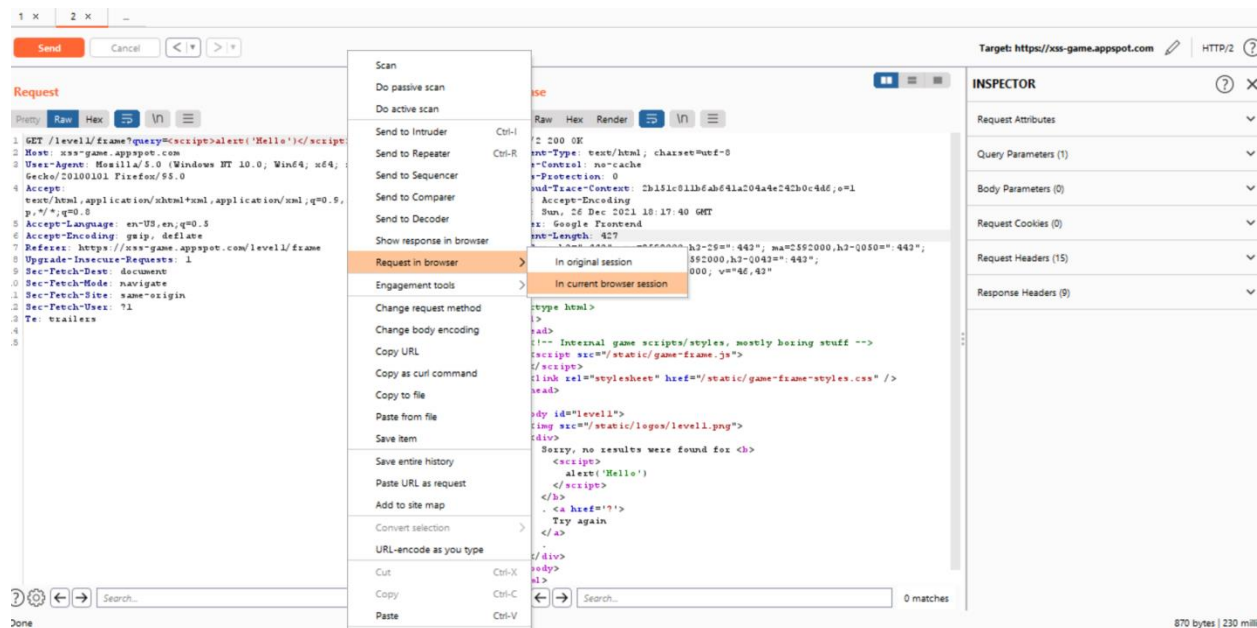


Figura 21. Dërgimi i kodit skriptues në sesionin e browserit që tashmë jemi duke e përdorur

Pamja pasi i kemi ndjekur hapat të cilët u thanë më lartë. Në këtë pikë klikojmë në butonin Copy.

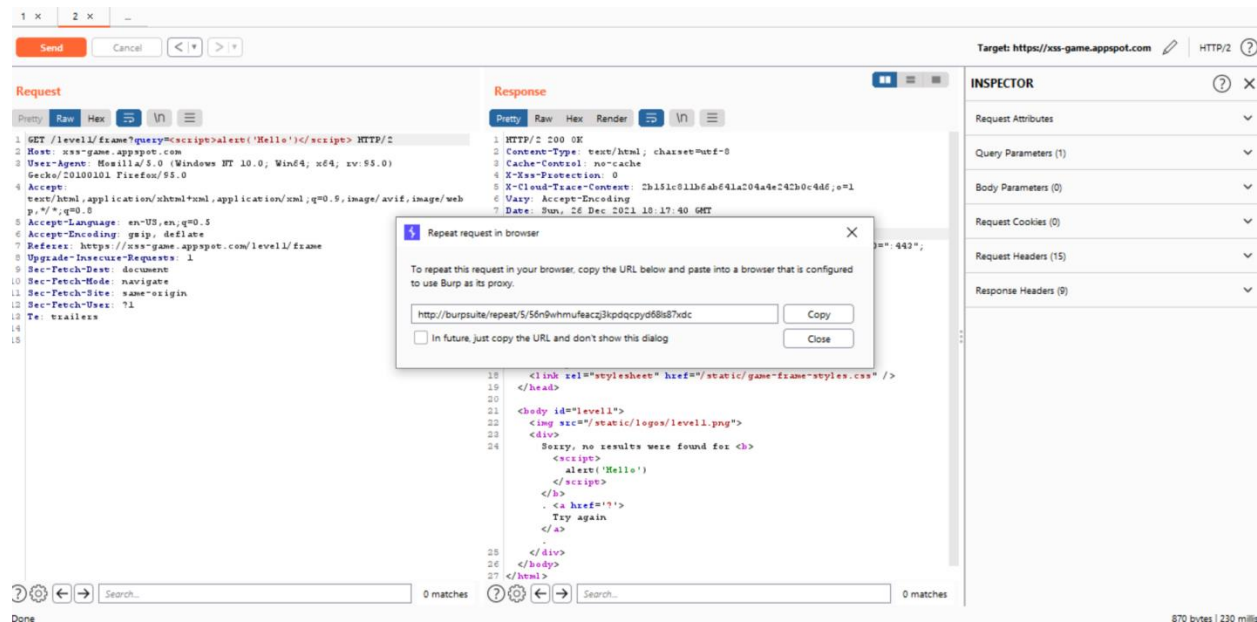


Figura 22: Pamja pas klikimit në opsionin e dytë

Linku i kopjuar vendoset në browser dhe kërkojmë na paraqitet kjo pamje, që i bie se skripta e shkruar te Repeater është ekzekutuar me sukses.

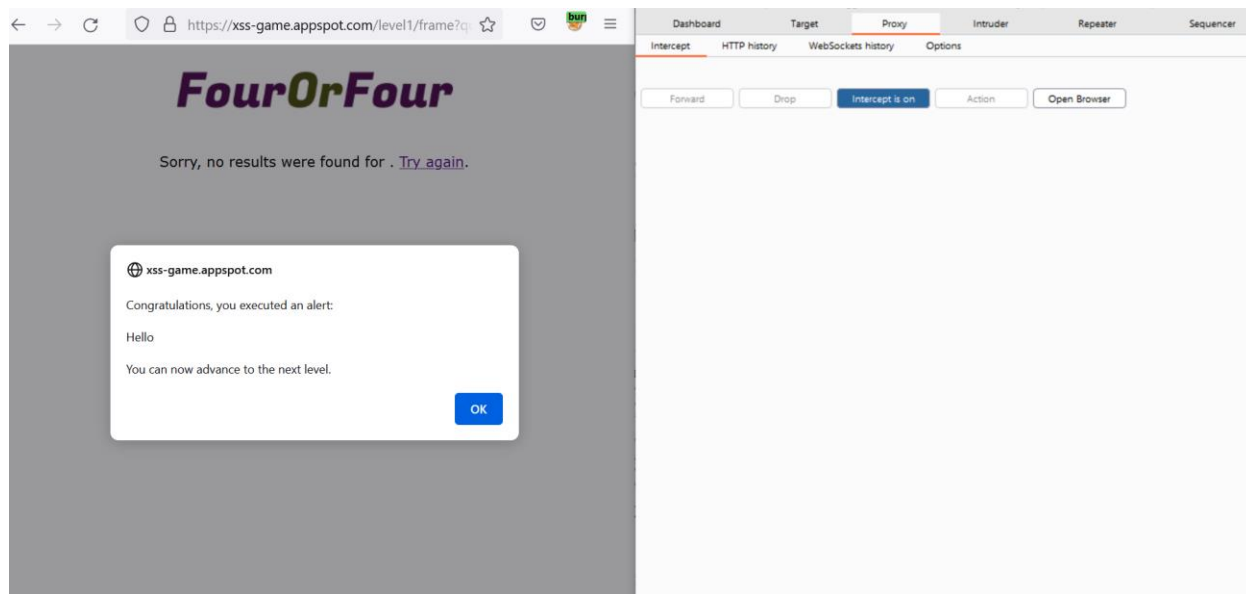


Figura 23: Pamja pas kërimit në browser të linkut që e bëmë kopje më sipër

Cookie Hijacking

Cookie Hijacking, i quajtur edhe Session Hijacking, është një mënyrë për hakerat për të hyrë dhe vjedhur të dhënat tuaja personale, dhe ata gjithashtu mund t'ju ndalojnë të hyni në llogari të caktuara.

Webfaqja e testuar: <http://testphp.vulnweb.com/>

Përshkrimi i dobësisë:

Cookie Hijacking mund të ndodhë kur një program malware pret që një përdorues të identifikohet në faqen e internetit. Më pas, malware vjedh cookie-n e sesionit dhe ia dërgon atë sulmuesit. Një sulm cookie shpesh inicohet kur një sulmues i dërgon një përdoruesi një hyrje të rreme. Viktima klikon lidhjen e rreme, e cila e lejon sulmuesin të vjedhë cookie - në fakt, çdo gjë që përdoruesi shkruan mund të kapet nga sulmuesi. Sulmuesi më pas e vendos atë cookie në shfletuesin e tij dhe është në gjendje të veprojë si ju. Ndonjëherë, një lidhje e rreme nuk është as e nevojshme. Nëse një përdorues është në një seancë në një lidhje të pasigurt, publike Wi-Fi, hakerët mund t'i vjedhin lehtësisht ato të dhëna që udhëtojnë përmes lidhjes. Dhe kjo mund të ndodhë edhe nëse faqja është e sigurt dhe emri juaj i përdoruesit dhe fjalëkalimi janë të koduara.

Shfrytëzimi i dobësisë:

Pasi sulmuesi të ketë skedarin e sesionit të një përdoruesi, ai mund të identifikohet në një faqe interneti dhe të bëjë pothuajse gjithçka që mund të bëni, duke përfshirë ndryshimin e fjalëkalimit tuaj. Dhe kjo shpesh është e automatizuar, kështu që ndodh në vetëm sekonda. Nëse një haker rrëmben sesionin tuaj ndërkohë që jeni regjistruar në një bankë, ata do të jenë në gjendje të ndërmarrin çdo veprim që do të mund t'i kryeni edhe kur jeni të kyçur. Kjo përfshin transferimin e parave, blerjen e produkteve nga një dyqan në të cilin jeni identifikuar, aksesin në informacione personale dhe më shumë. Nëse sulmuesi më pas mundëson vërtetimin me shumë faktorë (MFA) kundër viktimës, ata mund të mos kenë më kurrë akses në llogaritë e tyre.

Hapat për zhvillimin e sulmit:

E hapim web faqen testuese të cilën e kemi marrë.

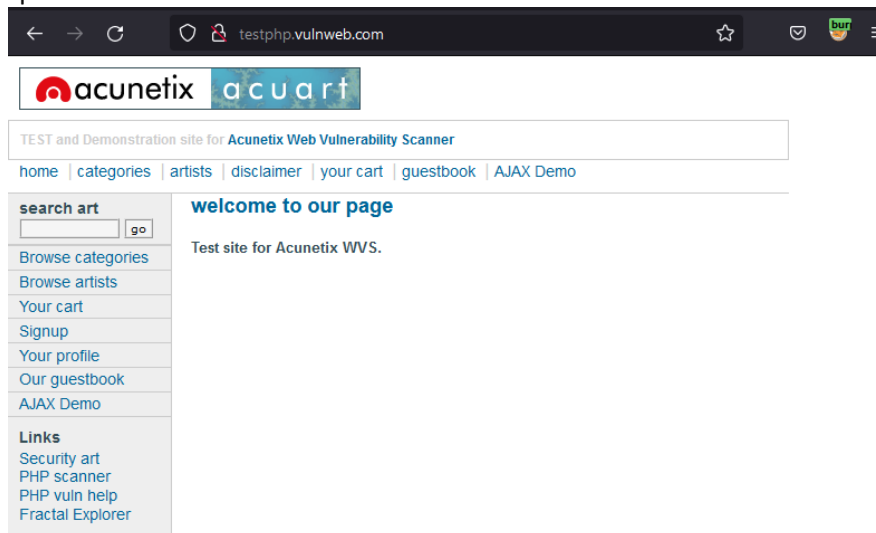


Figura 24. Web faqja testuese

E hapim llogarinë tonë në atë webfaqe.

If you are already registered please enter your login information below:

Username :	<input type="text" value="test"/>
Password :	<input type="password" value="...."/>
<input type="button" value="login"/>	

You can also [signup here](#).

Signup disabled. Please use the username **test** and the password **test**.

Figura 25. Vendosja e të dhënave per kyçe në llogarinë tonë

Pas kycjes në atë webfaqe në ekran na shfaqen të dhënat tona personale.

On this page you can visualize or edit you user information.

Name:	<input type="text" value="Hackerjohn"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="Hacker@email.com"/>
Phone number:	<input type="text" value="67676767767766"/>
Address:	<div>prueba de accesos</div>
<input type="button" value="update"/>	

Figura 26. Të dhënat tona personale

Në veglën tonë Burp Suite na shfaqen disa të dhëna rreth llogarisë tonë. Ato të dhëna ne i dërgojmë në Repeater që t'i ruajmë sepse duhet t'i përdorim më vonë.

```
Pretty Raw Hex ↕ \n ≡
1 GET /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:95.0) Gecko/20100101 Firefox/95.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: login=test%2Ftest
9 Upgrade-Insecure-Requests: 1
0
```

Figura 27. Të dhënat që na shfaqen në Burp Suite

Pasi i dërgojmë të dhënat në Repeater, ne duhet të dalim nga llogaria jonë dhe ta fshijmë historinë në browserin tonë.

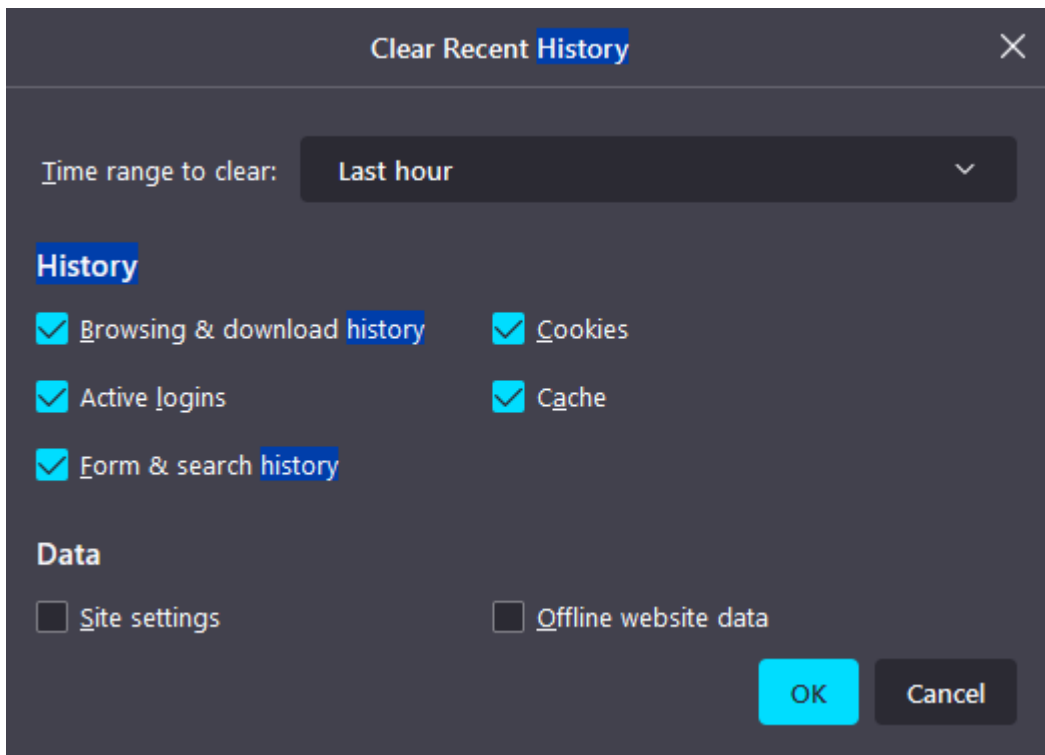


Figura 28. Fshirja e historisë së browser-it tonë

Kur historinë e fshijmë ne duhet që prapë ta hapim webfaqen e njejtë, ndërsa në Burp Suite i vendosim të dhënat që më herët i dërguam në Repeater. Për hapje më të shpejtë klikojmë ne butonin Forward disa herë.

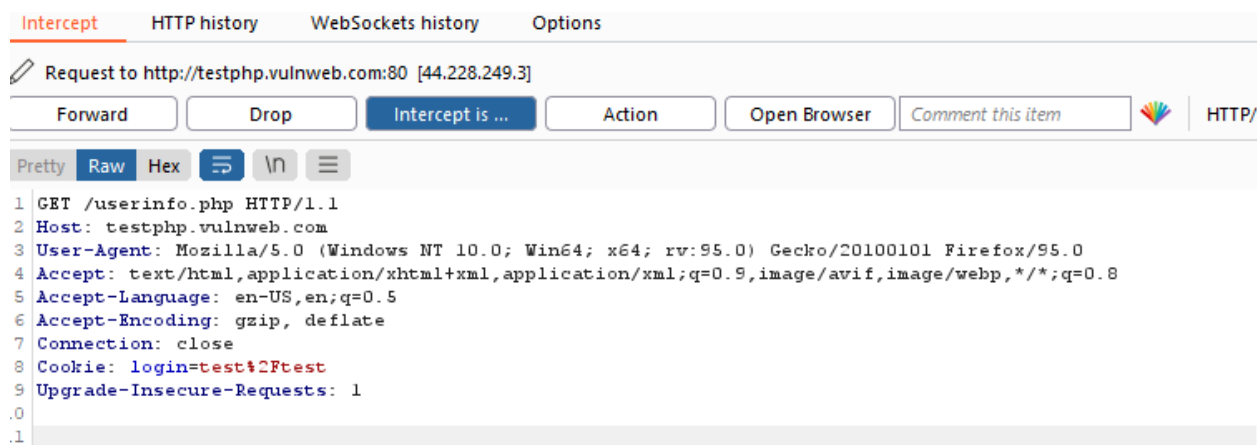


Figura 29. Vendorsja e të dhënave që i ruajtëm në Repeater

Si rezultat i këtij sulmi na shfaqen prapë të dhënat personale të llogarisë tonë të cilat janë ruajtur në cookies. Pra ky lloj sulmi është kryer me sukses.

Hackerjohn (test)

On this page you can visualize or edit you user information.

Name:	<input type="text" value="Hackerjohn"/>
Credit card number:	<input type="text" value="1234-5678-2300-9000"/>
E-Mail:	<input type="text" value="Hacker@email.com"/>
Phone number:	<input type="text" value="67676*67767766"/>
Address:	<div>prueba de accesos</div>
<input type="button" value="update"/>	

Figura 30. Shfaqja e të dhënave personale

OTP Bypass

One Time Password (OTP), i njohur gjithashtu si një PIN , kod autorizimi (OTAC) ose fjalëkalim dinamik, është një fjalëkalim që është i vlefshëm vetëm për një seancë hyrjeje ose transaksion, në një sistem kompjuterik ose ndonjë tjetër pajisje digjitale.

Webfaqja e testuar: <https://glamgalscosmetics.ng/>

Dobësia: Strict transport security not enforced

Përshkrimi i dobësisë:

Webfaqja e lartcekur nuk iu siguron përdoruesve që të jenë të lidhur në mënyrë të enkriptuar gjatë gjithë kohës. Një sulmues është në gjendje të modifikojë trafikun e rrjetit të përdoruesit dhe të anashkalojë përdorimin e enkriptimeve SSL/TSL nga webfaqja dhe ta përdorë webfaqen për sulme kundër përdoruesve të saj. Ky sulm kryhet duke rishkruar lidhjet HTTPS si HTTP në mënyrë që nëse një përdorues ndjek një link që e dërgon në një lidhje HTTP atëherë shfletuesi nuk perpiqet kurrë të ndjek lidhjen e enkriptuar. Për të shfrytëzuar këtë dobësi një sulmues duhet të pozicionohet në mënyrë të përshtatshme për të përgjuar dhe modifikuar trafikun e rrjetit të viktimës .

Shfrytëzimi i dobësisë:

Meqenëse webfaqja nuk e detyron përdoruesin që të lidhet në mënyrë të enkriptuar gjatë gjithë kohës, kjo dobësi është shfrytëzuar për të sulmuar sistemin për “bypass one time password” që dërgohet përmes SMS në numrin e përdoruesit gjatë krijimit të llogarisë si formë e identifikimit të identitetit. Problemi me OTP qëndron se ndërsa ato janë të lehta për implementim dhe zbatim ato janë mjaft të cenueshme dhe nuk ofrojnë siguri mjaft të mirë dhe si rezultat Instituti Kombëtar i Standardeve dhe Teknologjisë në SHBA (NIST) njoftoi se nuk duhet të përdorin më këtë formë për verifikim të identitetit gjatë krijimit të llogarisë pasi është lehtë e cenueshme por edhe në ditët e sotme vazhdon të përdoret ende në një numër të madh të webfaqeve dhe çdo ditë ndodhin sulme e krime kibernetike duke shfrytëzuar këtë dobësi.

Sistemi i sinjalizimit nr. 7, i njohur ndryshe si SS7, është thelbësor për të gjitha komunikimet celulare. Është një standard që lehtëson thirrjet, SMS, përkthimin e numrave, faturimin me parapagesë, pritjen/përcjelljen e thirrjeve dhe shumë funksione të tjera celulare. Megjithatë, që nga fillimi i tij në 1975, protokoli ka pasur gjithmonë të meta dhe hakerët mund ta përdorin atë për të përgjuar thirrjet dhe mesazhet SMS ashtu siç u shfrytëzua edhe në këtë rast duke përdorur veglën Burp Suite ku u përgjua trafiku komunikues dhe arritëm ta gjenim kodin 6 shifror i cili u gjenerua nga sistemi për të identifikuar identitetin e përdoruesit.

Hapat për zhvillimin e sulmit:

Së pari e krijojmë një llogari në platformën google, llogari të cilën e përdorim si viktimë për realizimin e këtij sulmi.

Figura 31. Krijimi i një llogarie në google që do të përdoret si viktimë

Nga fotoja e shohim që kur kyçemi në webfaqen kryesore lidhja është e enkriptuar me protokollin https por dobësia e kësaj webfaqe qëndron në faktin se nuk e mban këtë lidhje gjatë gjithë kohës në çdo mjedis të webfaqes.

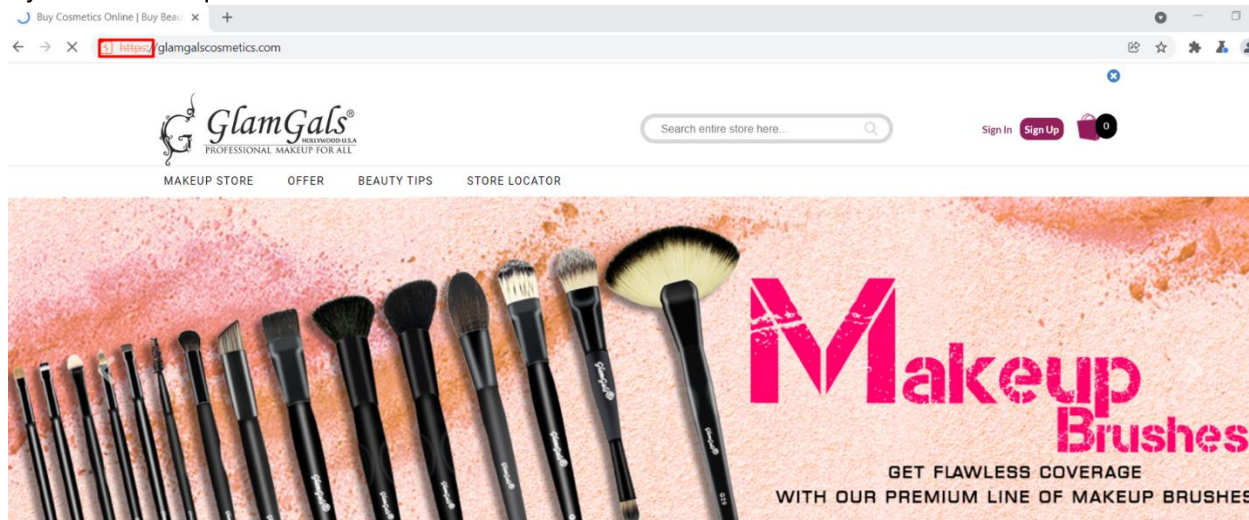


Figura 32. Krijimi i një llogarie në google që do të përdoret si viktimë

Me llogarinë e krijuar në google më herët tani e krijojmë një llogari në webfaqe me të dhënat si në foton më poshtë:

SIGN UP

Create account

IN +91 ▼

Get Code

SUBMIT

Already have an account? [Sign in](#)

Figura 33. Regjistrimi

Nga figura shihet se sistemi vepron brenda territorit te Indisë dhe për regjistrim kërkohet numri i telefonit në menyrë që të mund të dërgohet kodi 6 që të identifikojë përdoruesin. Gjatë gjithë kësaj kohe trafikun komunikues e përgjojmë përmes Burp Suite dhe e shohim që vazhdimisht paketat që janë pjesë e kërkesës shkojnë në server dhe presin një përgjigje nga serveri.

Pasi e shënojmë numrin e telefonit dhe klikojmë në butonin Get Code e bëjmë një kërkesë në server i cili na gjeneron një kod 6 shifrorë dhe na dërgon përmes SMS në telefon në numrin që e kemi shënuar. Por dobësi e sistemit është se nuk arrinë ta mbaj lidhjen e enkriptuar gjatë gjithë kohës dhe ne jemi në gjendje që duke e përgjuar trafikun komunikues ta kapim këtë kod para se ai të arrijë te përdoruesi i vërtetë përmes SMS edhe nëse nuk kemi fare qasje në telefon. Pra ne e zbulojmë kodin para se sistemi ta konfirmojë që kodi është dërguar me sukses te përdoruesi.

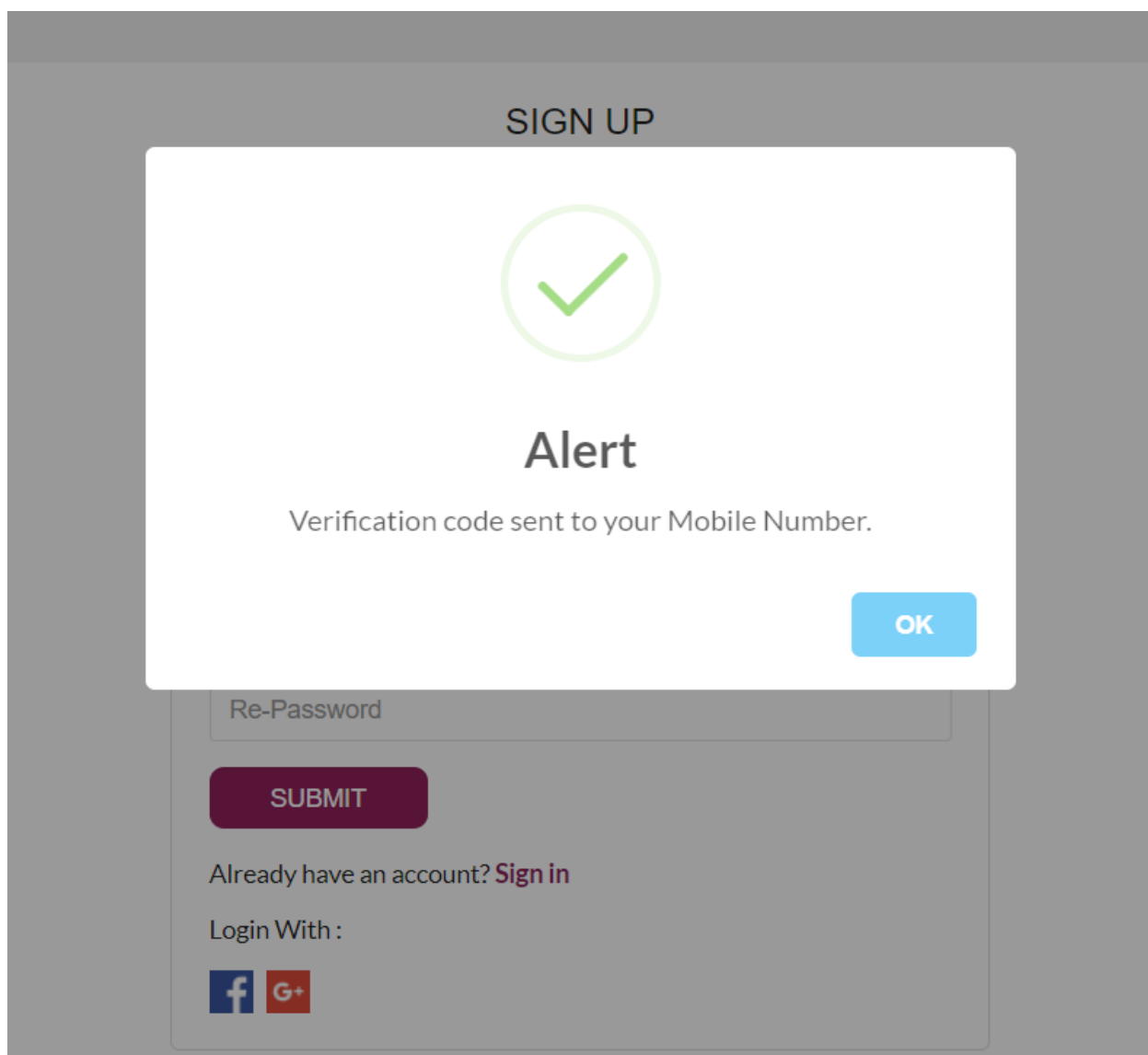


Figura 34. Sistemi e konfirmon që kodi i verifikimit është dërguar me sukses.

Pasi ti shikojmë paketat që na shfaqen në Burp Suite, këto paketa të cilat i ka dërguar serveri si përgjigje e shohim se në njërin prej tyre do të jetë edhe kodi verifikues i cili është i pa enkriptuar dhe mund të gjendet shumë lehtë.

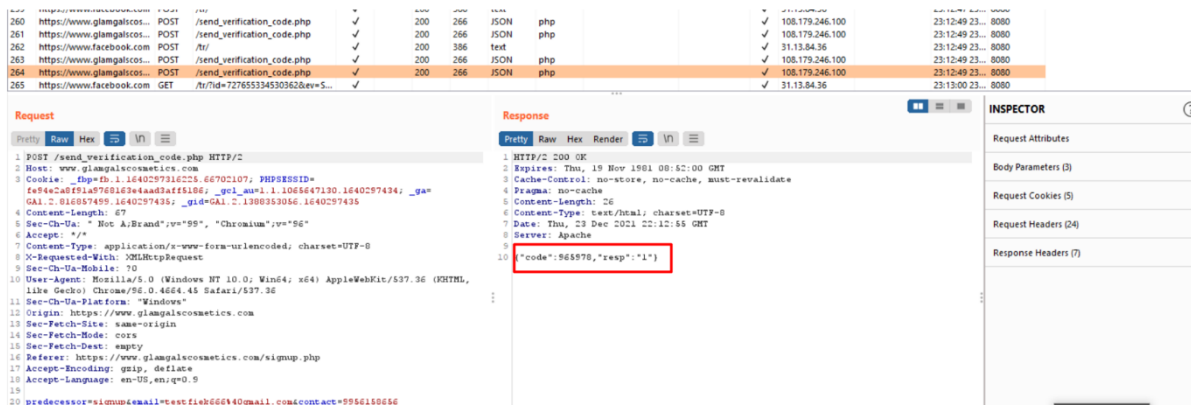


Figura 35. Shfaqja e kodit të pa enkriptuar të verifikimit

Nëse sulmuesi e kap këtë kod para përdoruesit të vërtetë atëherë ai i çaset llogarisë dhe mund ta përdorë identitetin e tij për të kryer shërbime të ndryshme brenda sistemit.

Pasi e shënon kodin e cakton edhe passwordin me këtë rast regjistrimi konsiderohet me sukses dhe me këto kredenciale mund të kyqemi sa herë që dëshirojmë.



Search entire store here...

Fiek 0

Figura 36. Qasja me sukses në sistem

Mbrojtja:

Webfaqja duhet t'i detyrojë shfletuesit e uebit që të përdorin vetëm lidhjen përmes protokollit HTTPS. Për ta bërë këtë duhet aktivizuar HTTP Strict Transport Security (HSTS) duke shtuar një header përgjigjeje me emrin 'Strict-Transport-Security' dhe vlerën 'max-age=expireTime', ku expireTime është koha në sekonda që shfletuesit duhet ta mbajnë në mend. Faqja duhet të aksesohet vetëm duke përdorur HTTPS dhe te gjitha te dhënat duhet të jenë të enkriptuara përmes algoritmeve më të sigurta që sugjerohen nga ekspertët e sigurisë.

Konkluzioni

Në këtë projekt u përdor Burp Suite si një ndër veglat kyqe në fushën e sigurisë kibernetike. Kjo vegël u përdor për web penetration testing, hakimin etik dhe për të rritur nivelet e sigurisë së sistemeve të ndryshme. Përdorimi i Burp Suite në testimin e webfaqeve është mjaft efikas dhe aftësitë e këtij mjeti për hakim i vleresojmë lart.

Përderisa cdo ditë e më tepër rritet numri i sulmeve dhe krimeve kibernetike është e rëndësishme që të kontrollohet rregullisht për dobësi të mundshme në sistem në mënyrë që ato të jenë të sigurta.

Nga testimet që u realizuan për webfaqe të ndryshme u kuptua që ndërsa kompanitë e ndryshme po digjitalizojnë operacionet dhe proceset e tyre ato priren të nënvleresojnë rreziqet e reja të teknologjisë ndaj të cilave ekspozohen dhe kanë sisteme të cilat janë të cenueshme dhe të pasigurta. Prandaj është nevojë urgjente që të investohet më shumë në këtë drejtim dhe të rritet niveli i vetëdijes së përdoruesve për rreziqet që ka përdorimi i internetit.

Referencat

- [1] <https://www.elegantthemes.com/blog/wordpress/what-is-cookie-hijacking-and-how-to-prevent-it>
- [2] <https://securityintelligence.com/articles/guide-to-cookie-hijacking/>
- [3] <https://portswigger.net/support/using-burp-to-manually-test-for-reflected-xss>
- [4] <https://www.hackingarticles.in/burp-suite-for-pentester-burp-sequencer/>
- [5] <https://portswigger.net/burp>
- [6] <https://www.sciencedirect.com/topics/computer-science/burp-suite>
- [7] <https://medium.com/@KDR9666/authentication-login-bypass-with-burp-suite-94561af8c87d>
- [8] <https://www.pentestgeek.com/web-applications/burp-suite-tutorial-1>
- [9] <https://deltarisk.com/blog/how-to-use-burp-suite-professional-for-web-application-security->
- [10] <https://www.softwaretestinghelp.com/how-to-use-burp-suite/>
- [11] <https://medium.com/r3d-buck3t/top-10-tips-for-b>
- [12] <https://www.contrastsecurity.com/knowledge-hub/glossary/penetration-testing>
- [13] <https://portswigger.net/burp/documentation/desktop/getting-started/intercepting-http-traffic>

Librat e përdorur

- [1] Gilberto Nájera-Gutiérrez - Kali Linux Web Penetration Testing Cookbook
- [2] Carlos A. Lozano, Shahmeer Amir – Bug Bounty Hunting Essentials

Fotografitë

- [1] Të gjitha fotot e paraqitura në këtë raport janë PrintScreen të realizuar gjatë testimeve përkatëse.