

# Universiteti i Prishtinës “Hasan Prishtina”

## Fakulteti Inxhinierisë Elektrike dhe Kompjuterike



### Dokumentim teknik i projektit

Lënda: Siguria në Internet

Titulli i projektit: Burp Suite

Emri profesorit/Asistentit

Prof. Dr. Blerim REXHA  
PhD.c Mërgim H. HOTI

Emri & mbiemri studentëve / email adresa

1. Arlinda Kastrati	arlinda.kastrati4@student.uni-pr.edu
2. Alberiana Tofaj	alberiana.tofaj@student.uni-pr.edu
3. Elsa Vitija	elsa.vitija@student.uni-pr.edu
4. Elona Rashica	elona.rashica@student.uni-pr.edu

Prishtinë, 2021

## Përbajtja

<b>Abstrakti .....</b>	3
<b>Hyrje .....</b>	4
<b>1. Qëllimi i punimit .....</b>	6
1.1 Avantazhet e Burp Suite .....	7
1.2 Disavantazhet e Burp Suite .....	8
<b>2. Pjesa kryesore.....</b>	9
2.1 Instalimi dhe nisja e veglës .....	9
2.2 Hapja e veglës.....	11
2.3 Veglat e Burp Suite .....	13
2.3.1 Target .....	13
2.3.2 Burp Proxy .....	14
2.3.3 Intruder.....	15
2.3.4 Repeater .....	16
2.3.5 Sequencer.....	16
2.3.6 Decoder.....	17
3.3.7 Comparer.....	18
3.3.8 Logger .....	18
3.3.9 Extender .....	19
2.3.10 Project options .....	19
3.3.11 User options .....	21
<b>3. Shembuj konkret.....</b>	22
3.1 SQL Injection.....	22
3.2 One Time Password (OTP).....	28
4.3 XSS Persistent.....	38
3.4     Brute Force me DVWA(Damn Vulnerable Web App).....	45
<b>4. Konkluzione.....</b>	53
<b>Referencat.....</b>	54

## Abstrakti

Ky rapport paraqet një përbledhje të informatave në lidhje me përshkrimin, instalimin, vetitë, funksionet, përdorimin dhe ekzekutimin e veglës softuerike Burp Suite në kuadër të lëndës Siguria në Internet. Burp Suite është një framework i bazuar në Java njëkohësisht edhe njëra nga veglat më të njobura për të testuar depërtimin dhe identifikimin e dobësive krasas sigurisë së informacioneve në internet. Burp Suite shumë shpesh përdoret për të kontrolluar sigurinë që e posedojnë aplikacionet në ueb. "Burp" është një vegël e bazuar në Proxy e që përdoret për të vlerësuar sigurinë e aplikacioneve të cilat janë të bazuara në ueb dhe realizimin e testimeve praktike. Për faktin që ka më shumë se 40,000 përdorues, Burp Suite konsiderohet si skaneri më i përdorur në botë per gjetjen e dobësive të uebit. Kjo vegël posedon një kornizë të fortë dhe modulare. Poashtu, Burp Suite përmban edhe shtesa të opsiioneve që mund të rrisin efikasitetin e testimit të aplikacioneve në internet. Objektivat kryesore të këtij reporti janë studimi i detajuar i veglës Burp Suite, procesi i instalimit, mënyrat dhe modet se si mund të përdoret duke përfshirë edhe disa shembuj konkret se si Burp Suite mund të detektojë dobësitë ashtu që zhvilluesit të mund ti eliminojnë ato.

## Hyrje

Jeta moderne në të cilën njerëzit janë duke jetuar në shekullin 21 anë e mbanë botës është krijuar nga përdorimi i Internetit. Duke filluar me metodat e komunikimit, leximin e lajmeve aktuale, kontrollimin e motit ose blerjen e çdo gjëje, rrjedhimisht arsyet e përdorimit të internetit po rriten vazhdimesh çdo ditë e më shumë.

Gjatë dekadave të fundit, pamja e faqeve të internetit në "World-Wide-Web" ka ndryshuar nga faqja statike, në aplikacionet dinamike të ueb-it, me të cilat lidhen vazhdimesh serverë të shumtë, duke ndër vepruar me përdoruesin dhe duke i ofruar të gjithëve një përvojë të ndryshme gjatë përdorimit. Sot është e mundur të bëni transaksione parash, të kontaktoni me të gjithë miqtë, të ndani të dhëna me grupe të vecanta përdoruesish ose thjesht kaloni kohë duke luajtur lojëra.

Njëkohësisht me këtë zhvillim të internetit dhe evoluimin e shërbimeve që ofron ai, numri i dobësive të aplikacioneve në internet është rritur gjithashtu. Në Figurën 1 kemi paraqitur përqindjen e sulmeve kibernetike që ndodhin gjatë viteve të fundit përmes dobësive të cilat janë të pranishme të aplikacionet e shumta ne internet.

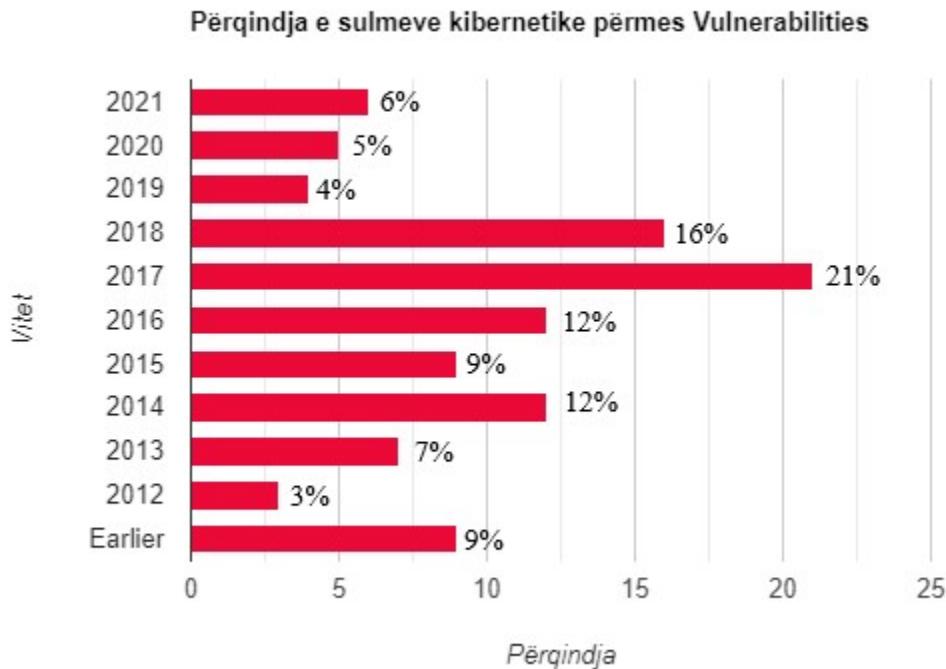


Figura 1: Përqindja e sulmeve kibernetike përmes vulnerabilities

Ndërsa në Figurën 2 kemi paraqitur përqindjen e sulmeve kibernetike që ndodhin gjatë viteve të fundit përmes dobësive të ndara sipas kategorive të cilat janë të cenueshme për aplikacionet tona.

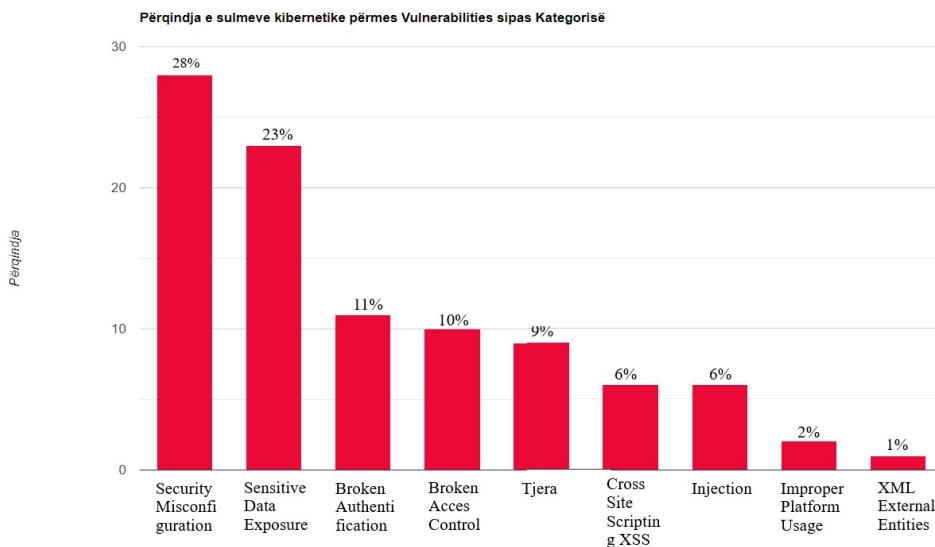


Figura 2: Përqindja e sulmeve kibernetike përmes dobësive sipas kategorisë

Andaj si rezultat i kësaj rritjeje, rëndësia e zhvillimit të metodave të reja për ti siguruar ato aplikacione gjithashtu është rritur. Për të kuptuar parimet se si të identifikohen dobësitë në lidhje me faktorët e përmendur më parë në mënyrë që të eliminohen duhet një kohë e gjatë studimi dhe përvojë praktike.

Edhe një person i cili ka një diapazon të gjerë teknik në lidhje me sigurinë e informatave dhe aplikacioneve në ueb, është gjithmonë e nevojshme të përditësohen njohuritë teknike në baza ditore, sepse ka vegla dhe shfrytëzime të reja të zbuluara nga studiues të shumtë të sigurisë në të gjithë botën.

Padyshim që njëra nga veglat që përdoret për sigurinë e informatave dhe aplikacioneve në ueb është edhe Burp Suite e cila është zhvilluar nga kompania PortSwigger në qershor të vitit 2003.

## 1. Qëllimi i punimit

Ueb aplikacionet janë rezultat i një pune intensive nga një person i vetëm ose një grup zhvillues softuerësh. Cilësia e këtyre programeve, veçanërisht nëse bëhet fjalë për mekanizmat e sigurisë është duke ndryshuar shumë çdo ditë. Edhe pse në ditët e sotme fokusi tek siguria në këto aplikacione është më lartë se që ka qenë vite më parë, ka ende shumë të meta sigurie të cilat duhet studiuar dhe zbuluar, pasi është e pamundur për garantimin e një sigurie 100 për qind. Qasja e paautorizuar ne faqe të internetit është një aktivitet i paligjshëm që ekzekutohet nga një numër i madh njerëzish nga e gjithë bota. Pavarësisht arsyes dhe qëllimit që kanë këta njerëz, këto aktivitete të cilat shkelin dhe cenojnë sigurinë nuk raportohen tek zhvilluesit e faqeve përkatëse. Në rast se pronari i një ueb aplikacioni zbulon një lloj keqpërdorimi që po ndodh, ai duhet të kuptojë se si ishte e mundur ajo qasje e paautorizuar në softuer. Andaj, zhvilluesit duhet që ueb aplikacionet e tyre të testohen nga komunitetet dhe veglat softuerike të cilat janë të besueshme për testim në mënyrë që të marrin informata dhe udhëzime të hollësishme përmes mënyrën se si ishte e mundur që të qaset softueri i tyre nga personat e paautorizuar.

Me këto informacione të dobishme, zhvilluesit do të rregullojnë dobësinë e identifikuar dhe do ta testojnë prape derisa të eliminohet. Rrjedhimisht, kjo form rritë jashtëzakonisht sigurinë e një faqe apo ueb aplikacioni në internet.

Burp Suite është një vegël e cila përdoret për qëllimet e tillë. Burp Suite është një platformë e integruar për kryerjen e testimtës së sigurisë së faqeve dhe aplikacioneve në Internet. Veglat e saj të ndryshme funksionojnë pa problem së bashku duke mbështetur të gjithë procesin e testimtës, që nga hartëzimi fillestar dhe analiza e sulmit të një aplikacioni apo faqeje, deri në identifikimin e dobësive të sigurisë. Burp lejon që përdoruesi të ketë kontrollin e plotë, duke e lejuar të kombinojë teknikat e avancuara manuale me automatizimet e fundit në mënyrë të atillë që procesi i testimtës jetë më i shpejtë dhe efektiv.

## 1.1 Avantazhet e Burp Suite

- **Ofron testimin e aplikacioneve ne ueb**

Burp Suite ofron që testimi i automatizuar si dhe ai manual mund të kryhet nga një vegël e vetme. Zakonisht, në industri veglat e automatizuara dhe manuale janë të disponueshme, por në vegla të ndryshme.

- **Skanimin dhe zbulimin e dobësive në ueb**

1. Injection
2. Broken Authentication and Session Management
3. Cross-Site Scripting (XSS)
4. Insecure Direct Object References
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Missing Function Level Access Control
8. Cross-Site Request Forgery(CSRF)
9. Burp to test Components with Known Vulnerabilities
10. Unvalid Redirects and Forwards

- **Disa lloje të skanimeve**

Krahas skanimeve që vegla Burp Suite ofron by default, ajo lejon krijimin e skanimeve të personalizuara dhe sulmeve ndaj aplikacioneve për qëllime sigurie.

- **Vepron si një shërbim Proxy**
- **Funksionon shkëlqyeshëm në një rrjet privat pa lidhje interneti.**
- **Ka një shumëllojshmëri të veglave dhe shtresave logjike.**

## 1.2 Disavantazhet e Burp Suite

- **Përdorimi**

Burp Suite nuk është një vegël nga e cili një fillestar i plotë i sigurisë do të mund të përfitojë shumë. Pasi që duhet të dihen bazat e sigurisë së aplikacioneve për të qenë në gjendje të përdoret siç duhet vegla në fjalë.

- **Përditësimi i veglës**

Burp Suite është duke u përditësuar vazhdimisht. Brenda një muaji mund të ketë nga një deri në tri versione dhe kjo shkakton pakënaqësi tek përdoruesit.

- **Ndërfaqja**

Ndërfaqja e Burp Suite është një problem i madh. Pa marrë parasysh se sa veçori ofron një softuer, nëse veçoritë nuk paraqiten mirë do t'ju mungojnë shumica e tyre kur ato të kërkohen realisht. Prezantimi i softuerit të veglës duhet të improvizohet dhe të bëhet më i paraqitshëm.

- **Mungesa e tutorialeve të Burp Suite.**

Një fillestar pothuajse humbet shumicën e kohës në gjetjen dhe kuptimin e veçorive dhe zbatimin e të njëjtave. Zhvilluesit e softuerit duhet të punojë në sigurimin e videove më të thelluara në mënyrë që njerëzit të mësojnë dhe kuptojnë konceptet.

## 2. Pjesa kryesore

### 2.1 Instalimi dhe nisja e veglës

Softueri i Burp Suite funksionon ne sisteme operative te ndryshme si Windows, Mac OS X dhe Linux. Pasi Burp Suite është i bazuar në Java, fillimisht duhet të keni të instaluar Java Runtime Enviroment (64-bit edition, verzioni 1.7 e tutje). Për të instaluar JRE-ne përmes terminalit përdorim komandën **sudo apt-get install openjdk-8-jre**.

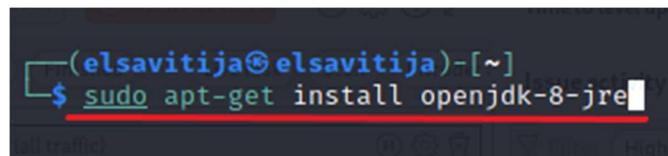


Figura 3: Komanda për instalimin e Burp Suite

Në Linux, Burp Suite është e para instaluar. Por, nëse nuk është e instaluar në ndonjë version, mund të instalohet përmes terminalit me komandën “apt-get install brupsuite”.

Në sistemet operative tjera mund të shkarkohet manualisht nga uebfaqja zyrtare e PortSwigger ne linkun <https://portswigger.net/burpsuite/download> ku versioni pa pagesë ofrohet si Community Edition.

### Professional / Community 2021.10.3



Figura 4: Instalimi manualisht i BurpSuite

Për të konfiguruar Burp Suite Community Edition përdorim këto dy komanda “**cd Downloads**” dhe “**sudo bash burpsuite community linux v2021 10 3.sh**”.

```
(elsavitija@elsavitija)-[~]
$ cd Downloads

(elsavitija@elsavitija)-[~/Downloads]
$ sudo bash burpsuite_community_linux_v2021_10_3.sh
Unpacking JRE ...
Starting Installer ...
```

Figura 5: Konfigurimi i Burp Suite Community Edition

I pranojmë termat dhe kushtet përmes opsjonit “**I Accept**”

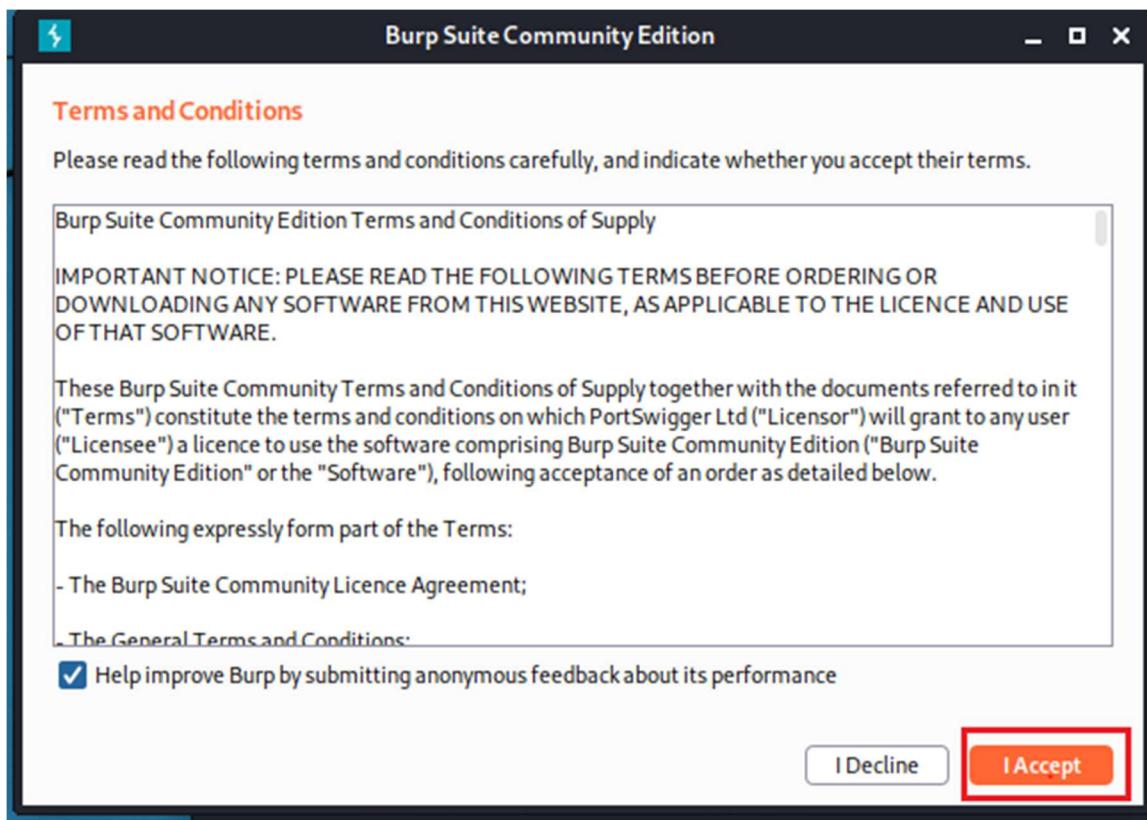


Figura 6: Dritarja e parë që shfaqet e Burp Suite

## 2.2 Hapja e veglës

Dritarja që hapet pasi pranojmë termat dhe kushtet është paraqitur ne figurën e mëposhtme e cila na lejon që të zgjedhim një projekt të përkohshëm, një projekt në të cilin kemi punuar më herët apo një projekt të ri. *Projekt i përkohshëm* zakonisht e zgjedhim si opsjon të parë sa për t'u njoftuar me aplikacionin (duke qenë edhe i vetmi opsjon i qasshëm në versionin Community), mirëpo për pentesting dhe studime të tjera të nevojshme është e preferueshme që të hapim një projekt të ri të cilil mund t'i referohemi më vonë.

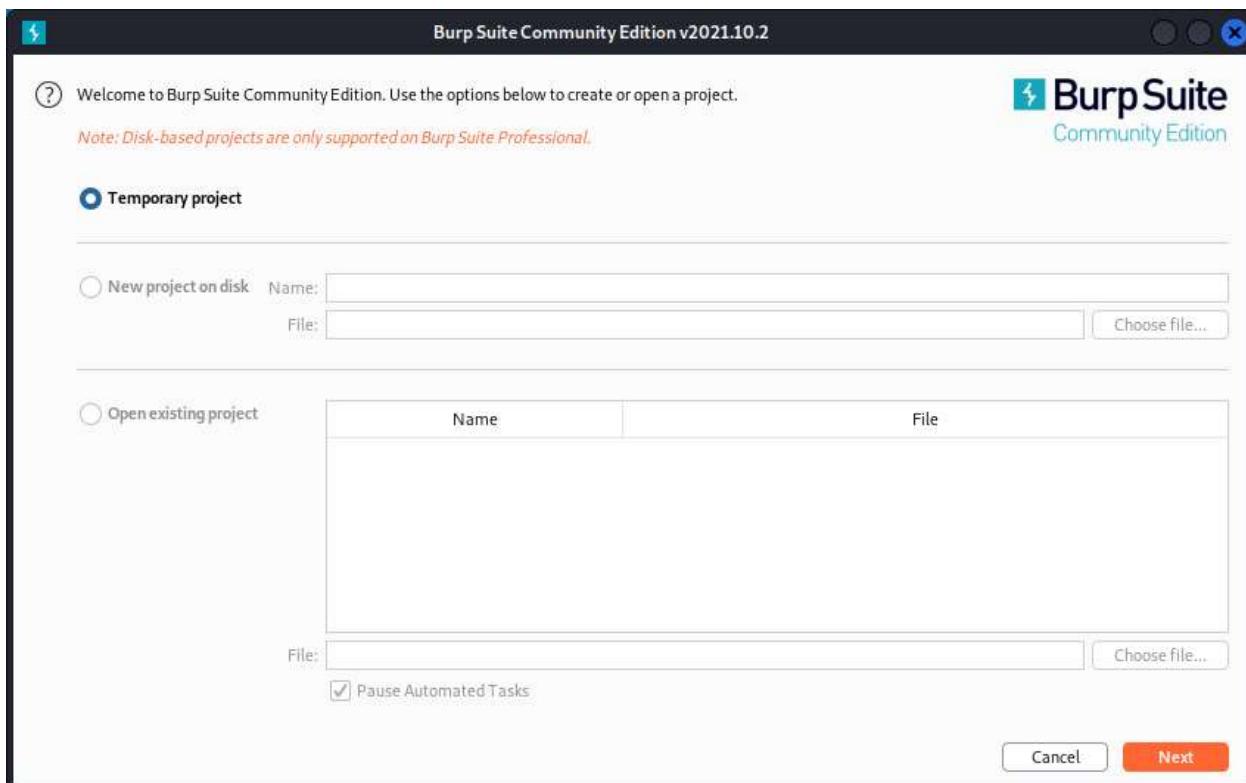


Figura 7: Burp Suite

Në dritaren e ardhshme qe është paraqitur ne figurën e mëposhtme për projektin mund të zgjedhim konfigurimet te parazgjedhura në opsjonin *Use Burp Defaults*, ose nëse janë ruajtur konfigurimet për përdorim të mëvonshëm, mund t'i hapim ato përmes opsjonit *Load from configuration file*. Në këtë rast, pasi që sapo është instaluar aplikacioni dhe nuk është përdorur më herët, është zgjedhur opzioni *Use Burp Defaults*.

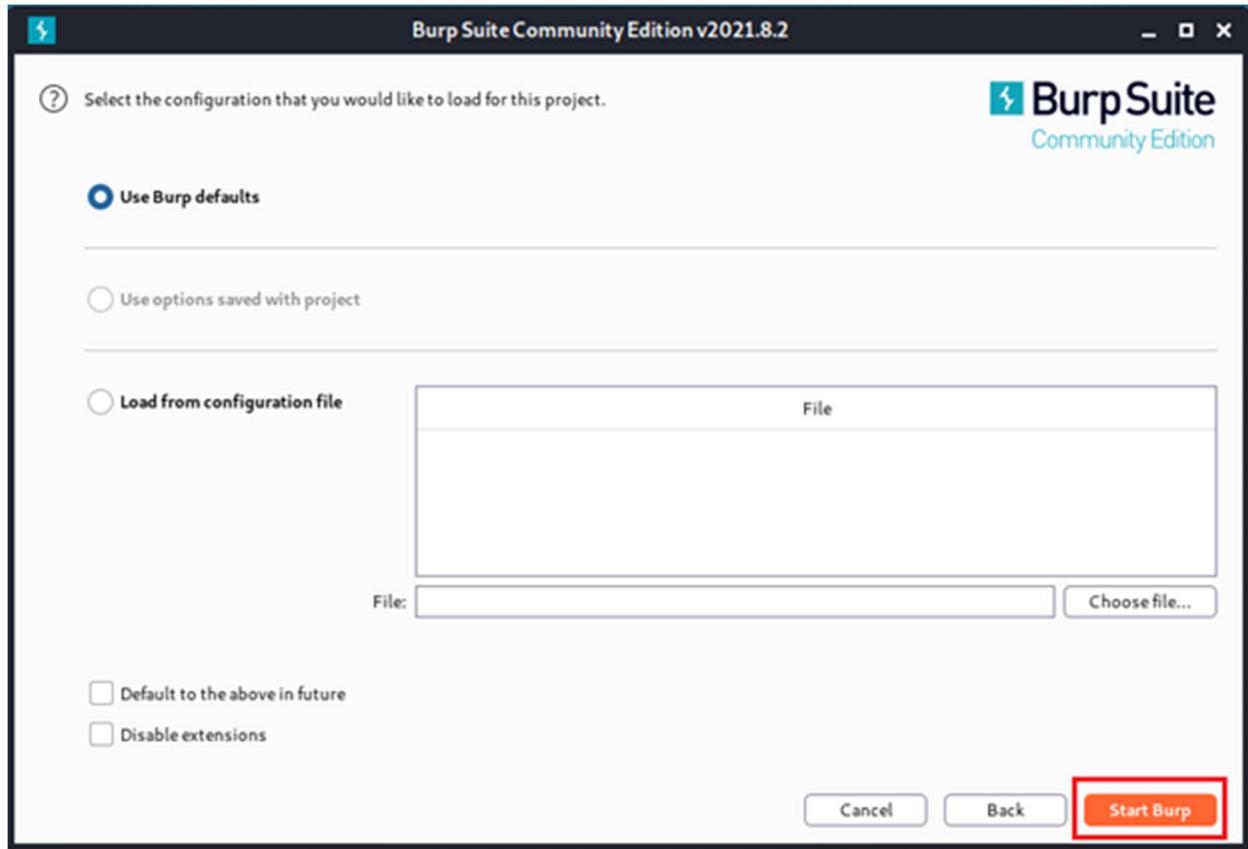


Figura 8: Burp Suite

Pasi klikohet *Start Burp*, dritarja e ardhshme paraqet dashbordin e Burp Suite Community bashkë më të gjitha opsonet që ofron ky edicion i këtij aplikacioni. Karakteristikat e secilës prej tyre do shqyrtohen në vazhdim.

# Burp Suite

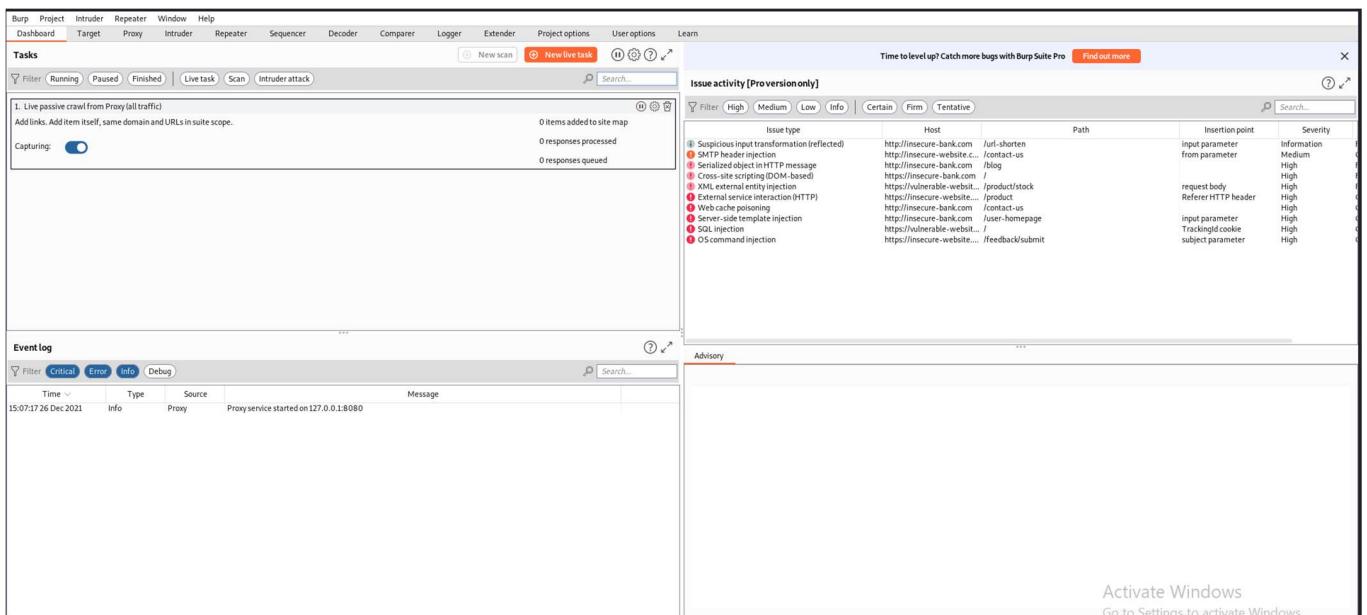


Figura 9: Burp Suite

## 2.3 Veglat e Burp Suite

Burp ose Burp Suite është një grup veglash që përdoren për testimin dhe qasjen në ueb aplikacione. Veglat te cilat gjenden ne Burp Suite jane: Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Extender, Scanner, Target, Comparer, Logger,

### 2.3.1 Target

Vegla Target ju jep një përbledhje të përbajtjes dhe funksionalitetit të aplikacionit tuaj të synuar dhe ju lejon të drejtoni pjesët kryesore të rrjedhës së punës së testimit. Vegla Target si nen meny ka edhe Site map, Scope, Issue definitions.

## Burp Suite

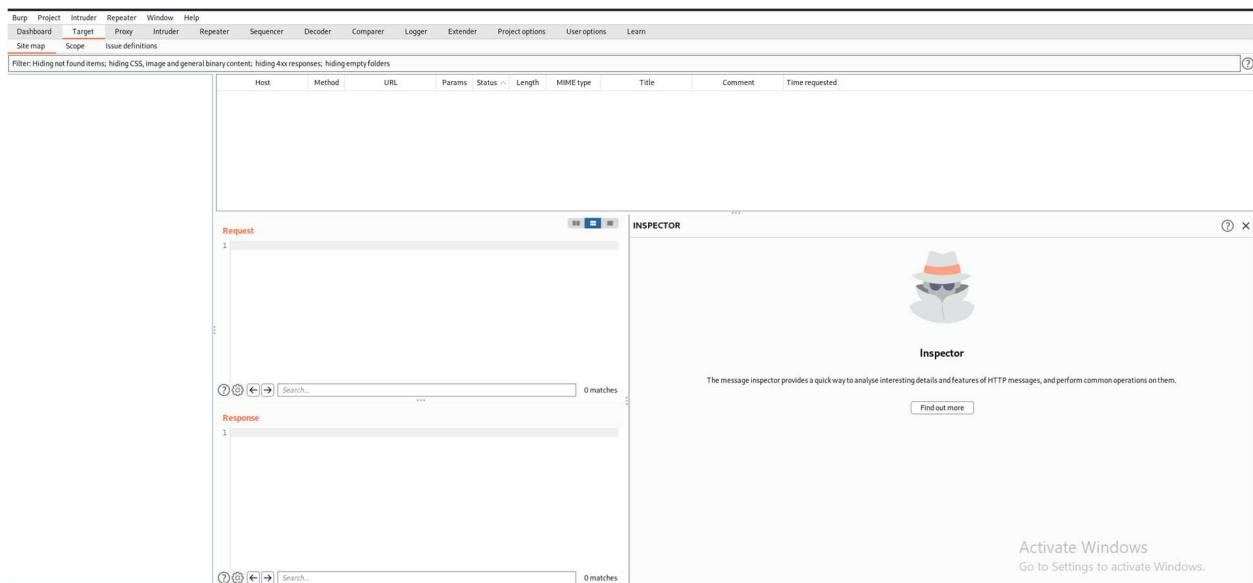


Figura 10: Target

### 2.3.2 Burp Proxy

Burp Proxy qëndron në qendër të rrjedhës së punës të drejtuar nga përdoruesit e Burp. Ai funksionon si një server proxy në internet midis shfletuesit tuaj dhe aplikacioneve të synuara, dhe ju lejon të përgjoni, inspektoni dhe modifikoni trafikun e papërpunuar që kalon në të dy drejtimet. Nëse aplikacioni përdor HTTPS, Burp prish lidhjen TLS midis shfletuesit tuaj dhe serverit, në mënyrë që edhe të dhënat e koduara të mund të shihen dhe modifikohen brenda veglave të Burp. Disa nga menyrtë e Proxy janë: Intercept, HTTP History, WebSockets history, Options.

## Burp Suite

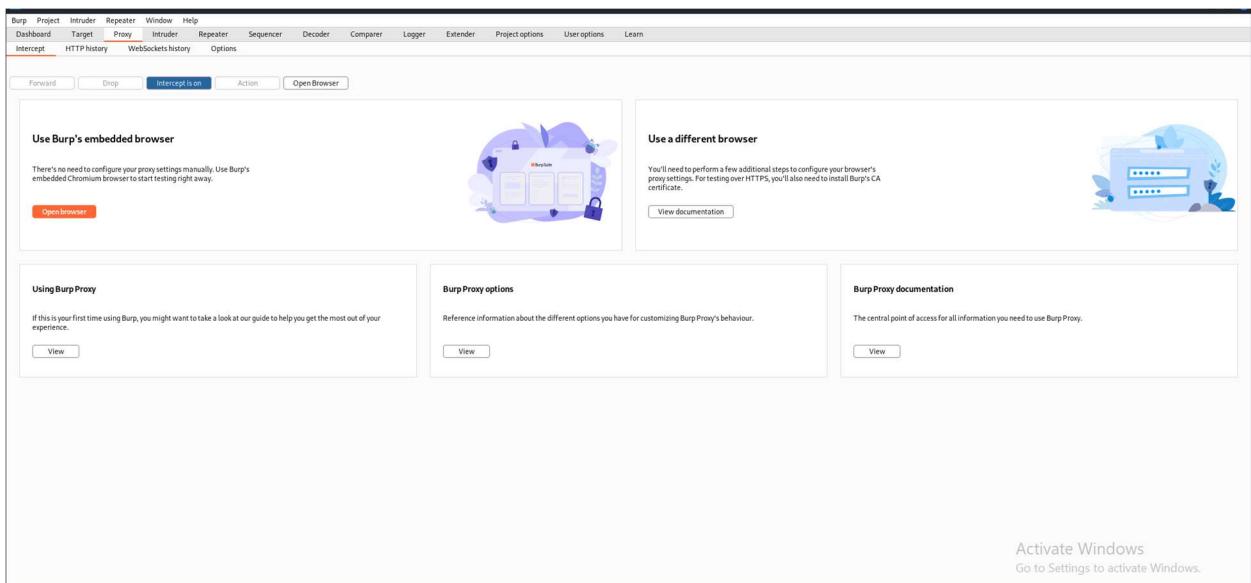


Figura 11: Proxy

### 2.3.3 Intruder

Burp Intruder është një mjet për automatizimin e sulmeve të personalizuara kundër aplikacioneve në ueb. Është jashtëzakonisht i fuqishëm dhe i konfigurueshëm dhe mund të përdoret për të kryer një gamë të madhe detyrash, nga hamendja e thjeshtë me forcë brutale e drejtorive të uebit deri te shfrytëzimi aktiv i dobësive komplekse të verbër të injektimit SQL. Disa nga opsjonet tek menya Intruder jane: Target, Positions, Payloads, Resource Pool, Options.

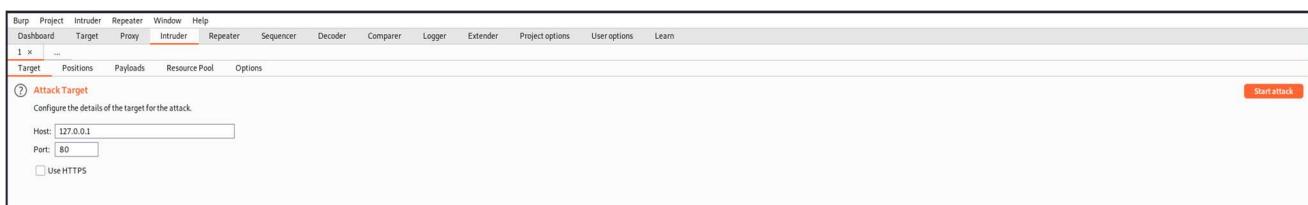


Figura 12: Intruder

### 2.3.4 Repeater

Për të përdorur Burp Repeater me mesazhe HTTP, mund të zgjidhni një mesazh HTTP kudo në Burp dhe zgjidhni Send to Repeater nga menya e kontekstit. Kjo do të krijojë një skedë të re të kërkesës në Përsëritës dhe do të plotësojë automatikisht detajet e synuara dhe redaktorin e mesazheve të kërkesës me detajet përkatëse. Përndryshe, mund të hapni manualisht një skedë të re Repeater dhe të zgjidhni opzionin HTTP.

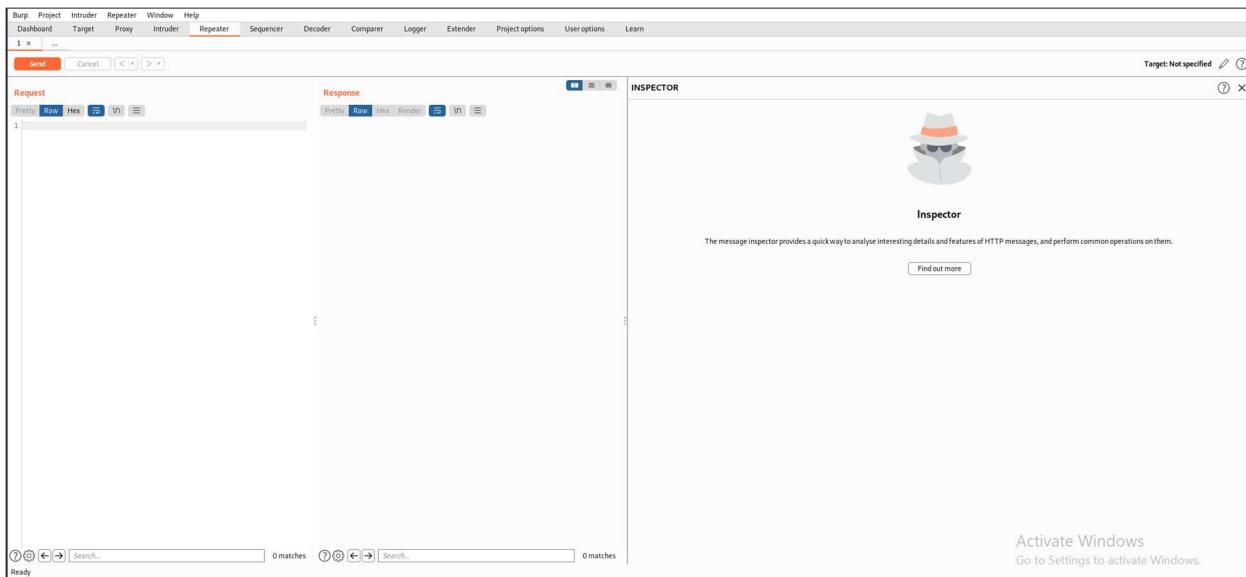


Figura 13: Repeater

### 2.3.5 Sequencer

Burp Sequencer është një mjet për të analizuar cilësinë e të dhënave. Mund ta përdorni për të testuar shenjat e sesionit të një aplikacioni ose elementët të tjera të rëndësishëm të të dhënave që synohen të jenë të paparashikueshëm, si p.sh. argumentet anti-CSRF, argumentet e rivendosjes së fjalëkalimit, etj.

# Burp Suite

The screenshot shows the Burp Suite interface with the 'Sequencer' tab selected. The main area is titled 'Select Live Capture Request' and contains instructions: 'Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".' Below this is a table with columns 'Host' and 'Request'. A 'Remove' button is on the left, and a 'Clear' button is at the bottom left. At the bottom is a 'Start live capture' button. Below this section is another titled 'Token Location Within Response' with instructions: 'Select the location in the response where the token appears.' It includes three radio buttons: 'Cookie:' (unchecked), 'Form field:' (unchecked), and 'Custom location:' (checked) with a text input field and a 'Configure' button. The final section is 'Live Capture Options' with a gear icon, containing settings for 'Number of threads' (set to 5), 'Throttle between requests (milliseconds)' (set to 0), and a checked checkbox 'Ignore tokens whose length deviates by [5] characters'.

Figura 14: Sequencer

## 2.3.6 Decoder

Burp Decoder është një mjet i thjeshtë për transformimin e të dhënave të koduara në formën e tyre kanonike, ose për transformimin e të dhënave të papërpunuara në forma të ndryshme të koduara dhe të hashuara. Ai është i aftë të njohë në mënyrë inteligjente disa formate kodimi duke përdorur teknika heuristike. Lejon enkodimin e mesazhit dekodimin apo hash-imin e tij.

The screenshot shows the Burp Suite interface with the 'Decoder' tab selected. The main area is a large empty text editor window. To its right is a toolbar with several buttons: 'Text' (selected), 'Hex', 'Decode as...', 'Encode as...', 'Hash...', and 'Smart decode'.

Figura 15: Decoder

### 3.3.7 Comparer

Burp Comparer është një mjet i thjeshtë për kryerjen e një krahasimi (një "ndryshim" vizual) midis çdo dy artikujve të të dhënave.

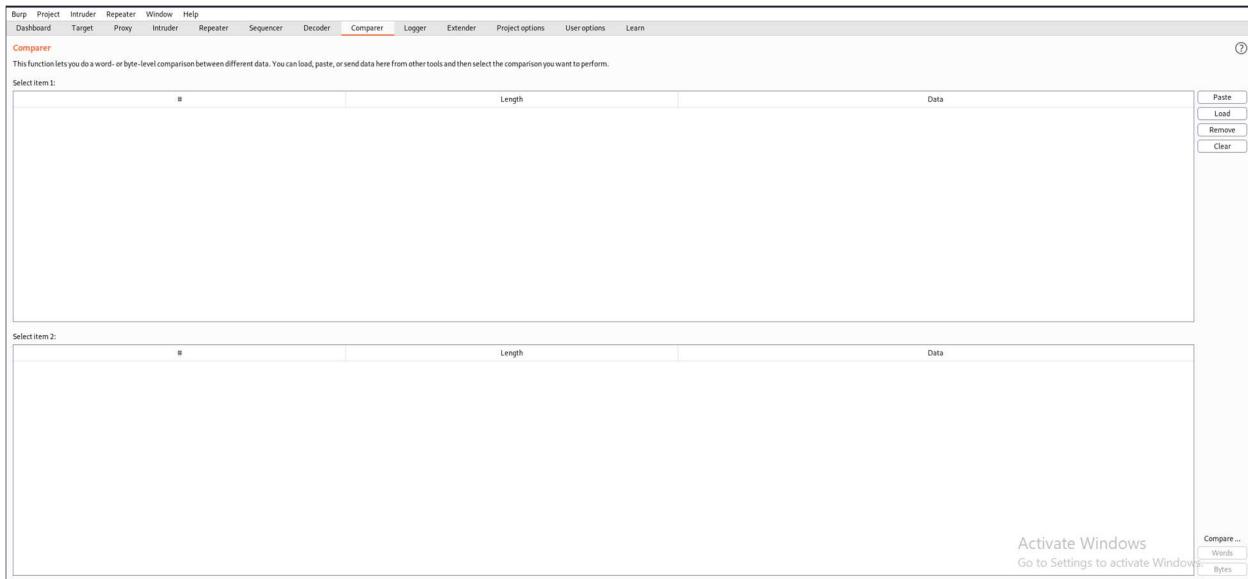


Figura 16: Comparer

### 3.3.8 Logger

Logger është një vegel për regjistrimin e aktivitetit të rrjetit. Logger regjistron të gjithë trafikun HTTP që gjeneron Burp Suite, për hetim dhe analizë.

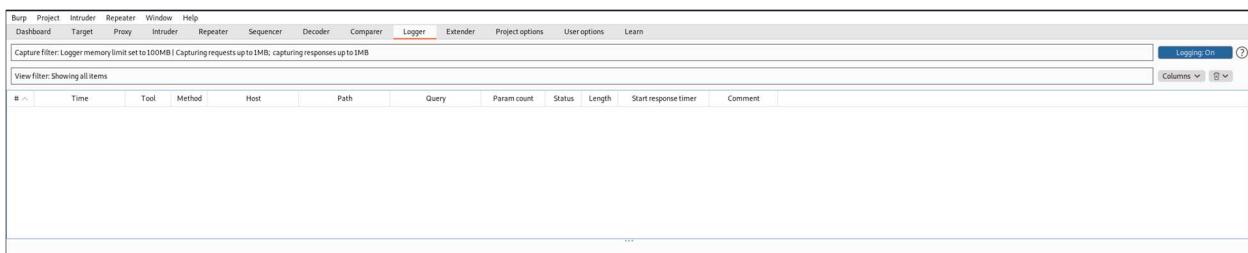


Figura 17: Logger

### 3.3.9 Extender

Burp Extender ju lejon të përdorni shtesat Burp, për të zgjeruar funksionalitetin e Burp duke përdorur kodin tuaj ose të palës së tretë. Mund të ngarkoni dhe menaxhoni shtesat, të shikoni detaje rreth shtesave të instaluara, të instaloni shtesa nga BApp Store, të shikoni API-në aktuale të Burp Extender dhe të konfiguroni opzionet se si trajtohen shtesat.

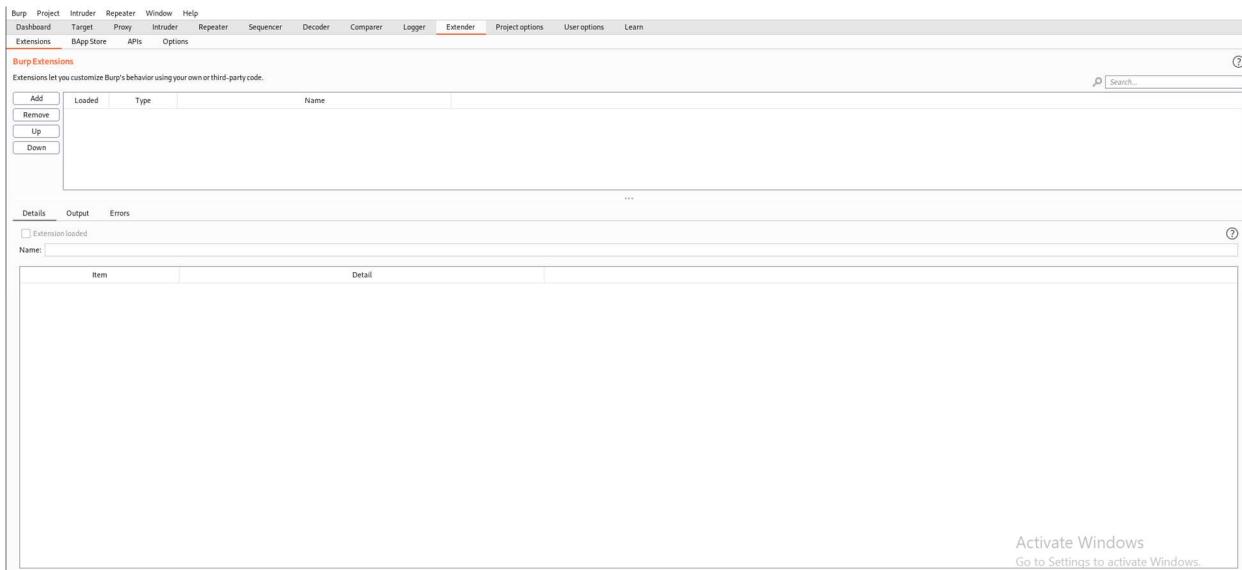


Figura 18: Extender

### 2.3.10 Project options

Burp përmban një numër të madh opSIONESH NË TË GJITHË GRUPIN QË NDIKOJNË NË SjELLJEN E TË GJITHA VEGLAVE. KËTO NDAHEN NË OPSIONE TË NIVELIT TË PROJEKTIT DHE TË NIVELIT TË PËRDORUESIT.

Disa opSIONE MUND TË PËRCAKTOHEN SI NË NIVELIN E PROJEKTIT ASHTU EDHE NË NIVELIN E PËRDORUESIT. PËR KËTO OPSIONE, JU MUND T'I KONFIGURONI OPSIONET TUAJA NORMALE NË NIVELIN E PËRDORUESIT DHE MË PAS T'I ANULONI ATO NËSE KËRKOHET NË BAZË TË PROJEKTIT.

# Burp Suite

The screenshot shows the 'Project options' tab selected in the Burp Suite interface. The main content area is divided into several sections:

- Platform Authentication:** A note states "These settings are configured within user options but can be overridden here for this specific project." with an "Override user options" checkbox.
- Upstream Proxy Servers:** A note states "These settings are configured within user options but can be overridden here for this specific project." with an "Override user options" checkbox.
- SOCKS Proxy:** A note states "These settings are configured within user options but can be overridden here for this specific project." with an "Override user options" checkbox.
- Timeouts:** A note states "These settings specify the timeouts to be used for various network tasks. Values are in seconds. Set an option to zero or leave it blank to never timeout that task." with four input fields:
  - Normal: 120
  - Open-ended responses: 10
  - Domain name resolution: 300
  - Failed domain name resolution: 60
- Hostname Resolution:** A note states "Add entries here to override your computer's DNS resolution." with a table and three buttons: Add, Edit, and Remove. The table has columns for Enabled, Hostname, and IP address.

Figura 19: Project options

## 3.3.11 User options

User options ruhen në Burp dhe ringarkohen automatikisht sa here që nis Burp. Ato gjithashtu mund të ngarkohen nga fajllat konfigurues.

The screenshot shows the 'User options' tab in the Burp Suite interface. It contains three main configuration sections:

- Platform Authentication:** This section allows you to configure Burp to automatically carry out platform authentication to destination web servers. It includes a note that these settings can be overridden for individual projects. A checkbox 'Do platform authentication' is checked, and there are buttons for 'Add', 'Edit', and 'Remove'. There is also a checkbox 'Prompt for credentials on platform authentication failure'.
- Upstream Proxy Servers:** This section determines whether Burp sends each outgoing request to a proxy server or directly to the destination web server. It lists rules based on destination host, proxy host, proxy port, auth type, and username. Buttons for 'Add', 'Edit', 'Remove', 'Up', and 'Down' are available.
- SOCKS Proxy:** This section configures Burp to use a SOCKS proxy at the TCP level. It includes a note that these settings can be overridden for individual projects. A checkbox 'Use SOCKS proxy' is checked, and input fields for 'SOCKS proxy host', 'SOCKS proxy port', 'Username', and 'Password' are provided.

Figura 20: User options

### 3. Shembuj konkret

#### 3.1 SQL Injection

Ne këtë shembull kemi përdorur ueb faqen [railsgoat.com](http://railsgoat.com) e cila është ueb faqe qe përdoret për testime. Për te hyre ne këtë ueb faqe si **admin** i saj dhe për te pasur qasjen ne email-at dhe fjalëkalimet e përdoruesve kemi përdorur **SQL Injection** me ndihmën e Burp Suite.

**Hapi 1:** Hapim një llogari ne ueb faqe qe është paraqitur ne figurën e mëposhtme. Shënojmë te dhënat e kërkuar dhe një fjalëkalim ne këtë rast fjalëkalimin e kemi vendosur 12345678.

The screenshot shows a web browser window with the URL [158.247.210.231/railsgoat/signup?](http://158.247.210.231/railsgoat/signup?). On the left, there's a sidebar with navigation links for various security tutorials. The main content area is titled "Sign Up" with the sub-instruction "Fill out the form below to login". It contains four input fields: "Email" (Alberana@gmail.com), "First Name" (Alberana), "Last Name" (Tufiq), and two "Password" fields (both containing the value "12345678"). A "Submit" button is at the bottom right. The browser's address bar shows the full URL.

Figura 21: Dritarja e Signup në ueb faqen Railsgoat

**Hapi 2:** Pastaj klikojmë Submit dhe shfaqet një dritare e re si shfrytëzues qe jemi.

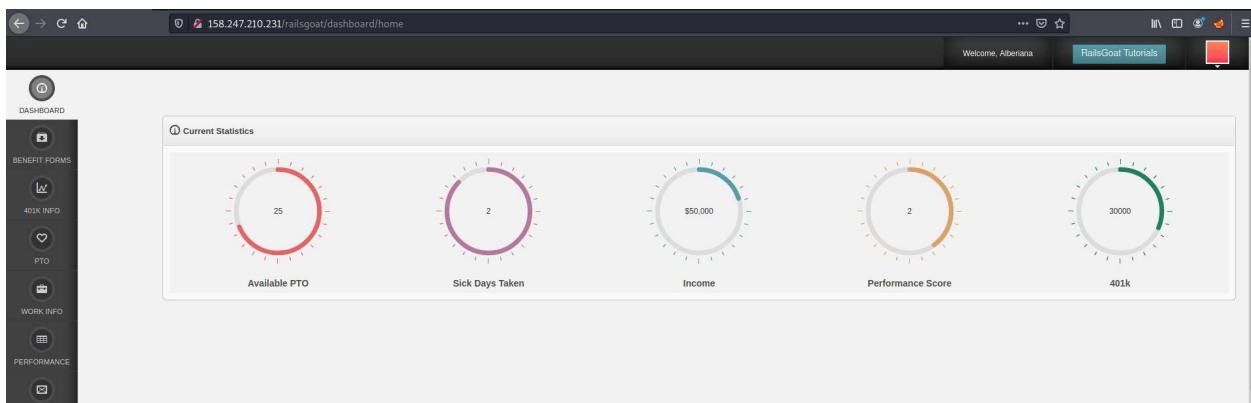


Figura 22: Dritarja e shfrytezuesit

Vazhdojmë tek **account settings** dhe shfaqet dritarja me të dhënat qe kemi shënuar ne fillim.

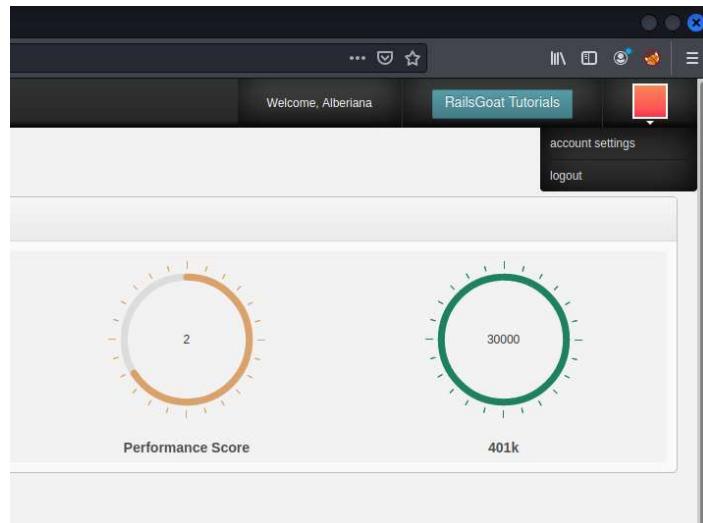


Figura 23: Profili i shfryezuesit

The screenshot shows a 'Profile Settings' form. On the left is a sidebar with icons for Dashboard, Benefit Forms, 401k Info, PTO, Work Info, Performance, Messages, and Pay. The main area has a title 'Profile Settings' with a note 'Edit your account details'. It contains fields for Email (Alberiana@gmail.com), First name (Alberiana), Last name (Tofaj), Password (Enter Password), and Password confirmation (Enter Password). A 'Submit' button is at the bottom right.

Figura 24: Account settings

**Hapi 3:** Në mënyrë që të vazhdojmë punën në **Burp Suite FroxyProxy-n e zgjedhim Burp Suite(127.0.0.1 8080).**

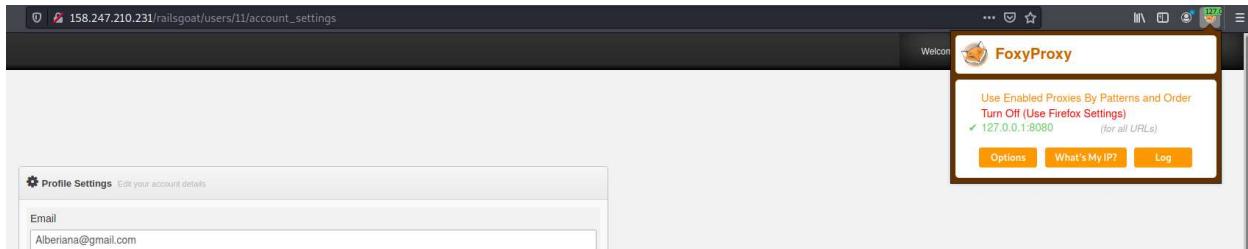


Figura 25: FoxyProxy ne Burp Suite

**Hapi 4:** Pastaj vazhdojmë në Burp Suite.

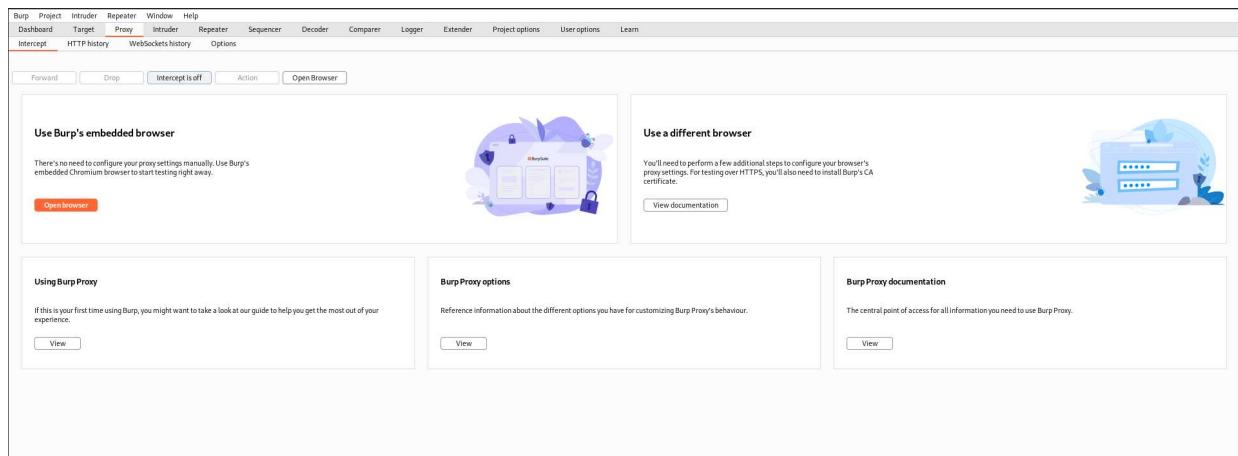


Figura 26: Burp Suite

**Hapi 5:** Shënojmë përsëri fjalëkalimin te **profile settings**.

**Profile Settings** Edit your account details

Email  
Alberiana@gmail.com

First name  
Alberiana

Last name  
Tofaj

Password  
\*\*\*\*\*

Password confirmation  
\*\*\*\*\*

Submit

Figura 27: Profile Settings

**Hapi 6:** Pasi klikojmë butonin **Submit** hapet dritarja e Burp Suite e paraqitur si më poshtë.

```

POST /railsgoat/users/11.json HTTP/1.1
Host: 158.247.210.231:80
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 277
Origin: http://158.247.210.231
Connection: close
Referer: http://158.247.210.231/railsgoat/users/11/account_settings
Cookie: railsgoat_session=BhA7C6H...; csrf_token=000gZP9k1JWiv2wRlMDMkHTlxMj002027TMhMwIwTQYzE509F8jsAVBzEP9jc3jwX8vra2wV8jsPARki1Mj9eGDEZm5K2h9JanlpM2PrJ0JUTY0T2[qMjJW0FphNT0]eJhB1S0k9bjcARKk1Dh7ZKjfaM002vB6aR430+994fd517757hd9cc09b9c4cce8315760c6f8d698
14
15 utfo=tEZ29C98L method=put&authenticity_token=j7x0enJe0iyy17akSRa0640ij9RUsAincS89PpbkC130&user_id=5011&user58email%50=Alberiana%40gmail.com&user58first_name%50=Alberianauuser58last_name%50=Tofaj&user58password%50=12345678&user58password_confirmation%50=12345678

```

Figura 28: Proxy Intercept

## Për të vazhduar pastaj në tab-in Repeater.

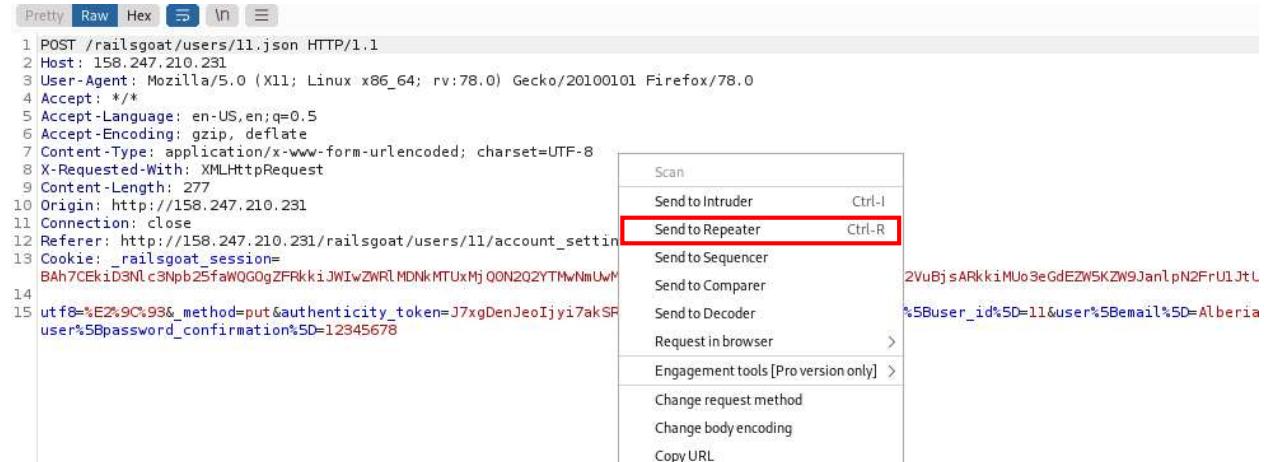


Figura 29: Proxy Intercept 2

## Tab-i Repeater është paraqitur në figurën e mëposhtme.

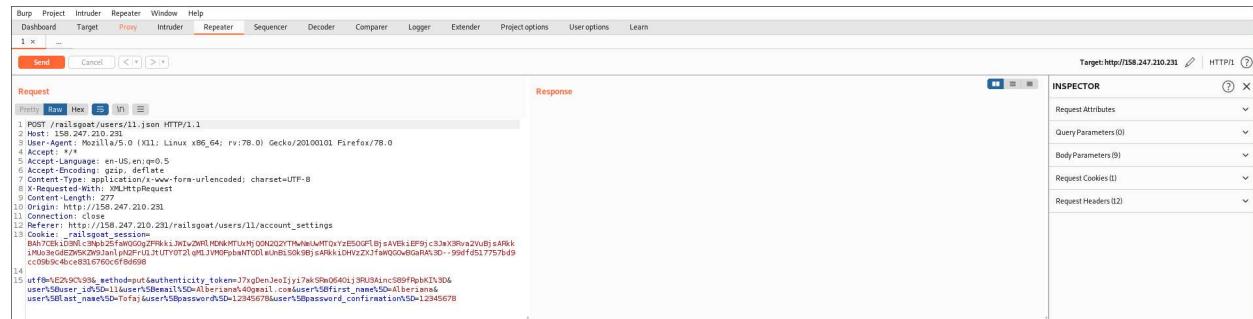


Figura 30: Kodi në Repeater para injektimit

Tek **Repeater** në pjesën e **Request** rreshtin e 15-te shënojmë kodin qe nevojitet për të pasur qasje në ueb faqe si **admin** me fjalëkalimin që e kemi shënuar më parë. Kodi i cili do të shtohet tek rreshti i 15 në pjesën pas **`id%5D=11`** shënohet ‘`) or admin='t' – ‘“`. Poashtu fshijmë pjesën tek kodi e cila nuk është e nevojshme. Dhe klikojmë **Send**.

## Burp Suite

Figura 31: Kodi në Repeater pas injektimit

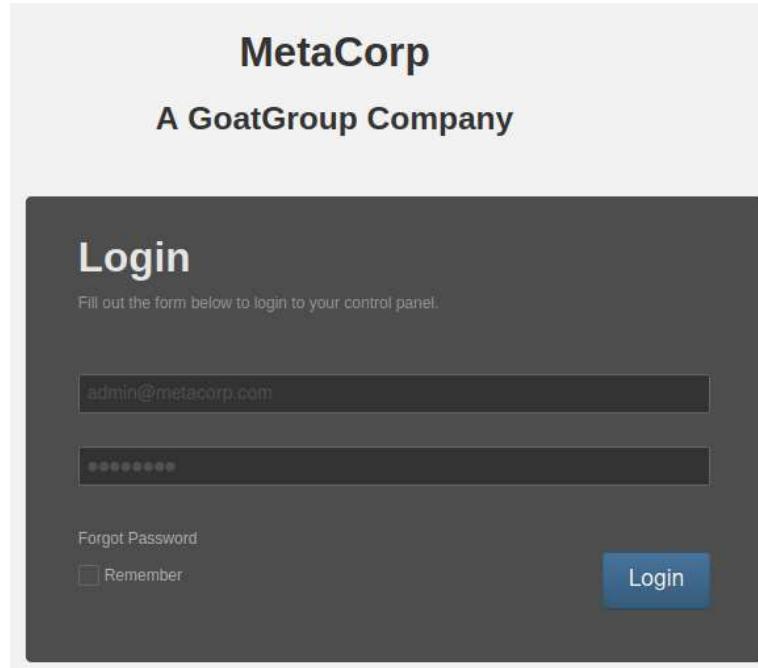


Figura 32: Login dritarja

Pasi klikojmë **login** në qasemi si **admin** mund të kemi qasje në të gjithë **account** të shfrytëzueseve.

Name	Email	Admin User	Action
Admin	admin@metacorp.com	✓	Edit
Alberiana Tofaj	Alberiana@ana.com		Edit
Alberiana.Tofaj	Alberiana@gmail.com		Edit
Jack Mannino	jack@metacorp.com		Edit
Jim Manico	jim@metacorp.com		Edit
k coin	kocinoy849@wolfpat.com		Edit
k for	kocinoy849@wolfpat.com		Edit
Ken Johnson	ken@metacorp.com		Edit
Mike McCabe	mike@metacorp.com		Edit
silent hm	maazm7391@gmail.com		Edit

Figura 33: Qasja në ueb faqe si admin

## 3.2 One Time Password (OTP)

**OTP(One Time Password)** është një fjalëkalim një kohor i cili përdoret një herë për të hyrë në një llogari të regjistruar. Ai është një mekanizëm përmes të cilit shfrytëzuesi mund të identifikohet në një rrjet vetëm gjatë një periudhe kohore të vetme.

Në vazhdim do ta gjeni të gjithë procesin të shpjeguar se si mund të anashkalojmë OTP duke përdorur Burp-Suite.

**Hapi 1:** Hapim një faqe e cila është e eksposuar ndaj dobësive: <https://glamgalscosmetics.ng/> dhe klikojmë **Sign Up**.

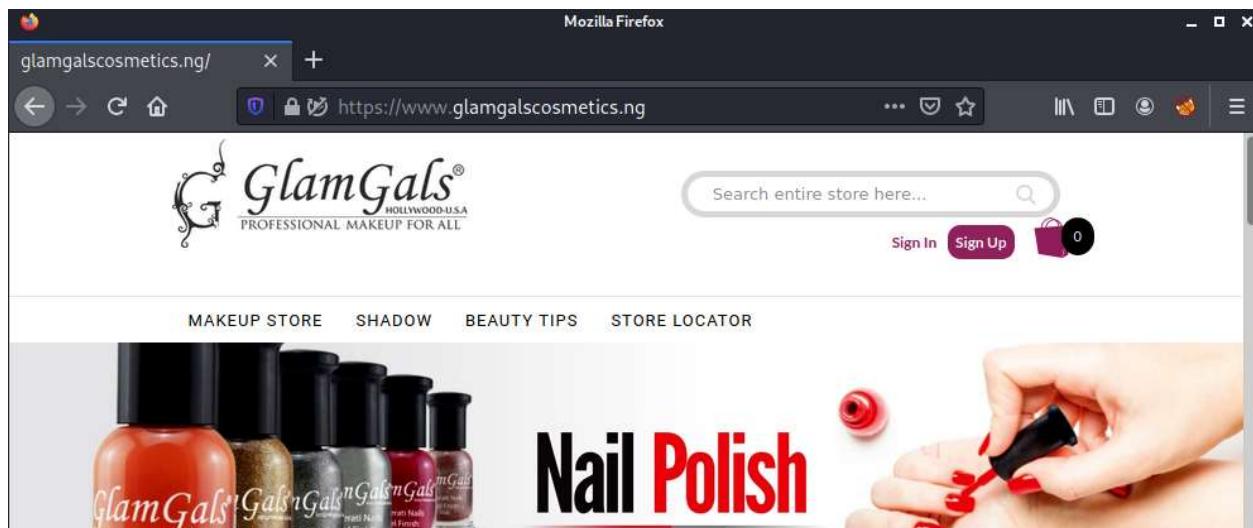


Figura 34: Startimi i faqe GlamGals e cila është e eksponuar ndaj dobësive

Pasi kemi klikuar në Sign Up hapet faqja e cila shihet ne figurën e mëposhtme e cila kërkon plotësimin e te dhënavë.

A screenshot of a Mozilla Firefox browser window showing the sign-up form for the GlamGals website. The URL is https://www.glamgalscosmetics.ng/signup.php. The form is titled 'SIGN UP' and has a 'Create account' section. It includes fields for 'Username' (filled with 'BlueBird'), 'Email' (filled with 'bluebbird2021@gmail.com'), 'Country' (selected 'NIG +234'), 'Verification code' (filled with '3834450712'), 'Get Code' (button), 'Password' (empty), 'Re-Password' (empty), and a 'SUBMIT' button at the bottom.

Figura 35: Plotësimi i username, emailit dhe numrit te telefonit

## Hapi 2: Hapim veglën Burp Suite

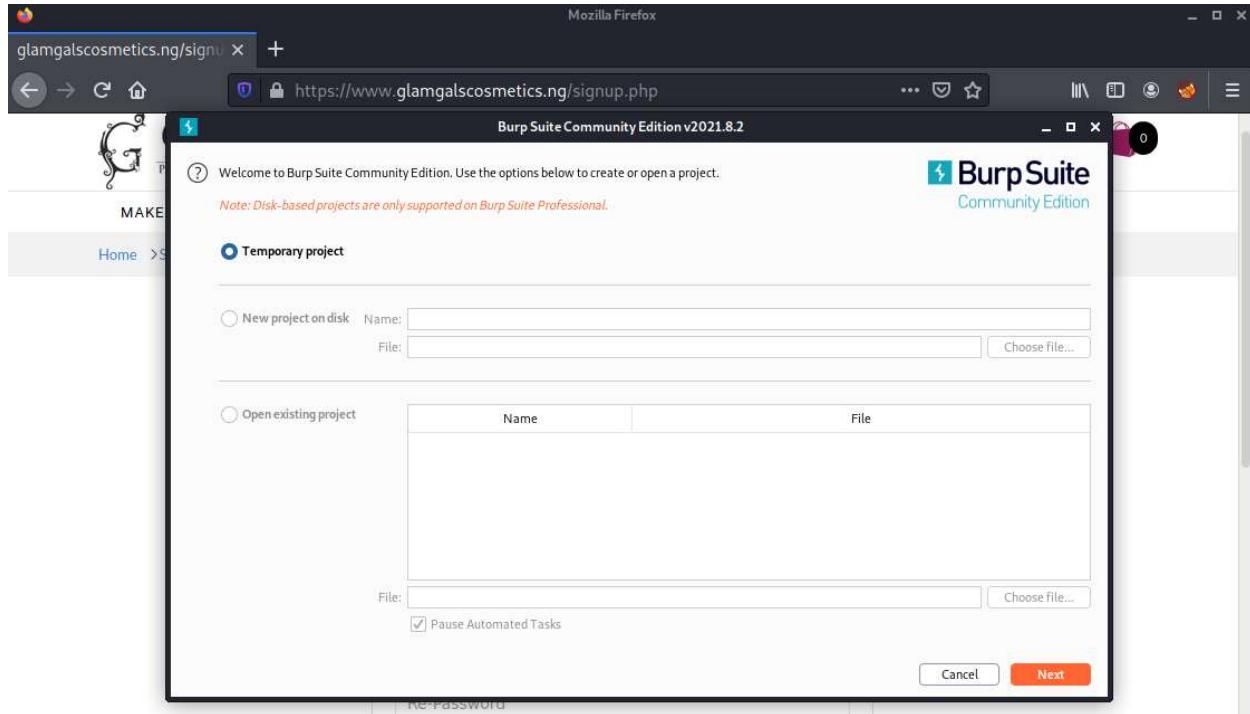


Figura 36: Startimi i Burp Suite 1

## Burp Suite

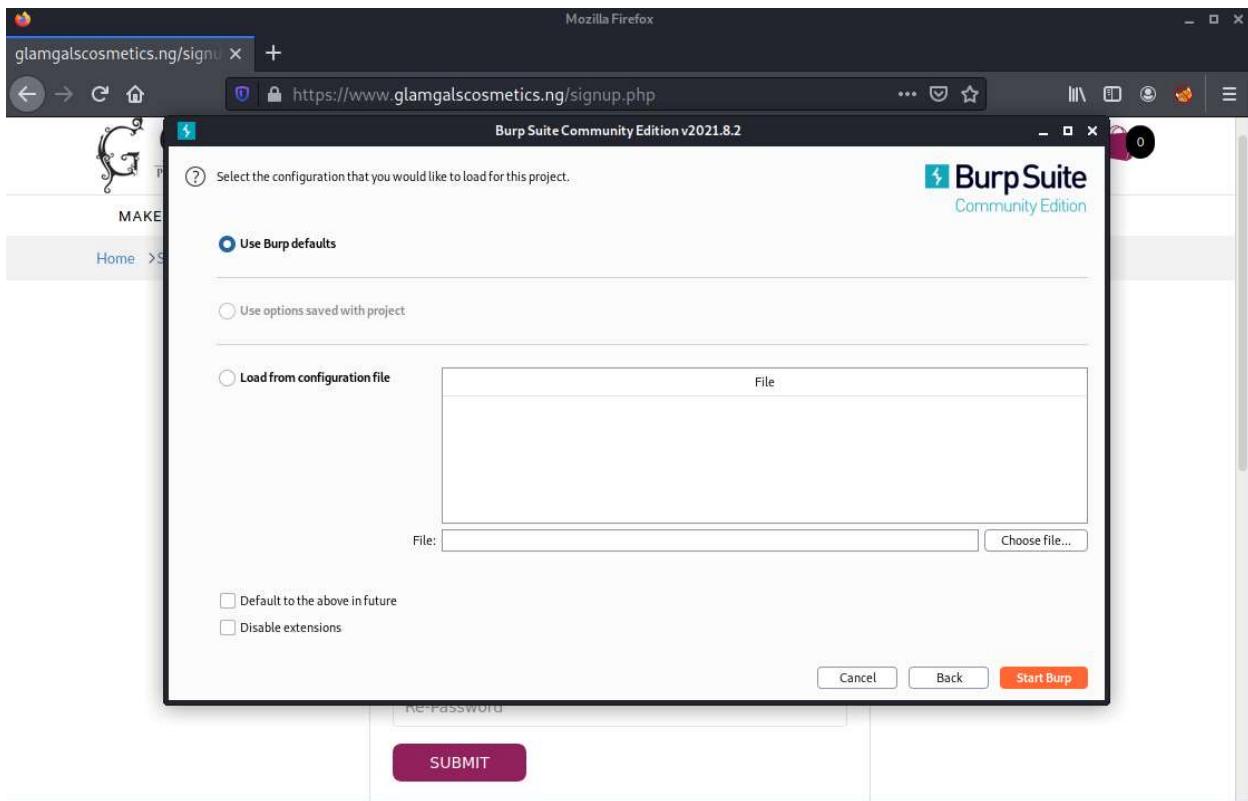


Figura 37: Startimi i Burp Suite 2

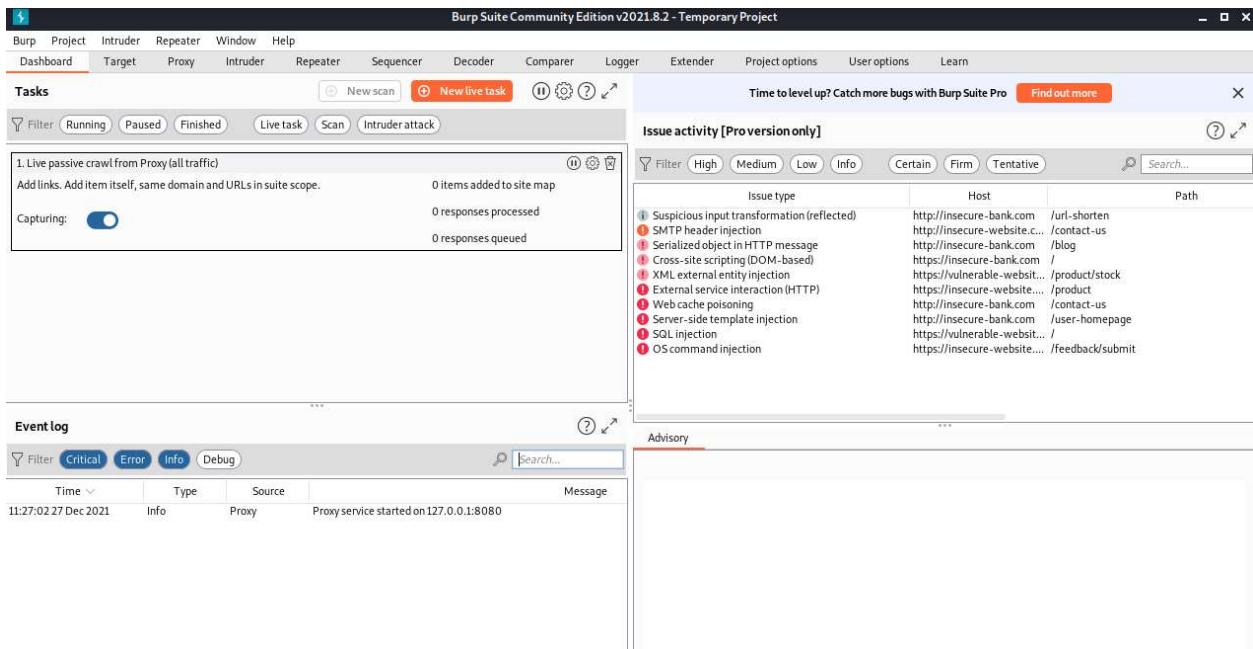


Figura 38: Startimi i Burp Suite 3

## Klikojmë tek menyja **Proxy** dhe nënmenyja e Proxy **Intercept**

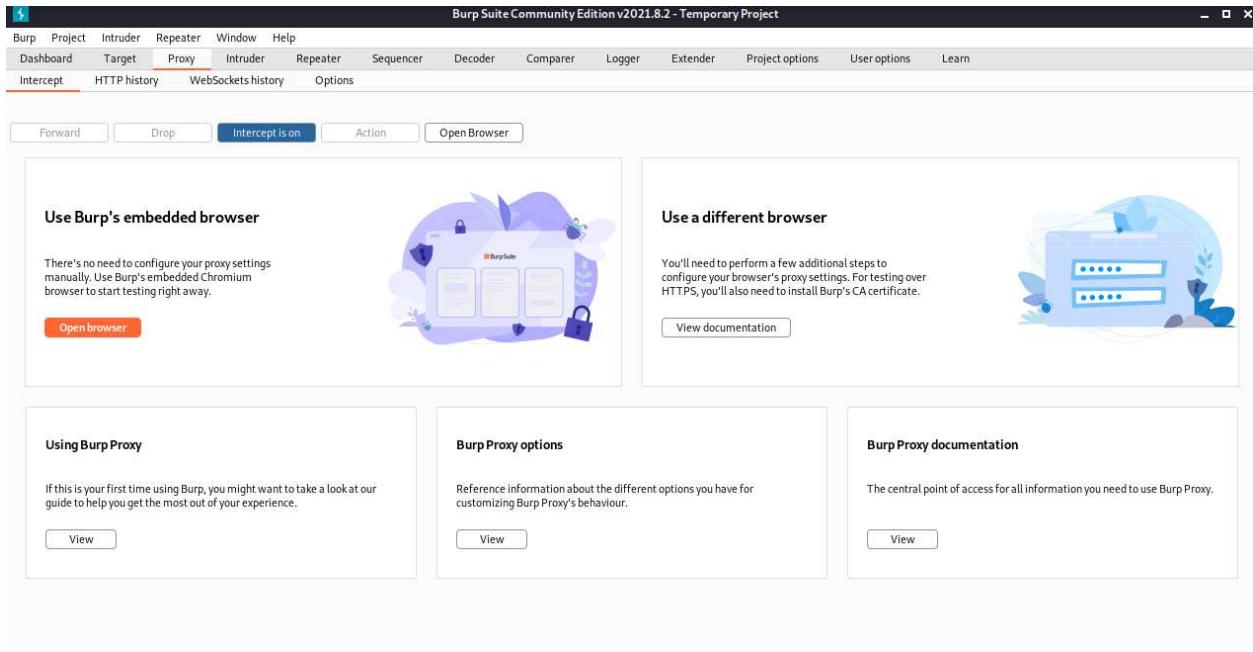


Figura 39: Burp Suite pasi kemi klikuar tek menyja **Proxy** dhe nënmenyja **Intercept**

Shohim se **Intercept** është **ON** tek Burp Suite, dhe klikojmë **GetCode** tek faqja paraprake:

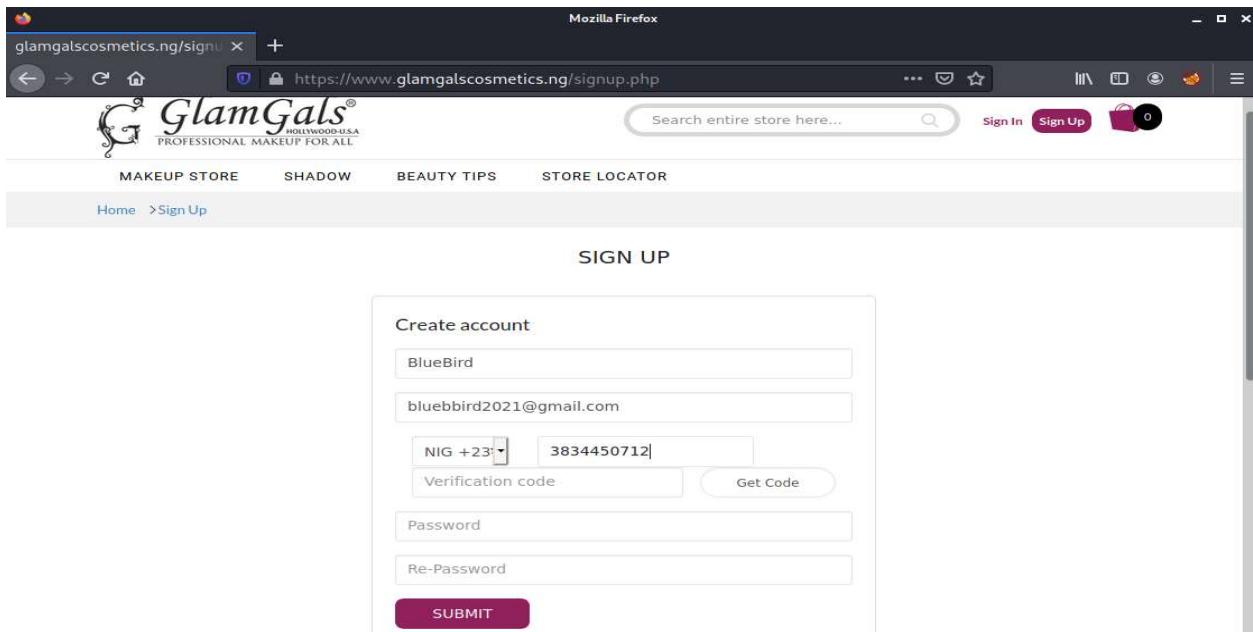


Figura 40: Klikimi i butonit Get Code te faqja Glam Gals

Ndërkohë, Burp Suite ka filluar ti detektojë dhe skanojë paketat me të dhëna në rrjet .

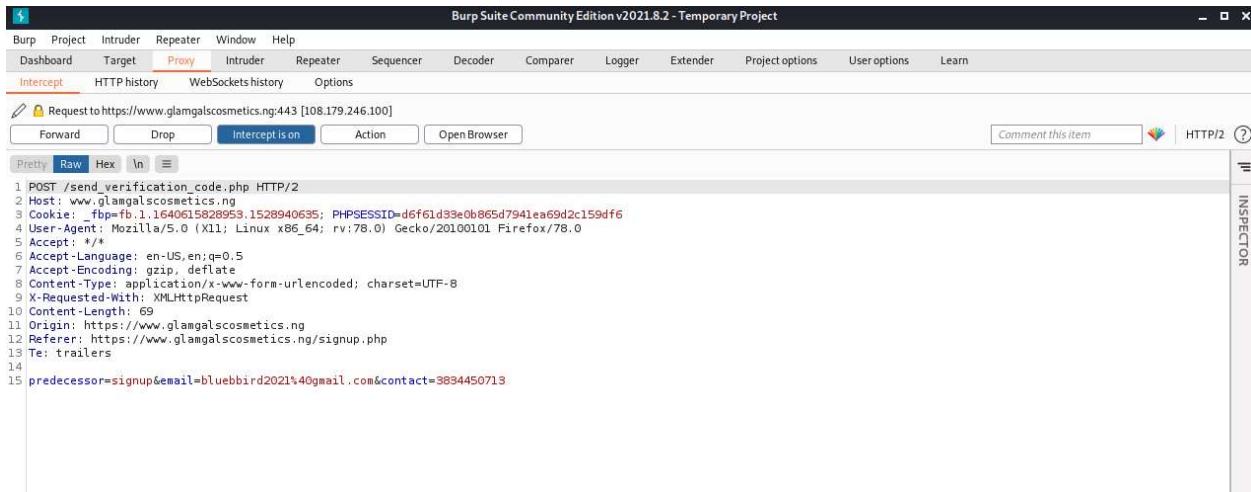


Figura 41: Detektimi i të dhënavës dhe mbledhja e informatave tek Burp Suite

Pasi që ka filluar detektimi dhe mbledhja e informatave tek Burp Suite, tek faqja paraprake është shfaqur një njoftim i cili është i shfaqur ne figurën e mëposhtme.

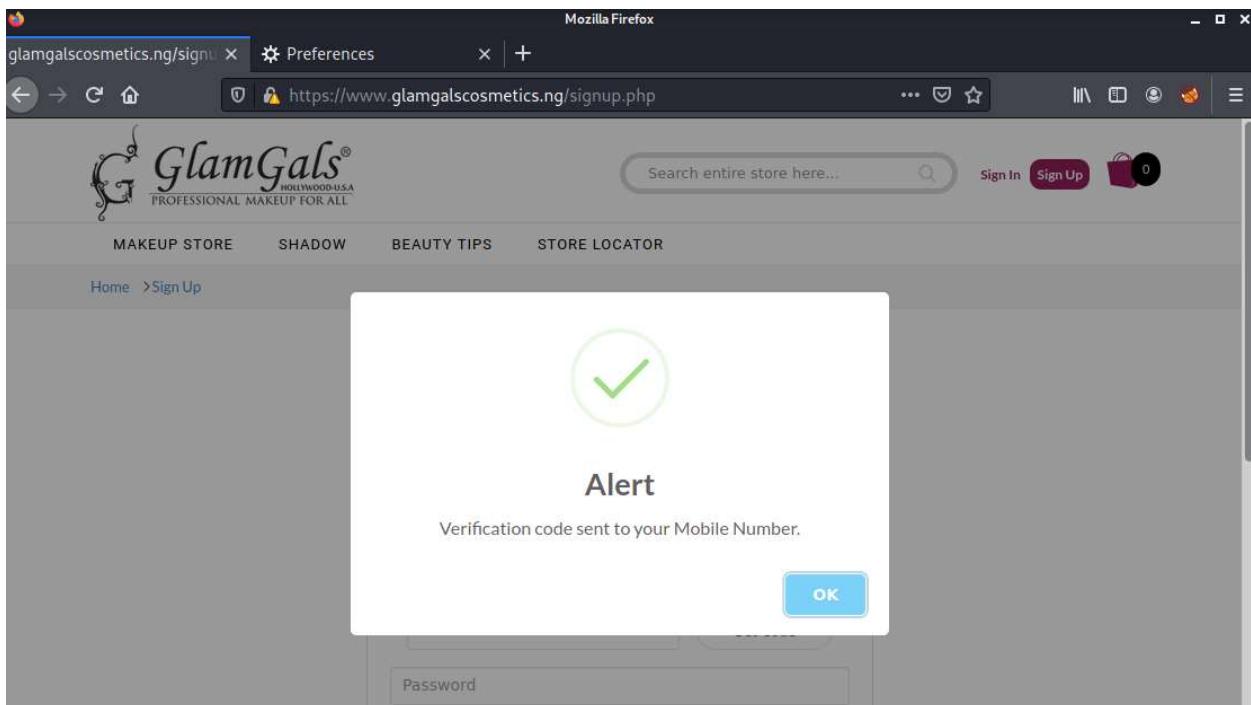


Figura 42: Njoftimi se kodi i verifikimit është dërguar ne numrin e telefonit qe përdoruesi ka plotësuar gjate fazës së regjistrimit.

### Hapi 3: Pasi qe rikthehemti tek Burp Suite, klikojmë tek nënmenyja **HTTP History** e menysë Proxy

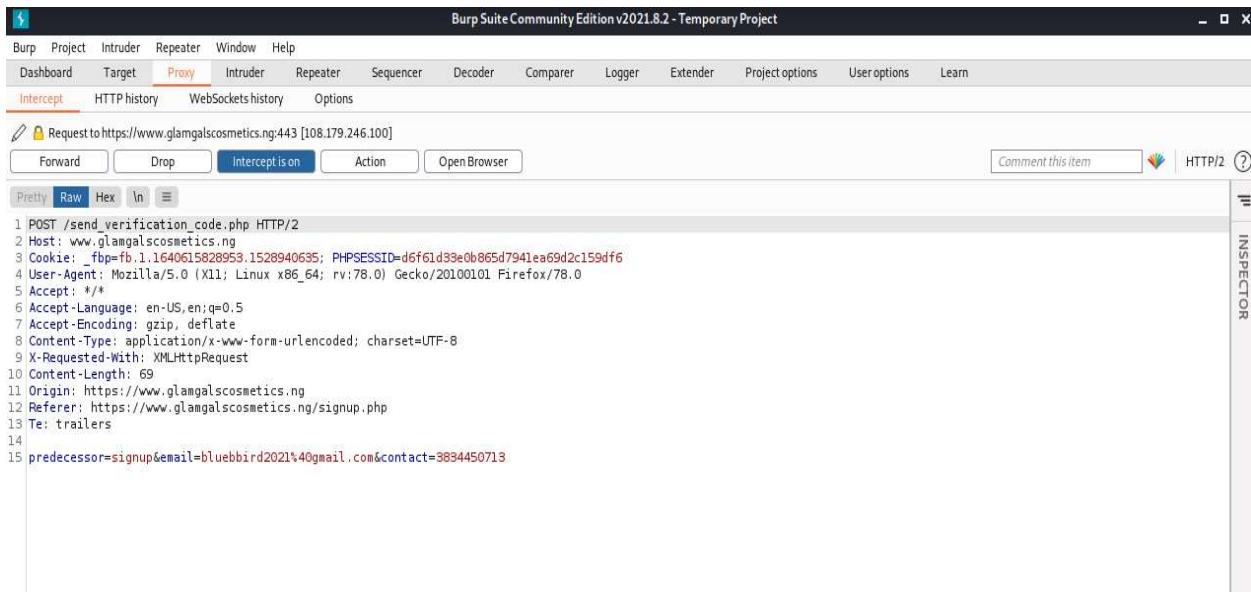


Figura 43: Nënmenyja HTTP History e menysë Proxy

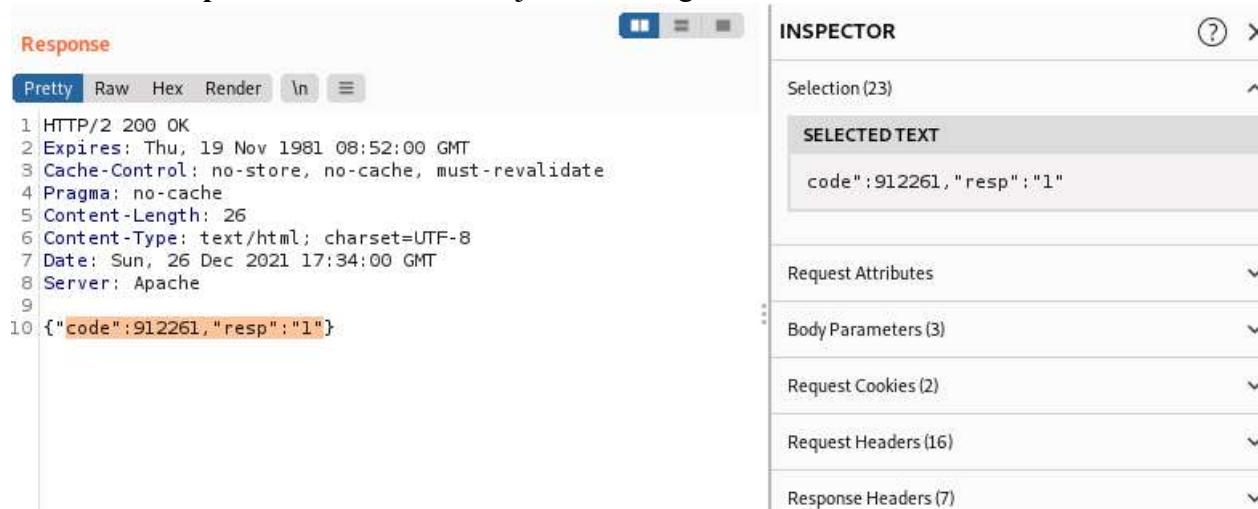
#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP
1	https://www.glamgalscosmetics...	GET	/signup.php			200	44209	HTML	php		✓	108.179.246.100	
3	https://www.glamgalscosmetics...	GET	/js/megamenu.js			304	148	script	js		✓	108.179.246.100	
6	https://www.glamgalscosmetics...	GET	/js/jquery-1.11.1.min.js			304	148	script	js		✓	108.179.246.100	
11	https://www.glamgalscosmetics...	GET	/js/jquery.scrollUp.min.js			304	148	script	js		✓	108.179.246.100	
12	https://www.glamgalscosmetics...	GET	/js/slides.js			304	148	script	js		✓	108.179.246.100	
13	https://www.glamgalscosmetics...	GET	/js/scrollBar.js?load=6			304	148	script	js		✓	108.179.246.100	
14	https://www.glamgalscosmetics...	GET	/js/owl.carousel.js			304	148	script	js		✓	108.179.246.100	
16	https://www.glamgalscosmetics...	GET	/js/bootstrap.min.js			304	148	script	js		✓	108.179.246.100	
17	https://www.glamgalscosmetics...	GET	/js/menu_jquery.js			304	148	script	js		✓	108.179.246.100	
18	https://www.glamgalscosmetics...	GET	/js/simpleCart.min.js			304	148	script	js		✓	108.179.246.100	
31	https://www.glamgalscosmetics...	GET	/signup.php			200	44209	HTML	php		✓	108.179.246.100	
32	https://www.glamgalscosmetics...	POST	/send_verification_code.php		✓	200	264	JSON	php		✓	108.179.246.100	
33	https://www.glamgalscosmetics...	POST	/send_verification_code.php		✓	200	266	JSON	php		✓	108.179.246.100	

Figura 44: Përbajtja e nënmenysë HTTP History

Pas klikimit te **HTTP History**, shkojmë tek tabela me informata qe ka mbledhur Burp Suite dhe klikojmë tek rreshti me url **send\_verification\_code.php**, sepse ne më herët kemi kërkuar kodin e verifikimit përmes numrit të telefonit.

Pasi klikimit të [url:send\\_verification\\_code.php](#) hapen dy tabela **Request** dhe **Response** me informata për faqen **Glam Gals**.

Tek tabela **Response** kemi informata vijuese si në figurë:



The screenshot shows the Burp Suite interface with the 'Response' tab selected. The response body is displayed in 'Pretty' format:

```

1 HTTP/2 200 OK
2 Expires: Thu, 19 Nov 1981 08:52:00 GMT
3 Cache-Control: no-store, no-cache, must-revalidate
4 Pragma: no-cache
5 Content-Length: 26
6 Content-Type: text/html; charset=UTF-8
7 Date: Sun, 26 Dec 2021 17:34:00 GMT
8 Server: Apache
9
10 {"code":912261,"resp":"1"}

```

The line "10 {"code":912261,"resp":"1"}" is highlighted in orange. To the right, the 'INSPECTOR' panel is open, showing the selected text "code":912261,"resp":"1" under the 'SELECTED TEXT' section. Other sections like Request Attributes, Body Parameters, Request Cookies, Request Headers, and Response Headers are also visible.

Figura 45: Përbajtja e tabelës Response

Tek teksti i selektuar kemi kodin verifikues për krijimin e llogarisë ne faqen Glam Gals, kodi ky i njëjtë i cili është dërguar edhe në numrin e telefonit.

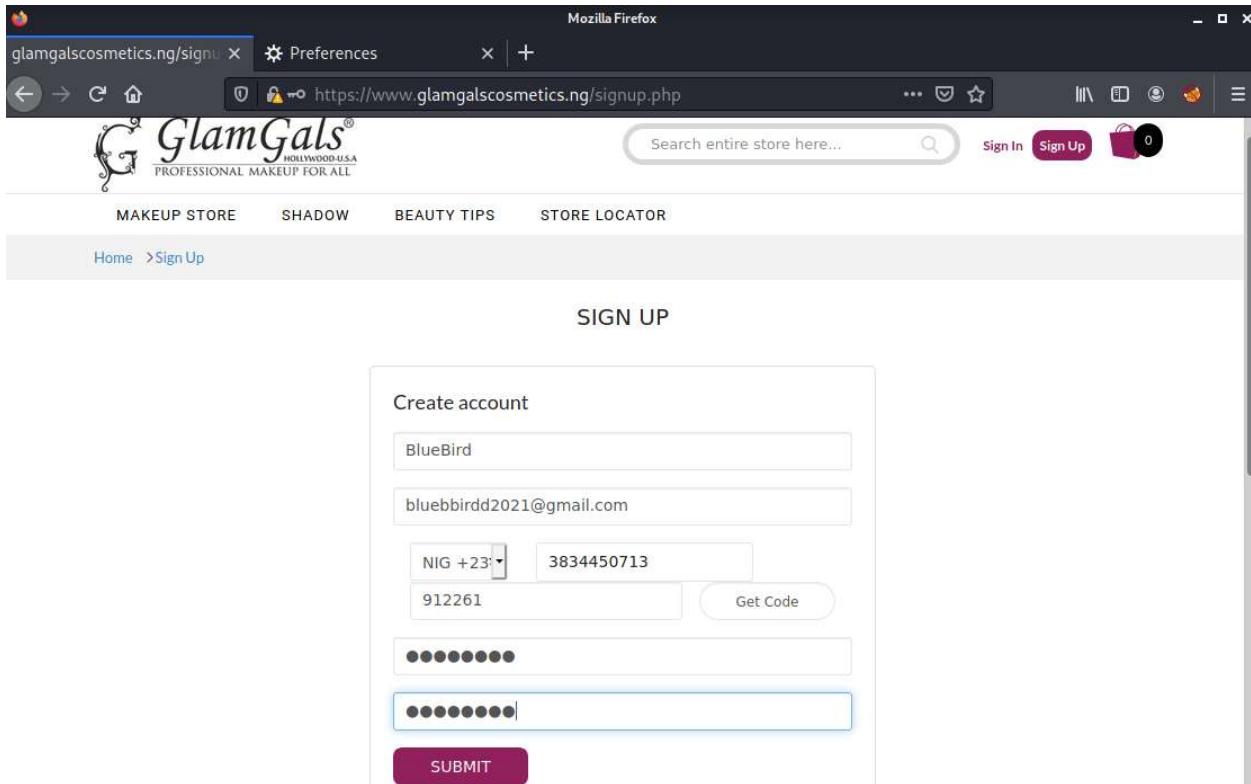


Figura 46: Plotësimi i të dhënave të mbetura dhe krijimi i llogarisë

Pas krijimit të llogarisë kemi kaluar tek dritarja e cila shihet ne figurën vijuese.

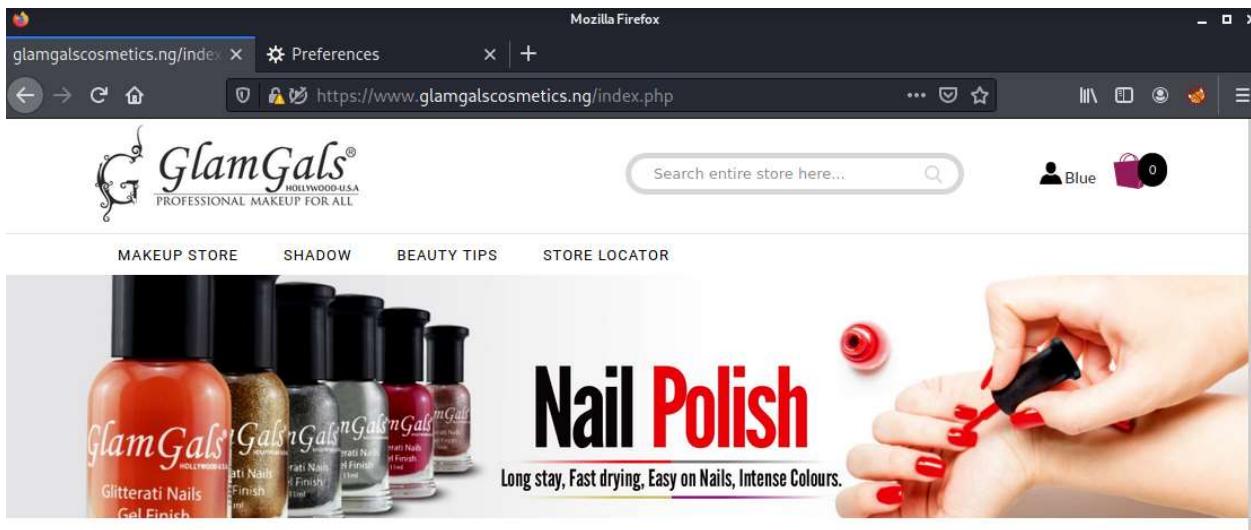


Figura 47: Dritarja e parë pas krijimit të llogarisë

**Hapi 4:** Verifikimi i llogarisë përmes **Sign In** duke anashkaluar OTP, por vetëm përmes **emailit** edhe **fjalëkalimit**.

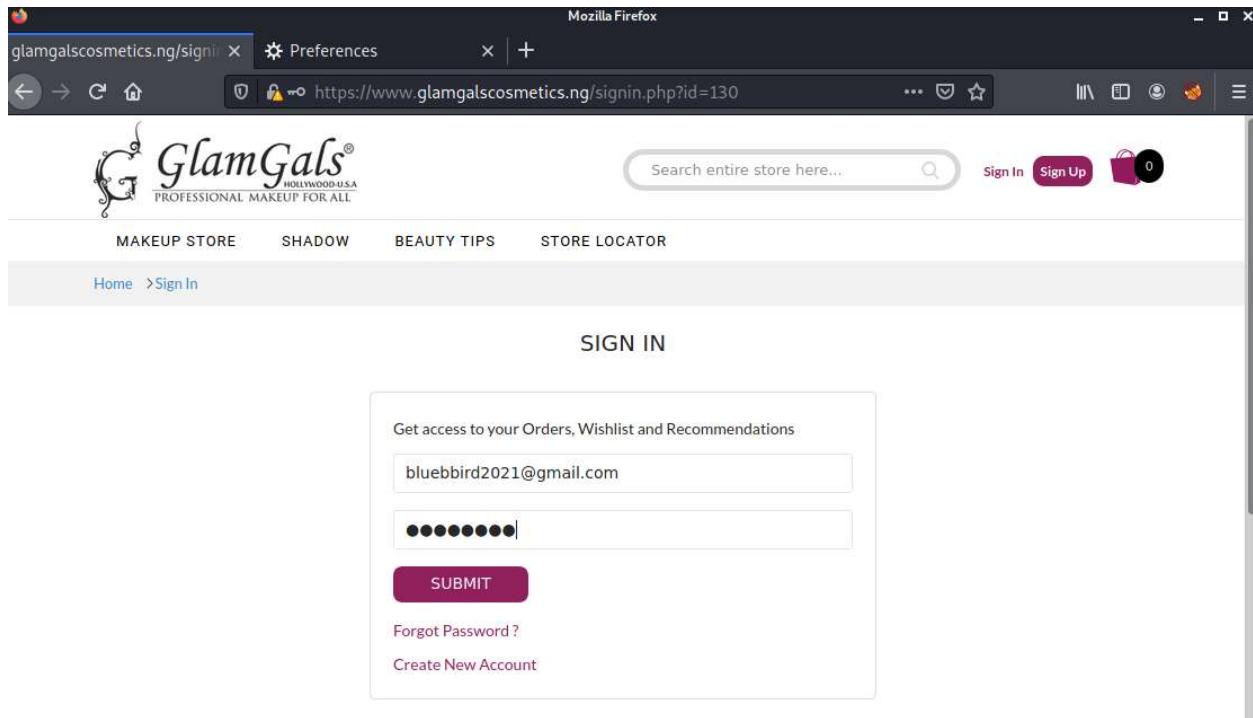


Figura 48: Plotësimi i të dhënave për Sign In

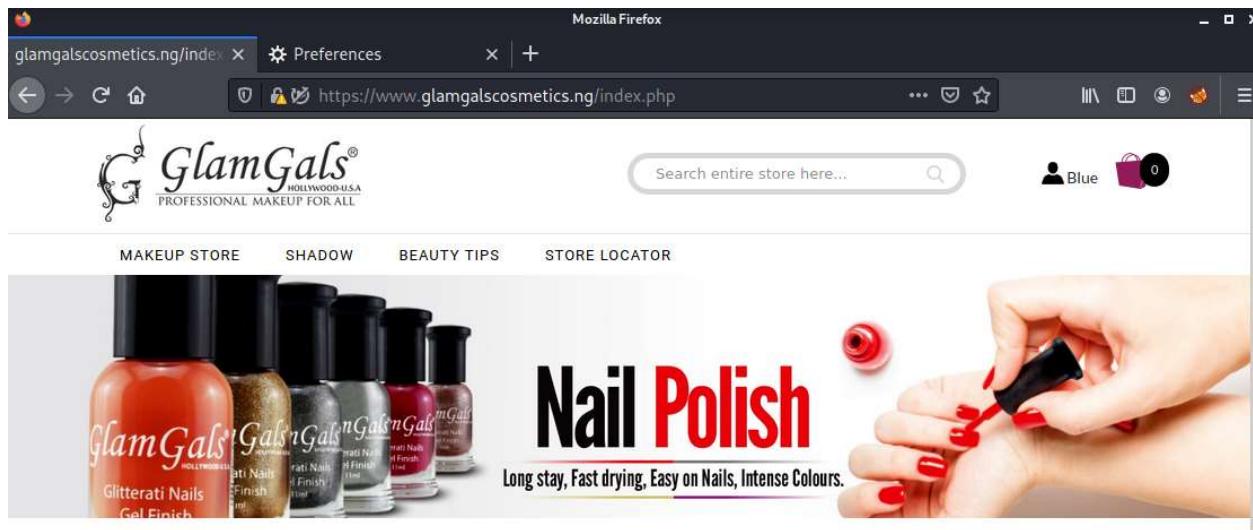


Figura 49: Dritarja e parë pas Sign In e shfrytëzuesit

#### 4.3 XSS Persistent

**Cross Site Scripting ose XSS** është një nga dobësitë më problematike në ueb aplikacionet në internet. Ai renditet në mesin e 10 dobësive të faqeve të internetit OWASP pothuajse çdo vit.

Me poshtë është e demostruar testimi i një faqje të internetit për dobësinë **Cross-Site Scripting(XSS)**.

**Hapi 1:** Hapim Kali Linux dhe Metasploit Server



Figura 50: Startimi i Kali Linux

## Burp Suite

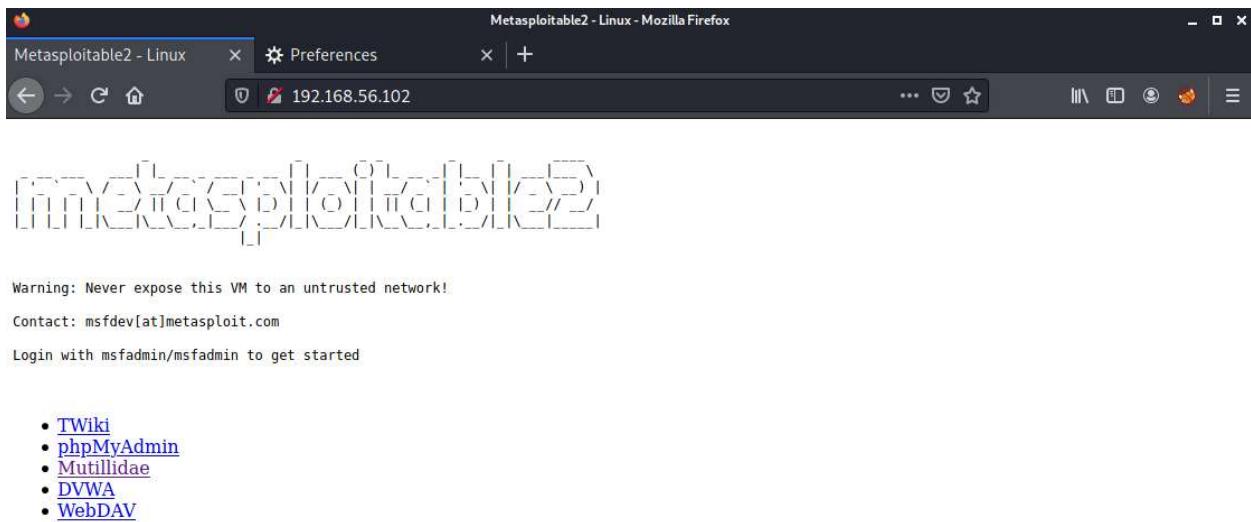


Figura 51: Startimi i Metasploitable Server përmes brosuerit të Kali Linuxit

## Hapi 2: Hapim Burp Suite

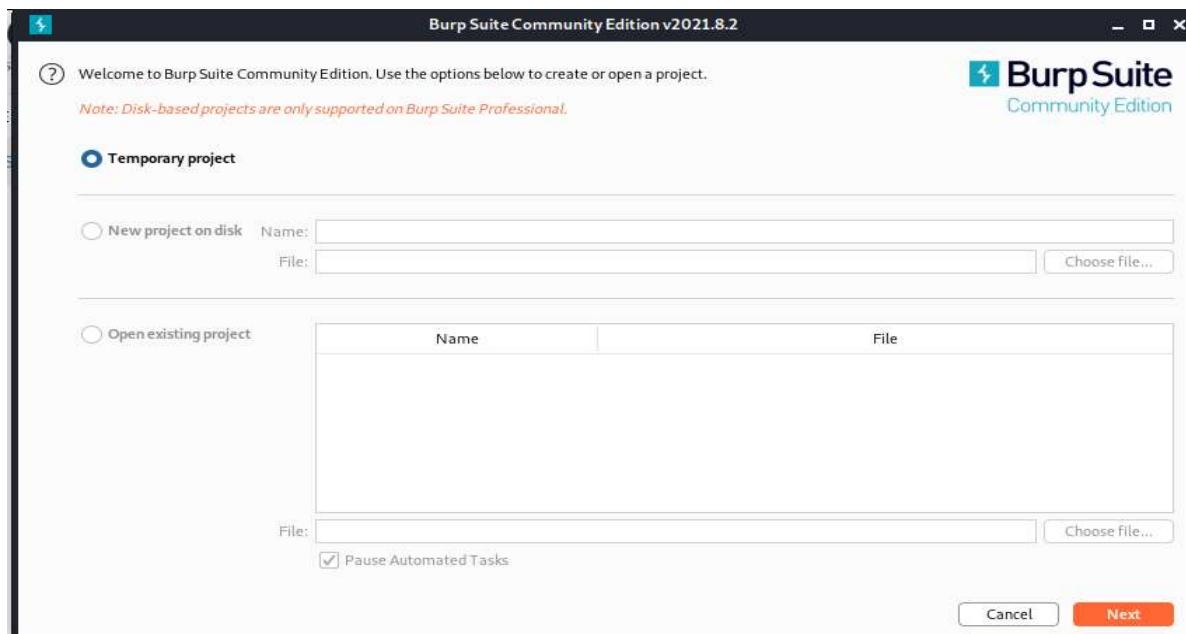


Figura 52: Startimi i Burp Suite 1

## Burp Suite

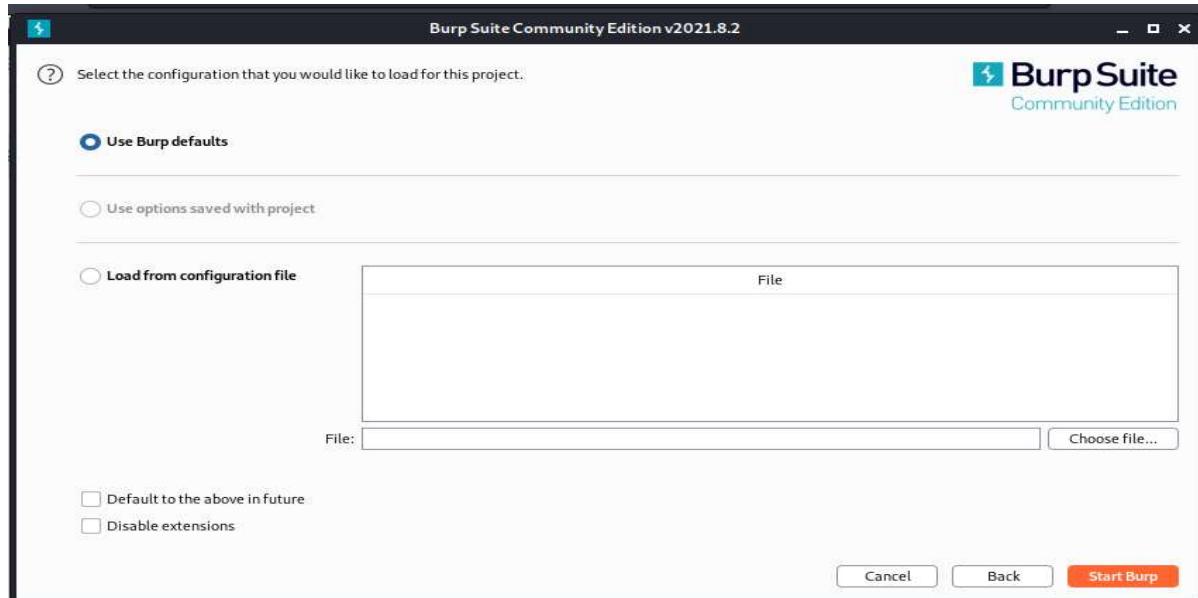


Figura 53: Startimi i Burp Suite 2

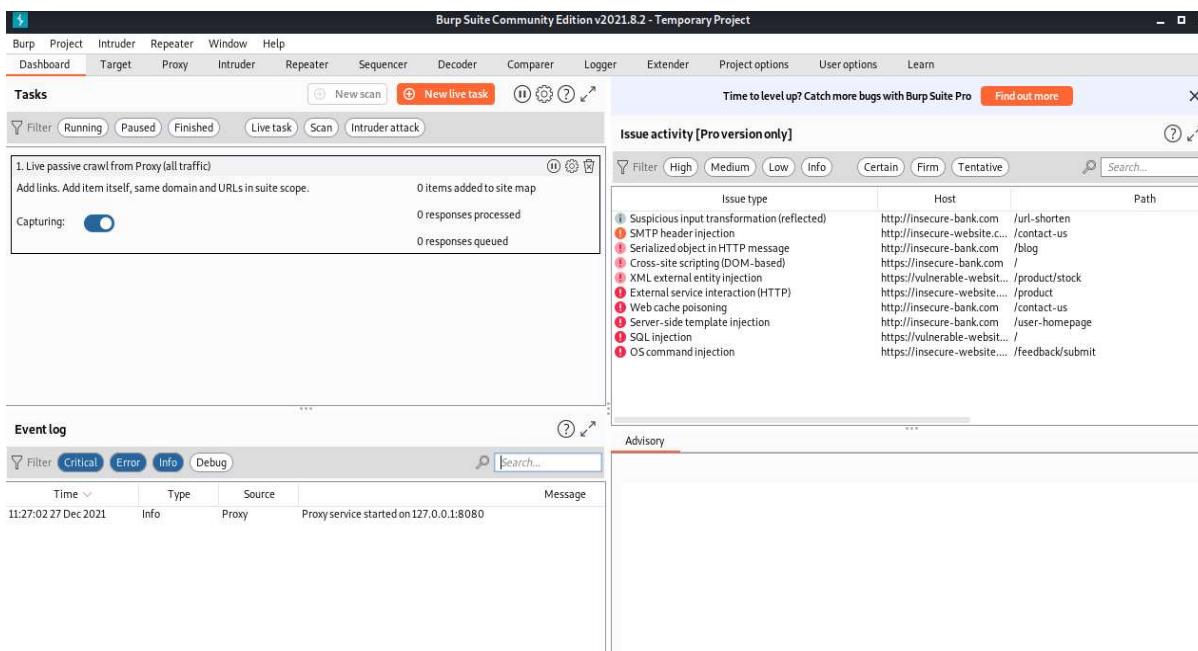


Figura 54: Startimi i Burp Suite 3

**Hapi 3:** Hapim Mutillidae në kuadër të Metasploitable Server

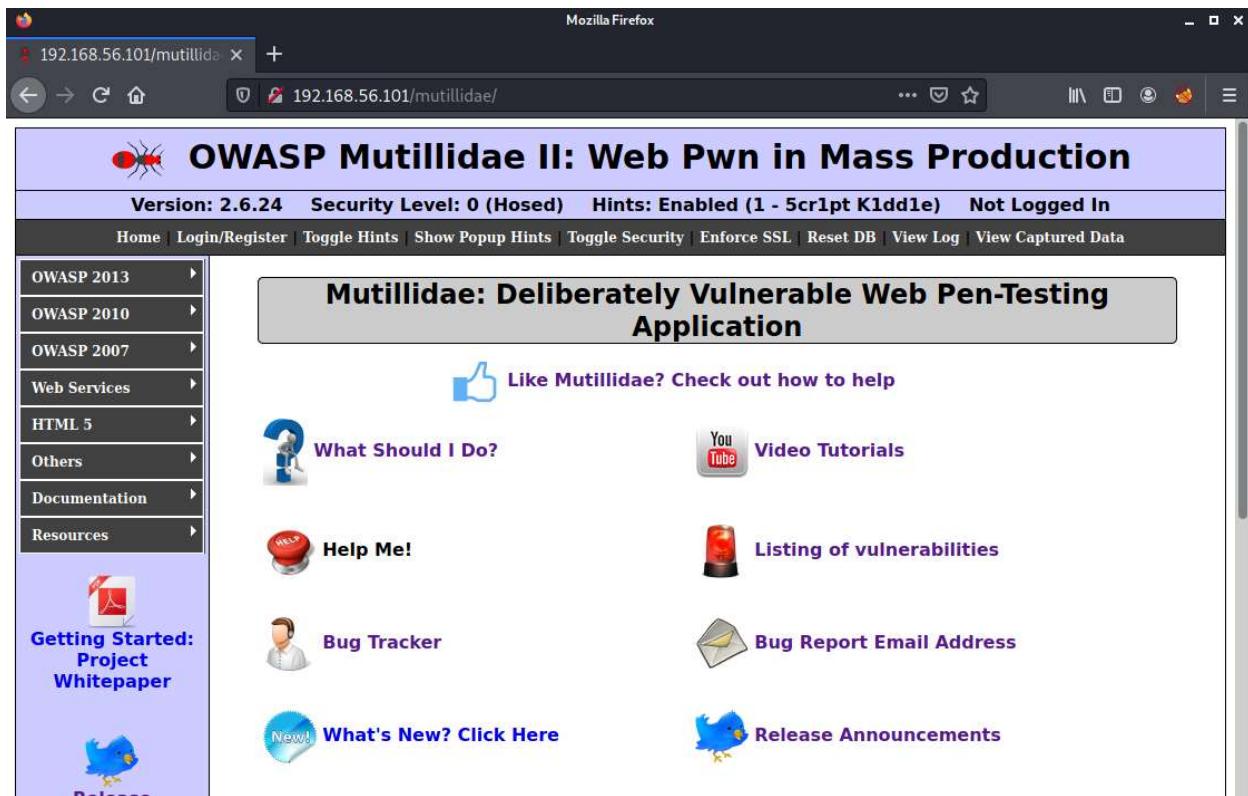


Figura 55: Startimi i Mutillidae II

Nga menyja Mutillidae II zgjedhim:

**OWASP 2013 ->A3-Cross Site Scripting(XSS)->Persistent(Second Order)->Add to your blog** për të shtuar një skriptë XSS në blogun e **Mutillidae II**.

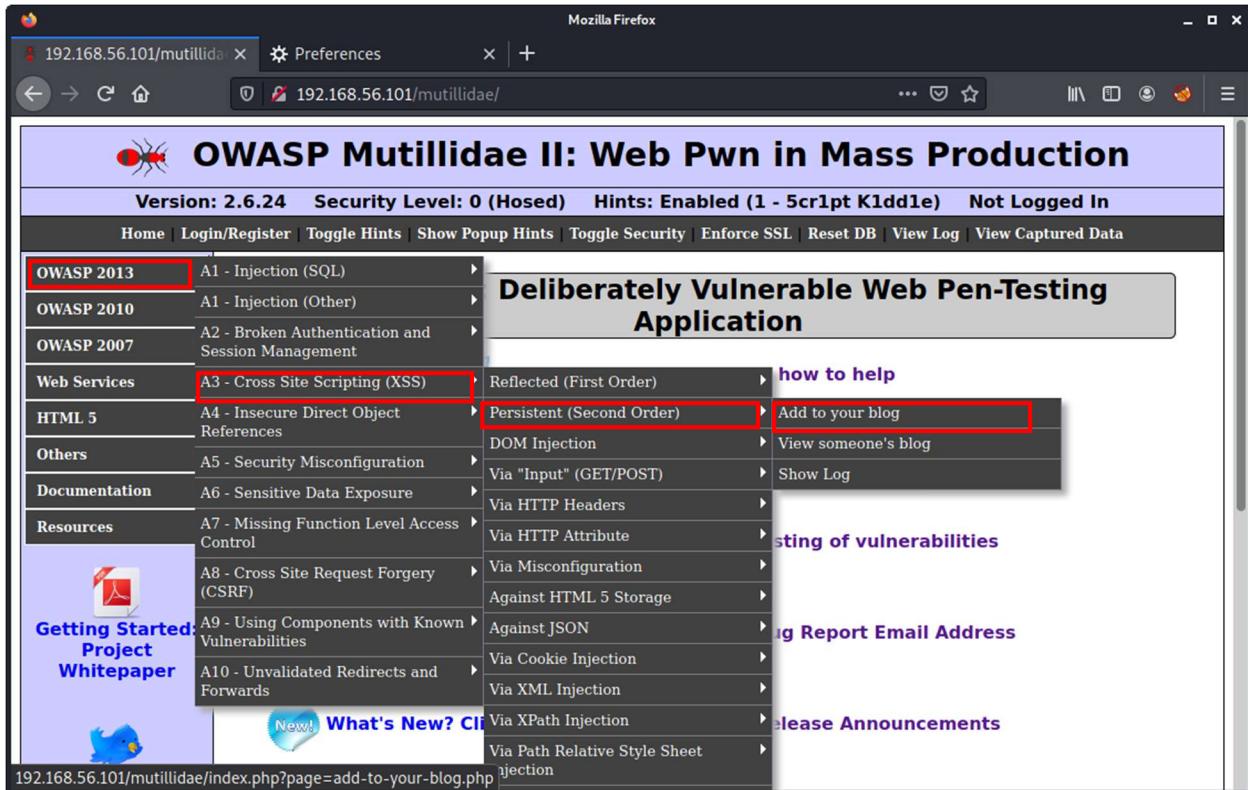


Figura 56: Selektimi i menyve për realizimin e një Persistent XSS

**Hapi 4:** Pas klikimit të menysë **Add to your Blog** hapet faqja e cila shihet në figurën e mëposhtme.

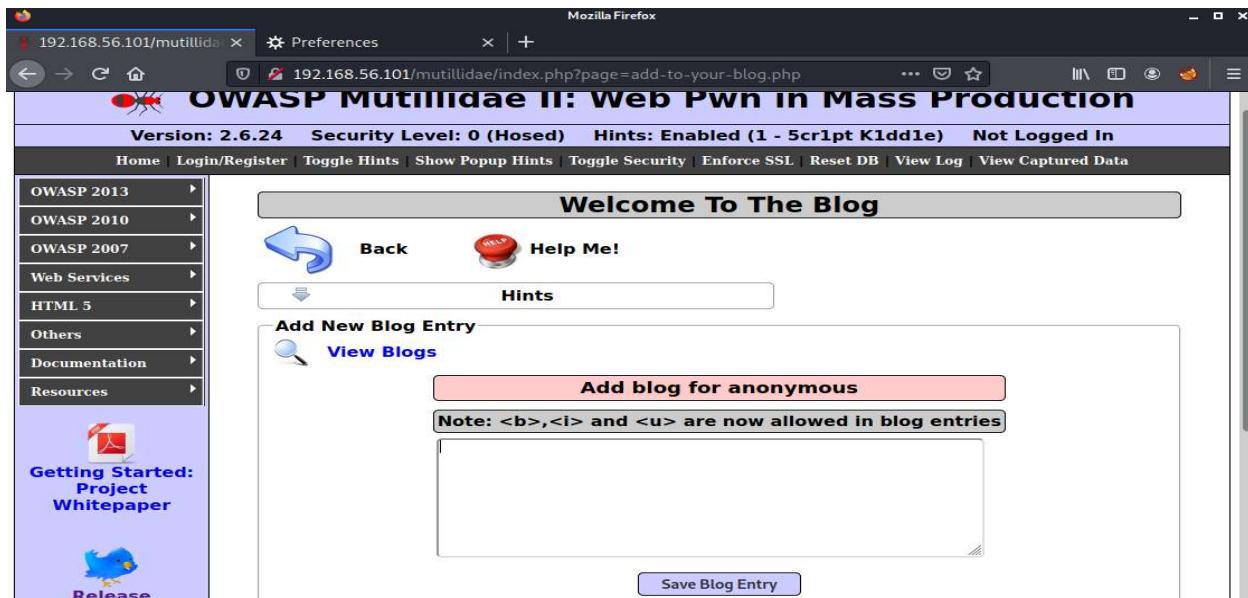


Figura 57: Faqja Add to your Blog

## Burp Suite

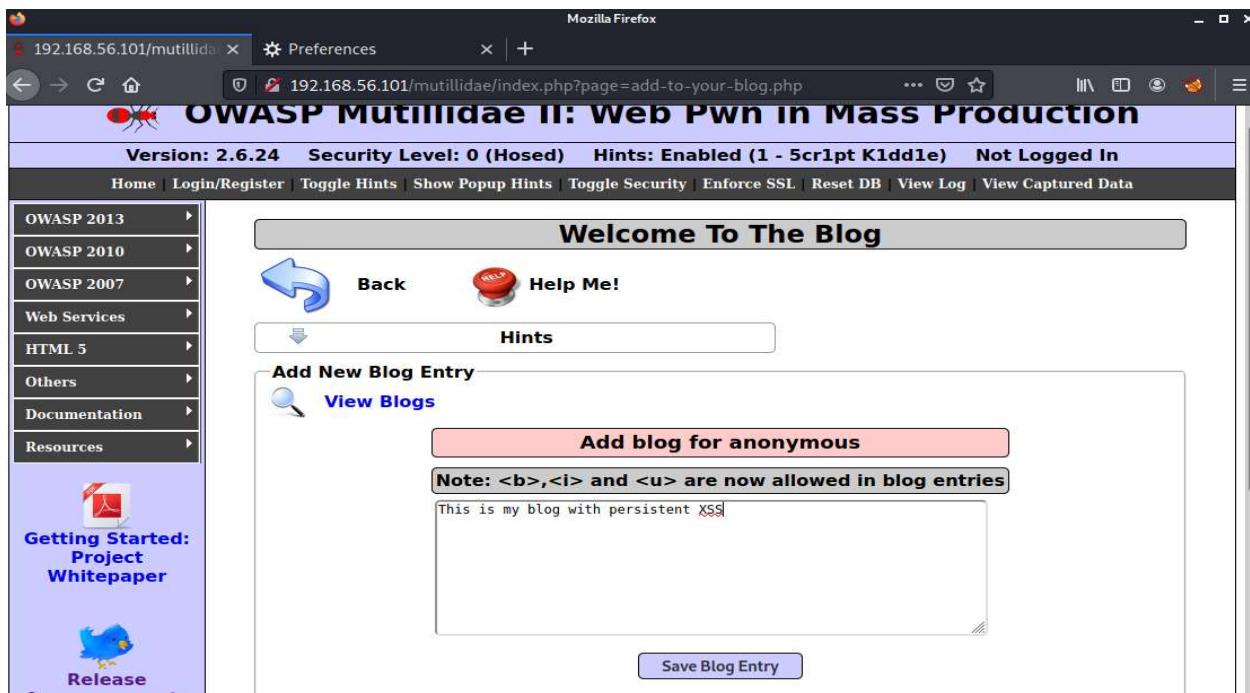


Figura 58: Teksti i cili do të insertohet përmes Add to your Blog në blogun e Mutillidae II

Tani, sigurohuni që **Intercept ON** në Burp Suite dhe më pas klikoni në "Save Blog Entry".

### Hapi 5: Intercept ON

Me intercept ON në BurpSuite tuaj në rreshtin e fundit, mund ta shihni postimin e blogut me ngjyrë të kuqe.

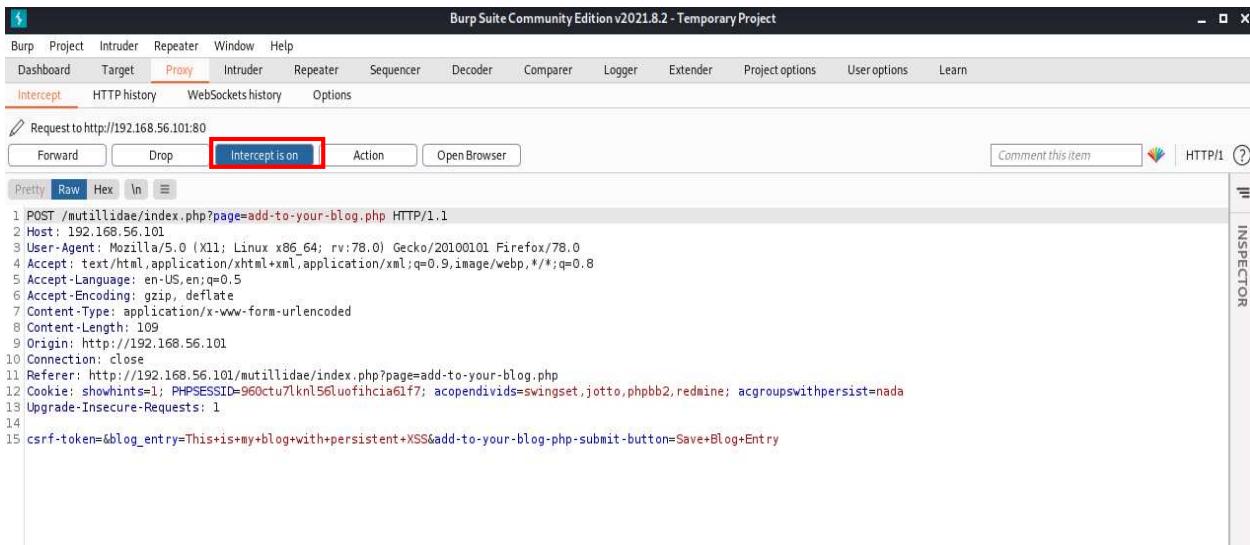
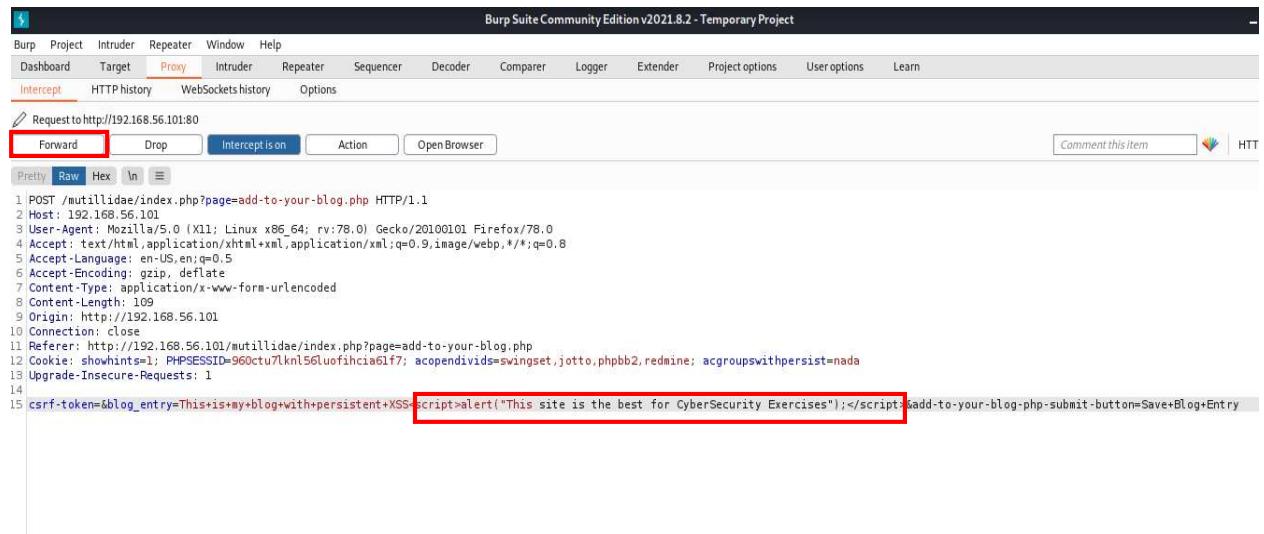


Figura 59: Intercept ON në Burp Suite

### Hapi 6: Shtimi i një skripte në postimin e blogut të Mutillidae II

Ky skripte do të ruhet në bazën e të dhënave të faqes së internetit te Mutillidae II dhe do të jetë e qëndrueshme.



```

1 POST /mutillidae/index.php?page=add-to-your-blog.php HTTP/1.1
2 Host: 192.168.56.101
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 109
9 Origin: http://192.168.56.101
10 Connection: close
11 Referer: http://192.168.56.101/mutillidae/index.php?page=add-to-your-blog.php
12 Cookie: showhints=1; PHPSESSID=960ctu7lkn156luofihcia6lf7; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada
13 Upgrade-Insecure-Requests: 1
14
15 csrf-token=&blog_entry=This+is+my+blog+with+persistent+XSS<script>alert('This site is the best for CyberSecurity Exercises');</script>&add-to-your-blog.php-submit-button=Save+Blog+Entry

```

Figura 60: Skripta e shtuar në postim të blogut

Pastaj,klikojme **Forward** dhe kur të ktheheni në shfletuesin tuaj, do të shihni një kuti alarmi të vazhdueshme dhe të bezdisshme që do të shfaqet në ekran.

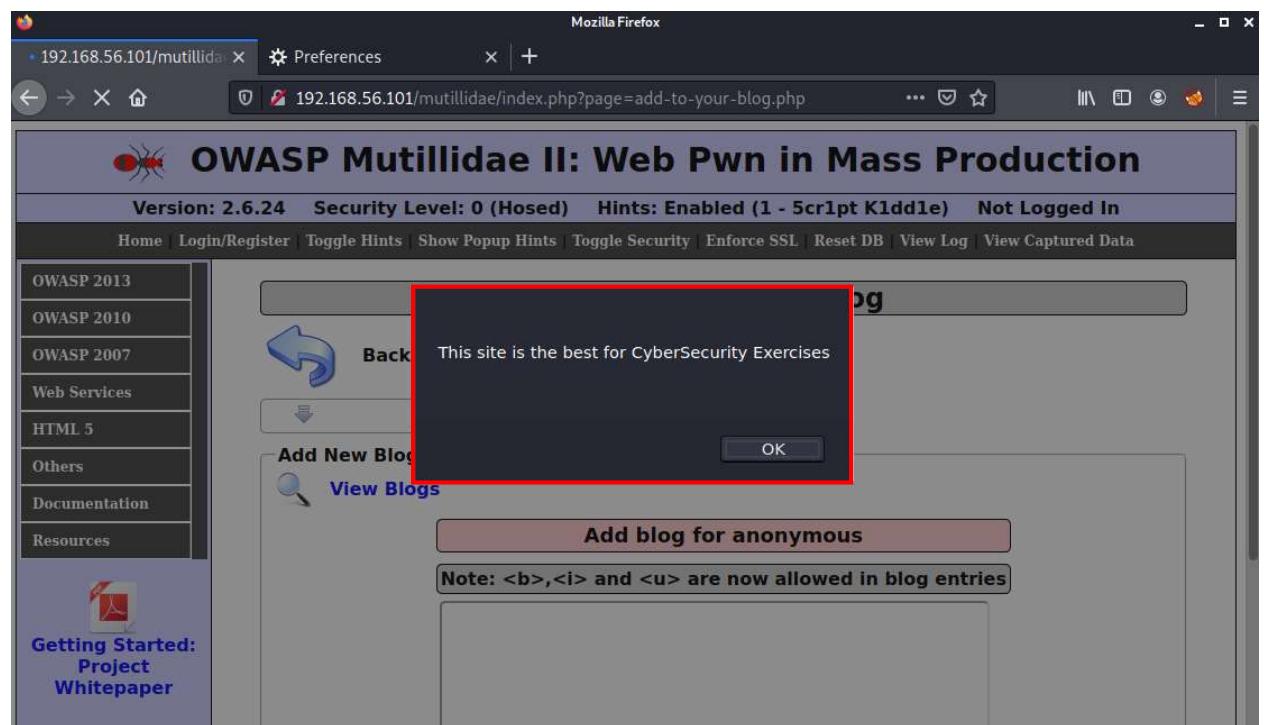


Figura 61: Kutia e alarmit me përbajtjen e skriptës së shtuar përmes Burp Suite

### 3.4 Brute Force me DVWA(Damn Vulnerable Web App)

Niveli i ulët i sigurisë:

**Hapi 1:** Hapja e Metasploitable tek shfletuesi i Kali Linuxit dhe selektimi i menysë DVWA.

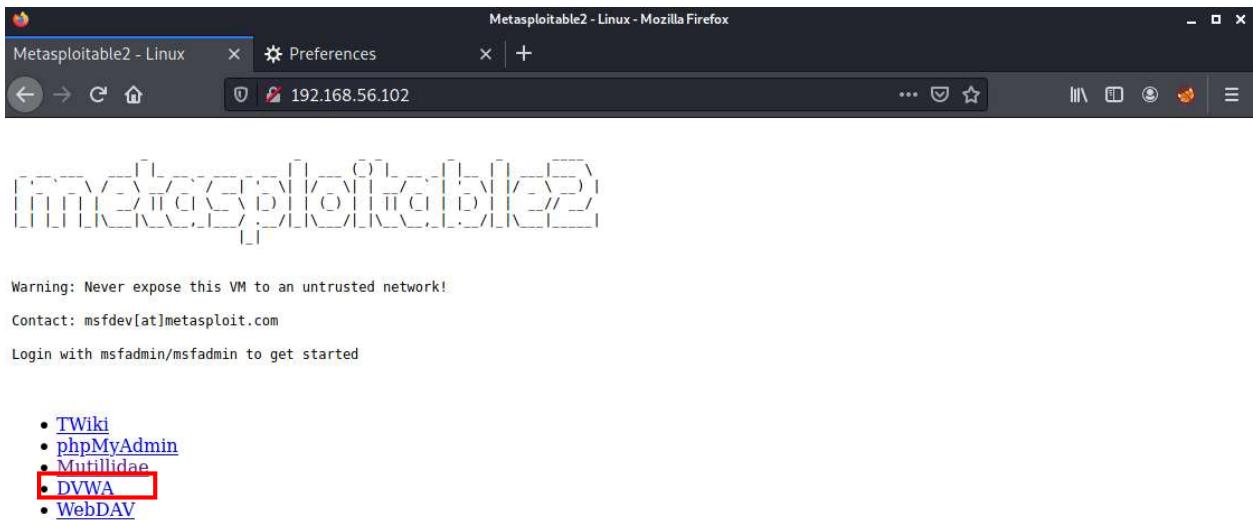


Figura 62: Startimi i Metasploitable Serveri dhe selektimi i DVWA

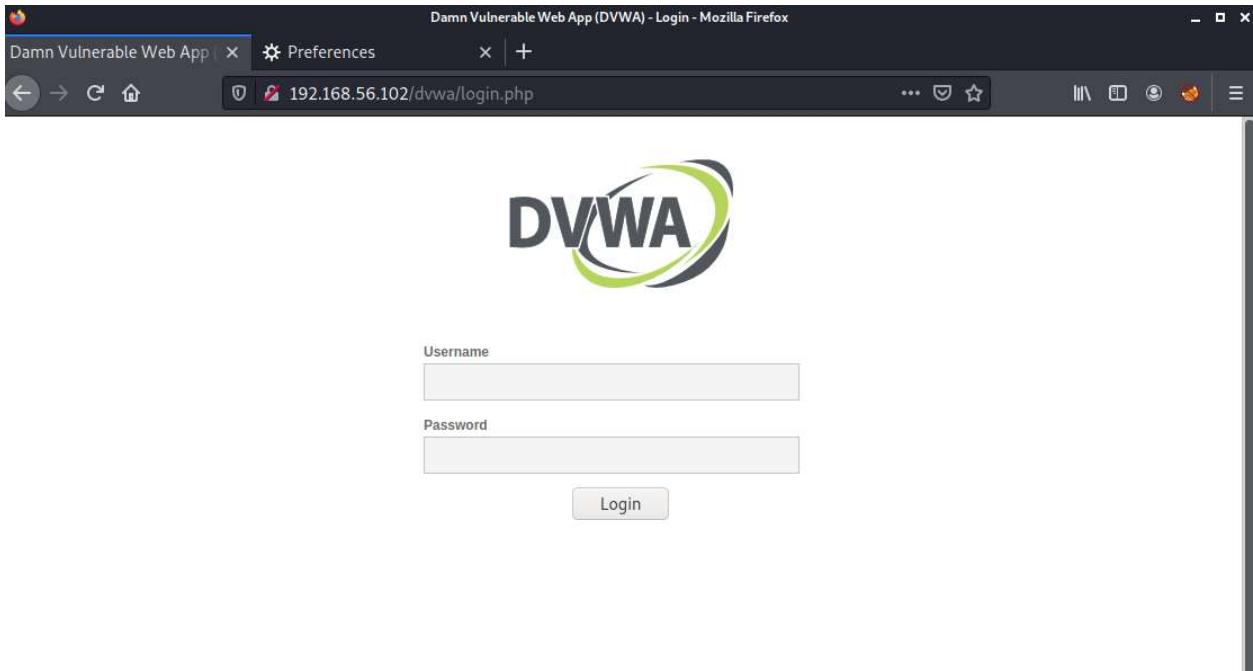


Figura 63: Hapja e faqes DVWA pas selektimit tek Metasploitable Serveri

**Hapi 2:** Identifikimi në DVWA përmes emrit të përdoruesit të paracaktuar "admin" dhe fjalëkalimit "fjalëkalimi".



The DVWA logo features the letters "DVWA" in a bold, dark grey sans-serif font. A thick, stylized swoosh graphic in green and black curves around the letters, starting from the top left of the 'D' and ending at the bottom right of the 'A'.

Username

Password

Figura 64: Hapja e faqes për kryqje e DVWA pas selektimit tek Metasploitable Serveri

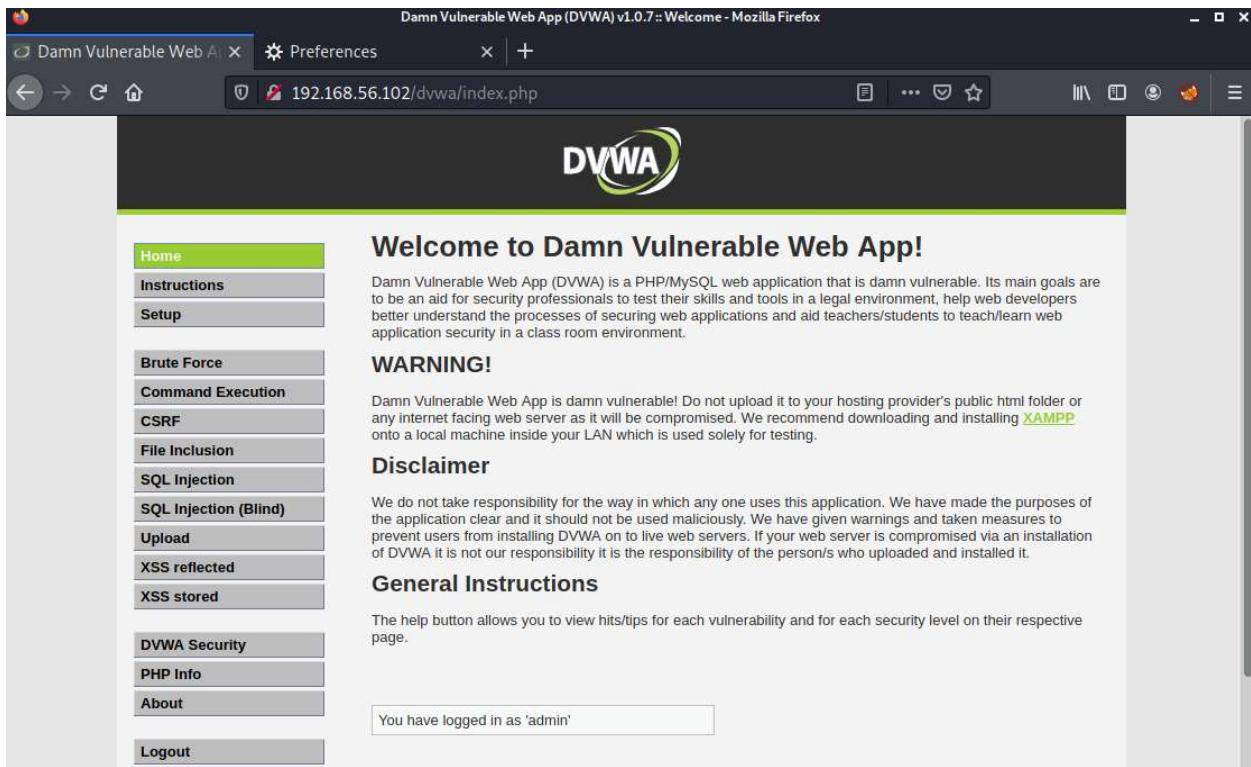


Figura 65: Hapja e faqes pas kyqjes e DVWA

**Hapi 3:** Vazhdojme duke vendosur sigurinë e DVWA (**DVWA Security**) në nivelin me të ulët dhe klikimi i modulit **Brute Force**

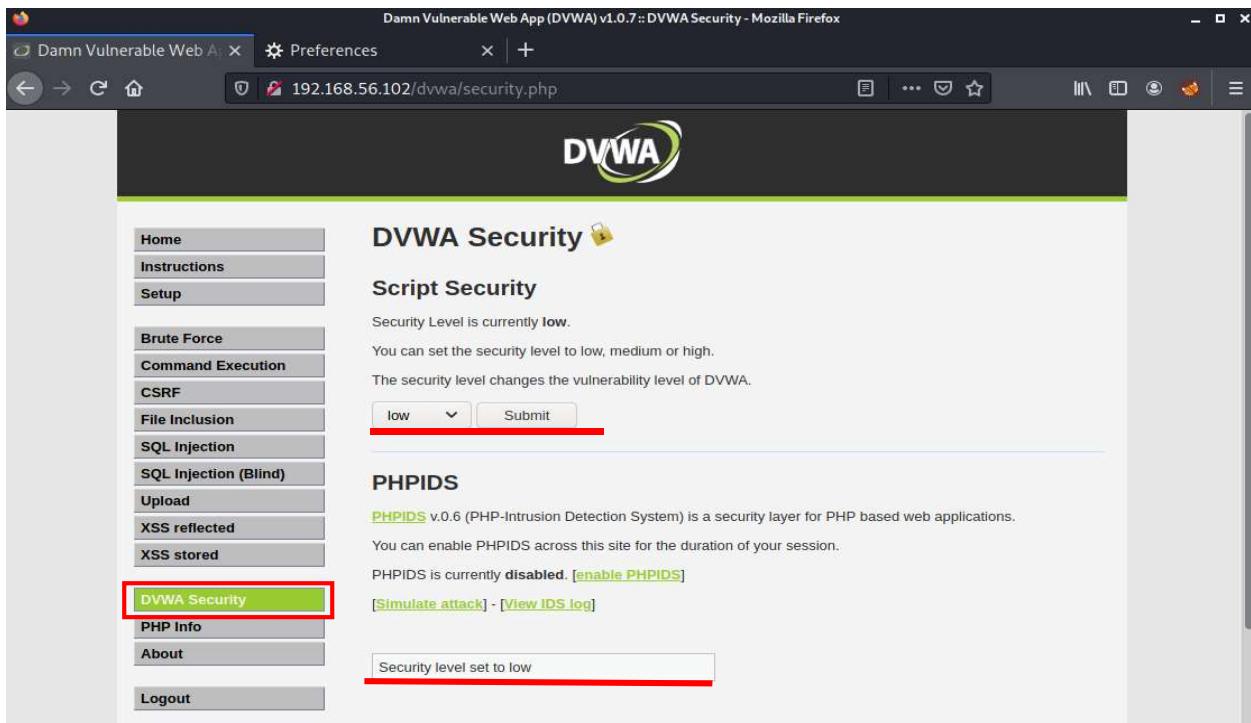


Figura 66: DVWA Security

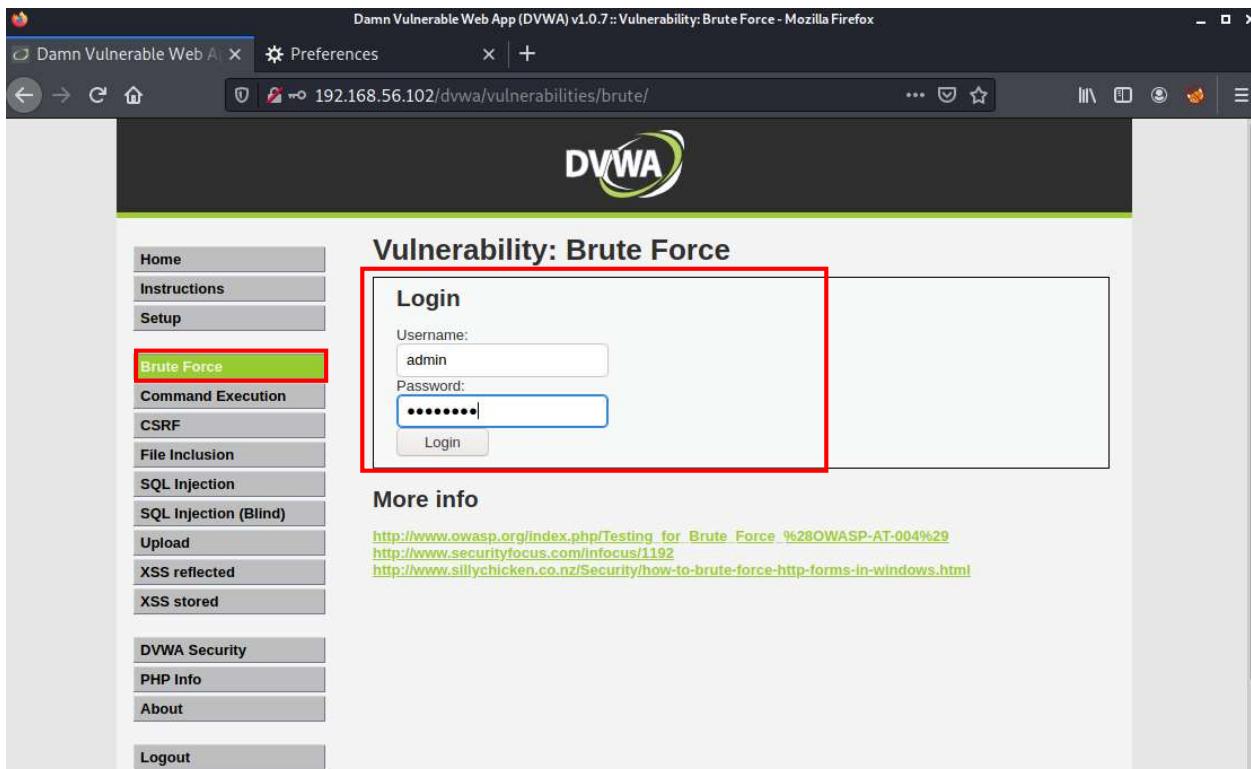
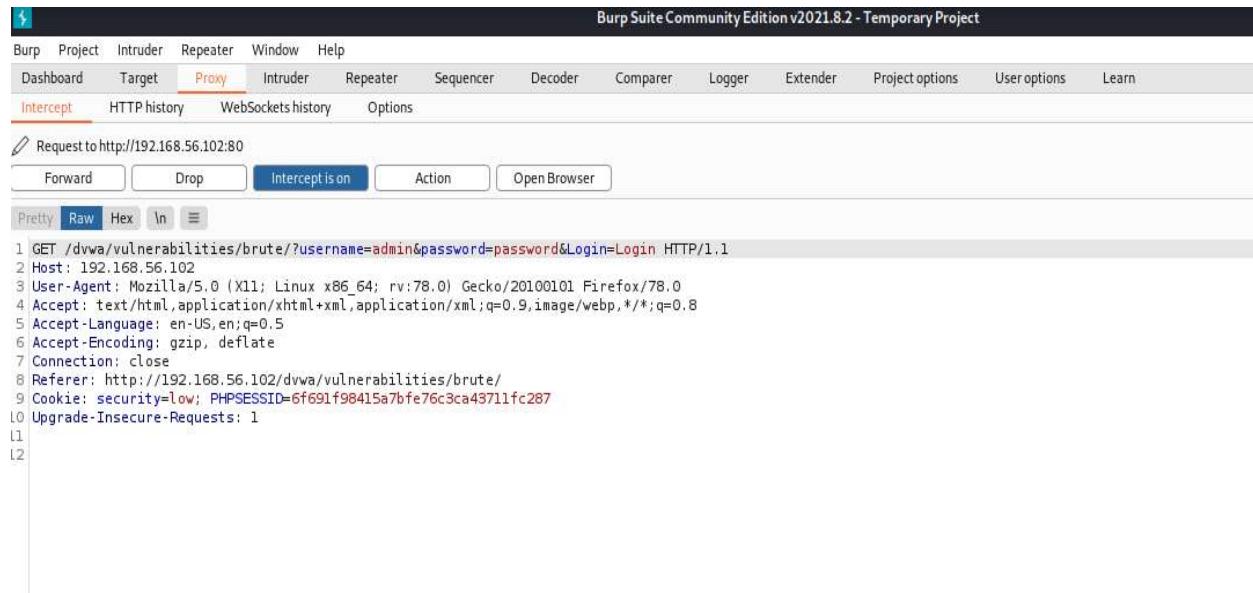


Figura 67: Brute Force DVWA

## Burp Suite

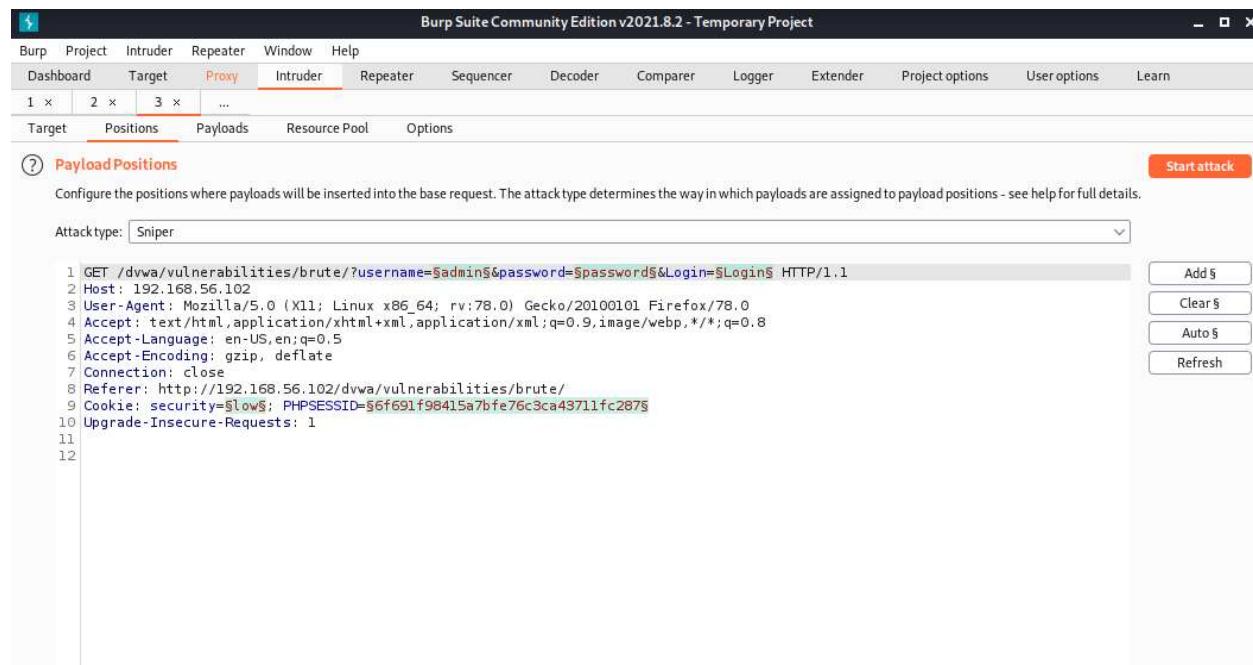
Vendosim emrin e saktë të shfrytëzuesit dhe një fjalëkalim të rastësishëm, më pas shtypni **Login** por duke u sigruar që **Intercept** eshte **ON** tek Burp Suite.



```
1 GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 192.168.56.102
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.56.102/dvwa/vulnerabilities/brute/
9 Cookie: security=low; PHPSESSID=6f691f98415a7bfe76c3ca43711fc287
10 Upgrade-Insecure-Requests: 1
11
12
```

Figura 68: Mbledhja e informatave te DVWA përmes Burp Suite

Të dhënat e mbledhura përmes Burp Suite i dërgojm tek **Intruder** përmes **Action->Send to Intruder**.



```
1 GET /dvwa/vulnerabilities/brute/?username=$admin$&password=$password$&Login=$Login$ HTTP/1.1
2 Host: 192.168.56.102
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://192.168.56.102/dvwa/vulnerabilities/brute/
9 Cookie: security=$low$; PHPSESSID=$6f691f98415a7bfe76c3ca43711fc287$;
10 Upgrade-Insecure-Requests: 1
11
12
```

Figura 69: Përbajtja e menyës Intruder

Tek moduli **Position** i menysë **Intruder** zgjedhim tipin e sulmit.

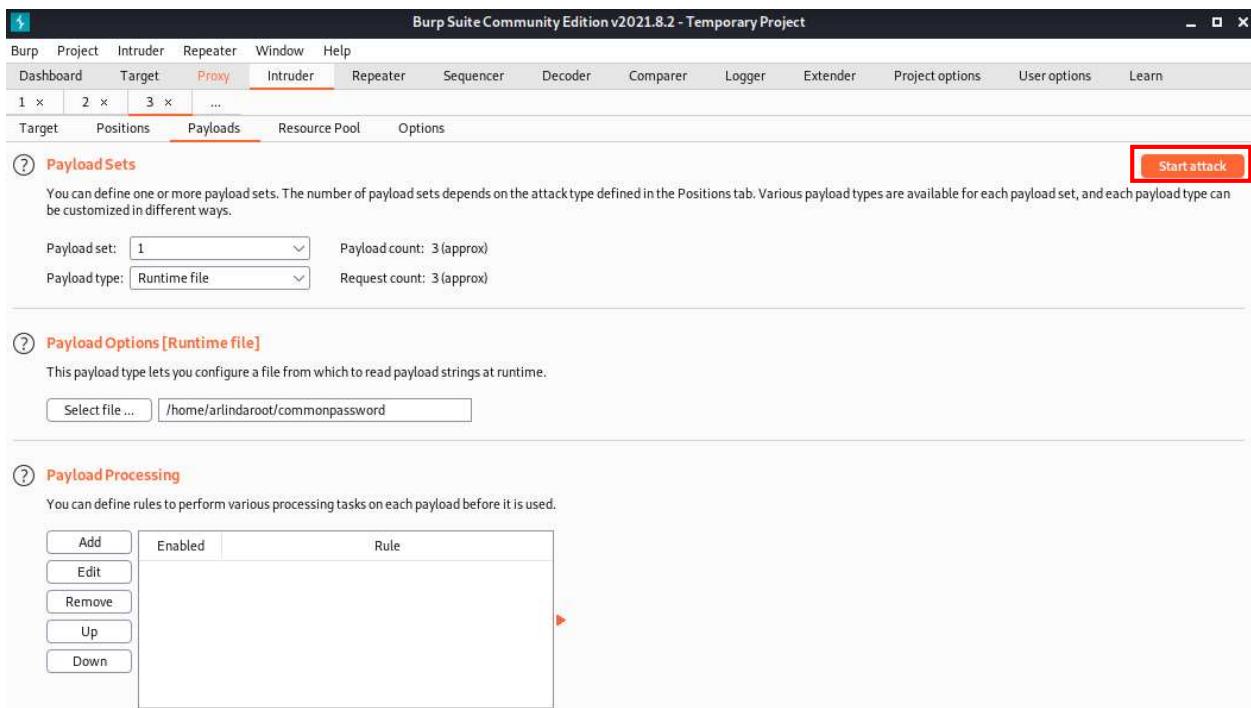


Figura 70: Përmbajtja e modulit Payloads

Tek moduli **Payloads** i menysë **Intruder** zgjedhim listën e fjälëkalimeve për sulmim dhe klikojmë **Start Attack**.

**Hapi 4:** Pas klikimi të butonit **Start Attack** në një dritare gjenerohet lista e tentimeve për gjetjen e fjälëkalimit të saktë.

## Burp Suite

2. Intruder attack of 192.168.56.102 - Temporary attack - Not saved to project file							-	x
Attack	Save	Columns	Results	Target	Positions	Payloads	Resource Pool	Options
Filter: Showing all items								
Request ▾	Payload	Status	Error	Timeout	Length	Comment		
0		200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
1	root	200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
2	msf	200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
3	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
4	administrator	200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
5	msfadmin	200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
6	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
7	123321	200	<input type="checkbox"/>	<input type="checkbox"/>	4882			
8	password	200	<input type="checkbox"/>	<input checked="" type="checkbox"/>	4948			

Request Response

Pretty Raw Hex \n =

```
1 GET /dvwa/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.1
2 Host: 192.168.56.102
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
```

Figura 71: Gjetja e fjalëkalimit për usernamin admin e DVWA

Mund të shohim se ka paketa që kanë gjatësinë të ndryshme por fokusi yne mbetet tek paketa speciale **4571**. Shohim se fjalëkalimi i adminit është **password**, dhe atëherë kalojmë tek shfletuesi i DVWA.

The screenshot shows a Mozilla Firefox browser window displaying the DVWA application. The title bar reads "Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Brute Force - Mozilla Firefox". The address bar shows the URL "192.168.56.102/dvwa/vulnerabilities/brute/". The main content area displays the DVWA logo and the heading "Vulnerability: Brute Force". On the left, there is a sidebar menu with various options like Home, Instructions, Setup, Brute Force (which is highlighted in green), Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, and About. The "Brute Force" section contains a "Login" form with fields for "Username" (set to "admin") and "Password" (represented by a series of asterisks). Below the form is a "More info" section with three links: "http://www.owasp.org/index.php/Testing\_for\_Brute\_Force\_%28OWASP-AT-004%29", "http://www.securityfocus.com/infosec/1192", and "http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html".

Figura 72: Plotësimi i të dhënave në DVWA

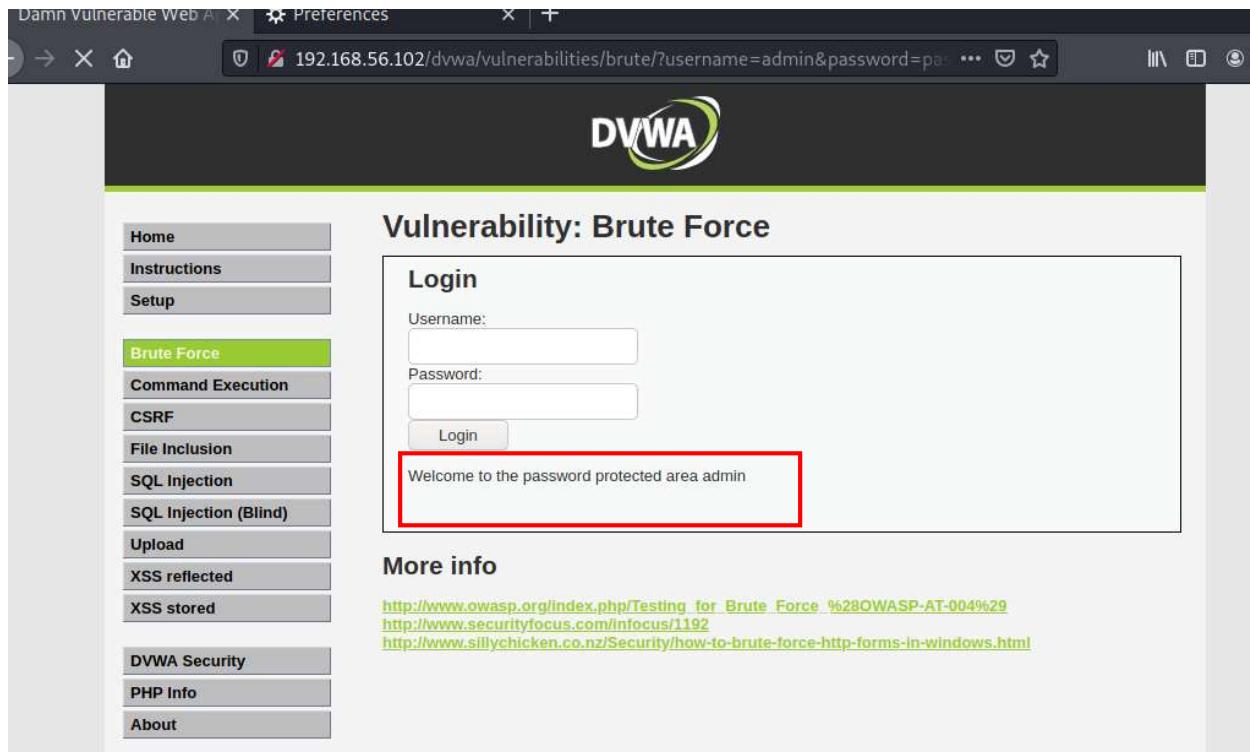


Figura 73: Verifikimi se të dhënat e plotësuara më parë në DVWA janë të sakta

E njëjta procedurë vlen edhe për nivelet tjera të sigurisë së DVWA si: **MEDIUM Level** dhe **HIGH Level**.

## 4. Konkluzione

Realizimi i gjithë projektit ishte shumë sfidues por njëkohësisht edhe argëtues. Ky projekt është projekti i dytë që e kemi punuar i kësaj natyre, dhe si student fillestar në këtë lëmi kemi hasur në disa pengesa gjatë realizimit të projektit. Por, me ndihmën e literaturës nga librat e huaj, koncepteve themelore të marra nga ligjératat dhe ushtrimet e lëndës Siguria në Internet, bashkëpunim, ide të përbashkëta dhe me hulumtime të shumta ne besojmë se kemi arritur me sukses studimin e veglës Burp Suite. Me anë të këtij projekti ne kemi arritur të kuptojmë dhe të përforcojmë më shumë njojuritë tona rreth sigurisë se të dhënave në ueb aplikacione. Ky dokumentim përmban të gjitha informacionet rreth veglës Burp Suite, duke përfshirë instalimin, mënyrat dhe shembujt konkret të cilët në mënyrë të qartë tregojnë se si mund të përdoret kjo vegël. Meqë në shumicën e rasteve Burp Suite duhet të bashkëpunoj me veglat tjera për skanimin e dobësive andaj ofrimi i licencës së saj pa pagesë për një skanim të tillë do të ndikonte pozitivisht në rritjen e përdorshmërisë së saj.

## Referencat

- [1] "GeeksforGeeks," 26 August 2019. [Online]. Available: <https://www.geeksforgeeks.org/what-is-burp-suite/>.
- [2] Y. Said, "linuxhint," 2020. [Online]. Available: [https://linuxhint.com/burp\\_suite\\_tutorial/](https://linuxhint.com/burp_suite_tutorial/).
- [3] L. Obbayi, "INFOSEC," 19 February 2019. [Online]. Available: <https://resources.infosecinstitute.com/topic/burpsuite-tutorial/>.
- [4] OCCUPYTHEWEB, "Wonder how to," 3 10 2015. [Online]. Available: <https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-web-form-passwords-with-thc-hydra-burp-suite-0160643/>.
- [5] "Hacking loops," 2021. [Online]. Available: <https://www.hackingloops.com/hydra-with-burp-suite/>.
- [6] S. Wear, "Burp Suite CookBook," Packt Publishing Ltd., Birmingham, 2018.
- [7] H. Dalziel, "How to Hack and Defend your Website in Three Hours," Elsevier Inc., 2014.
- [8] "HACKING TRUTH," 2016. [Online]. Available: <https://www.kumaratuljaiswal.in/2020/08/full-tutorial-of-burp-suite.html>.
- [9] "Trust Rdius," 2021. [Online]. Available: <https://www.trustradius.com/products/portswigger-burp-suite/reviews?qs=pros-and-cons>.
- [10] "PortSwigger," 2021. [Online]. Available:
  - ] <https://portswigger.net/burp/documentation/desktop/options>.
- [11] "PentestGeek," 2025. [Online]. Available: <https://www.pentestgeek.com/web-applications/burp-suite-tutorial-1>.
- [12] "Hackers-Arise," 30 November 2020. [Online]. Available: <https://www.hackers-arise.com/post/web-app-hacking-burpsuite-part-3-testing-for-persistent-xss?fbclid=IwAR2MGc3BYyPAEKB6tby8DZauBE9VNopv6gAgDP7G1d5xRtQczL-5XuOt5PM>.
- [13] "Whisper Lab," 2021. [Online]. Available: [https://whisperlab.org/introduction-to-hacking/notes/burpsuite?fbclid=IwAR293kxfDioSoaaMHAPoEc\\_0Hgx5bpMpJaJco1nwzqNNQq25m7ZGhegEXxU](https://whisperlab.org/introduction-to-hacking/notes/burpsuite?fbclid=IwAR293kxfDioSoaaMHAPoEc_0Hgx5bpMpJaJco1nwzqNNQq25m7ZGhegEXxU).
- [14] "Software Testing Help," 29 November 2021. [Online]. Available:
  - ] <https://www.softwaretestinghelp.com/burp-suite-tutorial/>.
- [15] "DELTA RISK," 18 May 2020. [Online]. Available: <https://deltarisk.com/blog/how-to-use-burp-suite-professional-for-web-application-security-part-one>.