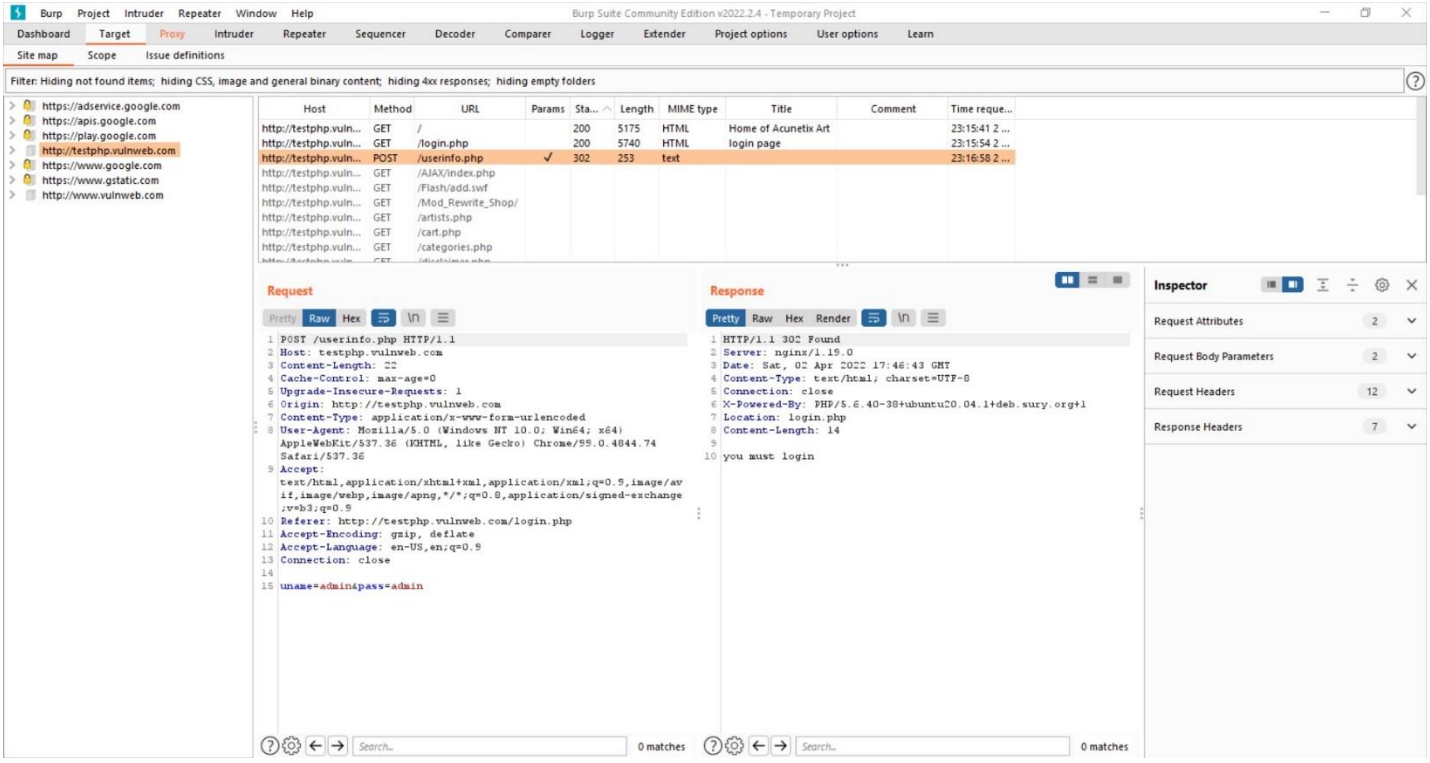
Lab 4 – Analysing Website using Burp Suite

Task 1: Capturing request and response.

Capture request and response while signing up and signing in into your website. Signup and sign in using your name as username. Try with both correct and incorrect credentials.

Incorrect credentials



Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.2.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
Inspector
Search...
0 matches
Search...
0 matches

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

- https://adservice.google.com
- https://apis.google.com
- https://play.google.com
- http://testphp.vulnweb.com
- https://www.google.com
- https://www.gstatic.com
- http://www.vulnweb.com

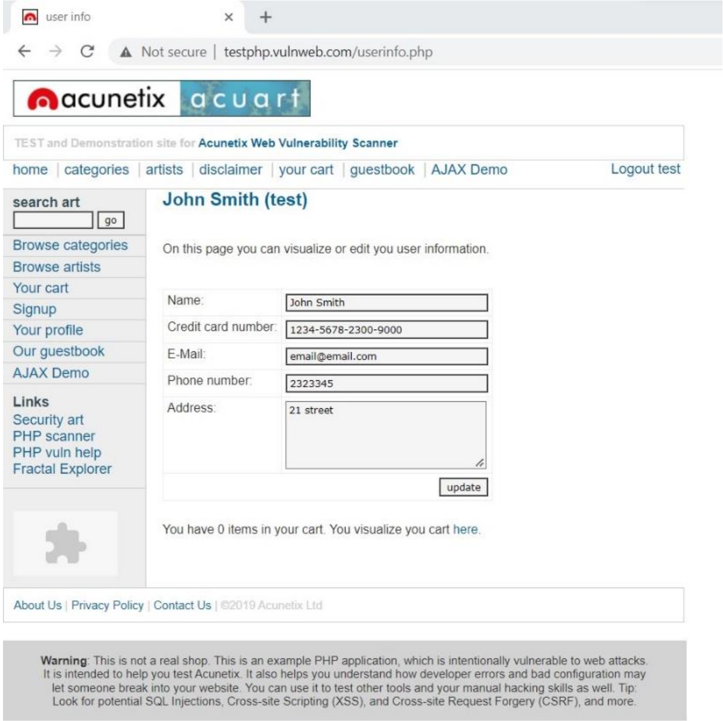
Host	Method	URL	Params	Sta...	Length	MIME type	Title	Comment	Time reque...
http://testphp.vuln...	GET	/		200	5175	HTML	Home of Acunetix Art		23:15:41 2 ...
http://testphp.vuln...	GET	/login.php		200	5740	HTML	login page		23:15:54 2 ...
http://testphp.vuln...	POST	/userinfo.php	✓	302	253	text			23:16:58 2 ...
http://testphp.vuln...	GET	/AJAX/index.php							
http://testphp.vuln...	GET	/Flash/add.swf							
http://testphp.vuln...	GET	/Mod_Rewrite_Shop/							
http://testphp.vuln...	GET	/artists.php							
http://testphp.vuln...	GET	/cart.php							
http://testphp.vuln...	GET	/categories.php							
http://testphp.vuln...	GET	/disclaimer.php							

```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 22
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=admin&pass=admin
```

```
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Sat, 02 Apr 2022 17:46:43 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
Content-Length: 14

you must login
```

Request Attributes	2
Request Body Parameters	2
Request Headers	12
Response Headers	7

Correct credentials



user info

Not secure | testphp.vulnweb.com/userinfo.php

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo   Logout test

search art [ ] go

Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo

Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer

John Smith (test)

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

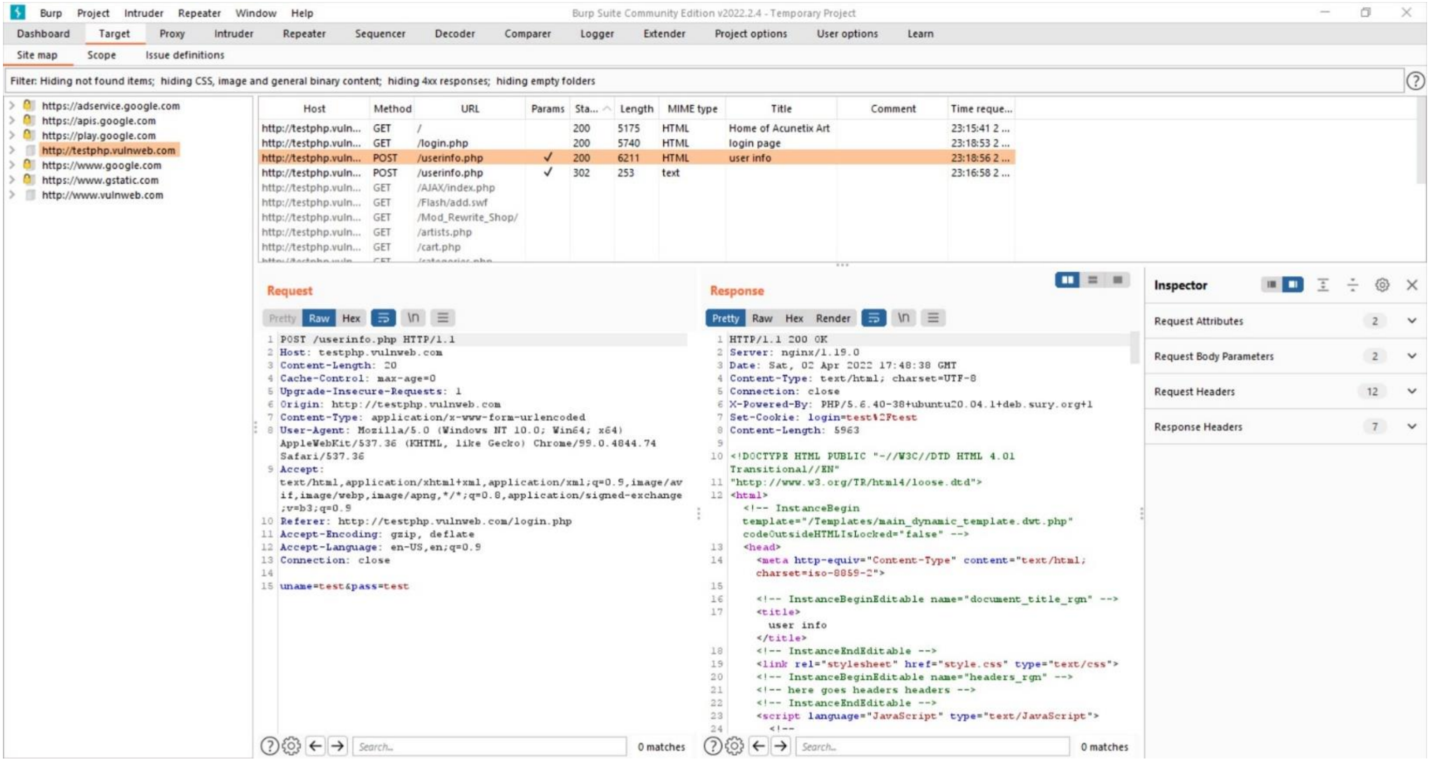
Name:	John Smith
Credit card number:	1234-5678-2300-9000
E-Mail:	email@email.com
Phone number:	2323345
Address:	21 street

update

You have 0 items in your cart. You visualize you cart here.

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.2.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Site map Scope Issue definitions

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

https://adservice.google.com
https://apis.google.com
https://play.google.com
http://testphp.vulnweb.com
https://www.google.com
https://www.gstatic.com
http://www.vulnweb.com

Host	Method	URL	Params	Sta...	Length	MIME type	Title	Comment	Time reque...
http://testphp.vuln...	GET	/		200	5175	HTML	Home of Acunetix Art		23:15:41 2 ...
http://testphp.vuln...	GET	/login.php		200	5740	HTML	login page		23:18:53 2 ...
http://testphp.vuln...	POST	/userinfo.php	✓	200	6211	HTML	user info		23:18:56 2 ...
http://testphp.vuln...	POST	/userinfo.php	✓	302	253	text			23:16:58 2 ...
http://testphp.vuln...	GET	/AJAX/index.php							
http://testphp.vuln...	GET	/Flash/add.swf							
http://testphp.vuln...	GET	/Mod_Rewrite_Shop/							
http://testphp.vuln...	GET	/artists.php							
http://testphp.vuln...	GET	/cart.php							

Request

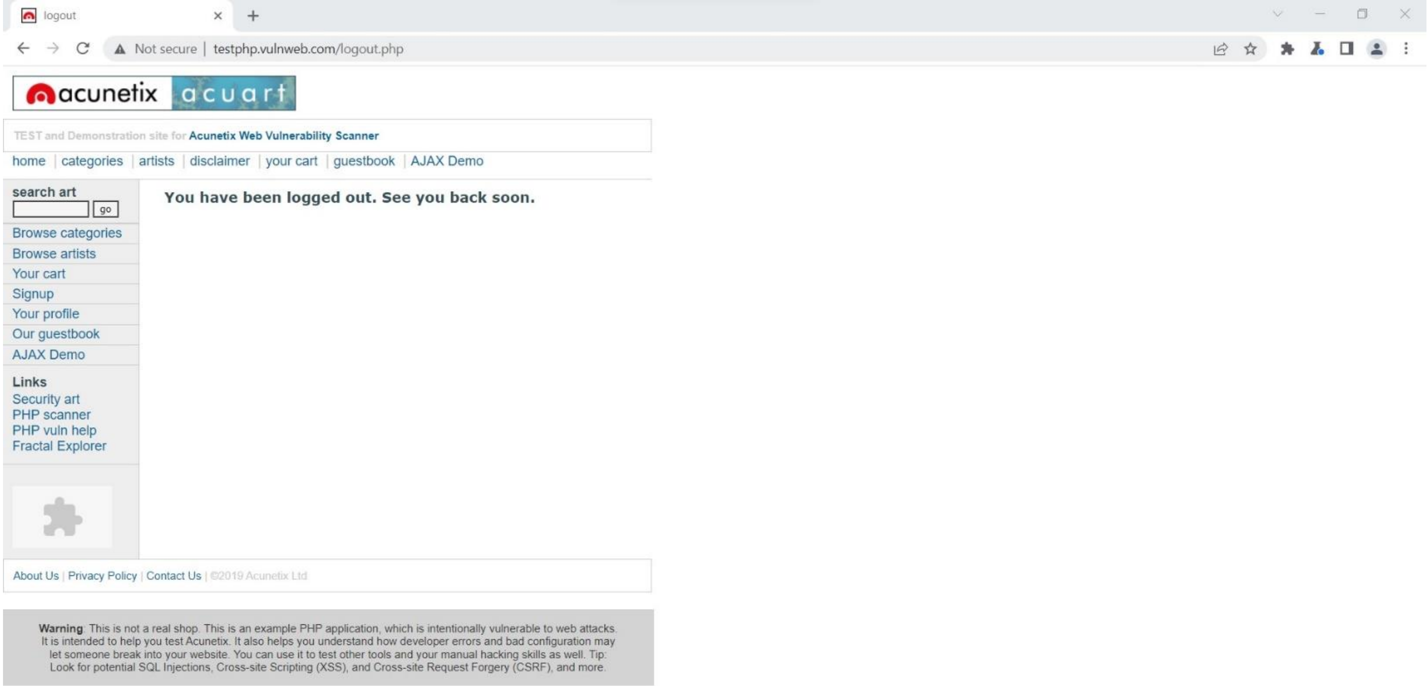
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 20
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/99.0.4844.74
Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/av
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange
;v=b3;q=0.9
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=test&pass=test
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sat, 02 Apr 2022 17:48:38 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Length: 5963

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01
Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <!-- InstanceBegin
  template="/Templates/main_dynamic_template.dwt.php"
  codeOutsideHTMLIsLocked="false" -->
  <head>
    <meta http-equiv="Content-Type" content="text/html;
    charset=iso-8859-2">

    <!-- InstanceBeginEditable name="document_title_rgn" -->
    <title>
      user info
    </title>
    <!-- InstanceEndEditable -->
    <link rel="stylesheet" href="style.css" type="text/css">
    <!-- InstanceBeginEditable name="headers_rgn" -->
    <!-- here goes headers headers -->
    <!-- InstanceEndEditable -->
    <script language="JavaScript" type="text/JavaScript">
      <!--
```

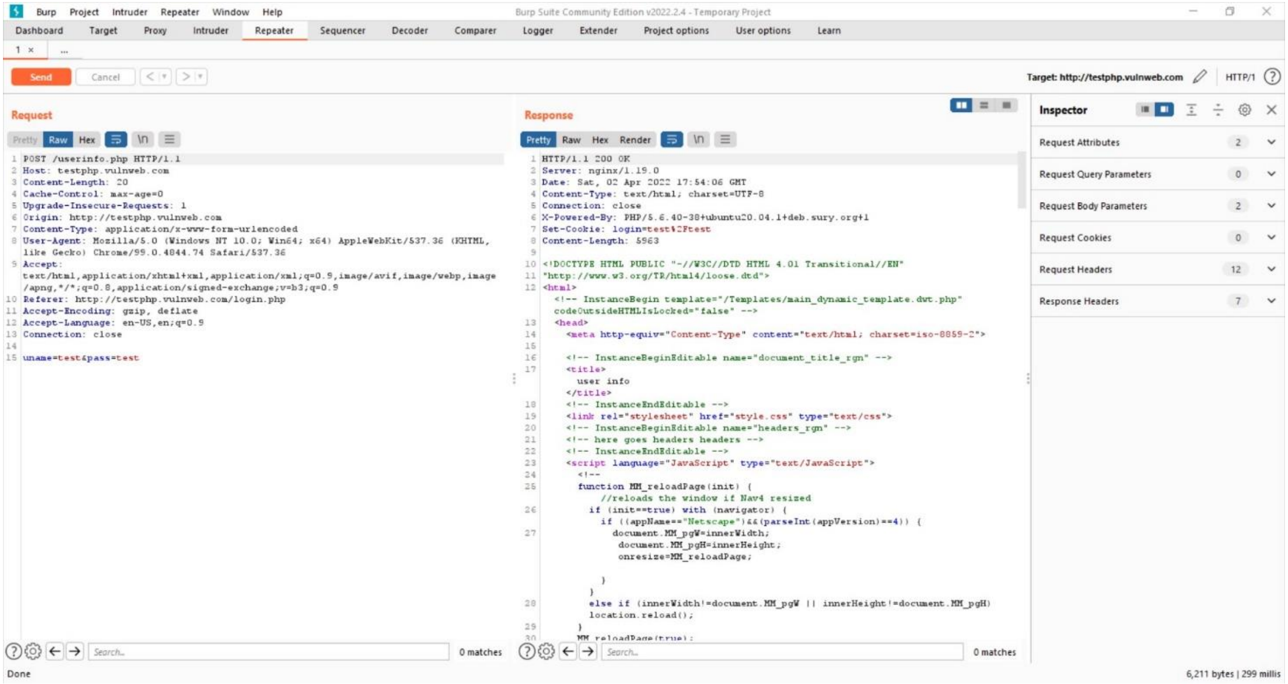
Task 2: Use of repeater.

Repeat the requests captured in Task 1 and see what response is coming from server.


logout
Not secure | testphp.vulnweb.com/logout.php
acunetix acuart
TEST and Demonstration site for Acunetix Web Vulnerability Scanner
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
search art
go
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

You have been logged out. See you back soon.

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2022.2.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
1 ×
Send
Cancel
Target: http://testphp.vulnweb.com
HTTP/1
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
Inspector
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 2
Request Cookies 0
Request Headers 12
Response Headers 7
0 matches
Done
6,211 bytes | 299 millis

Request

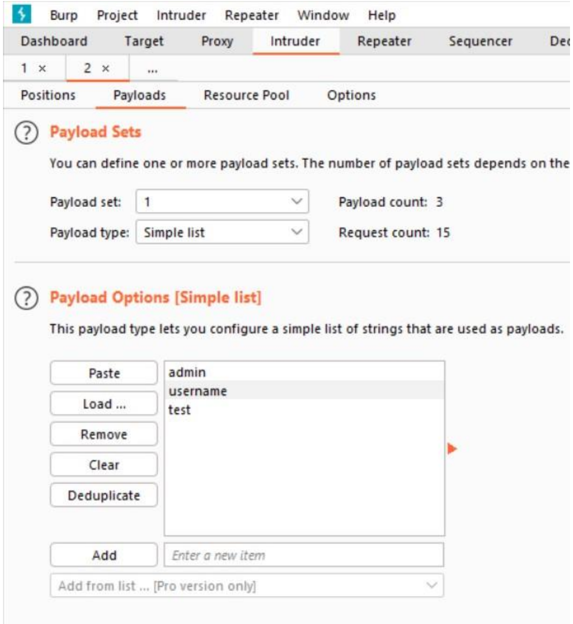
```
POST /userinfo.php HTTP/1.1
Host: testphp.vulnweb.com
Content-Length: 20
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://testphp.vulnweb.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/99.0.4844.74 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=0.9
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

uname=test&pass=test
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sat, 02 Apr 2022 17:54:06 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Set-Cookie: login=test%2Ftest
Content-Length: 5963

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html>
  <!-- InstanceBegin template="/Templates/main_dynamic_template.dwt.php"
  codeOutsideHTMLIsLocked="false" -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2">

    <!-- InstanceBeginEditable name="document_title_rgn" -->
    <title>
      user info
    </title>
    <!-- InstanceEndEditable -->
    <link rel="stylesheet" href="style.css" type="text/css">
    <!-- InstanceBeginEditable name="headers_rgn" -->
    <!-- here goes headers headers -->
    <!-- InstanceEndEditable -->
    <script language="JavaScript" type="text/JavaScript">
      <!--
      function MM_reloadPage(init) {
          //reloads the window if Nav4 resized
        if (init==true) with (navigator) {
          if ((appName=="Netscape")&&(parseInt(appVersion)==4)) {
            document.MM_pgW=innerWidth;
             document.MM_pgH=innerHeight;
             onresize=MM_reloadPage;

          }
        }
        else if (innerWidth!=document.MM_pgW || innerHeight!=document.MM_pgH)
        location.reload();
      }
      MM_reloadPage(true);
```

Task 3: Brute force.

Send a request to intruder and create 2 different payloads for usernames and passwords. Try cluster bomb attack type to find valid credential for that website.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the

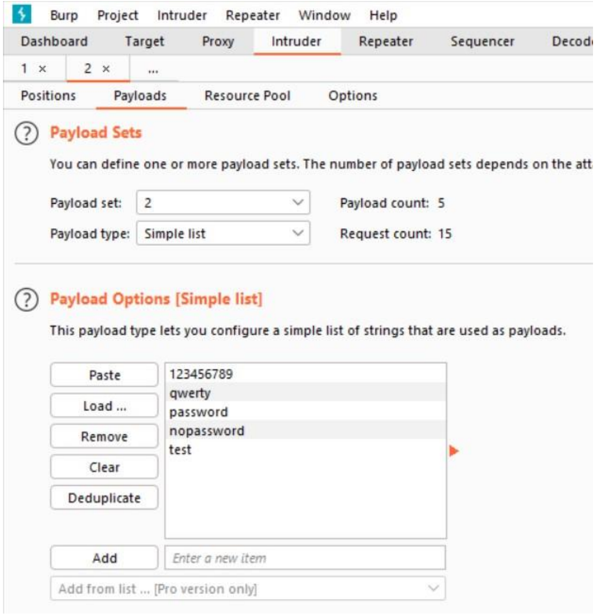
Payload set: 1 Payload count: 3

Payload type: Simple list Request count: 15

Payload Options [Simple list]

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

admin
username
test



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the att

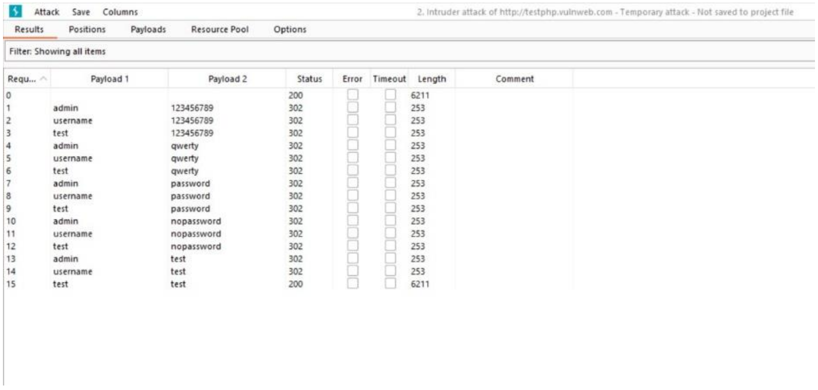
Payload set: 2 Payload count: 5

Payload type: Simple list Request count: 15

Payload Options [Simple list]

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

123456789
qwerty
password
nopassword
test



2. Intruder attack of http://testphp.vulnweb.com - Temporary attack - Not saved to project file

Filter: Showing all items

Requ...	Payload 1	Payload 2	Status	Error	Timeout	Length	Comment
0			200	□	□	6211	
1	admin	123456789	302	□	□	253	
2	username	123456789	302	□	□	253	
3	test	123456789	302	□	□	253	
4	admin	qwerty	302	□	□	253	
5	username	qwerty	302	□	□	253	
6	test	qwerty	302	□	□	253	
7	admin	password	302	□	□	253	
8	username	password	302	□	□	253	
9	test	password	302	□	□	253	
10	admin	nopassword	302	□	□	253	
11	username	nopassword	302	□	□	253	
12	test	nopassword	302	□	□	253	
13	admin	test	302	□	□	253	
14	username	test	302	□	□	253	
15	test	test	200	□	□	6211	