Project Report

Project :Brute-Force Attack using Burp Suite

Tools : Brup Suite (Kali Linux Community edition)

Target website : testphp.vulnweb.com (open for attack and ethical hacking)

Burp suite is powerful tool in kali linux. Burp suite provide critical info about website. Also find vulnerability from website which one you target for attack and brute-force attack use and it's helpful for find bugs and loophole from website.you can also used for bug bounty hunting and give report of issue and fix them and make for secure website.

In this project we used burp suite for perform the brute-force attack and fine login info about website like username.password and login panel of website let's look a forward for check and test website security for make our brute-force attack successful.

Step by step for perform brute-force attack using burp suite

1. First step is check kali linux update and upgrade for double check that our burp suite running on latest version .

2. after make sure that we go to go for run burp suite let's go start kali terminal and hit command burpsuite and start burp suite

3. after start burp suite successfully go to proxy section and check all configuration are done properly like proxy set on 127.0.0.1:8080 and browser config and check all details carefully

4. next step is go to proxy and open browser option and start and open browser that which you choose for perform operation .

5. next step is open browser and open website that which one you target for attack and after start intercept in burp suite for capture requsest and send to intruder for perform attack

6. after send to intruder go to select username and password field and ready for attack like snipper and cluster bomb.

7. after select field and attack type important step is set payload for both field and select wordlist and start the attack you will find the correct username and password .

8. after find correct username and password this brute-force attack is complete now

Login page capture with false username and password and ready for attack on select field

Request is below :

POST /userinfo.php HTTP/1.1

Host: testphp.vulnweb.com

Content-Length: 18

Cache-Control: max-age=0

Accept-Language: en-US,en;q=0.9

Origin: http://testphp.vulnweb.com

Content-Type: application/x-www-form-urlencoded

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 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

Referer: http://testphp.vulnweb.com/login.php

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

uname=abc&pass=xyz

after successfully find original login password and username response is below :

POST /userinfo.php HTTP/1.1

Host: testphp.vulnweb.com

Content-Length: 20

Cache-Control: max-age=0

Accept-Language: en-US,en;q=0.9

Origin: http://testphp.vulnweb.com

Content-Type: application/x-www-form-urlencoded

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 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

Referer: http://testphp.vulnweb.com/login.php

Accept-Encoding: gzip, deflate, br

Connection: keep-alive

uname=test&pass=test

login page pretty raw code of login page is below :

HTTP/1.1 200 OK

Server: nginx/1.19.0

Date: Thu, 23 Oct 2025 18:04:40 GMT

Content-Type: text/html; charset=UTF-8

Connection: keep-alive

X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1

Content-Length: 5523

<!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>login page</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);

//-->

```
</script>


</head>
<body>
<div id="mainLayer" style="position:absolute; width:700px; z-index:1">
<div id="masthead">
  <h1 id="siteName"><a href="https://www.acunetix.com/"><img src="images/logo.gif" width="306" height="38" border="0" alt="Acunetix website security"></a></h1>
  <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
  <div id="globalNav">
        <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
        <td align="left">
                <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists
                </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
                <a href="guestbook.php">guestbook</a> |
                <a href="AJAX/index.php">AJAX Demo</a>
        </td>
        <td align="right">
                </td>
        </tr></table>
  </div>
</div>
<!-- end masthead -->


<!-- begin content -->
<!-- InstanceBeginEditable name="content_rgn" -->
<div id="content">
```

```
        <div class="story">

        <h3>If you are already registered please enter your login information below:</h3><br>

        <form name="loginform" method="post" action="userinfo.php">

        <table cellpadding="4" cellspacing="1">

                <tr><td>Username : </td><td><input name="uname" type="text" size="20" style="width:120px;"></td></tr>

                <tr><td>Password : </td><td><input name="pass" type="password" size="20" style="width:120px;"></td></tr>

                <tr><td colspan="2" align="right"><input type="submit" value="login" style="width:75px;"></td></tr>

        </table>

        </form>

        </div>

        <div class="story">

        <h3>

      You can also <a href="signup.php">signup here</a>.<br>

      Signup disabled. Please use the username <font color='red'>test</font> and the password <font color='red'>test</font>.

   </h3>

        </div>

</div>

<!-- InstanceEndEditable -->

<!--end content -->


<div id="navBar">

  <div id="search">

    <form action="search.php?test=query" method="post">

      <label>search art</label>

      <input name="searchFor" type="text" size="10">

      <input name="goButton" type="submit" value="go">
```

```
  </form>
 </div>
 <div id="sectionLinks">
  <ul>
   <li><a href="categories.php">Browse categories</a></li>
   <li><a href="artists.php">Browse artists</a></li>
   <li><a href="cart.php">Your cart</a></li>
   <li><a href="login.php">Signup</a></li>
        <li><a href="userinfo.php">Your profile</a></li>
        <li><a href="guestbook.php">Our guestbook</a></li>
            <li><a href="AJAX/index.php">AJAX Demo</a></li>
        </li>
  </ul>
 </div>
 <div class="relatedLinks">
  <h3>Links</h3>
  <ul>
   <li><a href="http://www.acunetix.com">Security art</a></li>
        <li><a href="https://www.acunetix.com/vulnerability-scanner/php-security-scanner/">PHP scanner</a></li>
        <li><a href="https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/">PHP vuln help</a></li>
        <li><a href="http://www.eclectasy.com/Fractal-Explorer/index.html">Fractal Explorer</a></li>
  </ul>
 </div>
 <div id="advert">
  <p>
   <object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=6,0,29,0" width="107" height="66">
```

<param name="movie" value="Flash/add.swf">

<param name=quality value=high>

<embed src="Flash/add.swf" quality=high pluginspage="http://www.macromedia.com/shockwave/download/index.cgi?P1_Prod_Version=ShockwaveFlash" type="application/x-shockwave-flash" width="107" height="66"></embed>

</object>

<!--end navbar -->

 About Us | Privacy Policy | Contact Us | ©2019

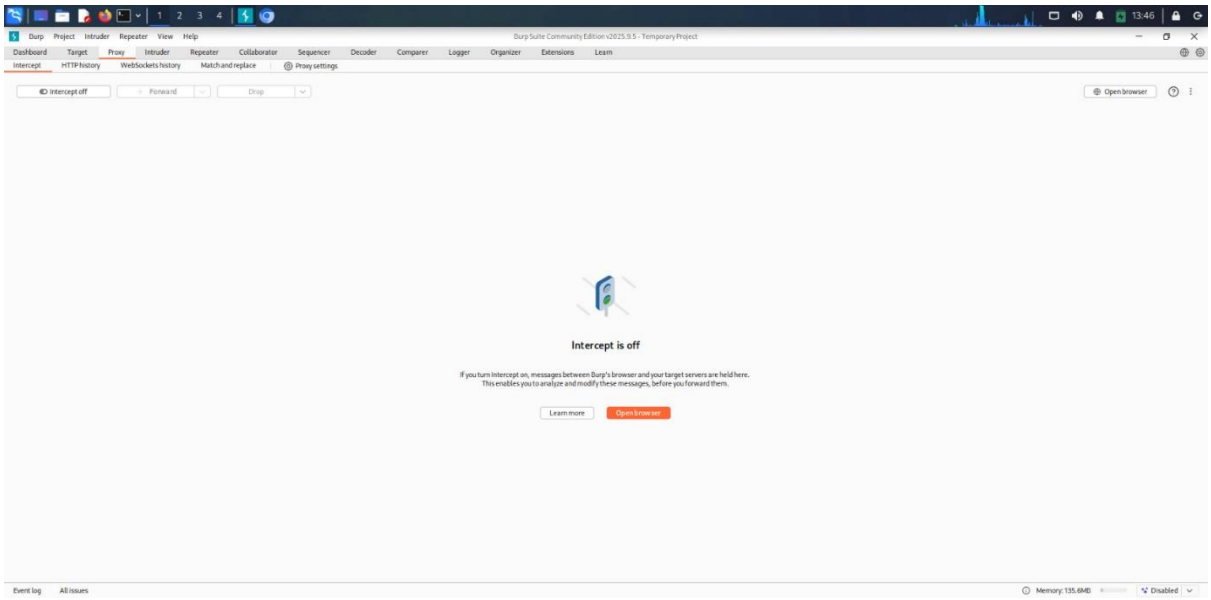
Acunetix Ltd

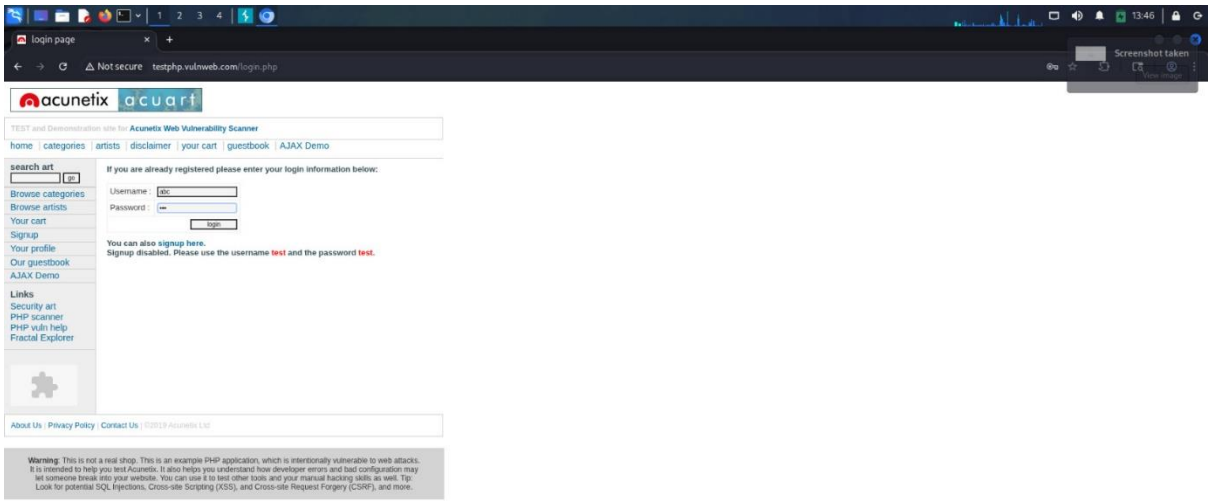
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other 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.

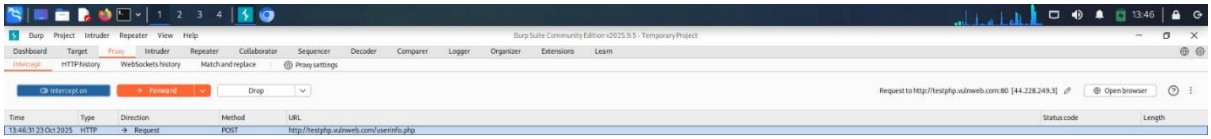
</body>

<!-- InstanceEnd --></html>

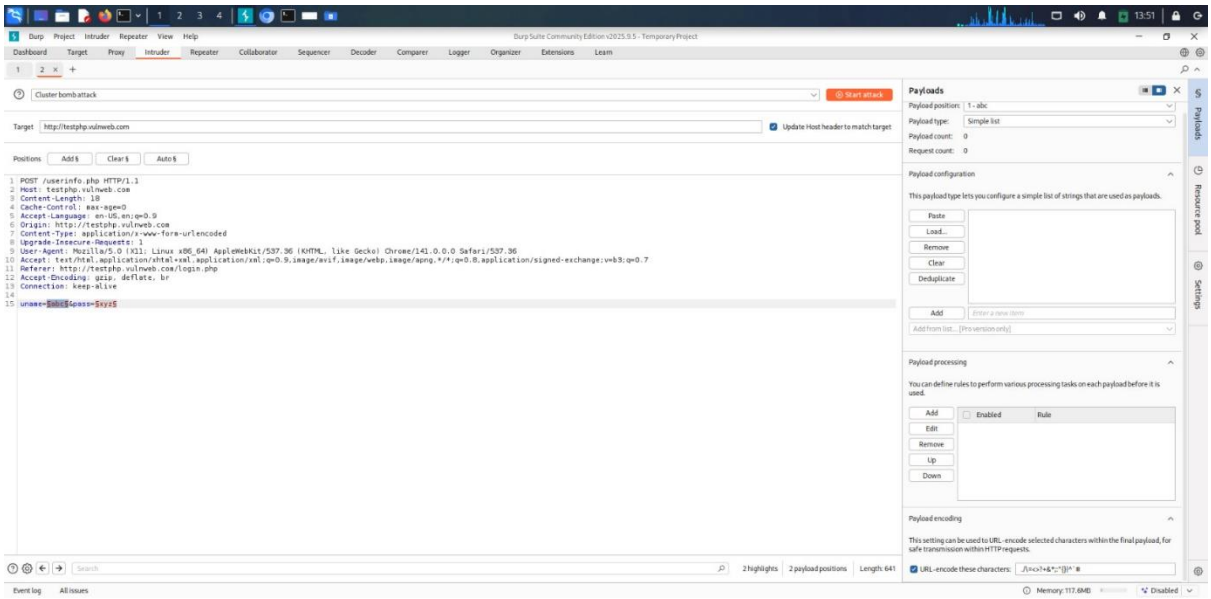
Screenshorts

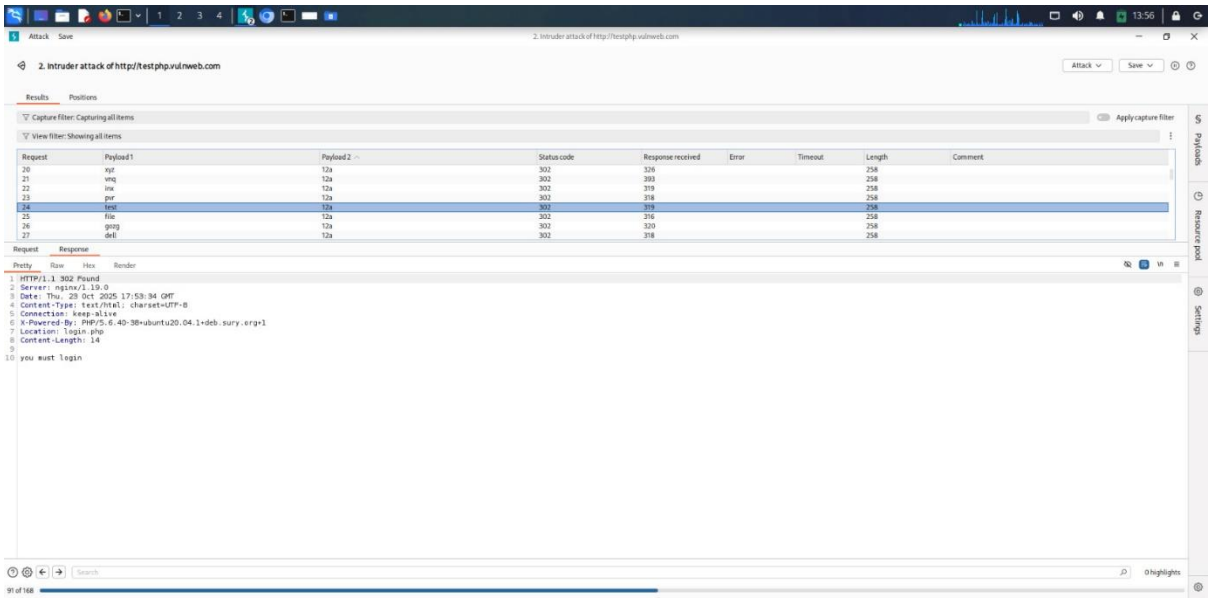


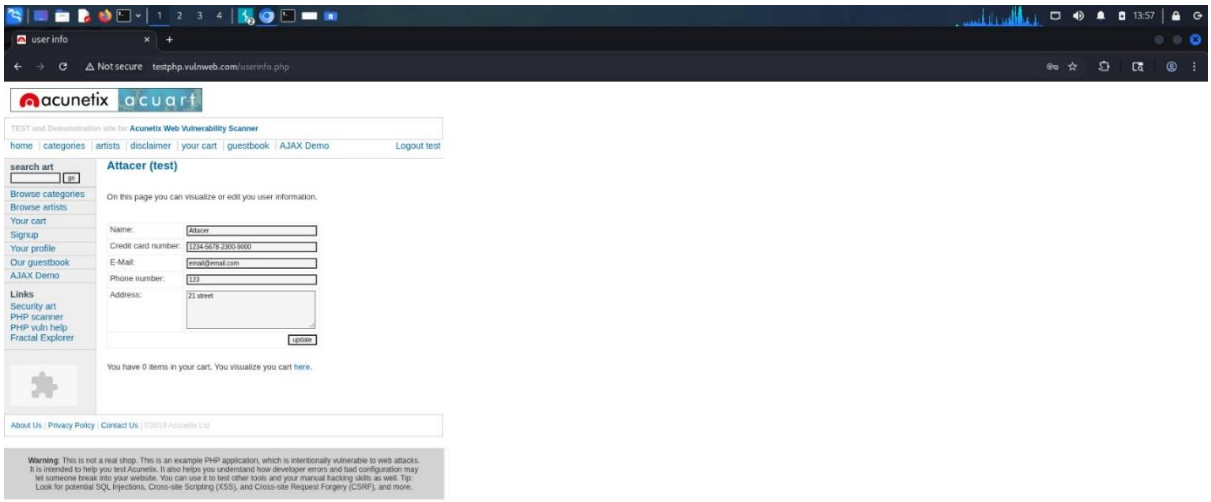



Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.9.5 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Request to http://testphp.vulnweb.com:80 [44.228.249.3]
Open browser
Time Type Direction Method URL Status code Length
13:46:31 23 Oct 2025 HTTP Request POST http://testphp.vulnweb.com/userinfo.php


Request
Pretty Raw Hex
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 18
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
10 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
11 Referer: http://testphp.vulnweb.com/login.php
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 uname=abc&pass=xyz
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 2
Request cookies 0
Request headers 12
Inspector
Notes
0 highlights
Event log All issues
Memory: 117.6MB
Disabled


Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Cluster bomb attack
Start attack
Target http://testphp.vulnweb.com
Update Host header to match target
Positions Add § Clear § Auto §
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 Content-Length: 18
4 Cache-Control: max-age=0
5 Accept-Language: en-US,en;q=0.9
6 Origin: http://testphp.vulnweb.com
7 Content-Type: application/x-www-form-urlencoded
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
10 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
11 Referer: http://testphp.vulnweb.com/login.php
12 Accept-Encoding: gzip, deflate, br
13 Connection: keep-alive
14
15 uname=§abc§&pass=§xyz§
Payloads
Payload position: 1 - abc
Payload type: Simple list
Payload count: 0
Request count: 0
Payload configuration
This payload type lets you configure a simple list of strings that are used as payloads.
Paste
Load...
Remove
Clear
Deduplicate
Add
Enter a new item
Add from list... [Pro version only]
Payload processing
You can define rules to perform various processing tasks on each payload before it is used.
Add
Edit
Remove
Up
Down
Enabled
Rule
Payload encoding
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.
URL-encode these characters:
Payloads
Resource pool
Settings
2 highlights
2 payload positions
Length: 641
Event log All issues
Memory: 117.6MB
Disabled


2. Intruder attack of http://testphp.vulnweb.com
Results
Positions
Request
Response
HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Thu, 23 Oct 2025 17:53:34 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
Content-Length: 14
you must login


user info
Not secure testphp.vulnweb.com/userinfo.php
acunetix acuart
home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo
Logout test
search art
Browse categories
Browse artists
Your cart
Signup
Your profile
Our guestbook
AJAX Demo
Links
Security art
PHP scanner
PHP vuln help
Fractal Explorer
Attacer (test)
On this page you can visualize or edit you user information.
Name:
Credit card number:
E-Mail:
Phone number:
Address:
update
You have 0 items in your cart. You visualize you cart here.
About Us | Privacy Policy | Contact Us
Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks.

---------- THE END ----------