WordPress XMLRPC All Methods Enabled

Pending Fix • ●LOW • Reported by fluhar on May 22, 2025 • #PT30497_9

Vulnerability Type

Server Security Misconfiguration

Description

It was observed that the WordPress applications have XML-RPC all methods enabled, which allows an attacker to perform various attacks on the application such as blind Server-Side Request Forgery (SSRF), password brute force attacks &, etc.

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:

- Publish a post
- Edit a post
- Delete a post.
- Upload a new file (e.g., an image for a post)
- Get a list of comments
- Edit comments

Affected Targets

```
https://slkohlercampaign.com/
```

```
https://npkohlercampaign.com/
```

```
https://bdkohlercampaign.com/
```

```
https://bhkohlercampaign.com/
```

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

Affected Resources

```
https://slkohlercampaign.com/blog/xmlrpc.php
```

```
https://npkohlercampaign.com/blog/xmlrpc.php
```

```
https://bdkohlercampaign.com/blog/xmlrpc.php
```

```
https://bhkohlercampaign.com/blog/xmlrpc.php
```

OWASP Severity

●LOW

CVSS v3.1 Score

●MEDIUM (5.3)

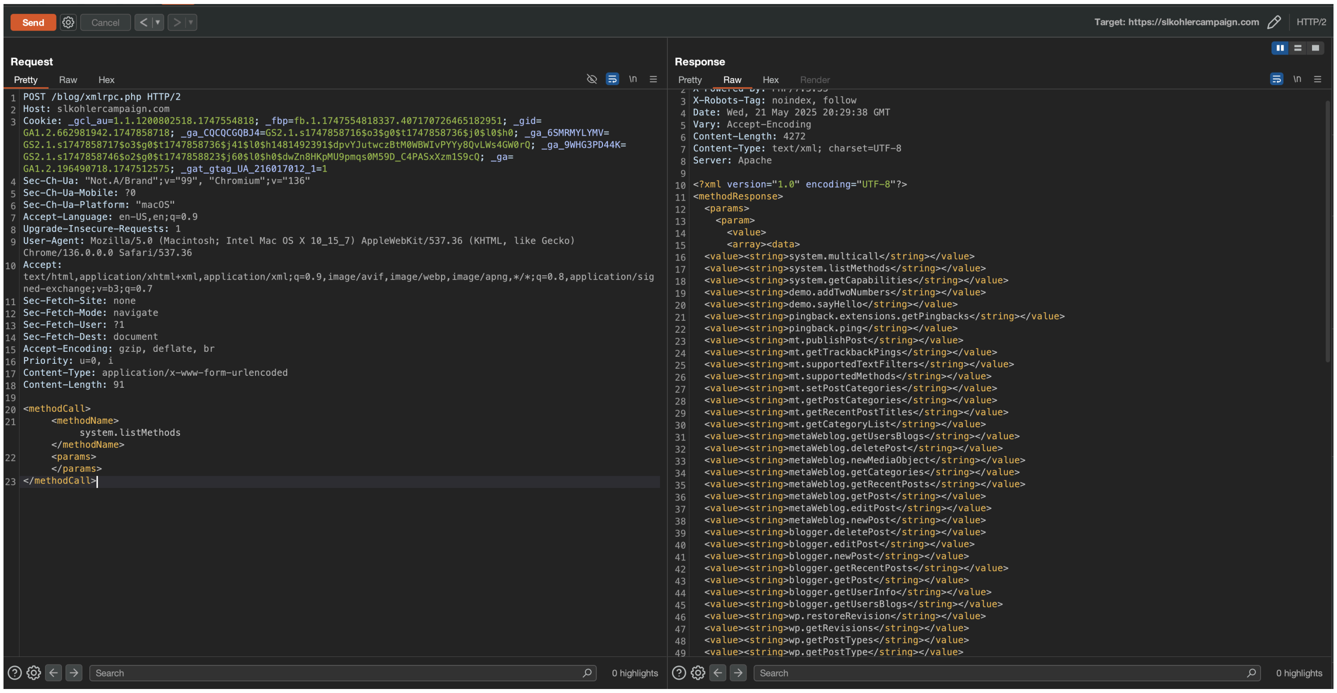
Proof of Concept

Step 1. Navigate the following URLs:

- https://slkohlercampaign.com/blog/xmlrpc.php
- https://npkohlercampaign.com/blog/xmlrpc.php
- https://bdkohlercampaign.com/blog/xmlrpc.php
- https://bhkohlercampaign.com/blog/xmlrpc.php

Step 2. Intercept the request using a proxy tool such as Burp Suite, send the request to the repeater tab, and change the request method (GET to POST).
Step 3. Enter the below XML data in the POST body and send the request.
Step 4: Observe that several methods are enabled.

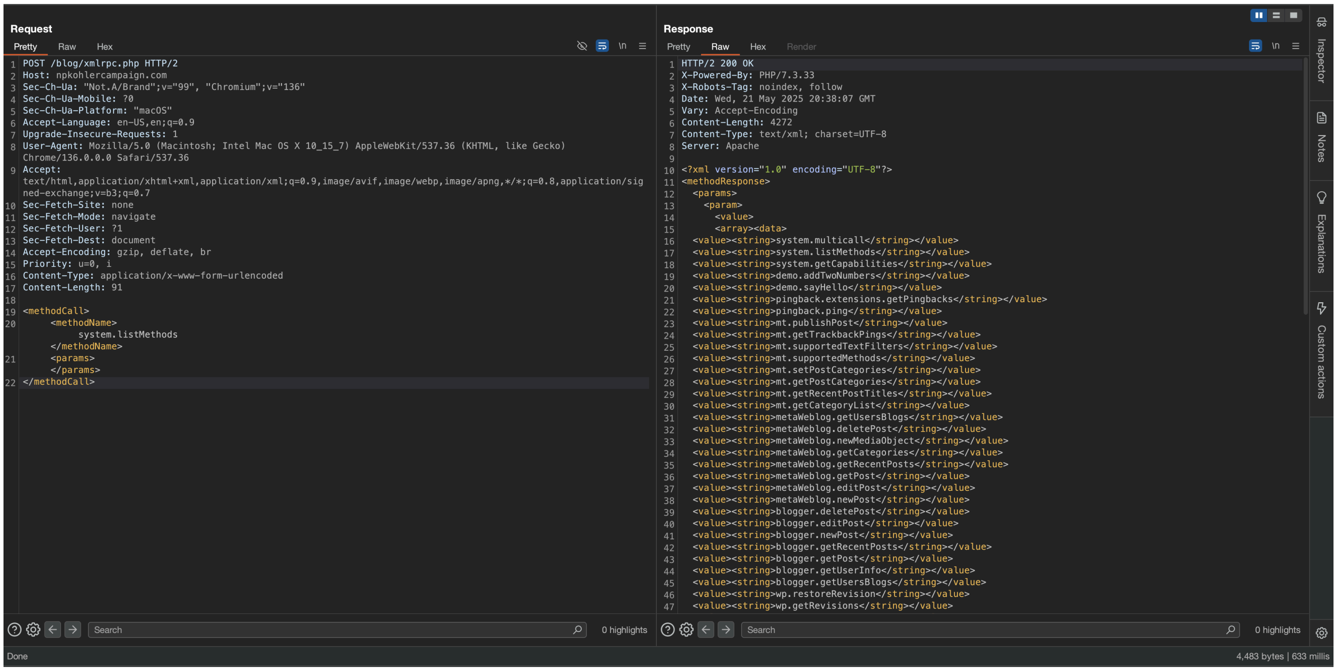
```
<?xml version="1.0" encoding="utf-8"?>
<methodCall>
<methodName>system.listMethods</methodName>
<params></params>
</methodCall>
```



```
POST /blog/xmlrpc.php HTTP/2
Host: slkohlercampaign.com
Cookie: _gcl_au=1.1.1200802518.1747554818; _fbp=fb.1.1747554818337.407170726465182951; _gid=
GA1.2.662981942.1747858718; _ga_CQCQCGQBJ4=GS2.1.s1747858716$o3$g0$t1747858736$j0$l0$h0; _ga_6SMRMYLYMV=
GS2.1.s1747858717$o3$g0$t1747858736$j41$l0$h1481492391$dpvYJutwczBtM0WBWIvPYYy8QvLWs4GW0rQ; _ga_9WHG3PD44K=
GS2.1.s1747858746$o2$g0$t1747858823$j60$l0$h0$dwZn8HKpMU9pmqs0M59D_C4PASxXzm1S9cQ; _ga=
GA1.2.196490718.1747512575; _gat_gtag_UA_216017012_1=1
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 91

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

```
X-Robots-Tag: noindex, follow
Date: Wed, 21 May 2025 20:29:38 GMT
Vary: Accept-Encoding
Content-Length: 4272
Content-Type: text/xml; charset=UTF-8
Server: Apache

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <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>
```

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

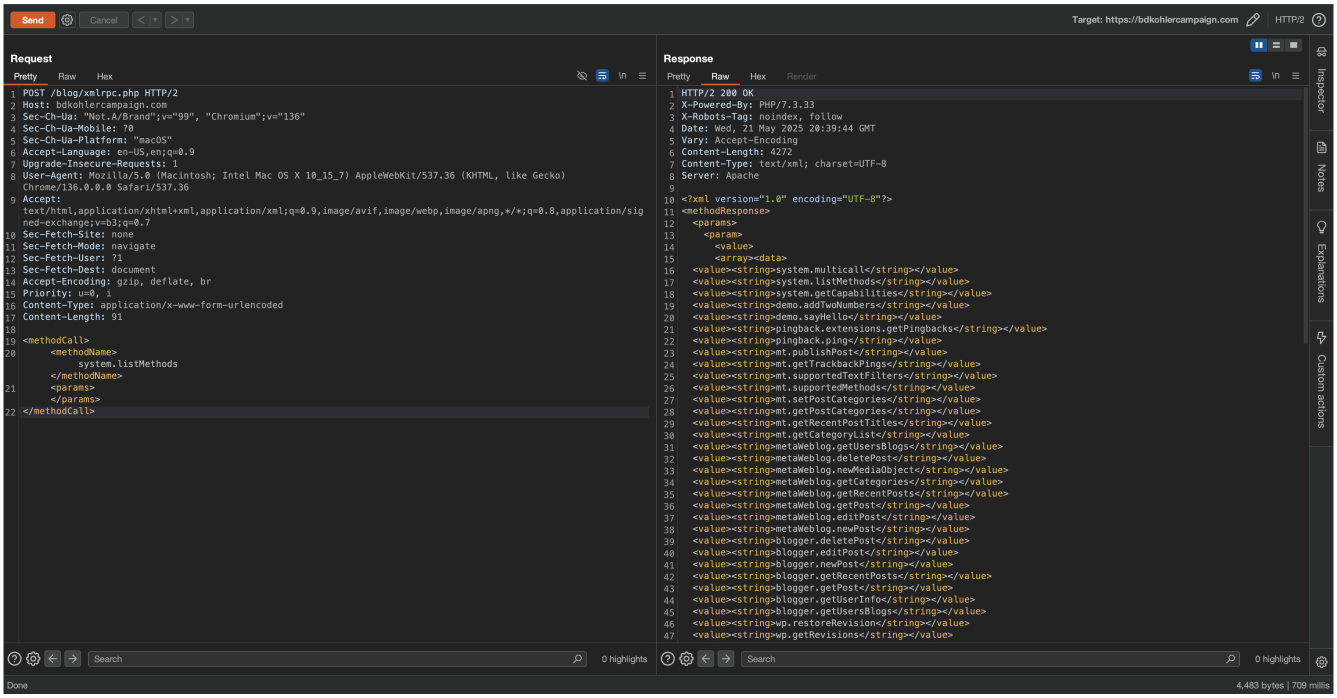


Request:

```
POST /blog/xmlrpc.php HTTP/2
Host: npkohlercampaign.com
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 91

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

Response:

```
HTTP/2 200 OK
X-Powered-By: PHP/7.3.33
X-Robots-Tag: noindex, follow
Date: Wed, 21 May 2025 20:38:07 GMT
Vary: Accept-Encoding
Content-Length: 4272
Content-Type: text/xml; charset=UTF-8
Server: Apache

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <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>
```



Target: https://bdkohlercampaign.com

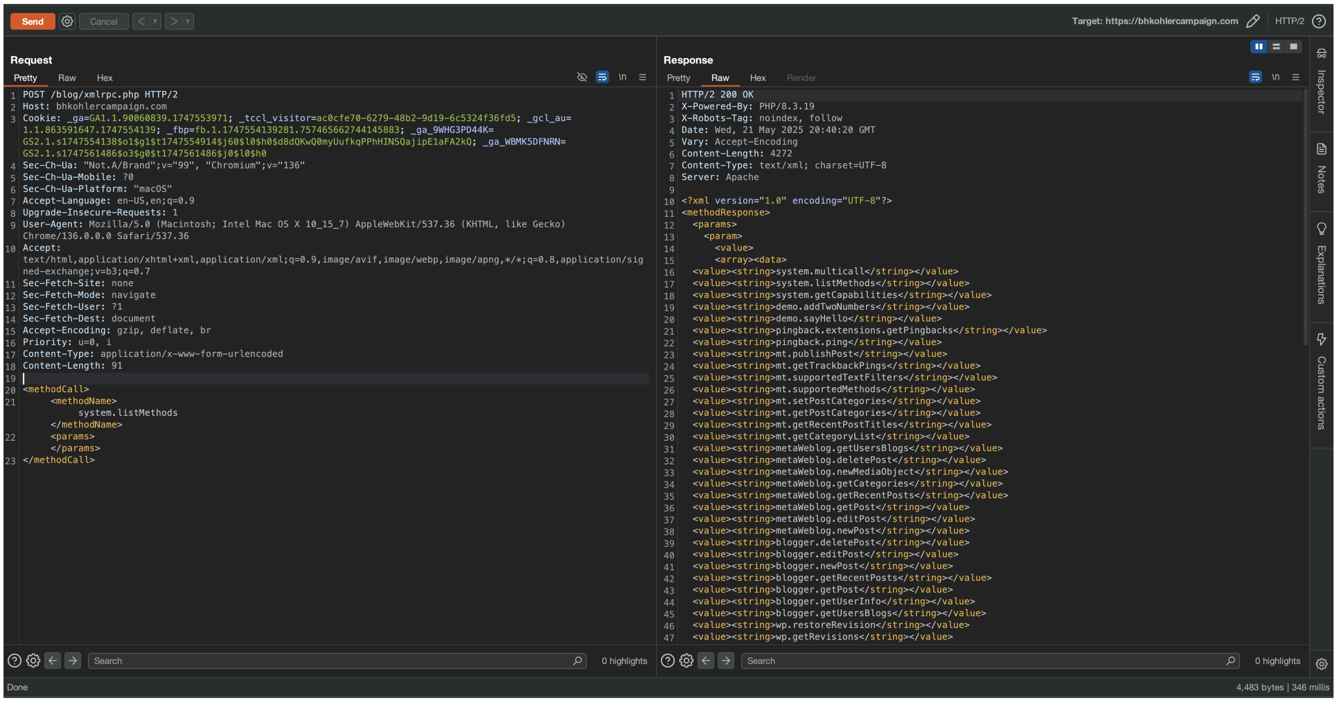
Request:

```
POST /blog/xmlrpc.php HTTP/2
Host: bdkohlercampaign.com
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 91

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

Response:

```
HTTP/2 200 OK
X-Powered-By: PHP/7.3.33
X-Robots-Tag: noindex, follow
Date: Wed, 21 May 2025 20:39:44 GMT
Vary: Accept-Encoding
Content-Length: 4272
Content-Type: text/xml; charset=UTF-8
Server: Apache

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <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>
```

© 2025 Cobalt Labs, Inc. | All Rights Reserved.



```
POST /blog/xmlrpc.php HTTP/2
Host: bhkohlercampaign.com
Cookie: _ga=GA1.1.90060839.1747553971; _tccl_visitor=ac0cfe70-6279-48b2-9d19-6c5324f36fd5; _gcl_au=
1.1.863591647.1747554139; _fbp=fb.1.1747554139281.757465662744145883; _ga_9WHG3PD44K=
GS2.1.s1747554138$o1$g1$t1747554914$j60$l0$h0$d8dQKwQ0myUufkqPPhHINSQajipE1aFA2kQ; _ga_WBMK5DFNRN=
GS2.1.s1747561486$o3$g0$t1747561486$j0$l0$h0
Sec-Ch-Ua: "Not.A/Brand";v="99", "Chromium";v="136"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Accept-Language: en-US,en;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/136.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
ned-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 91

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

```
HTTP/2 200 OK
X-Powered-By: PHP/8.3.19
X-Robots-Tag: noindex, follow
Date: Wed, 21 May 2025 20:40:20 GMT
Vary: Accept-Encoding
Content-Length: 4272
Content-Type: text/xml; charset=UTF-8
Server: Apache

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <params>
    <param>
      <value>
      <array><data>
  <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>
```

Impact

This flaw allows an attacker to perform various attacks on the WordPress application, such as blind Server-Side Request Forgery (SSRF), password brute force attack &, etc.

Suggested Fix

XMP RCP can be disabled. There is a plugin to disable XML-RPC.

- Disable XML-RPC

You can also configure the server to prevent this issue.
https://securecode.wiki/docs/lang/wordpress/

,

© 2025 Cobalt Labs, Inc. | All Rights Reserved.

ACTIVITY

fluhar changed the business impact to **Low**	10 hours ago
fluhar changed the likelihood to **Low**	10 hours ago
fluhar changed state to **Pending Fix**	10 hours ago

© 2025 Cobalt Labs, Inc. | All Rights Reserved.