

Hi Team

I am a freelance web security auditor and bug bounty hunter. I identify security loop holes and flaws that can lead to the website security 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:

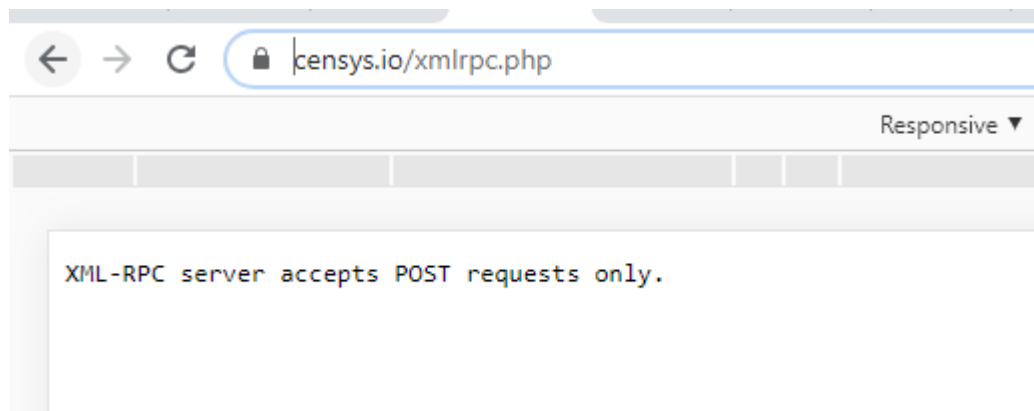
- Wp.getUserBlogs
- Pingback.ping
- System.listMethods
- System.multicall

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 DDOS 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 hundreds 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 hundreds of websites can be pinged in a single go if coupled with system.mutical.

Verification: <https://censys.io/xmlrpc.php>



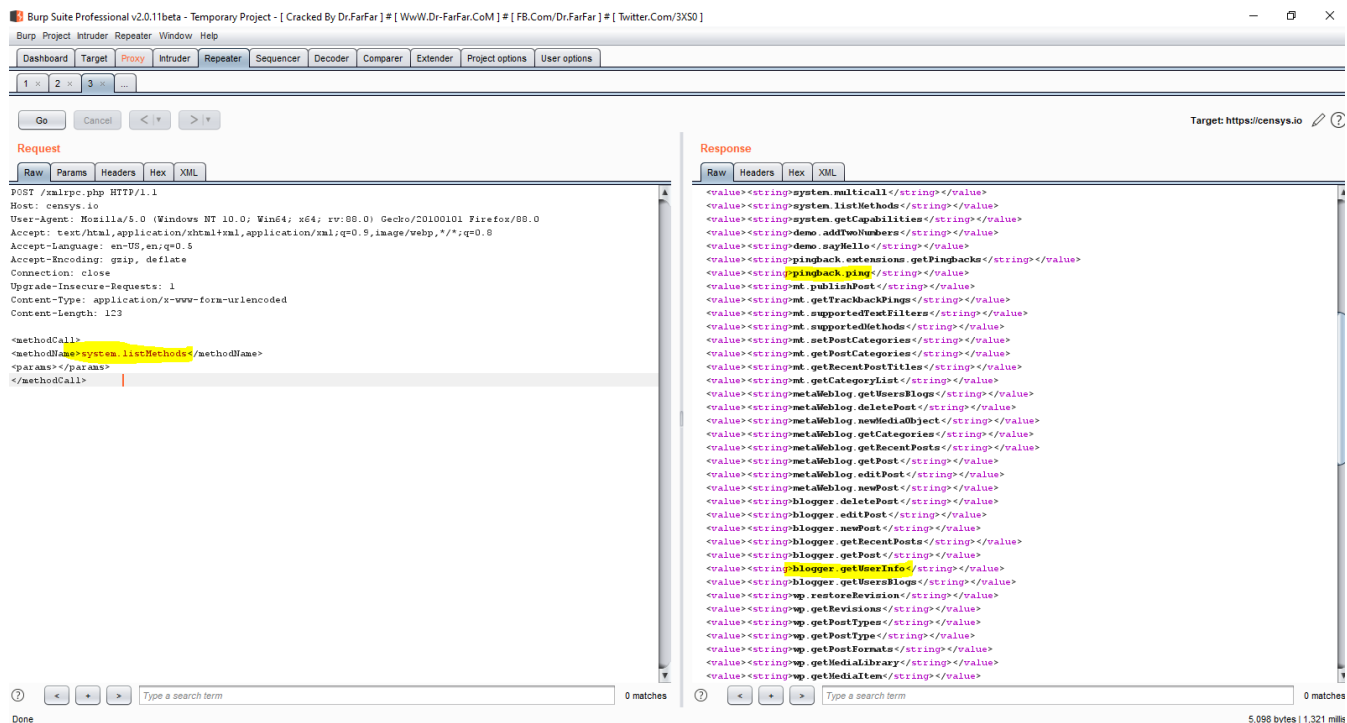
Available methods Check POC:

<methodCall>

<methodName>system.listMethods</methodName>

<params></params>

</methodCall>



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

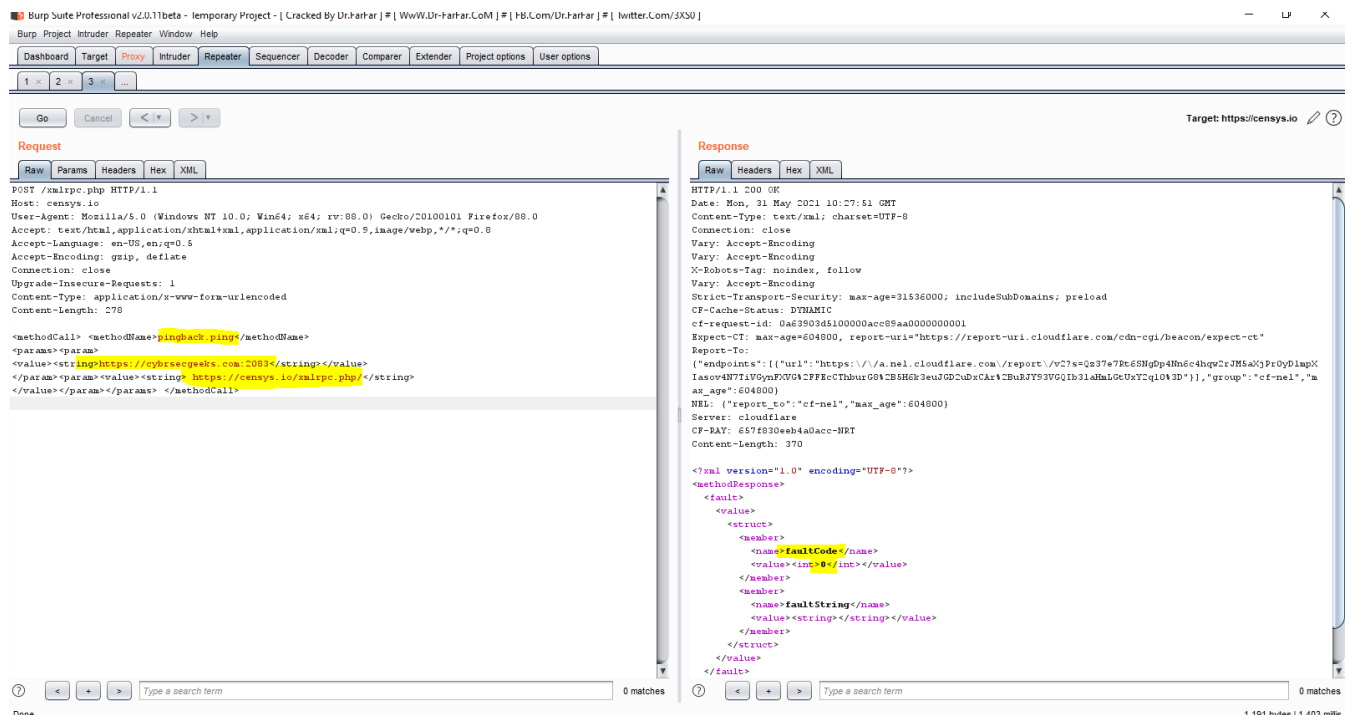
```
<methodCall> <methodName>pingback.ping</methodName>
```

```
<params><param>
```

```
<value><string>https://cybrsecgeeks.com:2083</string></value>
```

```
</param><param><value><string> https://censys.io/xmlrpc.php/</string>
```

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



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/wordpressxmlrpcphpcommonvulnerabilitieshowtoexploitthem-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/>