**Executive Summary**

The findings of a penetration test conducted on W4KEY’s SafeBank <https://10.0.0.3/>\* web application on November 11, 2023 are summarized in this report.

**Key Findings:**

A flaw that that may be exploited by a malicious actor was identified. The finding was an XMLRPC information disclosure vulnerability in the WordPress core configuration. This vulnerability could lead to an attacker being able to brute force WordPress users or perform a Denial-of-Service attack.

More information about this vulnerability here: <https://servebolt.com/articles/xmlrpc-php/>

The consequences of exploiting this vulnerability could lead to the disclosure of sensitive information, such as user credentials, which could be used to exfiltrate important information from the customer’s infrastructure

**Recommendations:**

We recommend that you disable XMLRPC using one of the methods below: <https://www.wpbeginner.com/plugins/how-to-disable-xml-rpc-in-wordpress/>

**Technical Summary**

**Scope:** [**https://10.0.0.3/\***](https://10.0.0.3/*)

**Vulnerability: XMLRPC Enabled**

**CVSS v3 5.3**

**Methodology**:

1. Check for vulnerable WordPress logins , using wpscan

--

wpscan --url https://10.0.0.3 -e u vp --disable-tls-checks

--

2. Results: xmlrpc endpoint available here: https://10.0.0.3/xmlrpc.php ,

Discovered Users SBSSiteAdmin

3. Confirming XMLRPC is

<?xml version="1.0" encoding="utf-8"?>

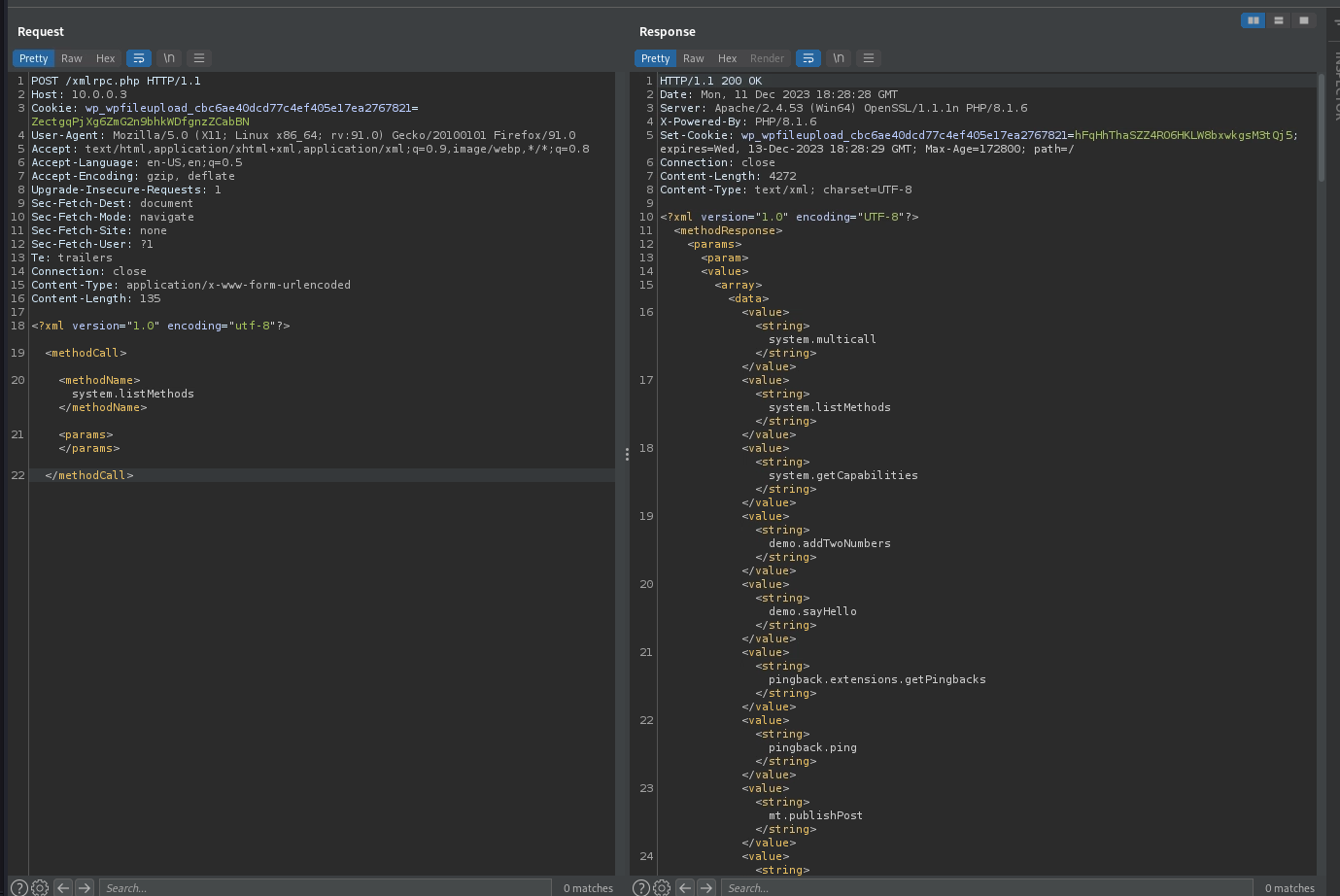
<methodCall>

<methodName>system.listMethods</methodName>

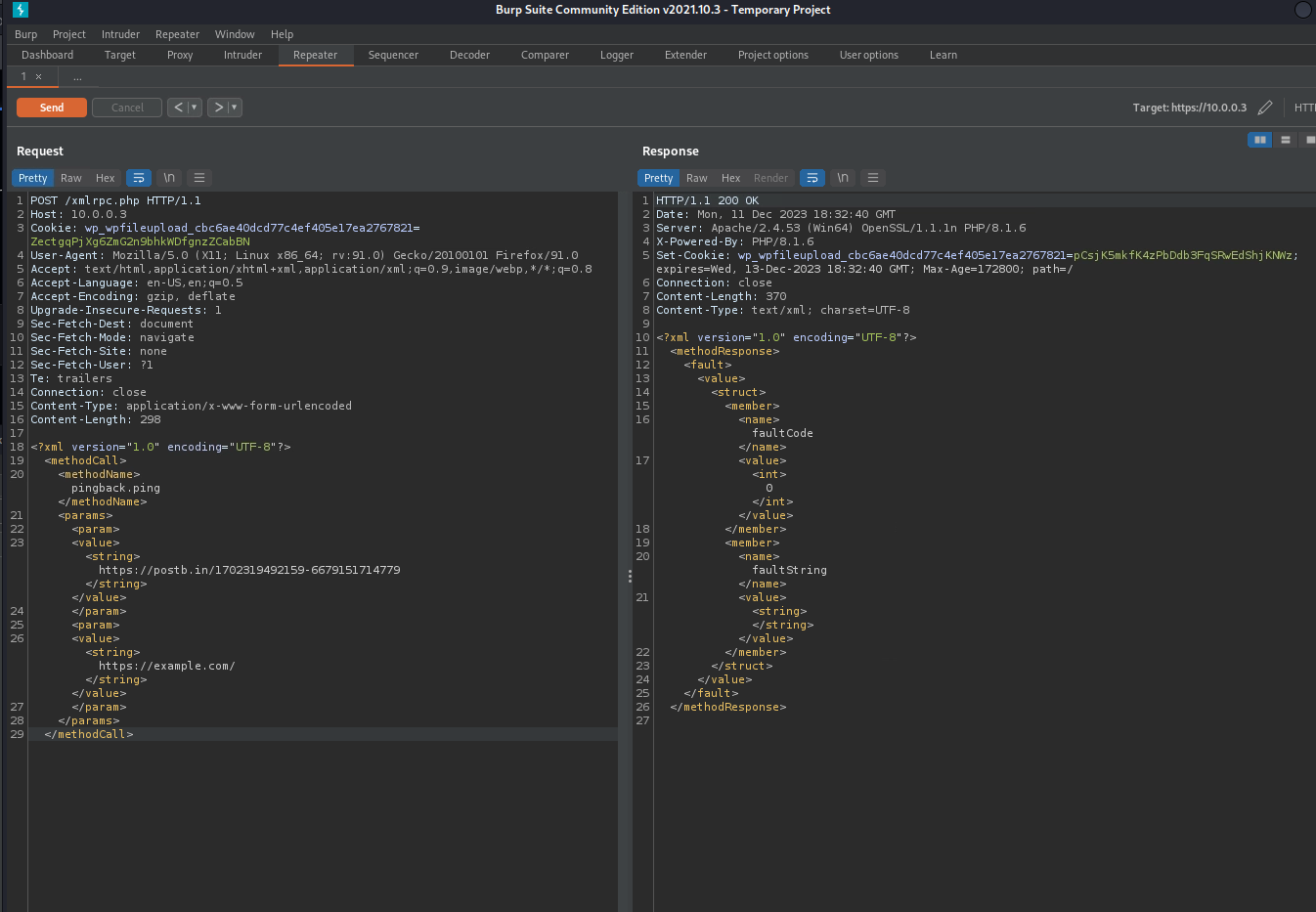
<params></params>

</methodCall>

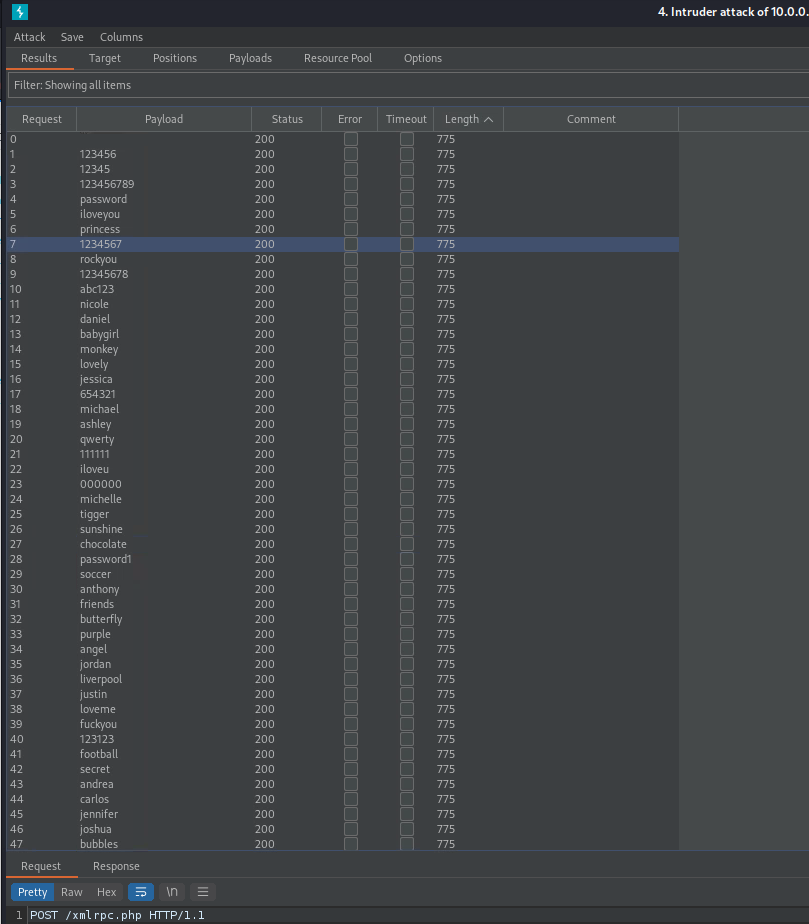
Response with available RPC method received => XMLRPC enabled (see screenshot)



Tried pingback to <https://www.toptal.com/developers/postbin/1702319492159-6679151714779>, which was unsuccessful (fault error, see screenshot)



Attempted bruteforce of SBSSiteAdmin using XMLRPC was unsuccessful, but using a different wordlist, it might be successful. At no point was the account locked out



**Recommendation**: disable XMLRPC