Soham Bakore

Follow

Feb 4, 2021 · 1 min read · Listen

# Multiple vulnerabilities in b2evolution version: 6.11.6-stable

**Vulnerability Details:**

1. **Reflected XSS in tab_type parameter in evoadm.php**
**Steps to Reproduce:**

1. Send the following URL : http://127.0.0.1/evoadm.php?ctrl=items&tab=type&tab_type=qnfya%22onmouseover%3d%22alert(document.domain)%22style%3d%22position%3aabsolute%3bwidth%3a100%25%3bheight%3a100%25%3btop%3a0%3bleft%3a0%3b%22gl4q0&filter=restore&blog=7 to the logged in victim.

2. When the victim opens the above link, Javascript code will be triggered

3. The vulnerable parameter in this case is “tab_type”

2. **Reflected XSS in tab3 parameter in evoadm.php**

**Steps to Reproduce:**

1. Send the following URL **http://127.0.0.1/evoadm.php?ctrl=comments&filter=restore&tab3=123%22onmouseover=%22alert(document.domain)%22&blog=1&blog=1** to the logged in victim.
2. When an unsuspecting user with admin privileges opens this URL, XSS will be triggered executing JavaScript malicious code

3. The vulnerable parameter in this case is “tab3”.

3. **Stored XSS in plugin name parameter**

**Steps to Reproduce:**
1. Login with an account having admin privileges

2. Change the plugin name and enter the following payload “><svg/onload=alert(123)>
3. Payload gets stored in the database

4. The payload gets executed after the victim checks the plugin page.

5. This vulnerability needs admin privilege and can affect other users with similar privileges

4. **Open redirect in redirect_to parameter in email_passthrough.php**

**Steps to Reproduce:**
1. Send the following link : http://127.0.0.1/htsrv/email_passthrough.php?email_ID=1&type=link&email_key=5QImTaEHxmAzNYyYvENAtYHsFu7fyotR&redirect_to=http%3A%2F%2Fgoogle.com to the victim user
2. The victim user will be redirected to Google.com or any other attacker controlled domain
3. This can be used to perform malicious phishing campaigns on unsuspecting users\

**Authors:** Soham Bakore | Nakul Ratti