

E107 2.1.9 Cross-Site Request Forgery Assigned CVE Number: CVE-2018-17081

Author: Himanshu Rahi

Email: hunny.rahi55@gmail.com

e107 2.1.9 allows CSRF via

e107_admin/wmessage.php?mode=&action=inline&ajax_used=1&id=, for changing the title of an arbitrary page.

CSRF:

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request. With a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

(Source: Owasp)

Steps to reproduce:

1. Victim (Admin) login their account first.
2. Attacker send a form/link to victim.
3. If victim click the form/link, An the title of page is changed by changing ID he can change any page title

Here is exploit code:

```
q}v 
kxm
α{v 
j l }rxwq}yxlj qx2h:9hj mv rwv n2j pn7qyHv xm2/ j l }rxw2wuwn/ m2m2
/j s 2h2nm2m2v n}qxm222 2222
rwy 2}22yn22qmmmw2vj v n23vj v n22j 2n22pnw/ , 2>2y 2222
rwy 2}22yn22qmmmw2vj v n22j 2n22j 2n22j l tnm222
rwy 2}22yn222kv n22j 2n222kv n22n22n2222
α{v 
kxm
q}v 
```