enferas / CVE-2022-36747.md

XSS vulnerability in Razor

CVE-2022-36747.md

XSS vulnerability in Razor project https://github.com/cobub/razor version 0.8.0

The path of the vulnerability.

In file https://github.com/cobub/razor/blob/2c991aff4a9c83f99e77a03e26056715706f15c0/web/application/controllers/manage/product.php

```
//line 98
function uploadchannel()
    {
        $platform = $_POST['platform'];
        $channel = $this->channel->getchanbyplat($platform);
        echo json_encode($channel);
    }
```

In file razor/web/application/models/channelmodel.php

```
 function getchanbyplat($platform)
//line 421
function getchanbyplat($platform)
    {
        $userid=$this->common->getUserId();
        $sql="select * from  ".$this->db->dbprefix('channel')."  where active=1 and
        select * from  ".$this->db->dbprefix('channel')."  where active=1 and platfo
        $query = $this->db->query($sql);
        if ($query!=null&&$query->num_rows()>0) {
```

```
                return $query->result_array();
            }
              return null;
        }
```

We can see that the $platform variable is used inside the the sql query without sanitization. So the attacker can use the UNION command inside the platform to join a harmful input to the results of the query. For example: $platform = 'something' UNION select '<script>alert(document.cookie)<\script>' AS '.

Thus the XSS will happen at echo json_encode($channel);