INFORMATION SECURITY ASSIGNMENT

BUG BOUNTY ATTACK

Name: Atmik Ajoy

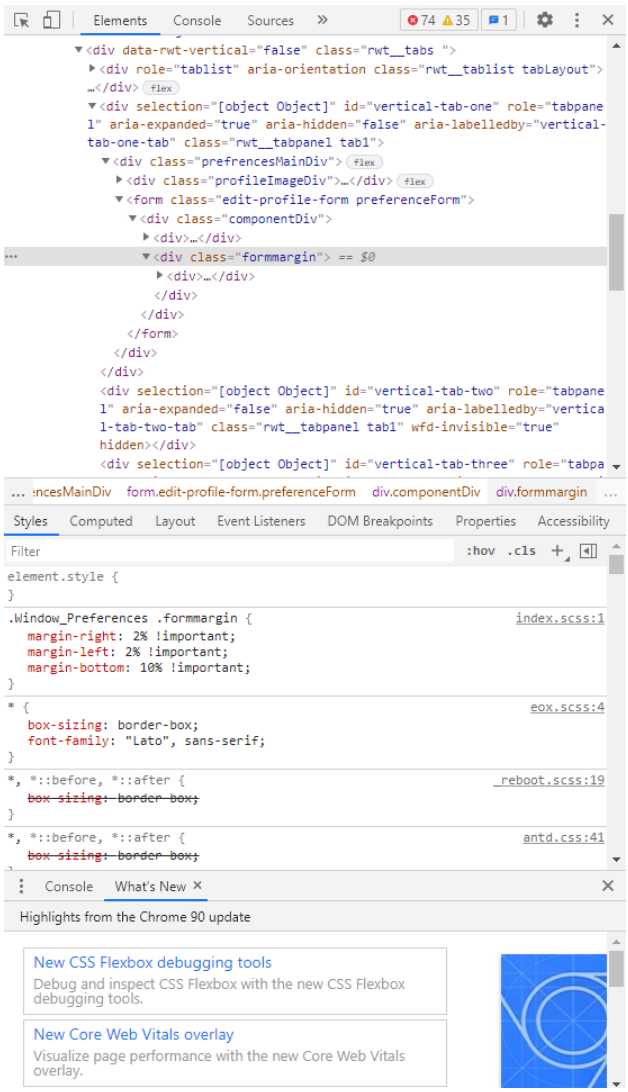
SRN: PES1201800189

Section: ‘A’

The task for this assignment was to perform a bug bounty attack and find bugs in the given website, https://demopes.eoxvantage.com

The following is a list of bugs found accompanied with the analysis behind finding said bugs.

1. HTML Injection



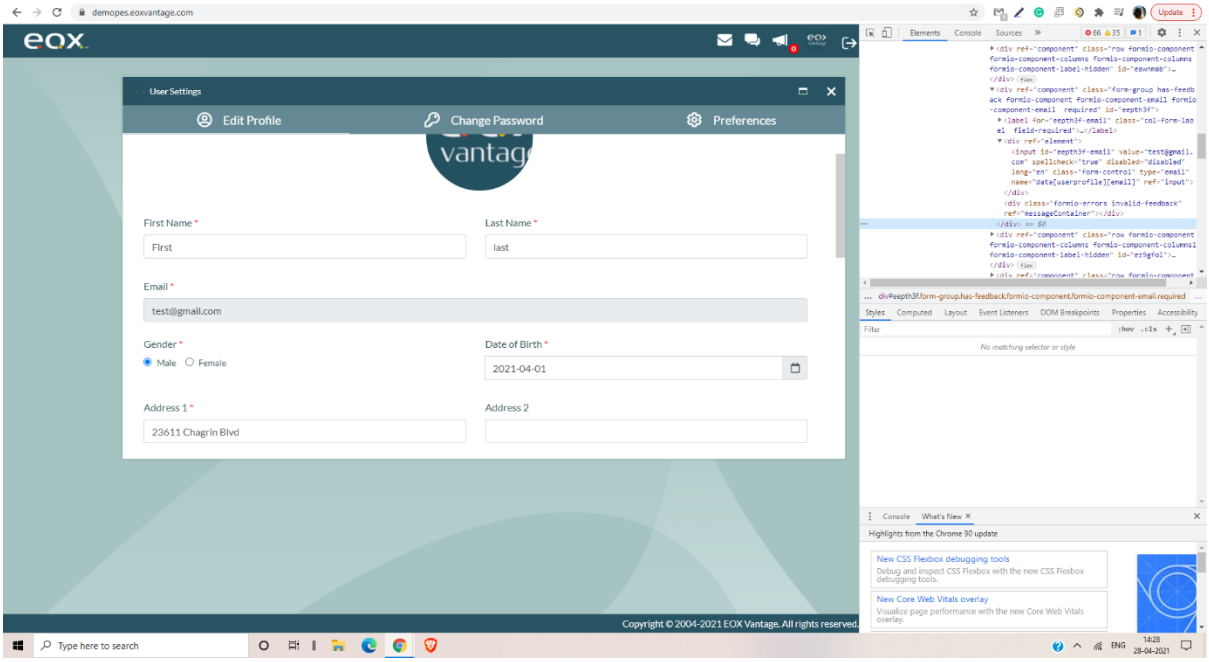
HTML Injection is a type of vulnerability that occurs when a user is able to control an input point and is able to inject arbitrary code into a vulnerable web page.

This would be simply just inserting HTML code using the inspect element and insert a form/field to collect data that seems genuine to the webpage.

The screenshot on the left indicated where we inject the HTML code.

2. Changing permanent fields

We can change some permanent fields that are not meant to be changed. The below screenshot represents the email field that isn't supposed to be able to get changed.

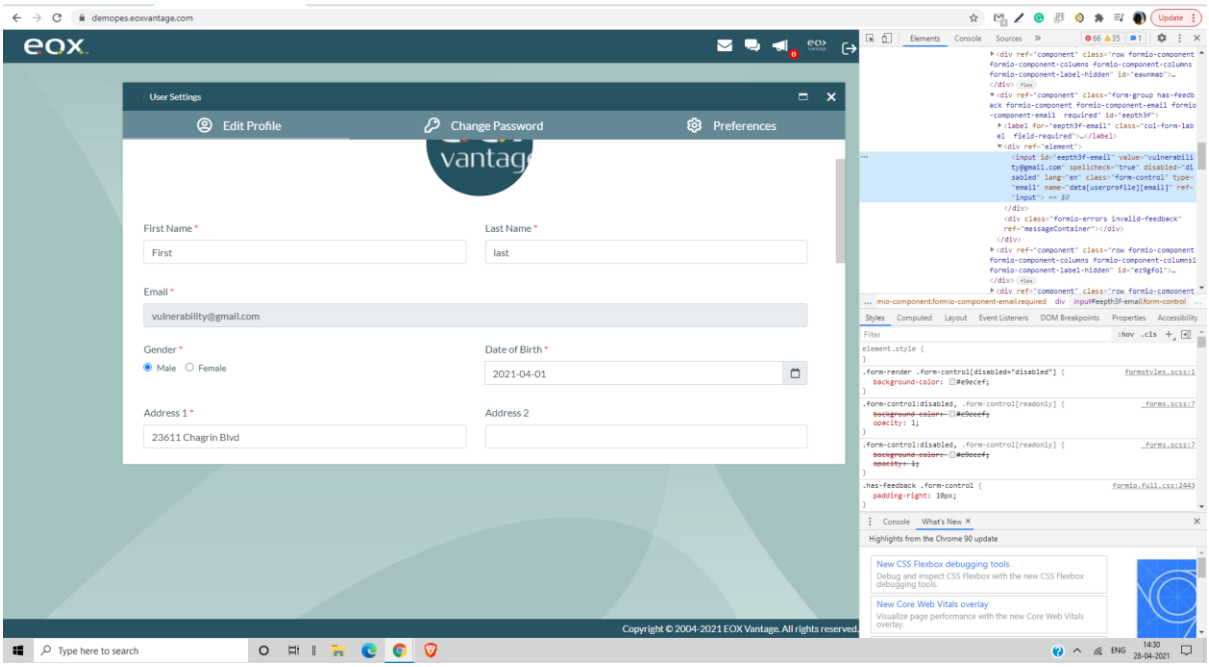


We see that test@email.com is not allowed to be changed as its greyed out.

We can see on inspecting element that we can change the email address, given by the below screenshot.

```
<div ref="element">
    <input id="eepth3f-email" value="vulnerabili
    ty@gmail.com" spellcheck="true" disabled="di
    sabled" lang="en" class="form-control" type=
    "email" name="data[userprofile][email]" ref=
    "input"> == $0
</div>
```

we see that value is changed to vulnerability@gmail.com and the screenshot below shows the newly saved email



This is a risk as we can change the email to whatever we want without explicit access that can prove to be dangerous.

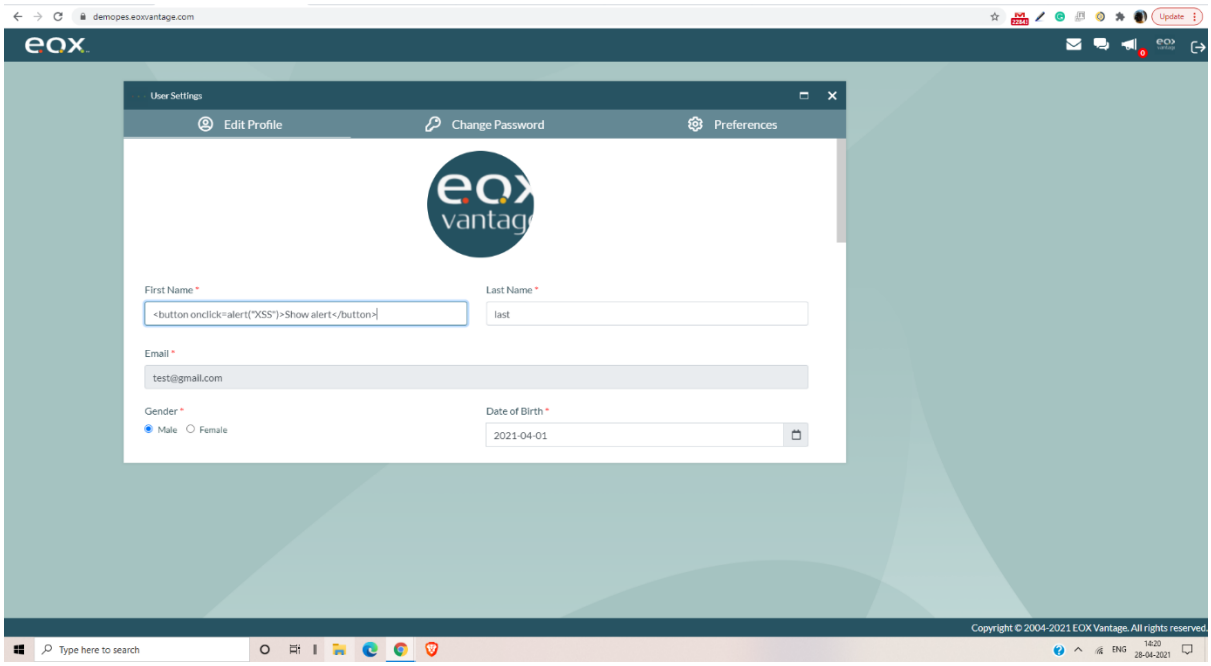
3. XSS attack

   This is a type of injection where malicious scripts are injected into sites. This usually happens when we inject client side scripts into web pages viewed by other users. It can be used for various malicious uses like bypassing access controls (like the same-origin policy), to obtain data in the form of an alert form from user (seeming original and authentic), etc.

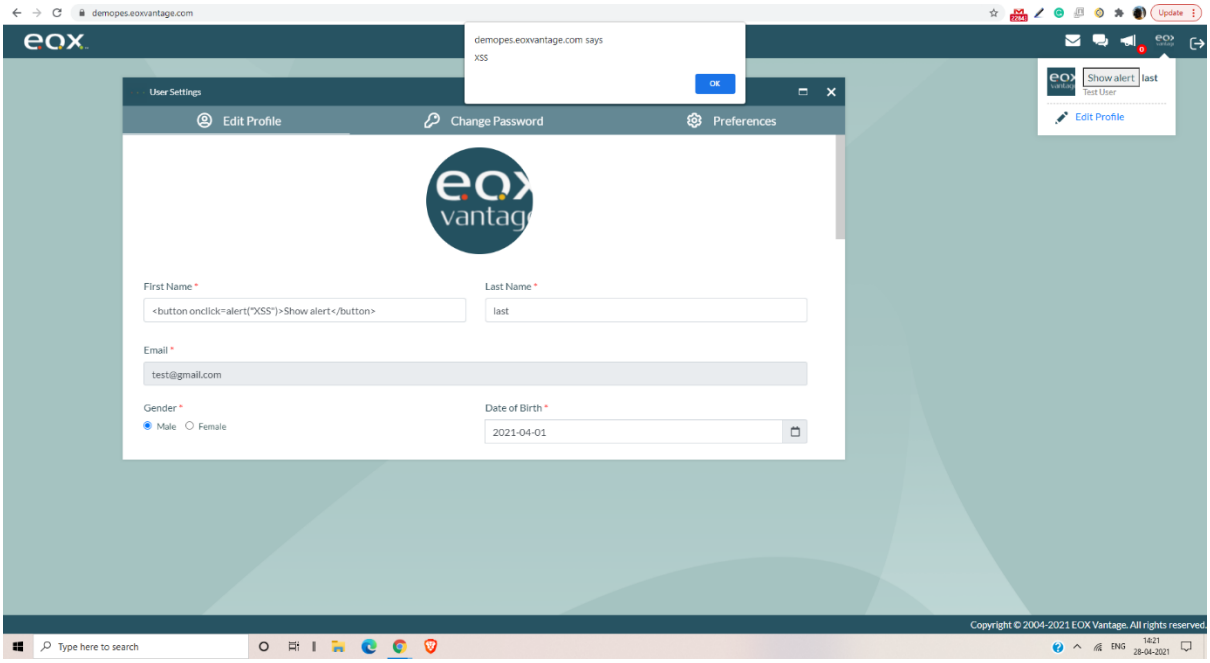
   There are 3 main types of XSS,

   a. Reflected RSS – data is not being stored on the web server but is reflected in the results.
   b. Stored XSS – data is being stored on web server and is also reflected in the results
   c. DOM

   Here we explore the XSS in a very simple way, we only display an alert to show that an XSS attack is possible. The above mentioned types can by carried out with simple modifications to the injected script.



The above is the screenshot of the injected script in the FirstName field.



The above screenshot shows the performed XSS command by inserting a button that when clicked by the user will show an alert.