Problem Set 1

What is XSS and how does it work

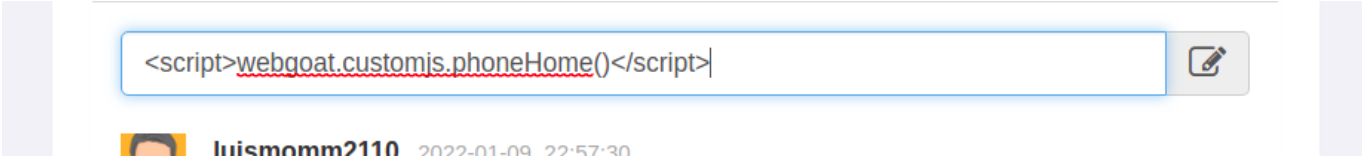
A type of security flaw in which the attacker send a maliciousious script through some trusted data not validated. With this flaw, an unadvised user can execute the script and have his/her data leaked.

Why is it important to prevent XSS attacks? Which of the Confidentiality, Integrity, and Availability (CIA) triad does XSS compromise?

As described above, the user can have some data leaked (Confidenciality) and the attacker can gain can gain some privileged acess through admin access and delete or modify data (Integrity/Avalability)

Cross Site Scripting (stored) activity you need to include the following:

2. The Flaw: Include a screenshot highlighting the vulnerable field. More points will be awarded if your screenshot shows a successful attack showing an “Alert” screen



Payload that works against the flaw. Include a single line of code/payload that can be inserted into the flawed field shown in #2

<script>alert()<script>

A patch to the flaw

```
userSessionData.setValue("xss-reflected1-complete", (Object) "false");
StringBuffer cart = new StringBuffer();
cart.append("Thank you for shopping at WebGoat. <br />You're support is appreciated<hr />");
String encoded_string = Encode.forHtml(field1);
cart.append("<p>We have charged credit card:" + encoded_string + "<br />");
cart.append("                              ------------------- <br />");
cart.append("                                $" + totalSale);
```

The patch encodes the input so it is not interpreteded as JS, but as HTML