Stored XSS Attacks

Sunday, October 29, 2017 7:49 PM

- It is always good practice to scrub all input, especially those inputs that will later be used as parameters to OS commands, scripts, and database queries
  - It is particularly important for content that will be permanently stored somewhere in the application
- Users should not be able to create message content that could cause another user to load an undesirable page or undesirable content when the user's message is received

Solution

- Enter JavaScript into the message field

```
<script>alert("LOL Ow3ned");</script>
```

- When users view the message the script will execute
- This script is stored in the message and thus will remain in the web app for as long as the message remains there
- In a practical scenario the JS code would be malicious and could pretty much do whatever the attacker wants to program it to do