Injections

SSI Injection

Server Side Includes

- SSI are generally the directives that are present on the Web applications which are used to feed an HTML Document with dynamic contents.
- In this scenario, generally the web server first analyzes the SSI before supplying the page to the end user.

SSI Injection

- The SSI Injection attack generally allows the exploitation of a web application by injecting scripts in the HTML pages or even by remotely executing arbitrary codes.
- It could be easily exploited through the manipulation of SSI in use in the web application or by forcing its use through the user input fields.
- The attacker could easily access sensitive information like password files or even execute shell commands.

Attack

- The SSI directives are usually injected in the input fields and are then sent to the web server.
- The web server parses them and then executes the directives before supplying the page.
- Hence, the result of this attack will be seen the next time that the page is loaded in the end user's browser.
- The commands used for SSI Injection generally vary on the server that is been implemented.

Example

This command could be used to get the output of a System Command. In this scenario , it is an “ls” command.

```
<!--#exec cmd="ls" -->
```

This command could be used by an attacker in order to get the directory listing on the root directory.

```
<!--#exec cmd="/bin/ls /" -->
```

Mitigations

- Disable SSI execution on pages that do not require it.
- To ensure that only the SSI directives which are needed for that page are enabled and all others are disabled.
- Encoding of the user supplied data before passing the data to the page with SSI Execution Permissions.
- Usage of SUExec[5] to make the pages execute only as the owner of the file and not of the web server.