Injections

(Command Injection)

Command Injection

- Command Injection is also known as Arbitrary Code Execution.
- In this attack, the attacker generally injects a malicious input which is passed onto the functions which execute shell commands based on the attackers input.
- They generally occur when the Web Application supplies the malicious user input data such as cookies, forms or Header Data to the system shell.

Crafting the attack parameters

- An attacker could craft the attack similarly to that used while SQL Injection.
- Shell commands are generally delimited with a semi-colon, so which allows multiple commands to be chained together.
- The symbol used for comments which is “hash symbol”(#) could be used as anything written after this is considered to be a comment and hence will be ignored.

Example Vulnerable Code

```
<?php print(“Enter the file that is to be deleted");
print("<p>");
$file=$_GET['filename'];
system("rm $file"); ?>
```

Request:

```
http://sitename.com/filedelete.php?filename=file.txt;ls
```

Response:

```
Enter the file that is to be deleted

Hello.txt      File1.c        a.out          Sym.l
H1.y           File2.c        esd.awk        fav.exe
```

Functions leading to Command Injection

- These are some of the Commands that generally lead to Command Injection Attacks.
  - exec()
  - passthru()
  - system()
  - shell_exec()
  - Backtick Operators

/e flag in preg_replace

- The /e flag in preg_replace function also allows for Command Injection vulnerability.

Example:

```
<?php
function formatDate($strn,$outformat='n/j/Y'){
 return preg_replace("/(\d{4})-(\d{2})-
(\d{2})/e","Date('$outformat',strtotime('$0'))",$strn);
}
?>
```

Mitigations

- Proper Input Validation is necessary.
- PHP generally has 2 commands which could be used to sanitize input before passing it to a command.
  - escapeshellarg()

    Used to escape any internal quotes by adding the quotes around the input.
  - escapeshellcmd()

    Used to interrupt or override execution by escaping all the special characters.