Module 3 Cheat Sheet: OWASP Application Security Risks

Package/Method	Description	Code Example
| bandit | Bandit is a tool designed to find common security issues in Python code. To do this, Bandit processes each file, builds an AST from it, and runs appropriate plugins against the AST nodes. Once Bandit has finished scanning all the files, it generates a report. | Example: Install Bandit:<br><br>```
pip install bandit
```<br><br>Run Bandit:<br><br>```
bandit -r ~/your_repos/project
```<br><br>The `-r` flag indicates that Bandit should run recursively through all files and subdirectories in the specified directory. |
| bash | Bash, or the Bourne Again Shell command, is a command-line interpreter commonly used in Unix-based operating systems. It runs in a text window where the user can interpret commands to carry out various actions. | Example: This generates a list of numbers and prints them:<br><br>```
#!/bin/bash
# Loop from 1 to 3 and print the numbers
for i in {1..3}; do
  echo "Number: $i"
done
``` |
| cd | Used to move efficiently from the existing working directory to different directories on your system. | ```
cd [directory]
``` |
| cursor. execute(operation, params=None, multi=False) | This method executes the given database operation (query or command). The parameters found in the tuple or dictionary params are bound to the variables in the operation. | ```
cursor.execute ("<SQL Query>")
```<br><br>Example:<br><br>```
cursor.execute("SELECT * FROM table_name")
``` |
| echo | Allows users to display lines of text or strings that are passed as arguments. | Syntax:<br><br>```
echo [option] [string]
```<br><br>Example:<br><br>```
echo "Hello, world!" # This prints Hello, world!
``` |
| export | Given directly to the shell (for example, bash ) to tell it to add or modify one of its environment variables. It is used to ensure the environment variables and functions are passed to child processes. | Syntax:<br><br>```
export - export [-f] [-n] [name[=value] ...] or export -p
```<br><br>Examples:<br><br>```
export PATH="$PATH:/path/to/new/directory" #Setting PATH variable
export PYTHONPATH="/path/to/python/modules"
``` |

		`export PYTHONSTARTUP="/path/to/python/startup/script.py" #Setting Python Environment Variables`
git clone	You can create a copy of a specific repository or branch within a repository.	`git clone REPOSITORY_URL [DESTINATION_DIRECTORY]`

hvac	HashiCorp Vault API client for Python 3.x. Tested against the latest release, HEAD ref, and 3 previous minor versions (counting back from the latest release) of Vault.	Examples: (for Python)
		
		`import hvac`
		`# Create a client object`
		`client = hvac.Client(url='http://localhost:8200',oken='your_vault_token')`

meta	HTML tags are used to provide additional information about a page to search engines and other clients.	Examples:
		
		`<meta name="title" content="Page Title"> #Title meta tag`
		`<meta name="description" content="Page description goes here."> #Description Meta tag` `<meta name="keywords" content="keyword1, keyword2, keyword3"> #Keywor`
		`<meta name="viewport" content="width=device-width, initial-scale=1.0"> #viewport meta tag`

pip	To make sure that requests will function, the pip program searches for the package in the Python Package Index (PyPI), resolves any dependencies, and installs everything in your current Python environment.	`pip list`
pip install	The pip install <package> command looks for the latest version of the package and installs it.	`pip install example_package`

python3	Python 3 is a widely used programming language known for its readability and versatility.	`sudo apt-get update`
		`sudo apt-get install python3`
		`python3 --version #to verify the python version`

script	This tag is used to embed a client-side script (JavaScript). The **script** element either contains scripting statements or points to an external script file through the src attribute.	Examples:
		
		Inline JavaScript Example
		
		`<script>`
		`    function function_name(name) {`
		`        alert("Hello, " + name + "!");`
		`    }`
		`    Function_name("Alice");`
		`</script>`
		
		External Script Example
		
		`<script src="myscript_name.js"></script>`

sudo apt	sudo apt-get update and sudo apt-get upgrade are two commands you can use to keep all of your packages up to date in	Syntax:
		
		`sudo apt update`
		`or`
		`sudo apt-get update`
		`or`
		`sudo apt-get update && sudo apt-get upgrade`

	Debian or a Debian-based Linux distribution.	
vault	vault-cli is a Python 3.6+ tool that offers simple interactions to manipulate secrets from HashiCorp Vault. This command shows a list of commands you can use with the tool.	Examples: (for `Bash`) ``` vault operator init #initialize vault vault login <token> #Login and authenticate vault help or vault-cli --help # command to see available options and subcommands. ```
VAULT_ADDR	Address of the Vault server expressed as a URL and port, for example, https://127.0.0.1:8200/.	Example: ``` export VAULT_ADDR=https://127.0.0.1:8200 ``` This command sets the `VAULT_ADDR` variable to the URL of your Vault server, which is typically running on port 8200 by default. Make sure to replace https://vault.example.com:8200 with the of your HashiCorp Vault server.
VAULT_TOKEN	Vault authentication token. Conceptually similar to a session token on a website, the VAULT_TOKEN environment variable holds the contents of the token.	Example: ``` export VAULT_TOKEN=my-secret-token-value ``` The `VAULT_TOKEN` environment variable holds the actual contents of the authentication token.
vault server	Starts a Vault server that responds to API requests.	Syntax: ``` vault server vault server -config=/path/to/config.hcl ``` Once the `Vault server` is running, you can access the Vault UI by opening a web browser and navigating to the appropriate address, typically http://127.0.0.1:8200, or as configured in your va file.
wget	Stands for web get. The wget is a free non-interactive file downloader command. Non-interactive means it can work in the background when the user is not logged in.	``` wget 'https://www.example.com/somefile.txt' ```