The Pipeline to Root: A Vulnerable Machine

Ariana Borlak, Devin Lewis, Charlie Roslansky
Advised by Jeff Ondich

Background

Pentesting: Breaking into systems to find their security vulnerabilities
Setting up vulnerable machines allows security researchers to simulate real-life systems to patch security holes
Privilege escalation is the technique an attacker uses to incrementally exploit bugs to increase their level of access in a system

Methods

Iterative Machines: Learned about and made demos for attacks
Set up OS: Installed an old Linux kernel on Ubuntu VM
Built a vulnerable web server: Created a website with an accessible log file that can execute PHP code
Sending emails: Used PHPMailer as a web client for an SMTP server

Parameter Pollution

Changing or duplicating existing HTTP GET or POST parameters or adding more parameters to manipulate how a server behaves.

Importance

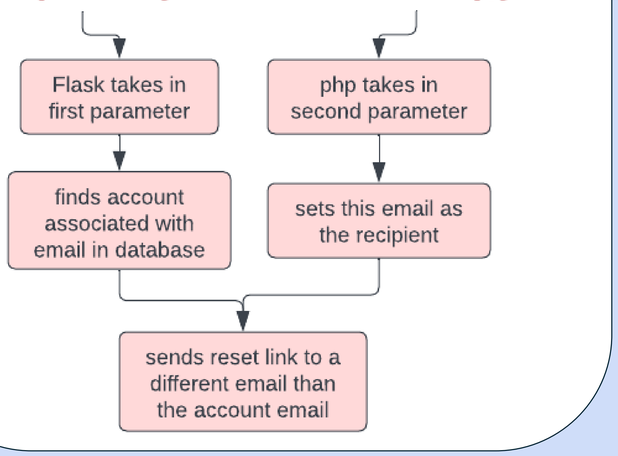
If values for duplicate parameters are conflicting, this can lead to different parts of an application using different values.

Intended HTTP parameter:

```
email=tonyaman00%40gmail.com
```

Duplicated parameters:

```
email=tonyaman00%40gmail.com&email=zereaux.day@gmail.com
```



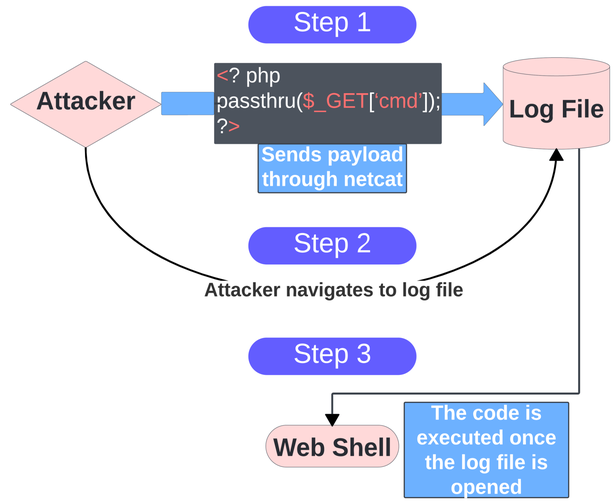
Log Poisoning

What is a Log File?

A software-generated file containing information about the operations, activities, and usage patterns of an application or server.

Importance/Vulnerability

A discoverable and unprotected log file can become subject to various malicious code injections, potentially gaining access to a web shell and dive deeper into a system.

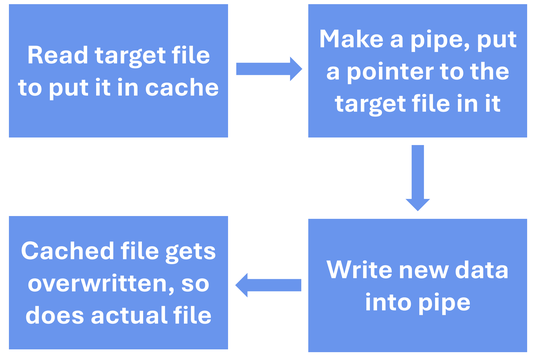


Dirty Pipe

- Linux kernel vulnerability, discovered in March, 2022
- Pipes chain commands together
  - E.g. `echo hello | wc –c`
- In some cases, the data in a pipe gets merged, meaning that changes to the cache get written back to main memory

Importance

Exploiting this vulnerability allows an attacker to write to any file they have read access to.



References