Securing Php-cURL Server-to-Server Communications

Presented By

Parthipan Natkunam

cURL Post

```php
<?php
// Data to be sent
$postData = ['key' => 'value'];
// Initialize cURL
$curl = curl_init('http://service1.example.com/api');
// Set options to POST
curl_setopt($curl, CURLOPT_POST, true);
curl_setopt($curl, CURLOPT_POSTFIELDS, $postData);
curl_setopt($curl, CURLOPT_RETURNTRANSFER, true);
// Execute and close session
$response = curl_exec($curl);
curl_close($curl);
?>
```

`CURLOPT_RETURNTRANSFER` returns the data rather than echoing it.

Prevent Infinite Redirects

- By default, cURL doesn't follow redirects.
- But in practice, we might run into situations where we may have to follow a redirect or two.
- **if you had enabled this redirect option then limit the maximum number of redirects to follow**

```
curl_setopt($curl, CURLOPT_MAXREDIRS, 3);
```

- `CURLOPT_FOLLOWLOCATION` option can be used to configure this.

MAXREDIRS Value	Implication
-1	Allow infinite redirections
0	Disable all redirections

⚠️ **Never use -1 as a value for this setting.**

Restrict Protocols

- Supports multiple protocols : FTP, LDAP, etc.
- Limit it to HTTPS and if required HTTP.

```
curl_setopt($curl, CURLOPT_PROTOCOLS, CURLPROTO_HTTP | CURLPROTO_HTTPS);
```

- Always restrict the the redirect protocols:

```
curl_setopt($curl, CURLOPT_REDIR_PROTOCOLS, CURLPROTO_HTTPS);
```

Set a Timeout

- To prevent servers from keeping the cURL session alive for longer periods than necessary,always set a reasonable time-out value to the session.

```
curl_setopt($curl, CURLOPT_TIMEOUT, 15);
```

- The value is in **seconds**.
- The above configuration will make cURL wait for 15 seconds per request before timing out.

⚠️ If a **server redirects, the timeout won’t be reset**. So in total, a server would have 15 seconds to respond with the final response, including responses from redirects if any.

Verify Certificate Domains

```
curl_setopt($curl, CURLOPT_SSL_VERIFYHOST, 2);
```

- verify that a Common Name field or a Subject Alternate Name field in the SSL peer certificate matches the provided hostname
- Always use value `2` in Prod.

⚠️ Never use the value `1` in production (this is due to certain vulnerabilities in the older versions of TLS, that were patched in later versions). **Support for value 1 removed in cURL 7.28.1.**

Verify Issuer

```
curl_setopt($curl, CURLOPT_SSL_VERIFYPEER, true);
```

- verifies if the certificate was issued by a trusted Certificate Authority (CA).
- If enabled cURL will start rejecting self-signed certificates.

Ensure the Certificate Hasn’t Been Revoked

```
curl_setopt($curl, CURLOPT_SSL_VERIFYSTATUS, true);
```

- Verify the SSL certificate status.
- If this option is set then, cURL will verify that the server attaches the Online Certificate Status Protocol (OCSP) response during the TLS handshake.

Thank You