gowthamaraj(@fuffsec) Follow
Sep 4 · 3 min read · Listen

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.

```
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  }
```

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

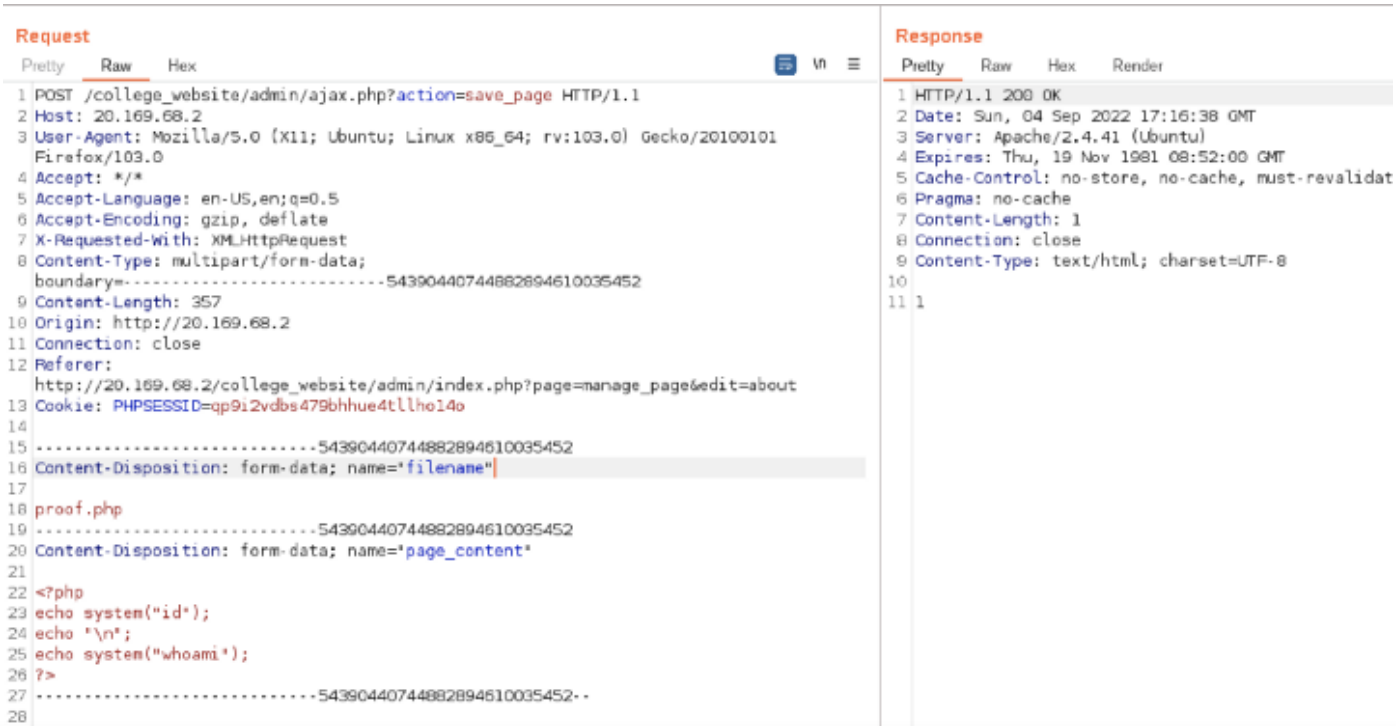
The function save_page can be called from the manage_page.php on UI.

Using the Burp to see the request and response,

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 :)



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

Exploit

Remediation

1. Authentication of requests made by the user.

2. Checking for filename when creating it.

3. Input sanitisation and validation.