New issue

Jump to bottom

There is a file upload vulnerability that can execute arbitrary code #10

Open **Aview17** opened this issue on Oct 21, 2020 · 0 comments

Aview17 commented on Oct 21, 2020

In hisiphpv2.0.11, after the administrator logs in, the installation package (.zip file) can be uploaded at the system -> local plug-in -> import plug-in

The code for uploading the logic is located in the import() function of the "app\system\admin\Plugins" class, where the zip file is extracted before being safely processed.

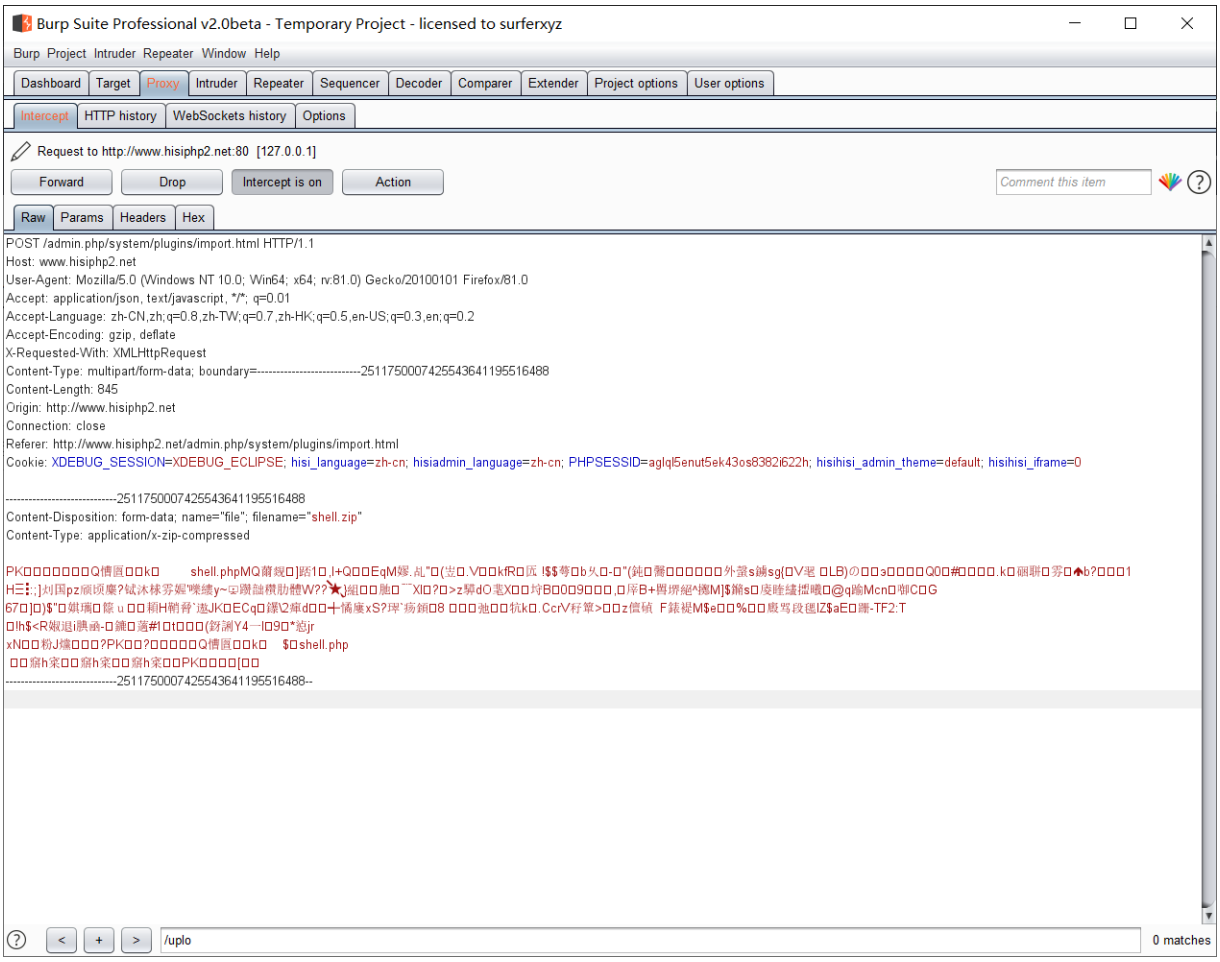
Special packets can be constructed in

```
$files = Dir::getList($decompath. '/ Upload/Plugins /');
```

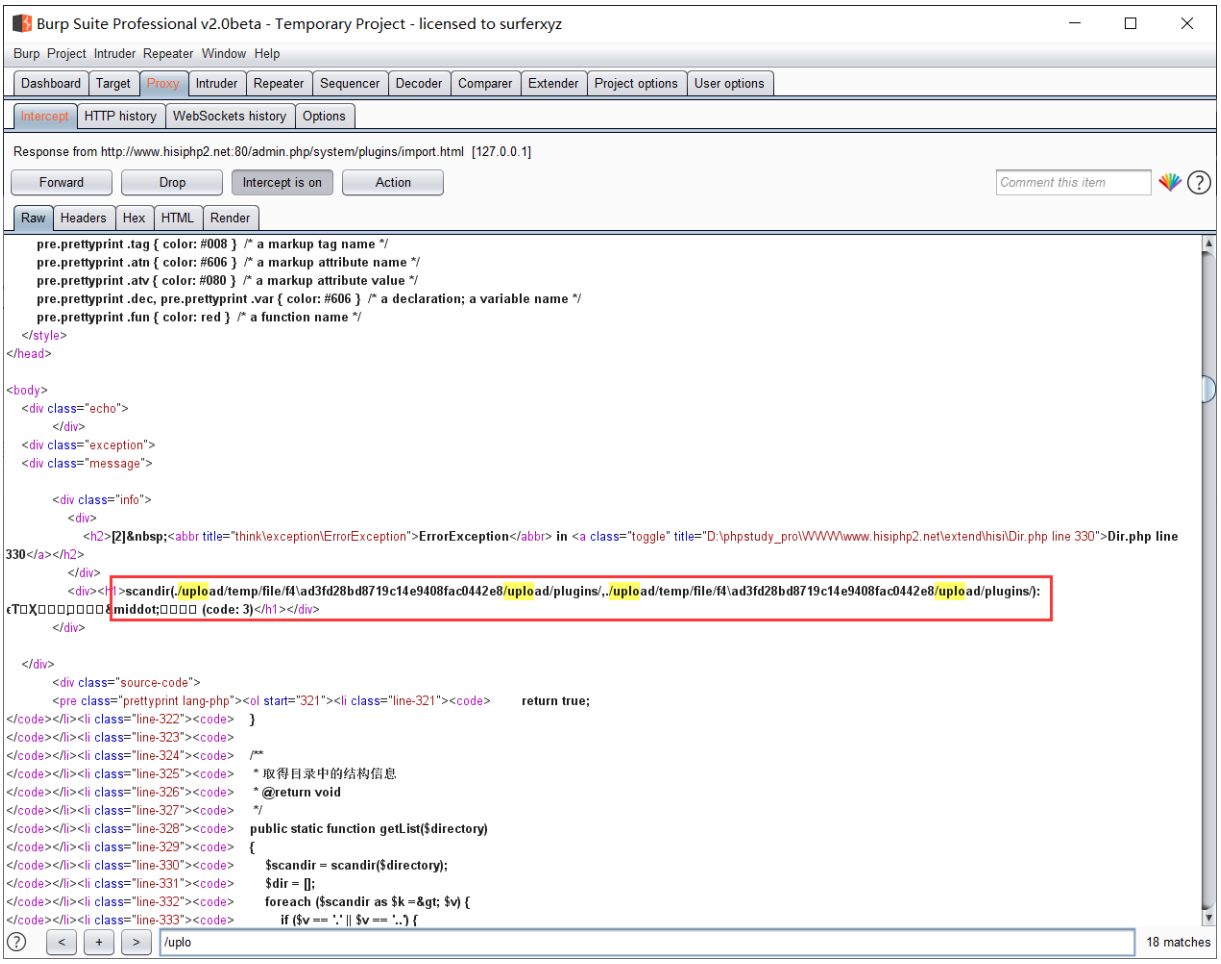
Throws an exception to bypass the security check

Package shell.php as a zip file (make sure there are no/Upload /plugins/ under the path)

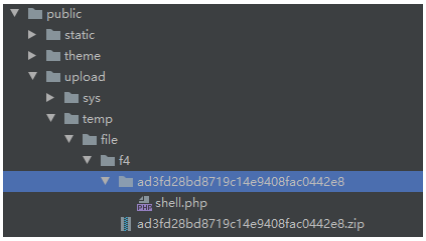
Poc as follows



The response contains the path



You can see that shell.php is uploaded



Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant