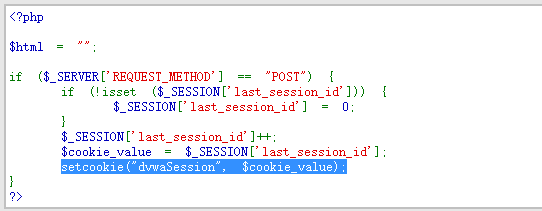
# Weak Session IDs

用户访问服务器的时候，一般服务器都会分配一个身份证 session id 给用户，用于标识。用户拿到 session id 后就会保存到 cookies 上，之后只要拿着 cookies 再访问服务器，服务器就知道你是谁了。  
但是 session id 过于简单就会容易被人伪造。根本都不需要知道用户的密码就能访问，用户服务器的内容了。

# Level:Low



根据这段源码看出每次请求都会给的session\_id加1

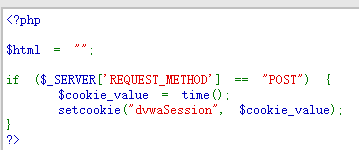


再请求几次就是



这么简单的cookie很容易会被伪造

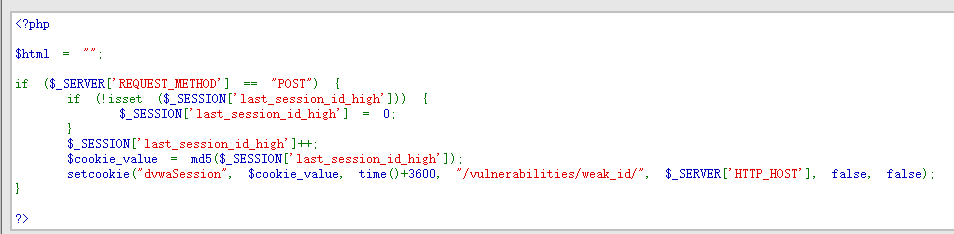
# Level:Medium



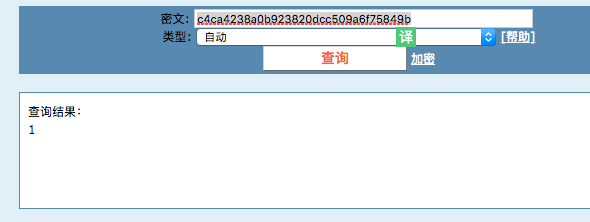
根据源码得出这次Medium等级的cookie是时间轴



# Level:High



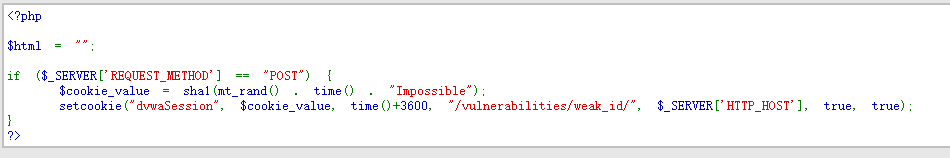
查看源码发现这个是用MD5加密的

再点一次



跟low等级是一样的点一次就加1

# Level:Impossible



Impossible级别的源码意思是

Cookie会随机生成数+时间+固定值“Impossible”并且一起用sha1加密