SQL注入漏洞

base on pikachu 

SQL Inject漏洞的防范

SQL Inject注入漏洞的防范

- 代码层面

1. 对输入进行严格的转义和过滤
2. 使用预处理和参数化（Parameterized ）

- 网路层面

1. 通过WAF设备启用防SQL Inject注入策略（或类似防护系统）
2. 云端防护（360网站卫士，阿里云盾等）

SQL Inject注入漏洞的防范-PHP防范转义+过滤

转义举例：

```
function escape($link,$data){
    if(is_string($data)){
        return mysqli_real_escape_string($link,$data);
    }
    if(is_array($data)){
        foreach ($data as $key=>$val){
            $data[$key]=escape($link,$val);
        }
    }
    return $data;
}
```

过滤举例：（黑名单）

str_replace("%","",$_POST['username']),把post里面的数据里面含有%的替换成空

SQL Inject注入漏洞的防范-PHP防范案例-PDO预处理（推荐）

推荐的做法：使用PDO的prepare预处理（预处理+参数化）

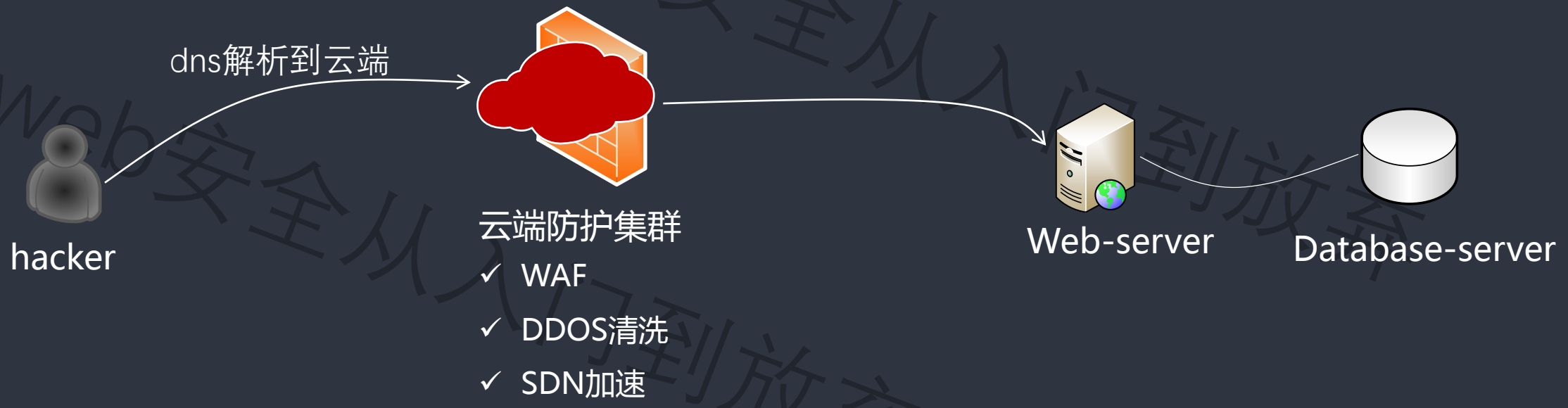
```
$username=$_GET['username'];
$password=$_GET['password'];

try{
    $pdo=new PDO('mysql:host=localhost;dbname=ant', 'root', 'root');
    $sql="select * from admin where username=? and passowrd=?";
    $stmt=$pdo->prepare($sql);//先不传参数，先预处理
    //    var_dump($stmt);
    $stmt->execute(array($username,$password));
    //这个时候在把参数传进去，以索引数组的方式传进去，而不是拼接，就成功防止了注入

}catch (PDOException $e){
    echo $e->getMessage();
}

?>
```

SQL Inject注入漏洞的防范-网络防护

在web应用服务器前部署WAF设备：topo

SQL Inject注入漏洞的防范-PHP防范案例

启用云端防护



谢 谢

“听”而不思则罔，思而不“练”则殆