

java代码审计 深度解析



第一课 sql注入原理

SQL注入

http://xxx/aa.jsp?id=1

```
HttpServletRequest request, HttpServletResponse response) {  
    JdbcConnection conn = new JdbcConnection();  
    final String sql = "select * from product where pname like '%"  
        + request.getParameter("id") + "%'";  
    conn.execqueryResultSet(sql);
```

```
    final String sql = "select * from product where pname like '%1' or '='='%'";
```



SQL注入

http://xxx/1022.html

```
String id = url.Substring(url.length-9,4);  
final String sql = "select * from product where id =" + id;  
conn.execqueryResultSet(sql);
```



SQL注入

The image shows a web application login page on the left and its corresponding HTTP request in a proxy tool on the right. The login page has a title "用户登录 LOGIN" and two input fields: "用户名: admin" and "密码: *****". Below the fields are "登录" and "返回" buttons. The proxy tool shows a request to "http://localhost:8080 [127.0.0.1]". The request details include: "POST /lcmsnewfujian/login/login4.action HTTP/1.1", "Host: localhost:8080", "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0", "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", "Referer: http://localhost:8080/lcmsnewfujian/jsp/login/NewLogin4.jsp", "Cookie: JSESSIONID=E9277EE04F4760863D659417CADA0500; Pycharm-a78b22bc=1f28a72c-29b1-4a91-ab73-d33de7a62882; PJBlog3Setting=ViewType=normal", "Connection: close", "Upgrade-Insecure-Requests: 1", "Content-Type: application/x-www-form-urlencoded", and "Content-Length: 29". The request body is highlighted as "username=admin&password=11111".

Request to http://localhost:8080 [127.0.0.1]

Forward Drop Intercept is on Action Comment this

Raw Params Headers Hex

POST /lcmsnewfujian/login/login4.action HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0
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
Referer: http://localhost:8080/lcmsnewfujian/jsp/login/NewLogin4.jsp
Cookie: JSESSIONID=E9277EE04F4760863D659417CADA0500; Pycharm-a78b22bc=1f28a72c-29b1-4a91-ab73-d33de7a62882; PJBlog3Setting=ViewType=normal
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 29

username=admin&password=11111



SQL注入

post型sql注入(post内参数)

username、password传入sql语句进行执行

```
String sql = "select * from usertable where  
name= '' +username+' ' and password= '' +password+ '' "
```



SQL注入

获取header中参数引起的sql注入

username、 cookie、 X-Forward-For等

```
String referer = request.getHeader( "referer" );
```

```
String sql = "update TABLE set referer= '" + referer + "' ";
```



SQL注入-JDBC

```
String sql = "select * from product where pname like '%"
            + request.getParameter( "name") + "%' " ;
```

```
String sql = "select * from product where pname like '%"
            + name + "%' " ;
```



SQL注入-Mybatis

```
<select>  
  select * from table where name like '%$value$%'  
</select>
```

```
Select * from news where id in (${id})
```

```
Select * from news where title = '新年' order by ${time} asc ,
```



SQL注入-Hibernate

```
String hql ="SELECT warehousename FROM Twarehouseinformation  
wh WHERE wh.teuint.unitguid = '"+GUID+ "' " ;  
Query query=session.createQuery(sql);
```



The image features a central figure of a person wearing a black hoodie, with their right hand pressed against their forehead in a gesture of stress or contemplation. The background is a vibrant blue digital landscape. On the right side, a glowing globe is partially visible, surrounded by intricate network lines and nodes. The entire scene is overlaid with a pattern of hexagons and small blue dots, some of which are accompanied by padlock icons, suggesting themes of cybersecurity or digital privacy. A semi-transparent horizontal band across the middle contains the text.

谢谢观赏