

开发相关的网络攻击

应对原则

- 程序自身逻辑问题
- 未经验证的客户端数据
 - 不要相信任何客户端传递的参数
 - HTTP Header中的信息不可信
 - 请求也可能并非才是真正的用户请求

参数被篡改的例子(URL)

<http://www.mydomain.com/orderdetail?id=23>

<http://www.mydomain.com/orderdetail?id=d296ae21-c5fe-11e8-acf2-10ddb1d4e7ac>

参数被篡改的例子(form)

服务员分成:

商户分成: 20%

保存

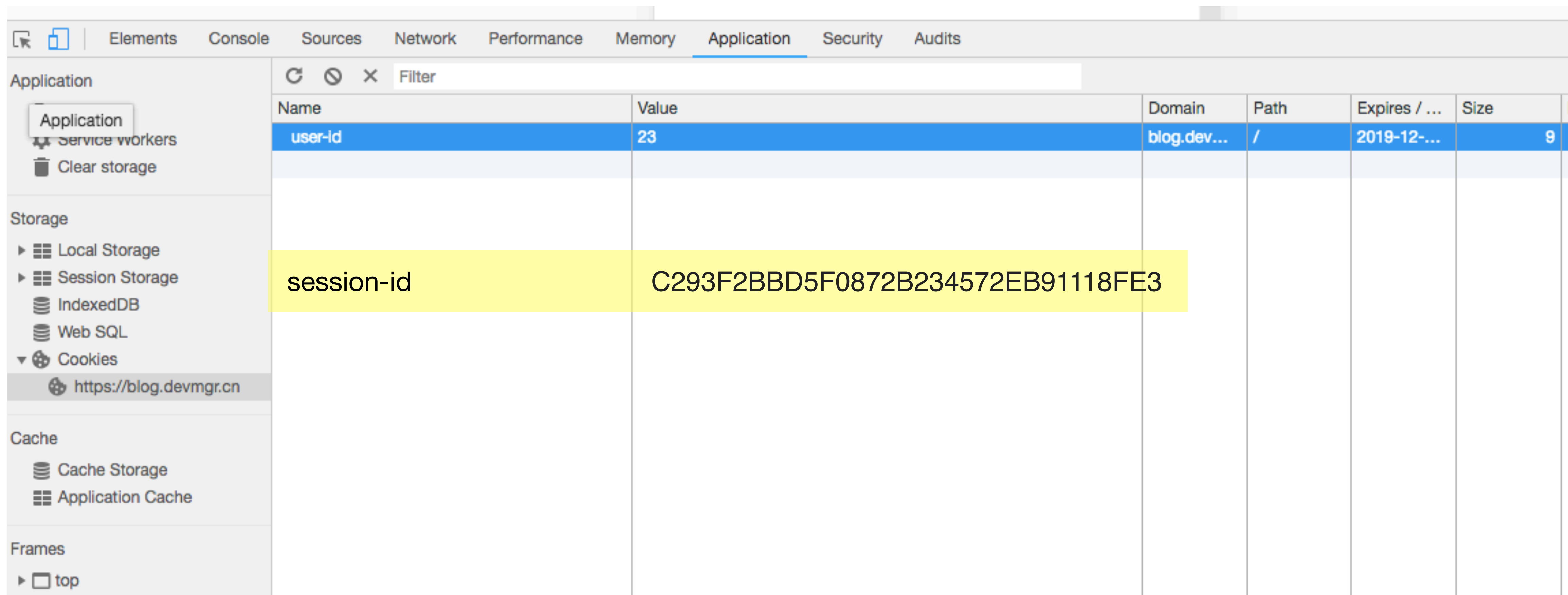
后端处理:

```
fuwuyuan = request.getParameter("fuwuyuanfencheng") / 100.0;  
shanghu = 1 - fuwuyuan;
```

```
request.getParameter("fuwuyuanfencheng") = 100000  
fuwuyuan = 1000  
shanghu = -999
```



参数被篡改的例子 (cookie)



The screenshot shows the Chrome DevTools Application tab. The left sidebar contains sections for Application, Storage, Cache, and Frames. The 'Cookies' section under 'Storage' is expanded, showing a list of cookies for the domain 'https://blog.devmmgr.cn'. The main table displays the following data:

Name	Value	Domain	Path	Expires / ...	Size
user-id	23	blog.dev...	/	2019-12-...	9
session-id	C293F2BBD5F0872B234572EB91118FE3				

RequestHeader不可信

- `request.getRemoteAddr()` `22.22.22.22`
- `request.getHeader("X-Forward-For")` `11.11.11.11, 22.22.22.22`

JSON->Object自动转换

Controller:

```
@PostMapping
```

```
public Order insertOne(@RequestBody Order order) {  
    // ..其他处理..
```

```
    if( order.getAmount() > 100 && 满百减十的活动 ) {  
        order.setDiscount(99);  
    }
```

```
    // ..保存...
```

```
    return order;
```

```
}
```

POJO:

```
public class Order{  
    private double discount = 0;  
    private Address address;  
    private String phone;  
    private List<OrderItem> items;  
    //....其他属性 ...
```

```
}
```

前端传输的数据:

```
{  
    "address": {  
        "province": "江苏省",  
        "city": "南京市"  
    },  
    "phone": "13500001111",  
    "items": [  
        {  
            "inventoryid": "a001",  
            "num": 2  
        },  
        {  
            "inventoryid": "b002",  
            "num": 1  
        }  
    ],  
    "discount": 100  
}
```

请求不一定可信

手机号

输入4位短信验证码

获取短信验证码

`http://xx.xx/yanzhengma?phone=13xxxx75&code=2363`

`json: {code: 2363, correct: true}`

135[REDACTED]675

2363



获取短信验证码

穷举验证码:

```
for (i=0; i<10000; i++){  
    result = HTTP.get('http://xx.xx/  
    yanzhengma?code=' + i);  
    if(result.correct){  
        alert('验证码是: ' + i);  
        break;  
    }  
}
```


- 参数要验证，校验范围
- 浏览器端JavaScript对数据的检测只起到提升用户体验的作用，后端一定要再校验
- cookie里存储的内容可能会被更改，也可能会泄露