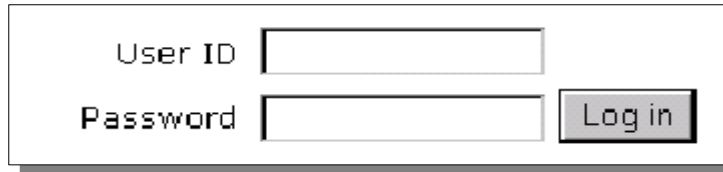


# Unvalidated Input

```
http://www.things.com/order/final&custID  
=101&part=555A&qy=20&price=10&ship=boat  
&shipcost=5&total=205
```

```
http://www.things.com/order/final&custID  
=101&part=555A&qy=20&price=10&ship=boat  
&shipcost=5&total=25
```

# SQL Injection



User ID

Password

```
"SELECT * FROM users WHERE username = ' " +  
  username + "' AND password = ' " + password + "' "
```

*Username: ' OR 1=1--*

```
SELECT * FROM users WHERE username = ' ' OR 1=1--
```

# Buffer Overflow

E.g. In unchecked loops:

```
for (i=0; i<daysWorkedThisMonth; i++)  
    hours[i] = hoursWorkedThatDay();
```

*Q) What is the worst case scenario for this program if the programmer did not check the size of daysWorkedThisMonth?*

In unchecked buffers:

H	e	l	l	o		W	o	r	l	d	\0
---	---	---	---	---	--	---	---	---	---	---	----

H	e	l	l	o		W	o	r	l	d		N	a	s	t	y		s	t	u	f	f		i	n		m	e	m	o	r	y	!	.	.	.
---	---	---	---	---	--	---	---	---	---	---	--	---	---	---	---	---	--	---	---	---	---	---	--	---	---	--	---	---	---	---	---	---	---	---	---	---