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 = 'qwertz'`	`42`
5	`admin'--`	`<anything>`	`SELECT id FROM users WHERE name = 'admin'`	`1`
6	`' OR 1=1--`	`<anything>`	`SELECT id FROM users`	`1`, `2`, …

Exercise 8.2 (ArrayList Deserialization)

```java
/**
 * 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 8.3 (HashSet Deserialization)

```
[illegible]
```

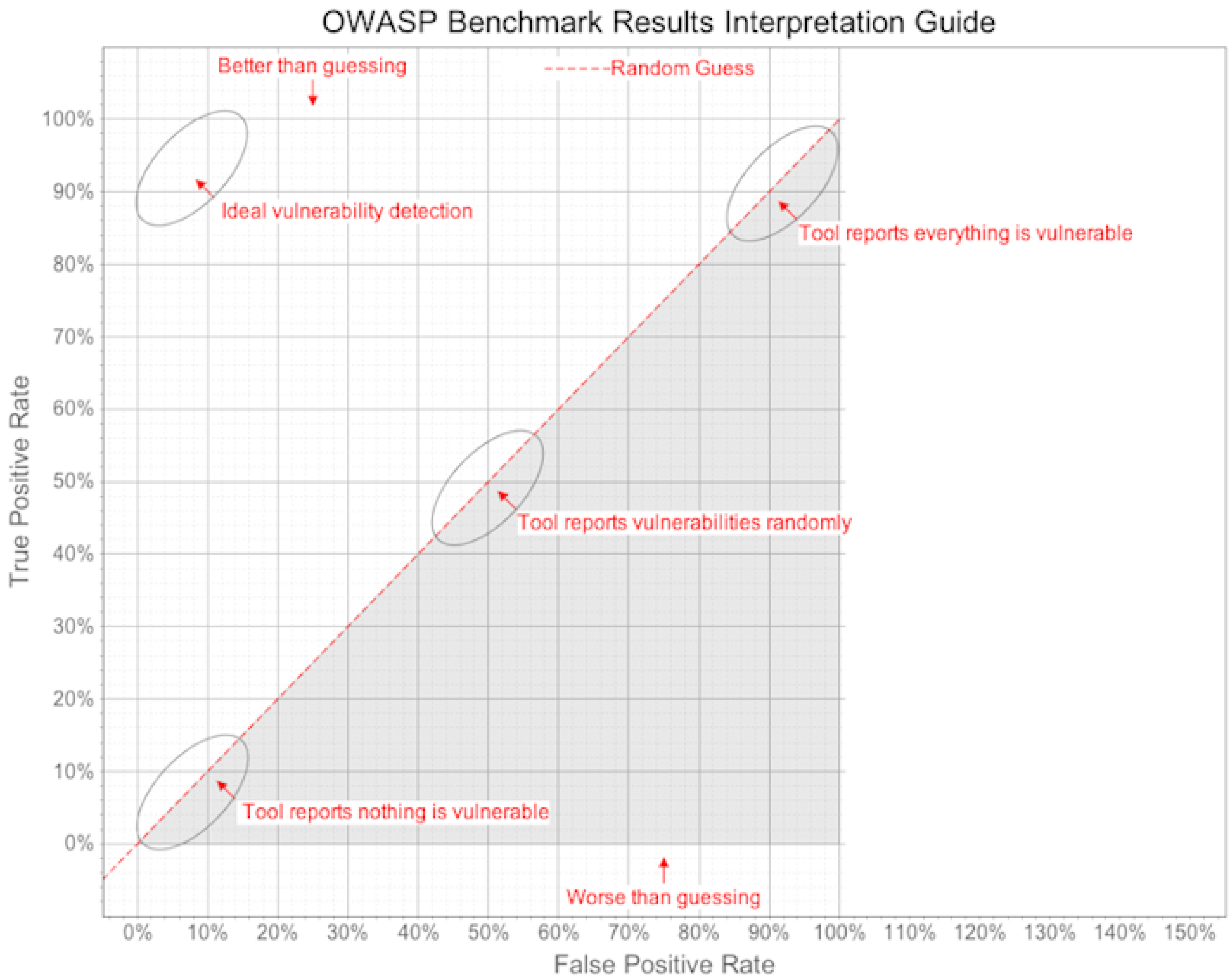
💥 *With its members recursively linked to each other, when deserializing `root`, the JVM will begin creating a recursive object graph. It will never complete, and consume CPU indefinitely.*

🔍 *If you view this as a PDF, zoom in as much as possible on the above code snippet to get an idea what is going on. You might want to look at the original Markdown file to actually be able to read something.*

Exercise 9.1 (Protection Req. Calc.)

Aspect / Application	Website	VCS	Webshop	B2B API
Business criticality	2 🔶	1 💛	5 🔴	2 🔶
Information classification	0 💚	2 🔶	2 🔶	2 🔶
Compliance requirements	0 💚	0 💚	2 🔶	1 💛
Exposure to threats	5 🔴	1 💛	5 🔴	5 🔴
Authentication mechanism	0 🔵	-2 💛	-1 🔶	-1 🔶
Total Score	7 🔶	2 💚	13 🔴	9 🔶
Rating	Medium	Low	High	Medium

Exercise 9.2 (OWASP Benchmark)


OWASP Benchmark Results Interpretation Guide
Better than guessing
------Random Guess
Ideal vulnerability detection
Tool reports everything is vulnerable
Tool reports vulnerabilities randomly
Tool reports nothing is vulnerable
Worse than guessing
True Positive Rate
False Positive Rate