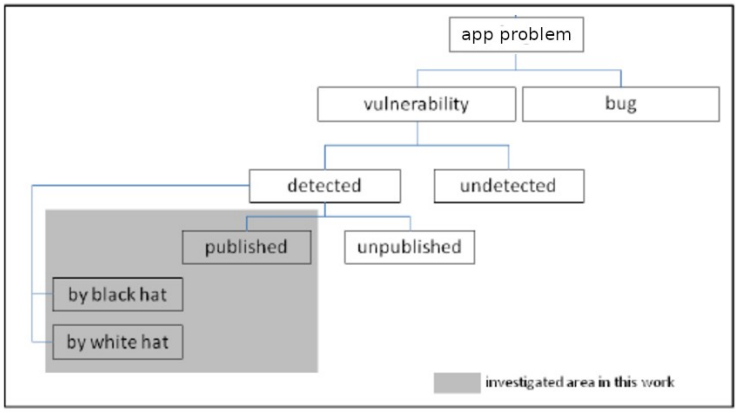
Bug vs. Vulnerability

Her bug zafiyet demek değildir.
Her zafiyet bug demek değildir.

Her bug bir zafiyet değildir. Bir bug programda bir hata olarak kalabilir ama zafiyet sunan bir yanı olmayabilir. Her zafiyet de bir bug değildir. Bir zafiyet programda bir güvenlik problemi doğurur, fakat programın çalışması noktasında hata sunan bir yanı olmayabilir. Dolayısıyla programda bug bulmak her zaman zafiyet bulmak anlamına gelemeyeceği gibi programda zafiyet bulmak da her zaman programda bug bulduk anlamına gelemeyebilir. Sonuç olarak yazılımcılar bug'sız program yaparak yazılımlarının güvenli olduğu kanısına varmamalıdır. Bug'sız bir program güvenli programdır şeklinde bir önerme yanlıştır.

> **Bug** (arıza), kullanıcının uygulamayı sunduğu özellikler doğrultusunda çeşitli kusurları nedeniyle kullanamamasına / faydalanamamasına yol açar.
>
> **Güvenlik zafiyeti** (açıklık), kullanıcının ve/veya sunucunun uygulamayı sunduğu özellikler doğrultusunda normal manada kullanabilmesi veya kullanamaması fark etmeksizin zararlı aktivitelerde bulunanların amaçlarına ulaşabilmesine yol açar.

Aşağıda uygulamada var olabilecek problem şeması (diyagramı) verilmiştir:



Aşağıda ise uygulamada bug ve/veya açıklık olup olmamasına göre var olan 4 olasılık ve örneklemeleri verilmiştir.

Olasılıklar:

> "*Bug teşkil etmez, ama güvenlik zafiyeti teşkil eder*",
> "*Bug teşkil eder, ama güvenlik zafiyeti teşkil etmez*",
> "*Bug teşkil eder, aynı zamanda güvenlik zafiyeti teşkil eder*",
> "*Bug teşkil etmez, aynı zamanda güvenlik zafiyeti teşkil etmez*".

Örnekler:

xss // Bug teşkil **etmez**. Ama güvenlik zafiyeti **doğurur**.

> - Web uygulamasındaki xss zafiyetinin varlığı arıza teşkil etmez ve uygulamanın çalışma dinamiğini bozmaz. Bir bug (yanlış / hatalı / bozuk kodlama) değildir. Ama bu güvenlik

zafiyeti istismar edildiğinde her güvenlik zafiyeti istismar edildiğinde olduğu gibi uygulama ve/veya kullanıcı zarar görür.

file inclusion // Bug teşkil **etmez**. Ama güvenlik zafiyeti **doğurur**.

- Web uygulamasındaki file inclusion zafiyetinin varlığı arıza teşkil etmez ve uygulamanın çalışma dinamiğini bozmaz. Bir bug (yanlış / hatalı / bozuk kodlama) değildir. Ama bu güvenlik zafiyeti istismar edildiğinde her güvenlik zafiyeti istismar edildiğinde olduğu gibi uygulama ve/veya kullanıcı zarar görür.

file upload // Bug teşkil **etmez**. Ama güvenlik zafiyeti **doğurur**.

- Web uygulamasındaki file upload zafiyetinin varlığı arıza teşkil etmez ve uygulamanın çalışma dinamiğini bozmaz. Bir bug (yanlış / hatalı / bozuk kodlama) değildir. Ama bu güvenlik zafiyeti istismar edildiğinde her güvenlik zafiyeti istismar edildiğinde olduğu gibi uygulama ve/veya kullanıcı zarar görür.

command execution // Bug teşkil **etmez**. Ama güvenlik zafiyeti **doğurur**.

- Web uygulamasındaki command execution zafiyetinin varlığı arıza teşkil etmez ve uygulamanın çalışma dinamiğini bozmaz. Bir bug (yanlış / hatalı / bozuk kodlama) değildir. Ama bu güvenlik zafiyeti istismar edildiğinde her güvenlik zafiyeti istismar edildiğinde olduğu gibi uygulama ve/veya kullanıcı zarar görür.

sqli // Bug teşkil **etmez**. Ama güvenlik zafiyeti **doğurur**.

- Web uygulamasındaki xss zafiyetinin varlığı arıza teşkil etmez ve uygulamanın çalışma dinamiğini bozmaz. Bir bug (yanlış / hatalı / bozuk kodlama) değildir. Ama bu güvenlik zafiyeti istismar edildiğinde her güvenlik zafiyeti istismar edildiğinde olduğu gibi uygulama ve/veya kullanıcı zarar görür.

slow http attacks // Bug teşkil **etmez**. Ama güvenlik zafiyeti **doğurur**.

- Apache web sunucu yazılımının paralel programlama metoduyla olan programlaması dolayısıyla (paralel programlama kodlamasının zorluğu (karmaşıklığı) nedeniyle) yaşanan teknik zorluklar sonucunda çok kullanıcıya aynı anda sunduğu hizmetteki thread yönetimi servisi çözümlenemeyen bir açığa sahiptir. Bu apache sunucularda dünden bugüne devam eden kronik bir açıklıktır. Bu zafiyet uygulama ve sunduğu hizmetlerin normal kullanımda işleyişini etkilememektedir. Dolayısıyla bir arıza (//bug) değildir. Fakat suistimal edildiğinde apache sunucunun cevap veremez hale gelmesine ve servis dışı kalmasına neden olur.

ms08-067 netapi // Bug teşkil **etmez**. Ama güvenlik zafiyeti **doğurur**.

- Windows sistemlerde yerel ağ içerisinde dosya paylaşımını sağlayan sistem kütüphanesi (.dll) içerisindeki dizin yolu genelleştirme kodunda yer alan parsing metodu normal işleyişte sorun teşkil etmediğinden bug değildir, fakat suistimal edildiğinde üzerinden zararlı aktiviteler yapılabildiğinden bir güvenlik açığıdır.

Improper Usage of + Operator in Java // Bug teşkil **eder**. Ama güvenlik zafiyeti **doğurmaz**.

- Genellikle her programlama dilinde syntax gereği yapılan / yapılabilen yaygın kodlama hataları (bug'ları) mevcuttur. Örneğin Java dilinde yapılan yaygın hatalardan biri + operatörünün java'da iki amaç için kullanılabiliyor olmasında yatar. Birisi matematiksel açıdan, diğeri concatenation (birleştirme) açısından kullanıldığından kullanımı karıştırılabilmektedir. Örneğin 5 değerini tutan y değişkeni ile 2 değerini matematiksel olarak toplayıp ekrana basmak istersek aşağıdaki kullanım hatalı bir kullanım olur,

```
Java:

y=5;

System.out.println("y + 2 = " + y + 2);                    // y + 2 = 52
```

ve milyonlarca satırlık yazılım içerisinde bir bug olarak yer ederek yazılımın hatalı çalışmasına neden olabilir. Matematiksel olarak kullanılacaksa şöyle kullanılması gerekecekti:

```
Java: (doğrusu)

y = 5;

System.out.println("y + 2 = " + (y + 2));                  // y + 2 = 7
```

[Custom Errors / Nonstandard Errors]

Hatalı / Yanlış Girdi Kuralı // Bug teşkil **eder**. Ama güvenlik zafiyeti **doğurmaz**.

- Örneğin; eposta textbox'ına konulan karakter seti kuralı dolayısıyla @ sembolünün koyulamaması

Hatalı / Eksik Kodlama // Bug teşkil **eder**. Ama güvenlik zafiyeti **doğurmaz**.

- "Yazı Sil" butonuna basılmasına rağmen uygulamanın istenilen tepkiyi vermemesi

Thread Safety Bugs (e.g. Concurrency Flaw in Shopping Cart) // Bug teşkil **eder**. Aynı zamanda
// güvenlik zafiyeti **doğurur**.

- Alışveriş sitesindeki thread safety bug'ı dolayısıyla eşzamanlılığın iyi çalışmaması durumunda doğabilecek müşterilerin aldığı ürünlerin farklı farklı fiyatlarda faturalandırılması (örn; çok daha pahalıya alınması) veya bug'ın varlığını fark eden kötü niyetli kişilerce vurgun yapmak bağlamında eşzamanlılık problemini exploit ederek bir çok müşteri profilinden düzinelerce ürünü çok ucuza kasıtlı olarak almak. Sonuç olarak thread safety iyi kodlanmadığı takdirde bir bug'tır, çünkü uygulama işleyişini bozmaktadır. Mağduriyetler doğurabilmektedir. Fakat aynı zamanda kötü niyetli kişilerce istismar edildiğinde bir güvenlik zafiyeti teşkil eder. Çünkü uygulama işletmecisinin kasasındaki parası gider.

NULL // Bug teşkil **etmez**. Güvenlik zafiyeti teşkil **etmez**.

- NULL. Yani ne bug ne de zafiyet var demektir. Yani uygulama kusursuzdur.

Yararlanılan Kaynaklar

Benim Not

Java How to Program, pg. 241

https://medium.com/bugbountywriteup/security-bugs-are-fundamentally-different-than-quality-bugs-9eb8f8663089

https://hacks.mozilla.org/2019/02/fearless-security-thread-safety/

http://www.includekarabuk.com/kategoriler/webgoatuygulamasi/Ders-28---Concurrency-%3E-Shopping-Cart-Concurrency-Flaw.php

https://www.researchgate.net/figure/Classification-of-software-bugs-and-vulnerabilities_fig1_220891308