TURKISH TECHNOLOGY

Server-side template injection - SSTI

Server-side Template Injection nedir?

- **Server-side template injection,** sunucu tarafında çalış
  template syntax'a zararlı payload eklendiğinde oluşur. Diğer inj
  saldırılarında olduğu gibi kullanıcı girdisi veri olarak geçil
  doğrudan template'e eklendiğinde meydana gel

  Saldırganın istenilen template direktifini template engine'e verm
  olanak sağlayarak sunucunun tamamen kontrolünün
  geçirilmesine olanak sağlar. Genellikle RCE ile sonuçlanır faka
  olmasa da sunucudan hassas veri okunmasına ve sunuc
  istenilen dosyanın okunmasına sebep olur

Server-side Template Injection

```
$output = $twig->render("Dear {first_name},", array("first_name" => $user.
```

```
$output = $twig->render("Dear " . $_GET['name']);
```

```
http://vulnerable-website.com/?name={{bad-stuff-here}}
```

Plaintext context

```
render('Hello ' + username)
```

```
http://vulnerable-website.com/?username=${7*7}
```

```
Hello 49
```

Code context

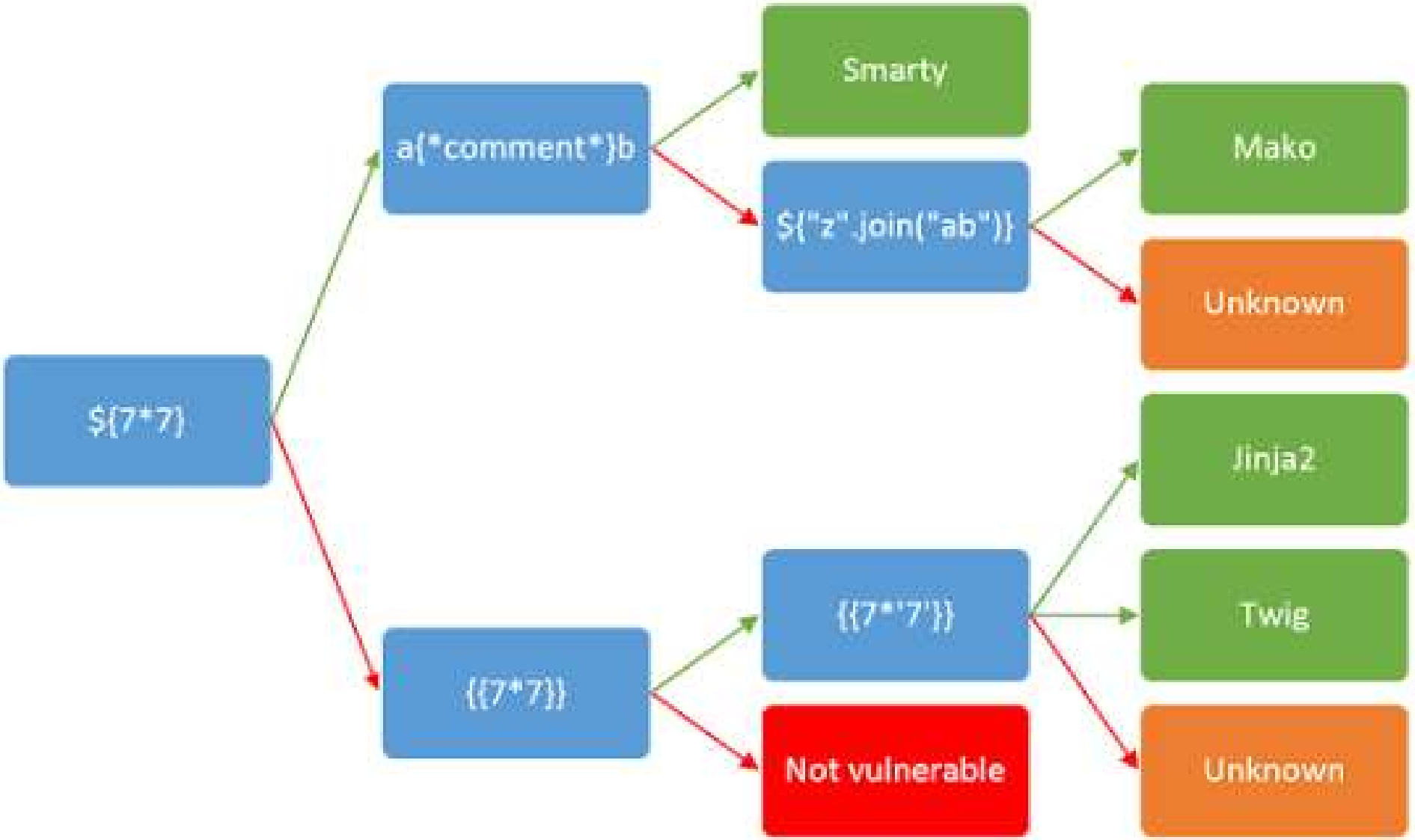
```
greeting = getQueryParameter('greeting')
engine.render("Hello {{"+greeting+"}}", data)
```

```
http://vulnerable-website.com/?greeting=data.username}}<tag>
```

```
Hello Carlos<tag>
```

Server-side Template Injection

Identify



LABS

Server-side Template Injection

https://portswigger.net/web-security/all-labs#server-side-te

Server-side Template Injection Önleme

- Kullanıcıların templateleri düzenlemesine ve yeni eklemesine izin verilmemelidir.
- **Mustache** gibi «logic-less» template engine kullanılmalıdır.
- Sandbox ortamlarda kullanıcıdan gelen code'lar çalıştırılıp potansiyel za modül ve fonksiyonlar silinmelidir. (Bypass edilmeye açık.)