### 1.1.1 Frame'lenebilir Login Sayfası (Frameable Login Page) (CWE-829)

**Açıklık Önem Derecesi:** Düşük

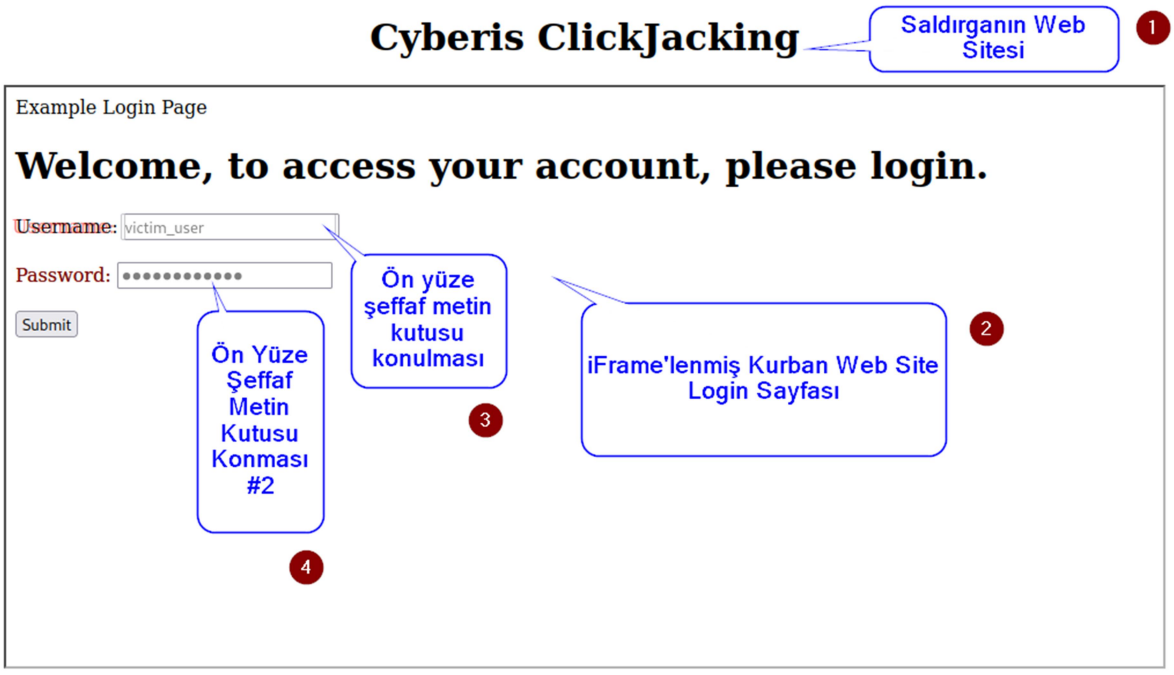
**Açıklığın Etkisi:** Bilgi İfşası

**Açıklığın Barındıran Dosyalar/Satırlar:**

| Proje Dosyası/Dosya Adı | Satır Numarası |
|---|---|
| | |
| | |

**Açıklığın Açıklaması:**

Kurum (meşru) web sitesinin login sayfası koruma bulunmamaktaysa iframe ile saldırgan web sitelerine yerleştirilebilir. Saldırgana ait web sitede iframe ile sergilenen meşru web sitenin login sayfası üzerine saldırgan yarı opak / şeffaf kullanıcı adı, parola <input metin kutuları ve buton yerleştirebilir. Örn;




Böylece kurban kişi meşru web sitesi login ekranını gördüğünde "oturum açtığımda varmaya çalıştığım içeriğe ulaşabileceğim" zannına kapılarak login denemesi yapabilir. Bu durumda saldırgan kontrollü web siteye bilgilerini kaptırmış olacaktır. Saldırgan bilgiler girildikten sonra kurbanın şüphesini çekmemesi için kurum (meşru) web sitesine yönlendirme ilaveten yapabilir.

Login web sayfalar iframe ile farklı web sitelerde sergilenebiliyorsa buna Frame'lenebilir Login Sayfası (CWE-829) açıklığı adı verilir. Kurum web uygulamada Frame'lenebilir Login Sayfası (CWE-829) açıklığı tespit edilmiştir.

[[[[[[[[[[[[[[ BULGU ]]]]]]]]]]]]]]

**Açıklığın Önlemi:**

Açıklığın giderilmesi için tavsiyeler şu şekildedir:

- Uygulamanın MVC mimarisindeki Controller katmanında ilgili (login view'ını return ile döndüren) metot (fonksiyon) içerisinde X-Frame-Options (XFO) önlemi Java projelerde şu satır eklenerek uygulanabilir.

```
response.addHeader("X-Frame-Options", "DENY")
```

- XFO önlemi yanında CSP (Content-Security-Policy) önlemi de ilave edilmelidir.

**Referanslar:**


1. https://portswigger.net/kb/issues/005009a0_frameable-response-potential-clickjacking
2. http://cwe.mitre.org/data/definitions/829.html
3. https://www.cyberis.com/article/five-minute-fix-frameable-responses-clickjacking
4. https://ehteshamulhaq198.medium.com/clickjacking-to-obtain-login-credentials-abee3ae9825e