Email Address Disclosure

a. Email Adres İfşası Nedir ve Neye Sebep Olur?

Web uygulamalarında eposta adreslerine yer verilmesine eposta ifşası adı verilir. Web uygulamaları içerisinde yer alan eposta adreslerinin varlığı bir güvenlik zafiyeti doğurur demek tam doğru olmasa da bir miktar doğruluk payına sahiptir. Saldırganlar web uygulamalarındaki eposta adreslerini otomatik eposta yakalayıcısı araçlar kullanarak elde edebilirler. Buradan hareketle bu adreslere yoğun bir spam yağmuru saldırısı yapabilirler (böylece epostanıza hergün / her saat yüzlerce / binlerce istenmeyen eposta gelebilir ve belki sunucunuzun kapasitesi zorlanabilir), aldatıcı epostalar gönderebilirler ve bu sayede kritik bilgileri almaya dönük sosyal mühendislik saldırıları yapılabilirler veya eposta adreslerinin şifresini kırmak için brute force saldırısı yapma imkanı elde edebilirler. Eğer web uygulaması içerisinde yer alan eposta adresleri "kişisel" eposta adresleri ise saldırganlar bu eposta adreslerinin üzerinde yer alan isim-soyisim, doğum tarihi, kullanıcı adı gibi bilgilerden yola çıkarak başka saldırı vektörleri elde edebilirler.

b. Email Adres İfşası Nasıl Kapatılır?

Normalde web uygulama içerisinde eposta adresi verilmesi olmazsa olmaz olabilir. Bu durumda saldırganlara karşı bir caydırıcılık olması amacıyla eposta adreslerine aşağıdaki önlemler uygulanmalıdır.

deneme[at]kurumadi.com
deneme[at]kurumadi[nokta]com
deneme(at)kurumadi.com
deneme(at)kurumadi(nokta)com
...

Bu önlemler ile birçok eposta yakalayıcı araç eposta adreslerini yakalayamayacağından geriye manuel tarama seçeneği kalacaktır ve saldırganların işi biraz daha güçleşecektir. Bu ise saldırıların önemli ölçüde azalmasıyla sonuçlanacaktır. Ancak bazı eposta yakalayıcı araçlar regexp desteğine de sahip olduklarından yukarıdaki önlemler uygulansa bile epostaların otomatize bir şekilde yakalanması halen mümkündür. Bu nedenle güvenliği bir kademe daha yükseltmek için @ sembolünün eposta adresi üzerinde resim olarak yerleştirilmesi önerilmektedir. Bu yöntem ile bütün eposta yakalayıcı araçları atlatabilirsiniz. Sonuç olarak spam, sosyal mühendislik ve brute force saldırılarını böylece minimize edebilirsiniz.

Güvenliği bir kademe daha arttırmak isterseniz uygulama içerisinde "kişisel" eposta adresleri yerine "genel" eposta adresleri (örn; destek@example.com, iletisim@example.com, support@example.com, contact@example.com, info@example.com,...) kullanmanız önerilmektedir. Bu sayede minimum bilgi paylaşımında bulunulmuş olacaktır ve sosyal mühendislik & brute force saldırıları daha da minimize edilmiş olacaktır.

Not:

Eğer eposta sunucunuz spam postalarına karşı koruma mekanizmasına sahip değilse eposta adreslerinizi web sayfalarınızda teşhir etmeniz epostanıza spam yağmuru olarak dönebilir. Bu nedenle spam saldırılarından korunmak için eposta adreslerinizi teşhir etmek yerine uygulamanıza captcha'si olan bir iletişim formu ekleyebilirsiniz. Bu sayede eposta yakalayıcı araçlar hedef web uygulamasında hiçbir eposta adresi yakalayamayacaklarından spam epostası gönderemeyecektirler ve iletişim formundaki captcha sayesinde de iletişim formunu flood'a tabi tutulamayacaktırlar. Sonuç olarak iletişim formu ile spam ve sosyal mühendislik saldırıları olabildiğince minimuma

indirgenmiş olacak ve eposta adresine brute force saldırısı ihtimali ortadan kaldırılmış olacaktır.

Kaynaklar

https://www.netsparker.com/web-vulnerability-scanner/vulnerability-security-checks-index/email-address-disclosure/
https://portswigger.net/knowledgebase/issues/details/00600200_emailaddressesdisclosed