YAVUZLAR WEB GÜVENLİĞİ & YAZILIM TAKIMI

Restoran App Pentest Görevi

Hazırlayan : Mustafa Batuhan ALUN

Açık – 1:Settings.php – Web Shell

Web Shell Nedir ?

Bir web Shell , bir web sunucusuna uzaktan erişilmesini sağlayan, genellikle siber saldırılar amacıyla kullanılan shell benzeri bir arayüzdür .

Zafiyet Nelere Sebep Olabilir ?

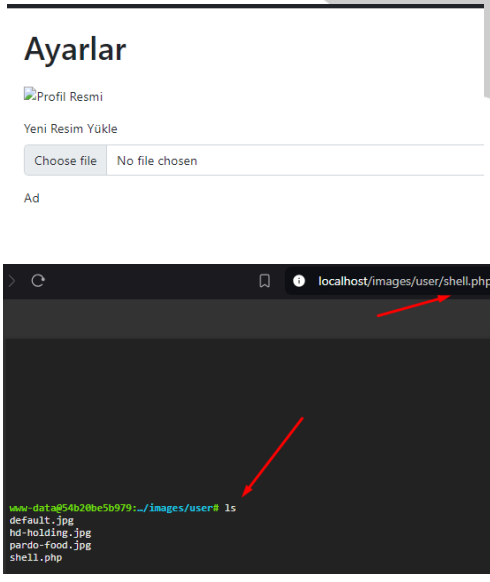
Bir shell açığı saldırgan kullanıcının isrediği gibi saldırılan sistemde komut yürütmesine olanak tanır.

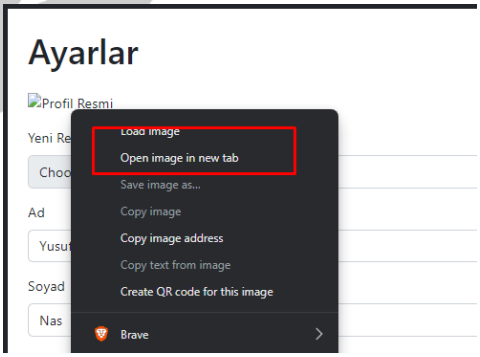
Zafiyetin Kapatılması için Öneriler:

Dosya yükleme kısıtlamaları getirilmelidir. Kullanıcıdan gelen her dosyanın dosya türü ve uzantıları kontrol edilmelidir. Bu örnekte verilen resim alanına sadece jpg png ve gif gibi resim dosyaları yüklenebilmeli aksi takdirde sistem kabul etmemelidir.Ayrıca kullanıcıdan gelen dosyaların sadece uzantıları değil MIME türlerinin de kontrolü sağlanmalıdır.

Dosya izinleri kısıtlanarak veya yüklenen dosyaların default olarak no executable olarak ayarlanması sağlanmalıdır.

Sömürmeye Ait Kanıt:





Açık – 2:restaurant-add.php – Web Shell

Web Shell Nedir ?

Bir web Shell , bir web sunucusuna uzaktan erişilmesini sağlayan, genellikle siber saldırılar amacıyla kullanılan shell benzeri bir arayüzdür .

Zafiyet Nelere Sebep Olabilir ?

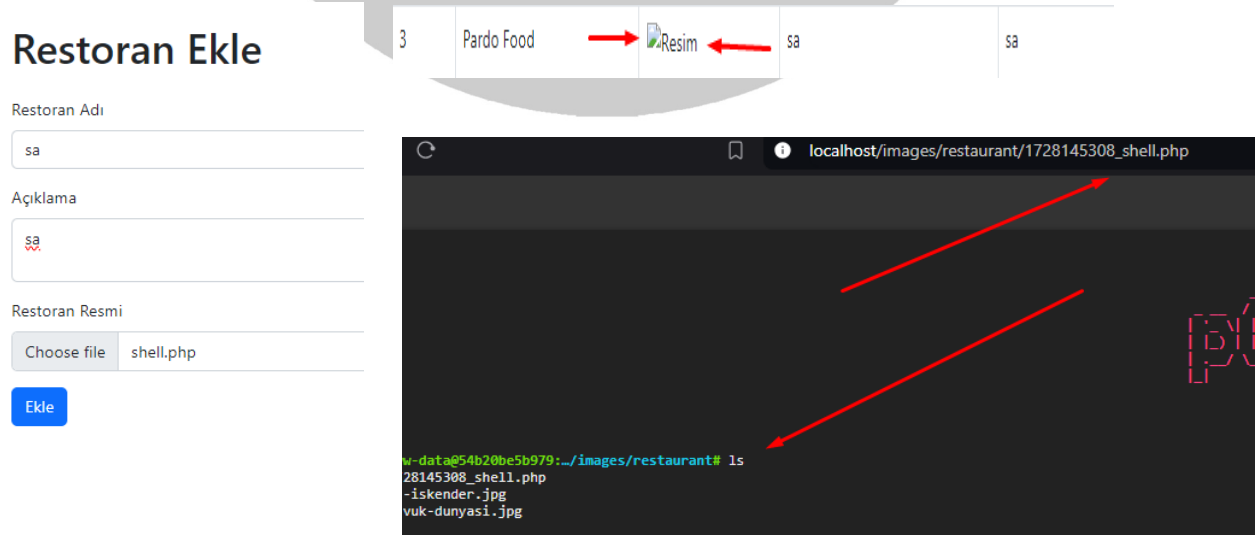
Bir shell açığı saldırgan kullanıcının isrediği gibi saldırılan sistemde komut yürütmesine olanak tanır.

Zafiyetin Kapatılması için Öneriler:

Dosya yükleme kısıtlamaları getirilmelidir. Kullanıcıdan gelen her dosyanın dosya türü ve uzantıları kontrol edilmelidir. Bu örnekte verilen resim alanına sadece jpg png ve gif gibi resim dosyaları yüklenebilmeli aksi takdirde sistem kabul etmemelidir.Ayrıca kullanıcıdan gelen dosyaların sadece uzantıları değil MIME türlerinin de kontrolü sağlanmalıdır.

Dosya izinleri kısıtlanarak veya yüklenen dosyaların default olarak no executable olarak ayarlanması sağlanmalıdır.

Sömürmeye Ait Kanıt:



Açık – 3:add-food.php – Web Shell

Web Shell Nedir ?

Bir web Shell , bir web sunucusuna uzaktan erişilmesini sağlayan, genellikle siber saldırılar amacıyla kullanılan shell benzeri bir arayüzdür .

Zafiyet Nelere Sebep Olabilir ?

Bir shell açığı saldırgan kullanıcının isrediği gibi saldırılan sistemde komut yürütmesine olanak tanır.

Zafiyetin Kapatılması için Öneriler:

Dosya yükleme kısıtlamaları getirilmelidir. Kullanıcıdan gelen her dosyanın dosya türü ve uzantıları kontrol edilmelidir. Bu örnekte verilen resim alanına sadece jpg png ve gif gibi resim dosyaları yüklenebilmeli aksi takdirde sistem kabul etmemelidir.Ayrıca kullanıcıdan gelen dosyaların sadece uzantıları değil MIME türlerinin de kontrolü sağlanmalıdır.

Dosya izinleri kısıtlanarak veya yüklenen dosyaların default olarak no executable olarak ayarlanması sağlanmalıdır.

Sömürmeye Ait Kanıt: