

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 ?

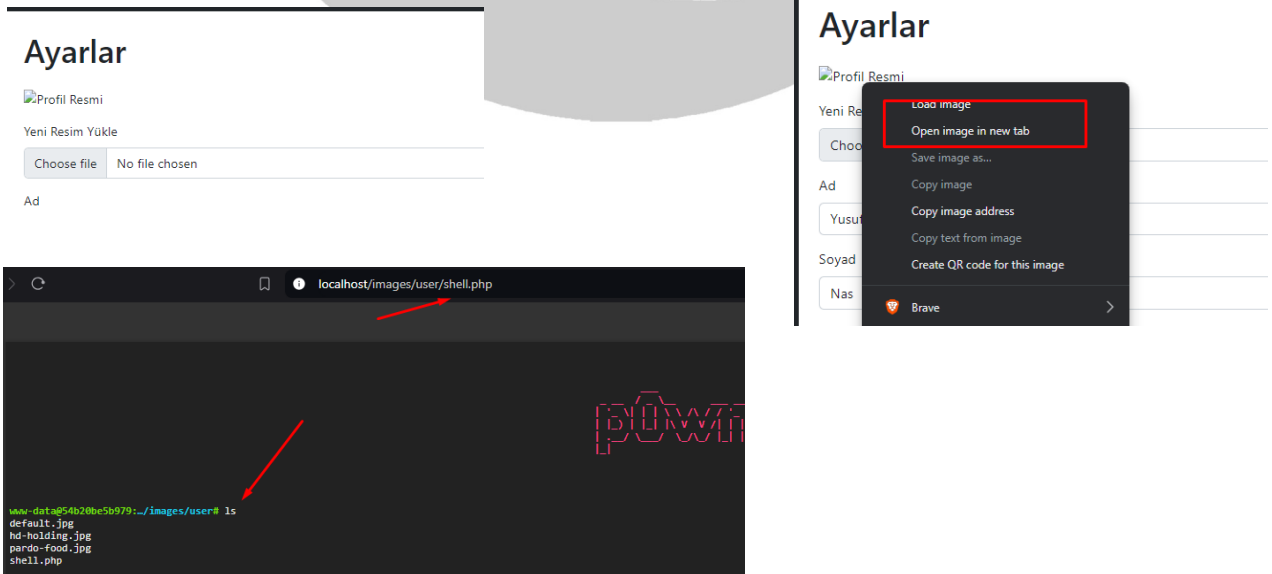
Bir shell açığı saldırgan kullanıcının istediği gibi saldırılan sistemde komut yürütmesine olanak tanır.

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 istediği 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:

Restoran Ekle

Restoran Adı

sa

Açıklama

sa

Restoran Resmi

Choose file

shell.php

Ekle

3	Pardo Food	→	Resim	←	sa	sa
---	------------	---	-------	---	----	----

```
localhost/images/restaurant/1728145308_shell.php  
  
w-data@54b20be5b979:~/images/restaurant# ls  
28145308_shell.php  
-iskender.jpg  
vuk-dunyasi.jpg
```

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 istediği 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:

The image shows a web application interface for adding a new food item. On the left, there is a form titled "Yemek Ekle" (Add Food) with fields for "Restoran Seç" (Select Restaurant), "Yemek Adı" (Food Name), "Açıklama" (Description), "Ücret (TL)" (Price in TL), "İndirim (%)" (Discount (%)), and "Yemek Resmi" (Food Image). The "Yemek Resmi" field has a "Choose file" button and a "shell.php" file selected. A red arrow points to the "Ekle" (Add) button. On the right, there is a table with columns "Tavuk Dünyası", "Food Image", "sa", and "sa". The "Food Image" column has a red box around it. Below the table, there is a terminal window showing the command "ls" and the output of the command, which lists files in the directory: "1728145502_shell.php", "1728145818_shell.php", "ayran.jpg", "iskender.jpg", "kola.jpg", "kremalar.jpg", "mercimek.jpg", "salata.jpg", "sutlac.jpg", and "tursu.png". A red arrow points to the terminal window.