NATAS20

Buradaki zaafiyet myread ve mywrite fonksiyonundan kaynaklanmaktadır.

Myread fonksiyonu şu şekilde tanımlanmış:



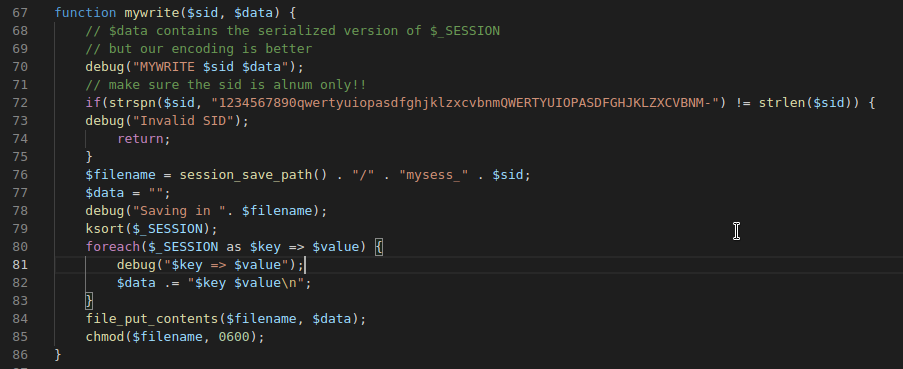
Buradaki kodu adım adım incleyelim:

47. satırdaki validasyonun bir önemi yok validasyondan başarılı bir şekilde geçiyor

51. satırda $filename değişkinine bir dosya yolu ve dosya yolunun sonuna da session id değeri atanıyor.

52. ve 54. satırlar arasında $filename değişkininde bulunan dosya yolu ve dosya isminde bir dosya olup olmadığı kontrol ediliyor eğer dosya yok ise fonksiyondan çıkılıyor.

Myread fonksiyonundan çıktıktan sonra session handler ın da tanımlı olan bir diğer fonksiyona yani mywrite fonksiyonuna gidiliyor.



My write fonksiyonunda ise işler şu şekilde:

72. satırda ufak bir validasyon

75. satırda gene bir dosya yolu tanımlanması

79. satırda SESSION ksort fonksiyonunda geçiliyor:

<https://www.php.net/manual/tr/function.ksort.php>

Parametre olarak aldığı diziyi varsayılanda alfabetik olarak sıralar

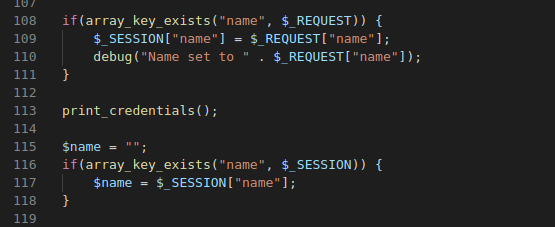
Pek bir işimiz yok açıkçası

80. ve 83. satırlar arasında SESSION değişkeni foreach ile dönülüyor ve data değişkenine atılıyor.

84. satırda ise $data değişkenine atanmış olan değer $filename değişkeninde bulunan dosya içerisine aktarılıyor.

86. satırda ise chmod fonksiyonu ile oluşturulan dosyanın izinleri değiştiriliyor.

Şimdi gelelim asıl kod bloğumuza:



108. satırda $\_REQUEST değişkeninde “name” isminin geçip geçmediği kontrol ediliyor ve eğer POST veya GET ile gönderilmiş name adında bir değişken var ise if kontrolünden geçiyor

109. satırda ise $\_SESSION içindeki “name” değişkenine formdan gelen veri aktarılıyor.

Buraya kadar herhangi bir sıkıntı yok print\_creadentials fonksiyonuna baktığımız zaman bir session oluşturulmuş olmasını ve session içerisinde bir admin değerinin tanımlanmış olması gerekiyor.

Şimdi ilk isteğimizi attığımız ve bizim için bir session oluştuğunu var sayalım. İkinci isteği attığımız zaman tekrardan myread fonksiyonuna girilecek. Myread fonksiyonunu tekrar ele alalım:

İlk isteği atarken 52. satırdaki if koşuluna girmiştik ve fonksiyon return vermişti.

Şimdi ise ilk isteği atarken oluşmuş bir session dosyamız bulunuyor.(mywrite fonksiyonu 84. satır)

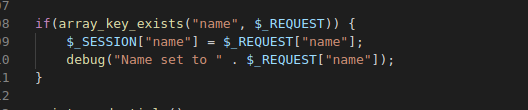
myread fonksiyonunda adım adım ilerleyelim:

57. satır $data değişkenine dosya içeriğini atıyor

59. satırda dosyayı “\n” parçalıyor yani dosya içerisinde \n değerine geldiği zaman diziye farklı bir eleman ekliyor ve foreach ile bu diziyi dönüyor.

61. satırada dizinin elemanını boşluğa göre parçalıyor. Ve eğer parçalanan değer boş değil ise $\_SESSION a yazıyor.

Session a admin değerini atamak için tam olarak buradaki açıktan faydalanıcağız. Peki bunu nasıl yapcağız:

Kod bloklarında dolaylı olarak dokunabildiğimiz alanlar sınırlı. En göze çarpan alan ise mywrite fonksiyonundaki file\_put\_contents fonksiyonu. SESSION dan gelen değerleri olduğu gibi dosyaya yazıyor. SESSION a değerler de alttaki kod bloğundan aktarılıyor

mywrite fonksiyonunda herhangi bir validasyon yok bu yüzden gönderdiğimiz veri ne olursa olsun dosya yazılıyor ve o dosya myread fonksiyonunda okunup session a aktarılıyor.

Myread fonksiyonunda ki 59. satırdaki foreach I hatırlayalım “\n” e göre explode ediyordu.

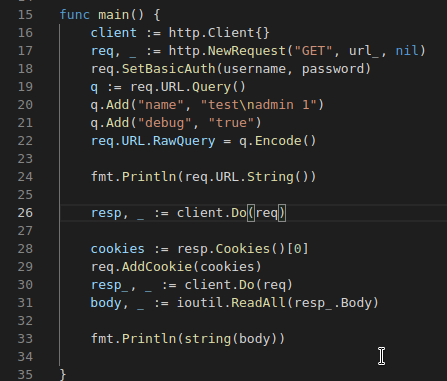
Name değişkenine test1\ntest2 şeklinde bir payload gönderirsek bu foreach in iki kere tekrar edeceği anlamına geliyor

ilk tekrarda $line değişkenini içinde test ikinci tekrarda ise test2 değerleri olacak ve bu değerleri boşluk karakterine göre parçalayacak.

Son olarka “test1\ntest2 1” payloadını gönderdiğimiz zaman ikinci tekrarda session a şöyle bir veri yazacak $\_SESSION[‘test2’] = 1

Açığı yakalamak için tam olarak buradan faydalanacağız.

Payload olarak “test1\nadmin 1” gönderdiğimiz zaman $\_SESSION[“admin”] = 1 ataması yapacak ve print\_credentials fonksiyonuna başarılı bir şekilde gireceğiz. Bunu go ile yapan kod satırı şu şekilde:



16., 17. ve 18. satırda istekleri yapabilmek için gerekli olan tanımlamalar yapılmakta.

19, 20, 21 ve 22. satırlarda ise payloadı gönderebilmek için gerekli tanılmamalar yapılmakta. 22. satırdaki Encode fonksiyonunu çağırmaz ise yani payloadı url encode etmeden gönderir isek “\n” karakteri dosyaya düzgün şekilde yazılmayacaktır. O yüzden el ile yaptığınız denemelerde payloadı url encode etmeyi unutmayın.

26. satırda ilk istek atılıyor mywrite fonksiyonu ile dosya oluşturuluyor.

28. satırda ikl atılan isteğin sessionid değeri ikinci atılacak isteğe ekleniyor. Bunu yapıyoruz ilk istekteki session id değeri ile ikinci istekteki session id değeri aynı olsun ve ilk istekte açılan dosya okunabilsin

geri kalan satırlarda istek atılıyor ve 21. adım bilgileri elimize geçiyor