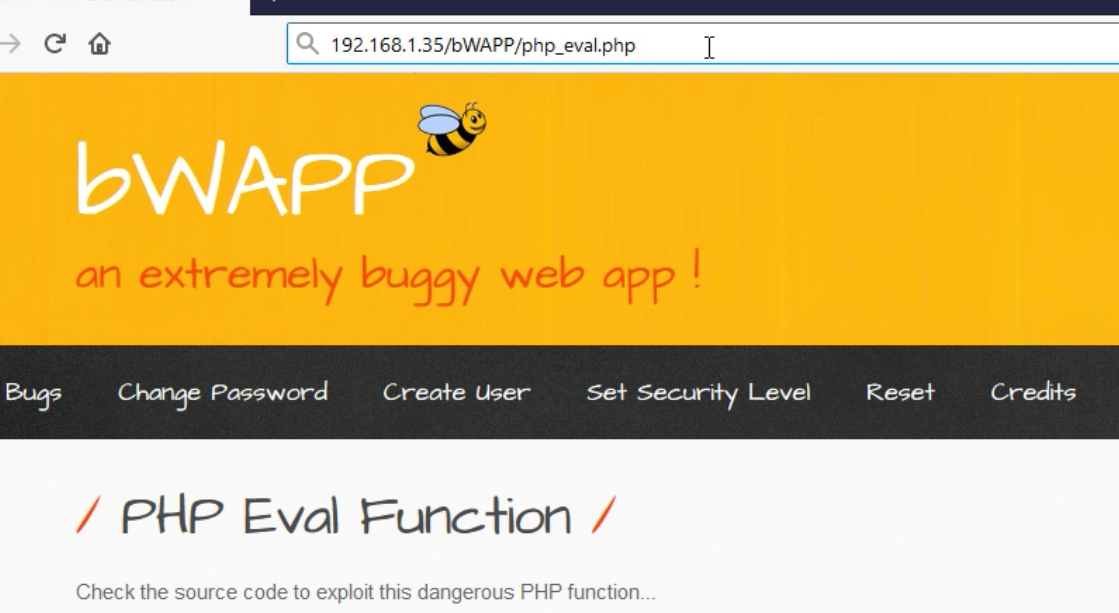
|  |
| --- |
| ***Web Uygulama Zafiyet*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Bwapp laboratuvarı üzerinde bulunan PHP Code Injection,PHP Eval Function,IFRAME Injection açıklarını birlikte çözeceğiz. |

**08.11.2021**

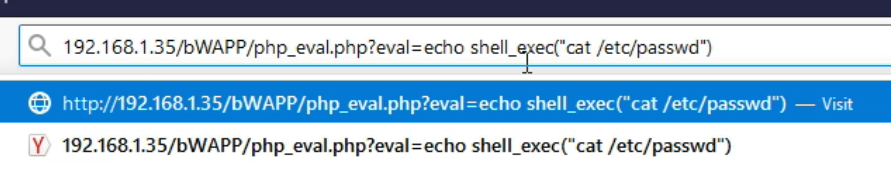
PHP Eval Function

-Bu zafiyet php\_eval fonksiyonu sayesinde ortaya çıkmaktadır.Normalde kaynak kodu analizinde karşımıza çıkmaktadır.

-Bu zafiyet için zafiyet testi gerçekleştirebileceğimiz bwAPP aracını kullanacağım.



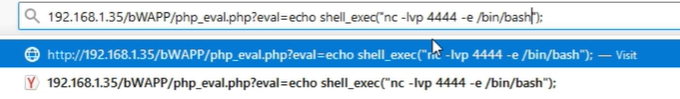
-bwAPP üzerinden zafiyeti başlattığımda karşıma böyle sayfa çıkıyor.



- Burada ilk önce eval fonksiyonunu çağırıyorum ve içerisine passwd dizinini görüntülememi sağlayacak bir kod dizini ekliyorum.



- Döndürdüğü sonuçlara baktığımda başarılı bir şekilde passwd dosyasını görüntüleyebildim.



- URL içerisine bir netcat komutu ekleyip shell almaya çalışacağım.URL üzerinde bu kod dizinini çalıştırıyorum.

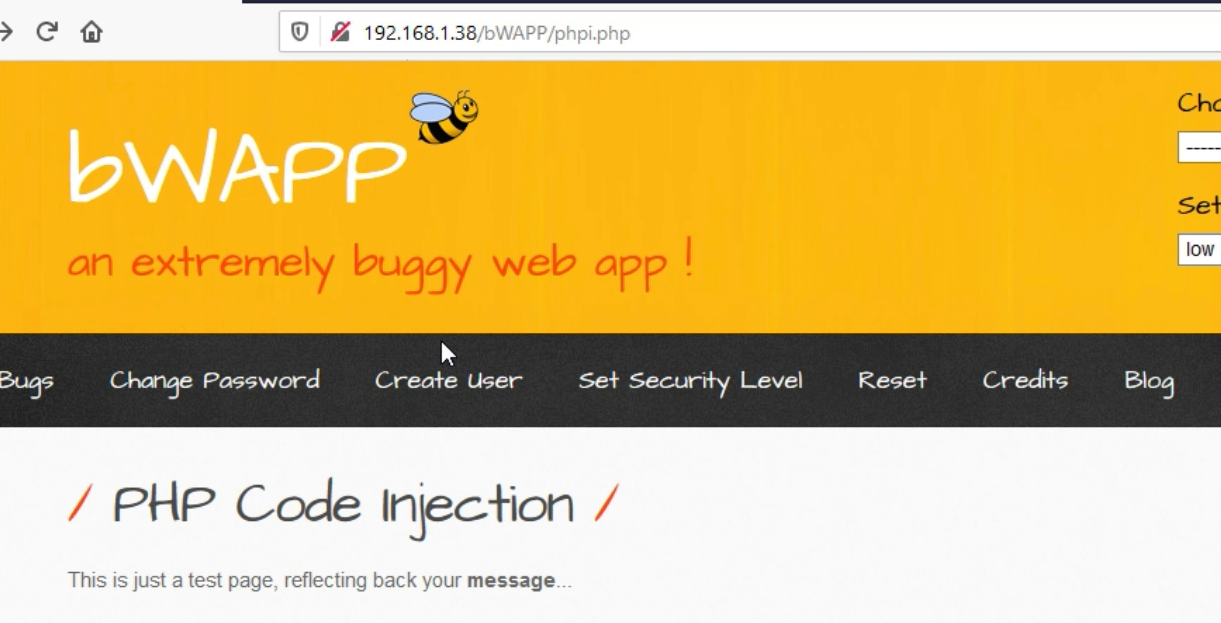


- Ardından başarılı bir şekilde shell aldığımı görüntüleyebiliyorum.

PHP Code Injection

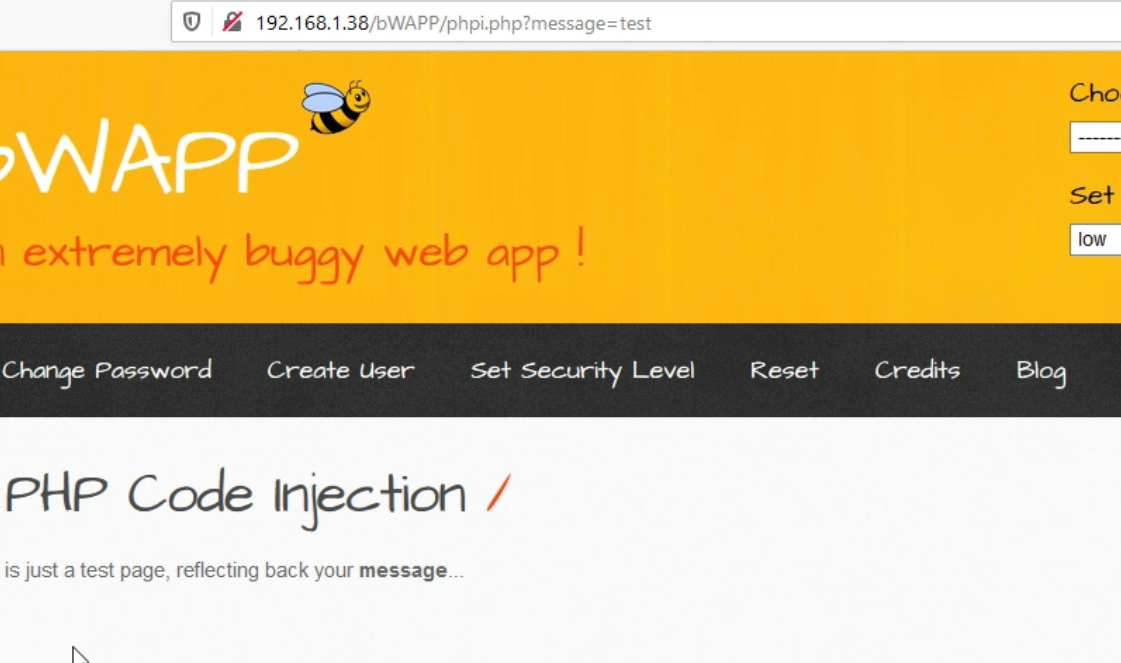
-Bu zafiyeti uygulayarak göstermek istiyorum.

-Bu zafiyet için zafiyet testi gerçekleştirebileceğimiz bwAPP aracını kullanacağım.

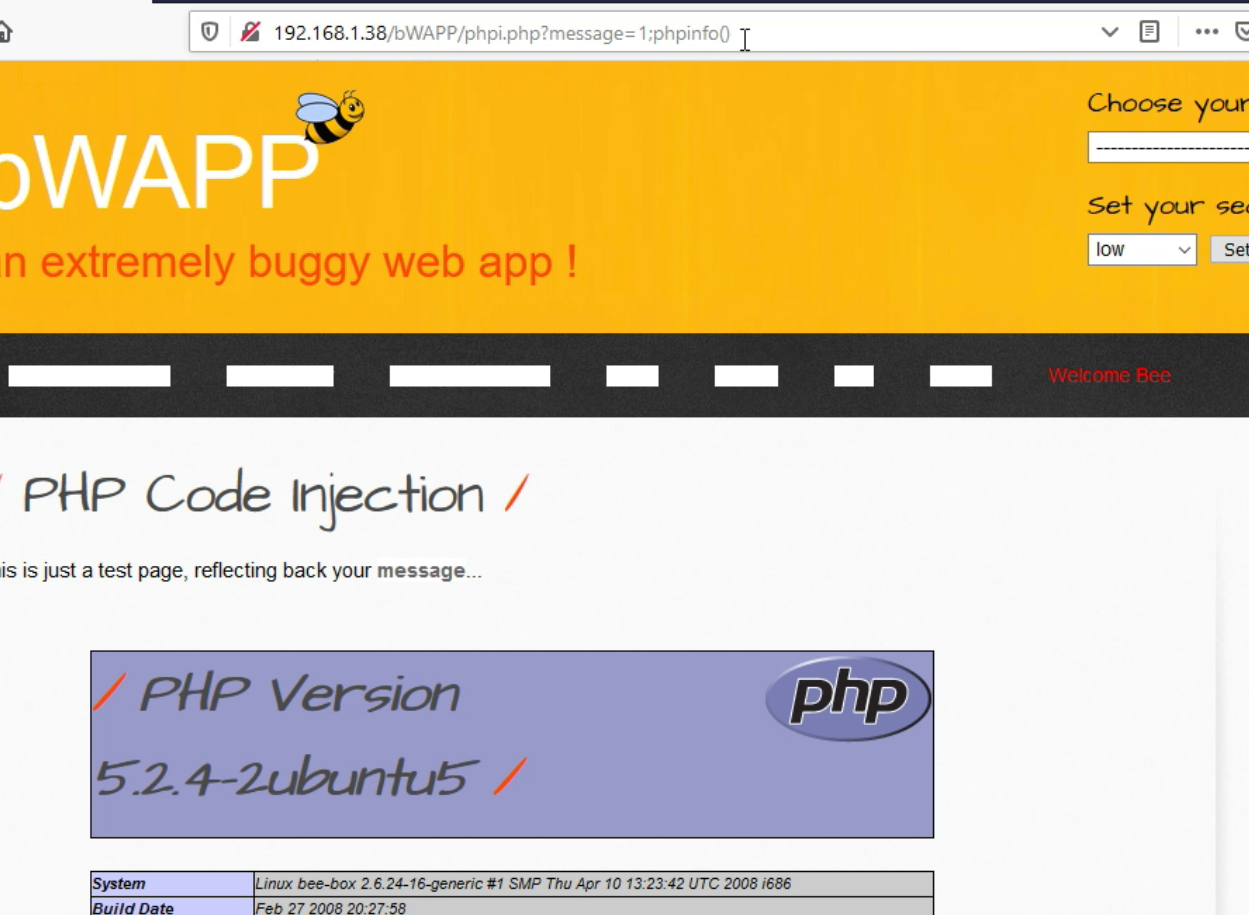


- bwAPP üzerinden zafiyeti başlattığımda karşıma böyle sayfa çıkıyor.

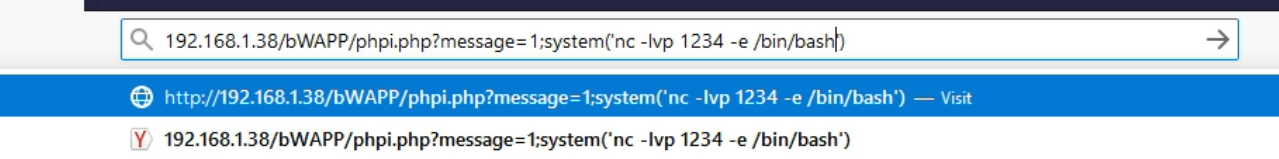
-Sayfada sadece message kısmına tıklandığını görüntülüyorum.



-URL kısmına baktığımda bir değişiklik olduğunu görüyorum.Buradan bir zafiyet yakalayabileceğimi düşünüyorum.



-Burada ;'den sonra bir phpinfo() komutu ekliyorum.Başarılı bir şekilde php versiyonu hakkında bilgi sahibi olabildim.



- URL kısmına bir netcat bağlantısı üzerinden dinleme işlemi gerçekleştiriyorum.Buradan bir shell almayı deneyeceğim.

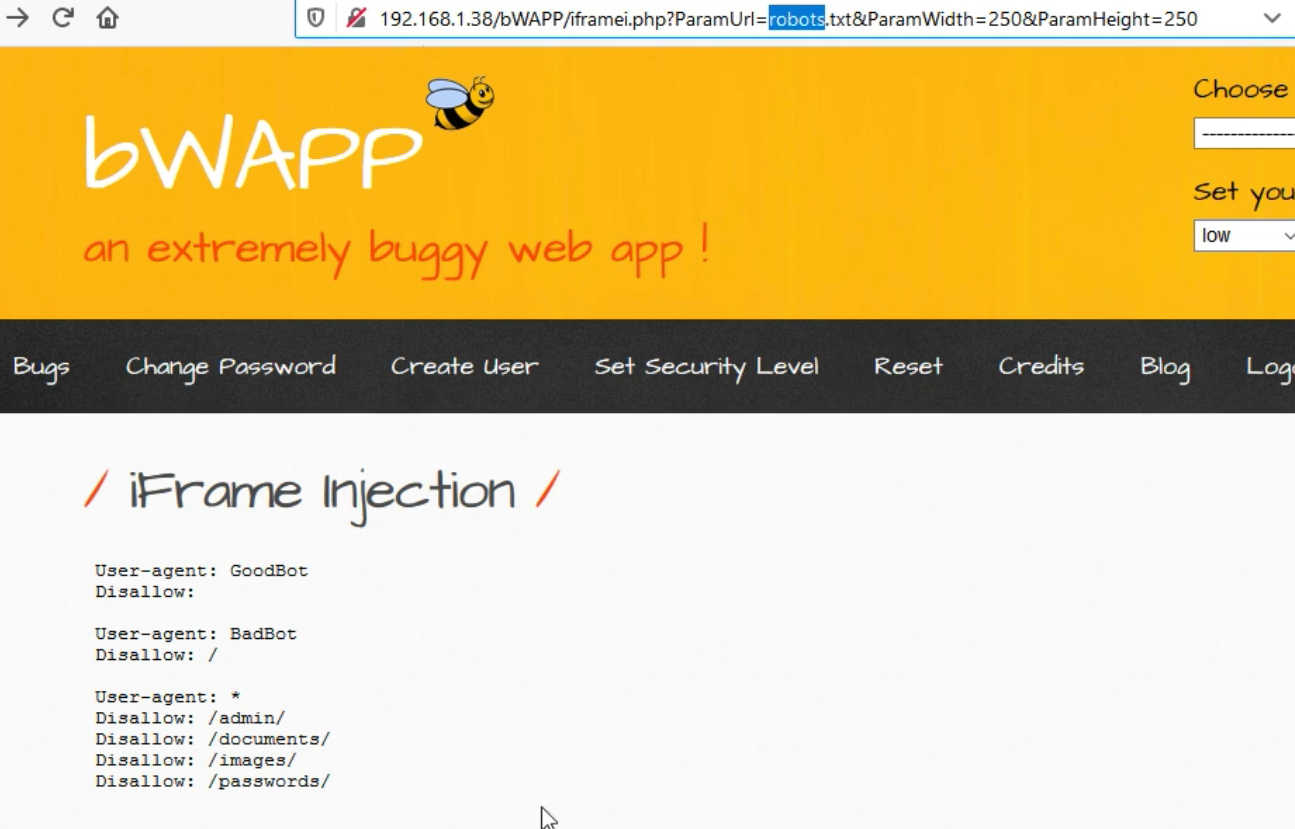


-Netcat üzerine geçiş yaptığımda başarılı bir şekilde shell aldığımı görebiliyorum.

IFRAME Injection

-Bu zafiyeti uygulayarak göstermek istiyorum.

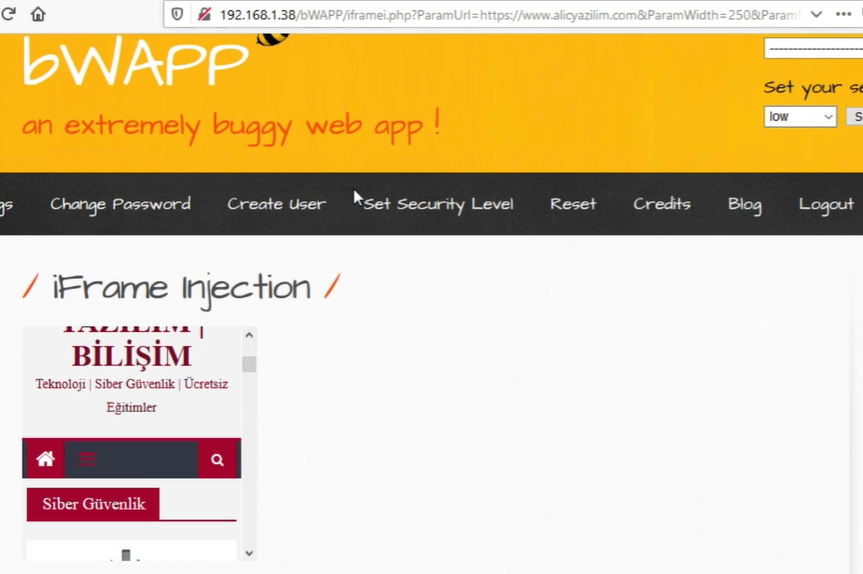
-Bu zafiyet için zafiyet testi gerçekleştirebileceğimiz bwAPP aracını kullanacağım.



- bwAPP üzerinden zafiyeti başlattığımda karşıma böyle sayfa çıkıyor.

-URL kısmına baktığımda burada bir dosya görüntülenmesi yaptığını görüntülüyorum.

-POST metoduyla gönderilmediği için burada bir açık ortaya çıkmıştır.



- URL kısmına bir web sitesi gizliyorum ve siteyi burada açıkca görüntüleyebiliyorum.

Buraya eklediğim popüler bir sosyal medya benzeri bir uygulama ile bilgi çalma şansım olabilir.