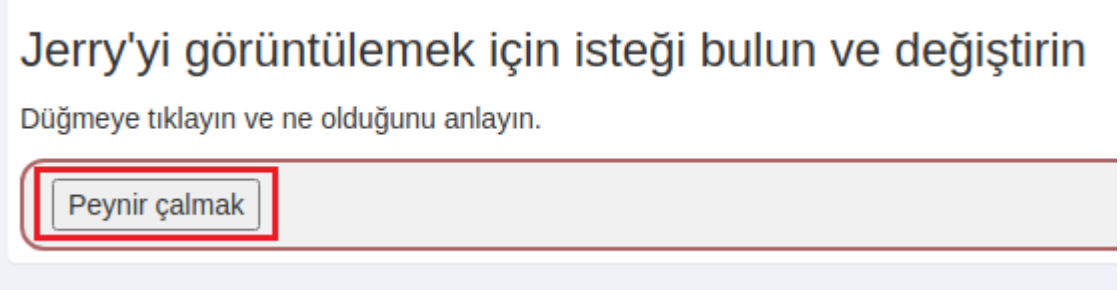
Server Side Request Forgery (SSRF) Zafiyeti Nedir? SSRF Zafiyetinden Nasıl Korunulur?

SSRF (Server Side Request Forgery/Sunucu Tarafı İstek Sahteciliği), bir saldırganın veya saldırganların sunucu tarafında uygulamayı istenmeyen bir konuma istekte bulunmasına neden olmasına izin veren web güvenlik açığıdır.

Sıradan SSRF saldırısında, saldırgan veya saldırganlar sunucunun kuruluşun altyapısındaki sadece dahili hizmetlere bağlantı kurmasına neden olabilmektedir. Öteki durumlardaysa sunucuyu rastgele harici sistemlere bağlanmaya zorlayabilir ve yetkilendirme kimlik bilgileri gibi hassas verileri potansiyel olarak sızdırabilmektedir. Üstelik harici üçüncü taraf sistemlere bağlantılara neden olan bir SSRF istismarı, güvenlik açığı bulunan uygulamayı barındıran kuruluştan geliyormuş gibi görünen kötü niyetli saldırılara neden olabilmektedir.

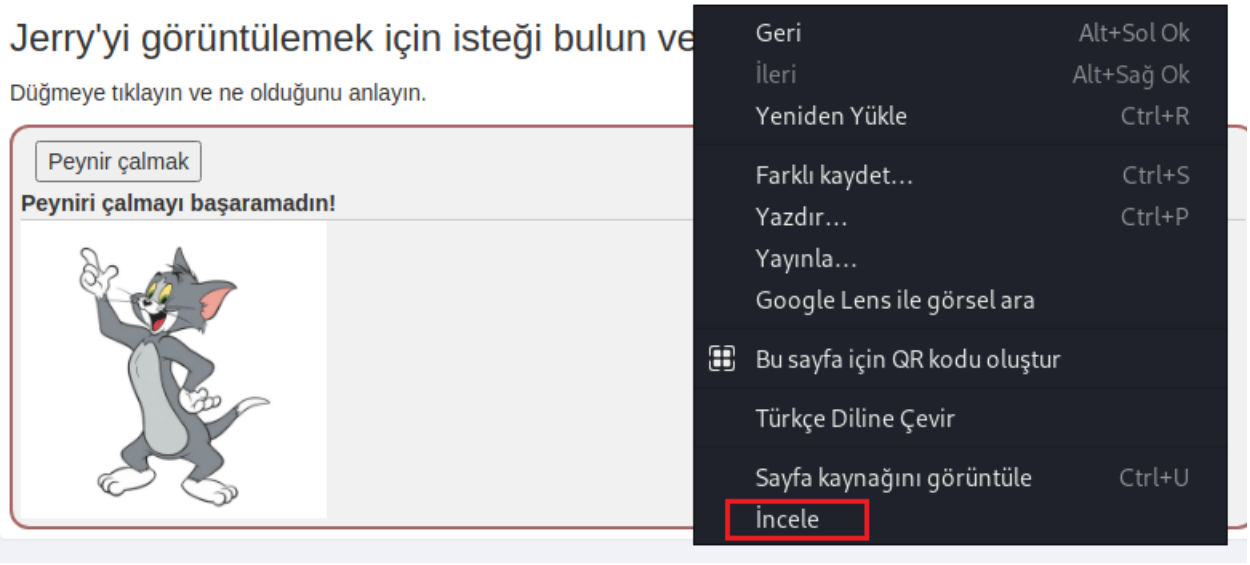
SSRF Zafiyeti içeren örnek bir uygulama:

OWASP'ın WebGoat adlı laboratuvar ortamının SSRF zafiyeti anlatımında "Peynir çalmak" butonuna basılmıştır.

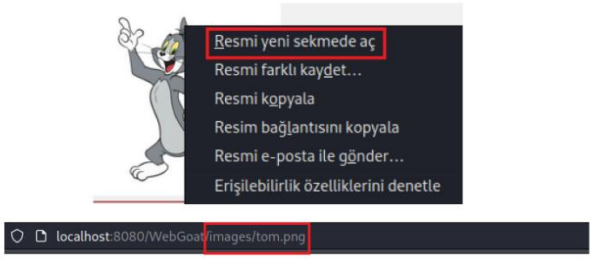


Butona basılmasıyla aşağıdaki görselde yer aldığı üzere "Tom ve Jerry Show" adlı çizgi filmdeki "Tom" karakteri ekrana gelmiştir.

Sayfanın kaynak kodlarına sağ tıklayarak "İncele"ye basarak incelemelere başlanmıştır.

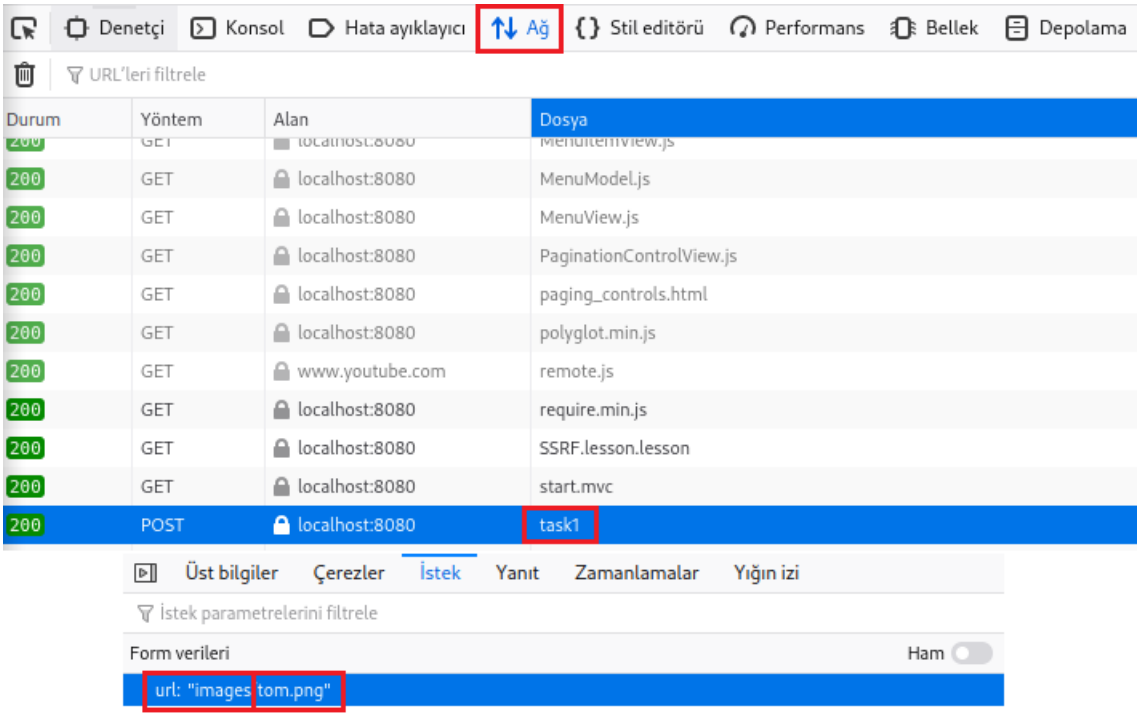


İncelemelere kaynak kodundan devam edilirken şüpheli bir şeye rastlanmamıştır. Resmin tamamına yeni sekmede bakılmıştır ki derinlemesine incelenebilirliği adına URL adresindeki dosya uzantılarına vb. noktalara mutlaka bakılmalıdır.

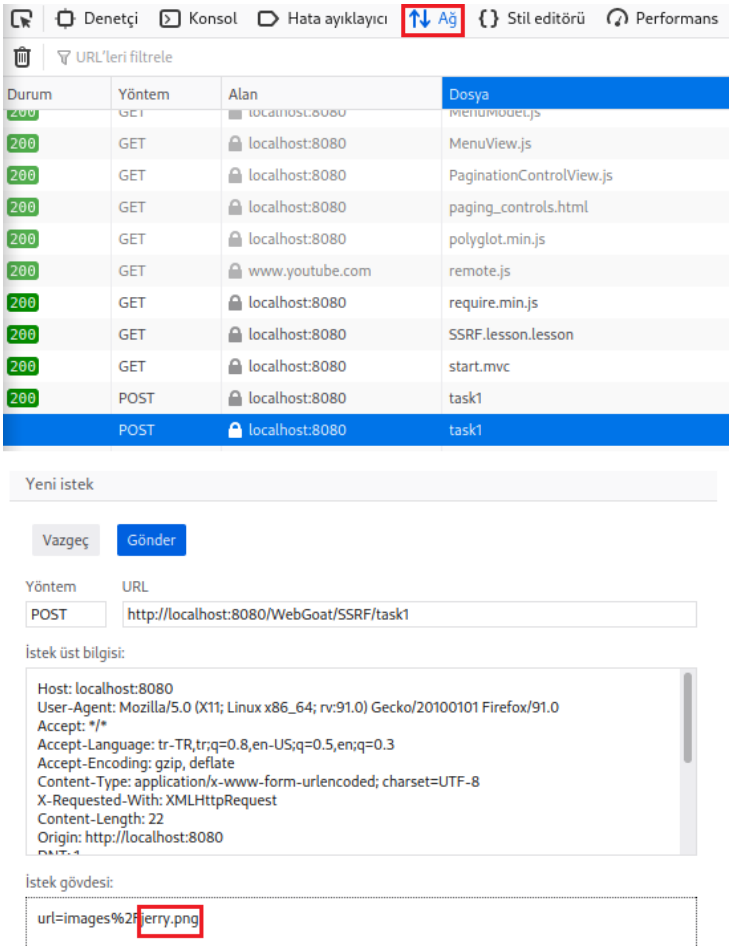


Resmin “images” adlı dosya yolundan çekildiği tespit edilmiştir. Notunu alırken “Tom ve Jerry Show” adlı çizgi filmin “Tom” karakterinin yanı sıra “Jerry” karakterinin de “images” dizini altında yer alabileceği düşüncesiyle yeni sekmede değiştirilmiştir.

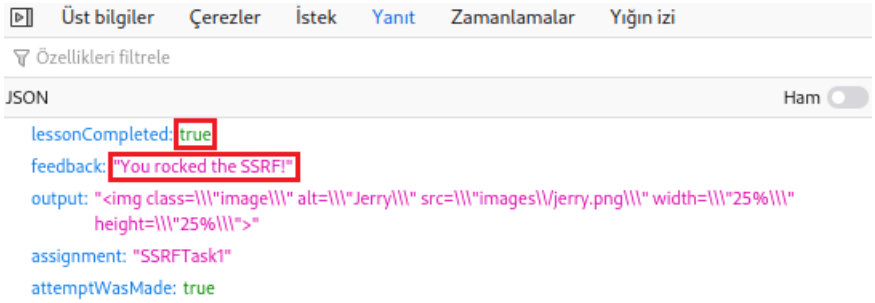
Değişikliğin yapılmasıyla yukardaki görselde yer aldığı üzere başarılı olunduğu saptanmıştır. Erişilebilirliğin söz konusu olduğundan yola çıkılarak butonda bize görüntülenen karakterin resmini SSRF zafiyeti vasıtasıyla değiştirebiliriz.



Yukardaki görselde yer aldığı üzere “İncele” sekmesinin “Ağ” özelliği aracılığıyla resmin görüntülendiği yere gidilir ve değer “tom”dan “jerry” değerine çekilir.



Değerin değiştirilmesiyle “Gönder” butonuna basılır ve bizlere farklı dönüş sağlandığı aşağıdaki resimde görüldüğü üzere verilmiştir.



Böylelikle başarılı olunmuştur.

SSRF ZAFİYETİNE KARŞI ALINABİLECEK ÖNLEMLER

SSRF zafiyetine karşı sistem tarafında alınabilecek bazı önlemler vardır.

- Uygulamanızın erişmesi gereken ana bilgisayar adını (DNS adı) veya IP adresini beyaz listeye (whitelist) almalısınız. Beyaz liste (whitelist) yaklaşımı size uymuyorsa ve bir kara listeye (blacklist) güvenmeniz gerekiyorsa, kullanıcı girişini doğru şekilde doğrulamak önemlidir.
- Kullanıcı girişine uygulanan basit kara listeler (blacklist) ve normal ifadeler, SSRF zafiyetini azaltmak için kötü bir yaklaşımdır ve sıklıkla tercih edilir. Bypasslanabilirlik (atlatılabilirlik) durumları söz konusu olduğundan saldırgan veya saldırganlar her zaman farklı metotlara başvuracaktır. Bu ve benzeri söz konusu durumları en aza indirgeyebilmeniz için wildcard DNS çözümlerinin IP bloklandırılmasını yapmalısınız.
- Yanıt verilerinin saldırgana sızmasını önlemek için alınan yanıtın beklendiği gibi olup olmadığından emin olmalısınız. Hiçbir koşulda sunucu tarafından gönderilen istekten gelen ham yanıt gövdesi istemciye teslim edilmemelidir.
- Web adresinizin isteklerinde sadece HTTP veya HTTPS kullanılıyorsa, yalnızca HTTP veya HTTPS URL yapılarına izinlendirme tanımlamalısınız. Kullanılmayan URL şemalarını devre dışı bırakırsanız, saldırgan veya saldırganlar “file:///”, “ftp://” vb. potansiyel tehlikeli yapıları kullanarak isteklerini yapabilmeleri için web uygulamasını kullanamaz hale gelecektir.
- Varsayılan haliyle gelen Memcached, Redis, Elasticsearch ve MongoDB vb. hizmetler kimlik doğrulama gerektirmemektedir. Saldırgan veya saldırganlar, bu ve benzeri hizmetlerden bazılarına herhangi bir kimlik doğrulaması olmadan erişebilmek için SSRF güvenlik açıklığını kullanabilir. Dolayısıyla, hassas bilgilerinizi korumak için yerel ağdaki hizmetler için bile mümkün mertebe her yerde kimlik doğrulamasını etkinleştirmeniz gerekmektedir.