ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/web-uygulama-saldirilari-ve-klasik-cozumlerin-yetersizligi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Web%20Uygulama%20Sald%C4%B1r%C4%B1lar%C4%B1%20ve%20Klasik%20%C3%87%C3%B6z%C3%BCmlerin%20Yetersizli%C4%9Fi.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Web uygulamalarında yapılan hatalar daha fazla dikkat çeker.

(Page 11)

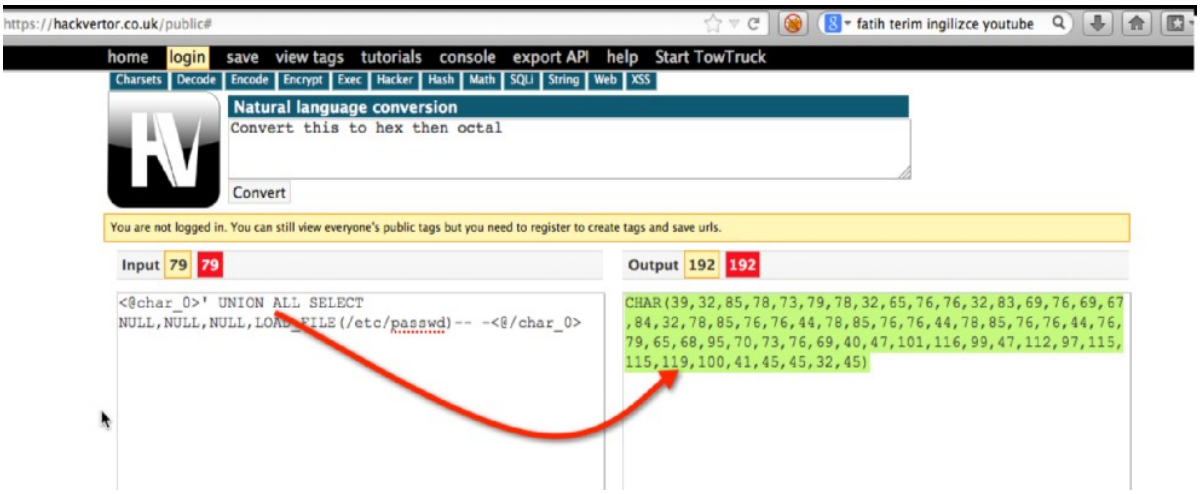
2)

Web sitenizin hack'lenmesi için birinin sizi takip etmesine gerek yoktur. Google üzerinden dork aramalarıyla sayfanız hack'lenebilir.

(Page 11)

3)

Encoding Yöntemi ile IPS Atlatma



Bir network'te güvenlik katmanları şu şekildedir:

Internet ---------- Router ---------- IDS/IPS ---------- Firewall ---------- Server

Encoding ile kodlanmış bir input - örneğin URL'deki parametreden kargaşık burgaşık gelen bir input - web server'daki $_POST[“...”] ya da $_GET[“...”] tarafından önce decoding edilecektir ve sonra işlenecektir. Yani input web server'a gelene kadar encode halinde iletilecektir ve web server'a geldiğinde ise $_POST ya da $_GET ile decode edilerek çalıştırılacaktır. Haliyle eğer IDS/IPS cihazı saldırı kodu tanımlamalarını plain text olarak kaydetmişse encode edilmiş halde gelen saldırı kodunu tanımlayamayacaktır ve saldırı kodu doğrudan web sunucuya gidecektir. Web sunucu da gelen input'u $_POST ya da $_GET ile decode edip işlendiğinde saldırı amacına ulaşmış olacaktır. Yani encoding ile IDS/IPS cihazı bypass edilmiş olacaktır.

(Benim NOT)

(Page 16)

4)

IDS/IPS'in olmadığı bir web sunucusuna url'den encode edilmiş SQL Injection kodları da koysak encode edilmemiş SQL Injection kodları da koysak sql sorgusunun sonundaki $_GET ya da $_POST saldırı kodunu encode edilmiş halde gelmişse decode edip sql sorgusuna servis edecektir, encode edilmeden gelmişse de olduğu gibi sql sorgusuna servis edecektir. Yani iki türlü de saldırı başarıya ulaşacaktır. Web script dili ile input filtrelemesi şayet yaparsak iki türlü de $_POST ve $_GET plain text formatında input'u vereceğinden encoding yapmak filtreyi aşmamızı sağlamayacaktır. O zaman encoding işe yaramayacaksa saldırılarda niye kullanılıyor diyebiliriz? Encoding “saldırı tespit sistemlerinin” olduğu network'lerde saldırı tespit sistemlerini atlatmak için kullanılan bir tekniktir. Saldırı tespit sistemi atlatıldığında eğer web script dili ile de input filtrelemesi konmamışsa o zaman saldırı başarıya ulaşacaktır.

(Benim Not)