Yazılım Güvenliği Dersi Dönem Ödevi Raporu

İbrahim Ethem Gürbüz / 210710065 Numan Taha Kotan / 210710062

XSS Zafiyeti: CVE – 2024 – 54317

Google’ın eski bir sürümünde bulunan stored XSS zafiyetidir. Daha sonraki Google güncellemeleriyle birlikte bu durum ortadan kalkmıştır. Tanım olarak, saldırganların uygulamada kullanıcıların tarayıcılarında zararlı js kodları çalıştırmasına olanak tanır. XSS zafiyetleri genellikle, kullanıcıdan gelen girdilerin uygun bir şekilde filtrelenmediği veya temizlenmediği durumlarda ortaya çıkar.

- Kullanıcı gizliliğini tehlikeye atabilir ve yetkisiz verilere erişim sağlayabilir.

Google güncellemeleriyle ortadan kalkmış bu zafiyetin gösterilmesi adına BugBountyHunter adlı siteden elde edilen FastFoodHacking isimli site üzerinde çalışılmıştır.

Çalışma Raporu;

Site uzantısının sonuna ‘robot.txt’ yazıldığında bize

Disallow: /admin

Disallow: /go

Çıktısını veriyor bu aldığımız ‘admin’ ve ‘go’ çıktılarını site urlesinin sonuna .php ekleyerek sırayla deniyoruz. Ve deneme sonucunda go.php eklentisiyle gelen sayfada bizden bir URL istediğini görüyoruz. Site anasayfasında F12 tuşuyla network alanından bulduğumuz .js kodlarını tek tek inceliyoruz ve “custom-script.js” isimli scriptte “redirectUrl” alanı gözümüze çarpıyor bu scripti bir yönlendirme olma ihtimaline karşı not ederek devam ediyoruz.

OPEN REDIRECT AÇIĞI

Site uzantısı sonuna go.php ekleyince bizden URL yönlendirmesi istemekteydi test amacıyla google.com yazıyoruz. Sonuç olarak Google anasayfasına yönlendirildiğini gözlemliyoruz. Fakat uzantı normal şartlarda olması gerekenden(google.com) dan farklı olarak sonunda type=0 adresiyle karşımıza çıkıyor. Emin olmak adına farklı varyantlarla testimize devam ediyoruz. Ve testlerimizin sonucunda zafiyetin doğruluğundan emin oluyoruz. Bu açık ile banka gibi önemli kurumların sitelerini kendi sitemize yönlendirerek kullanıcıların bilgilerini çalabiliriz.

XSS AÇIĞI

Bulduğumuz açık devamında “https://www.bugbountytraining.com/fastfoodhackings/” site URL sinin sonuna “go.php?returnUrl=javascript:alert("hacked");&type=1” yazarak yönlendirmeyi bir javascript kodu üzerinden test etmeye devam ediyoruz. Bunu denerken js de type=1 yönlendirmesi olmadığı için type=1 kısmını “//” ile yorum satırına alıyoruz. Script ekleme işlemini yaptıktan sonra ekrana bir alert geldiğini görmekteyiz bu da javascript kodunun başarılı şekilde site üzerinde çalıştığını göstermektedir.

HTML INJECTION

Site içerisinde farklı açıklar aramaya devam ederken anasayfadaki “login” butonunu test ediyoruz.

Rastgele bir kullanıcı adı ve şifreyle denerken site URLsinin sonuna ‘act=login’ parametresi geldiğini gözlemledik. Bu parametreyi silip sildiğimiz yere farklı bir şey yazdığımızda HTML kodunun en üstüne yorum satırı şeklinde eklendiğini gördük fakat yorum satırı şeklinde eklenmesi bizim işimize yaramamaktadır. Bunun önüne yazdığımız mesajı yorum satırından çıkartarak geçebiliriz. <!-- numan --> şeklinde gelen yorum satırından kurtulmak adına URL sonuna ’ --> numan’ şeklinde eklemeliyiz. Bu sayede siteye istediğimiz HTML kodunu enjekte edebiliriz.

XSS 2. AÇIK

Bulduğumuz HTML Injection açığını XSS saldırısı şeklinde değerlendirmek istiyoruz bunun için javascript kodu eklemeliyiz. Ekleyeceğimiz kodu google’da xss-payload-list diye aratarak açılan github sayfasından random şekilde seçebiliriz. Biz test amacıyla ‘<img src =q onerror=prompt(8)’ kodunu seçtik bu kodu sitemizin uzantısına ekliyoruz. ‘https://www.bugbountytraining.com/fastfoodhackings/index.php?act=--><img src =q onerror=prompt(8)’ test sonucunda başarılı bir şekilde alert aldık.

STORED XSS

Sayfa kaynağını incelendiğinde en alt kısımda bir script olduğunu gözlemledik. Bu script kullanıcının IP si üzerinden bulunduğu bölgeyi bularak o bölgeye ait promosyonları göstermeye yarıyor.

Script;

var userCountry = response.country;

if (userCountry == "GB") {

document.getElementById("ad").innerHTML = '<div class="alert alert-warning" role="alert"><i class="fab fa-adversal icon-2x text-red"></i> <a href="book.php?promoCode=UKONLY">UK promotion: Buy one meal get <u>two</u> free!</a></div>';

document.getElementById("gmap").src = "https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d6738.972484852003!2d-1.7305805611669134!3d53.33275538645695!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x487a2b86abe63895%3A0x2c872aeb36297d4!2sBrough%20Ln%2C%20Hope%20Valley!5e0!3m2!1sen!2suk!4v1628522822227!5m2!1sen!2suk";

} else {

document.getElementById("gmap").src = "https://www.google.com/maps/embed?pb=!1m18!1m12!1m3!1d15609.52149200314!2d-6.98960860473787!3d61.632818183680115!2m3!1f0!2f0!3f0!3m2!1i1024!2i768!4f13.1!3m3!1m2!1s0x0%3A0x0!2zNjHCsDM3JzU3LjgiTiA2wrA1OCczOS40Ilc!5e0!3m2!1sen!2suk!4v1628523417848!5m2!1sen!2suk";

}

Kod incelendiğinde kampanyalar için kullanıcı gb ülkesinden girerse diye bir if bloğu bulunmakta.

Bu esnada ‘www.bugbountytraining.com/fastfoodhackings/book.php?promoCode=UKONLY’ uzantısında yer alan UKONLY alanı yerine ‘/book.php?promoCode=';ppromptrompt(10);var test='’ yazarak sayfaya giren her kullanıcının görebileceği ve kullanıcıları manipüle ederek istediğimiz bilgiyi toplayacağımız bir durum ortaya çıkarabilmekteyiz.

YOUTUBE VİDEOSU LINKİ

<https://youtu.be/JC35WTCNYT8>