Hackerlar’ın Gözünden Flash Uygulamaları

written by Mert SARICA | 30 January 2011
Ah o Netsec etkinliğinde bende olsaydım deyipte katılamayanlar için yapmış olduğum sunumu kısaca yazıya dökmeye karar verdim.

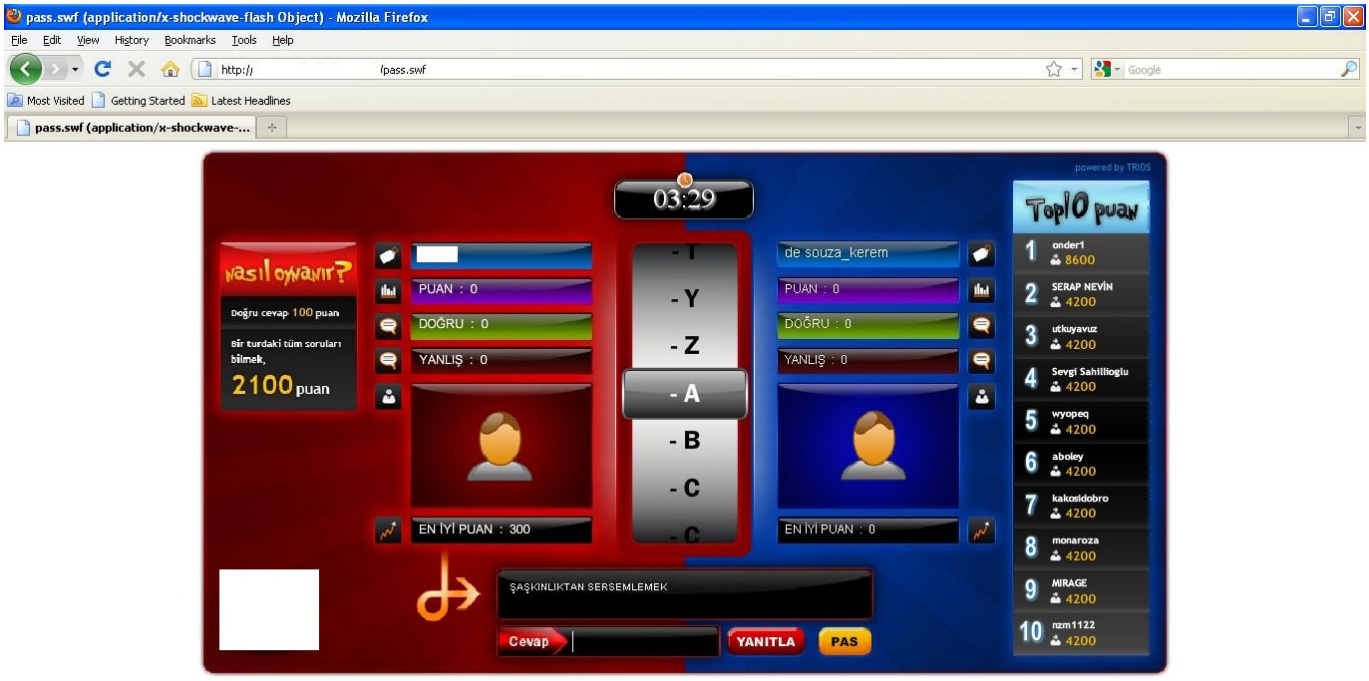
Ön bilgi olarak Flash kısaca web sayfalarına animasyon, video ve etkileşim eklemek amacıyla kullanılan ve Actionscript adında nesne yönelimli (object oriented) programlama dili içeren bir multimedya platformudur. Flash uygulamalarına çoğunlukla reklamlarda ve oyunlarda rastlarız. Flash dosyaları çoğunlukla SWF (ShockWave Flash) formatında olur ve aslında bir sanal makine olan Flash oynatıcısı tarafından çalıştırılır. Flash oynatıcısının bir sanal makine olması sayesinde SWF formatındaki bu dosyalar her platformda çalıştırılabilir. Durum böyle olunca Java’da da olduğu gibi SWF formatındaki bir dosya kolaylıkla baytkoddan (bytecode) kaynak koduna çevrilebilir (decompile). Actionscript, ilk olarak animasyonları kontrol etmek için tasarlanmıştır fakat geliştirilen yeni sürümleri ile web tabanlı oyunlardan görüntü ve ses yayını yapmaya imkan tanıyan zengin internet uygulamaları geliştirilebilmesine imkan tanımaktadır ve Javascript ile aynı kodlama imlasına (syntax) sahiptir. Actionscript’in 2. sürümü, Flash oynatıcı 8 ve öncesi sürümlerde, 3. sürümü ise 9 ve sonrası sürümlerde çalışmaktadır.

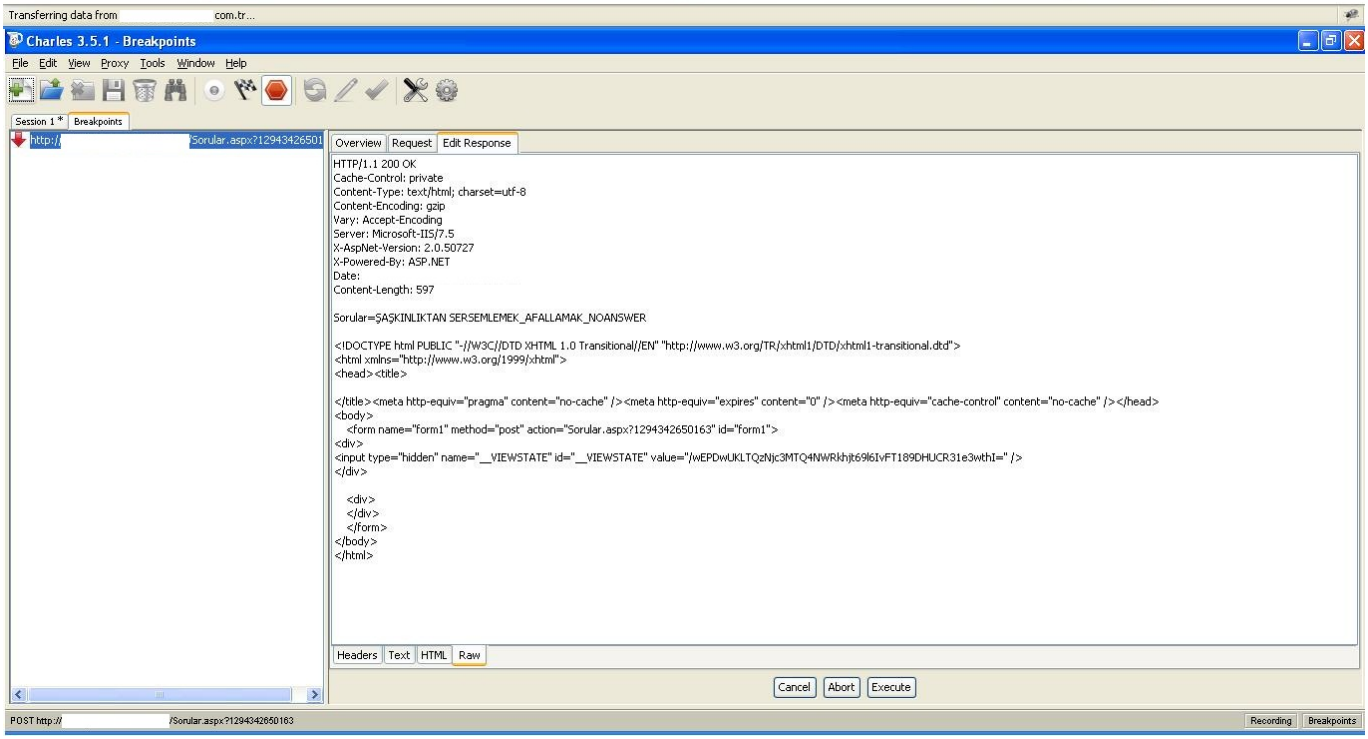
Aralık 2010 yılında Millward Brown tarafından gerçekleştirilen ankete göre Adobe Flash oynatıcısı, internet erişimi olan bilgisayarların %99’unda yüklüymüş. Anket bir yana zaten gün içinde gezdiğimiz sitelerin içeriğine biraz daha dikkat edecek olursak çoğunda Flash ile geliştirilmiş bir kısım olduğunu görebiliriz. Web uygulama güvenliğinde çoğunlukla Flash uygulama güvenliği göz ardı edilmekte ve art niyetli kişilerin hedefi haline gelebilmektedir.

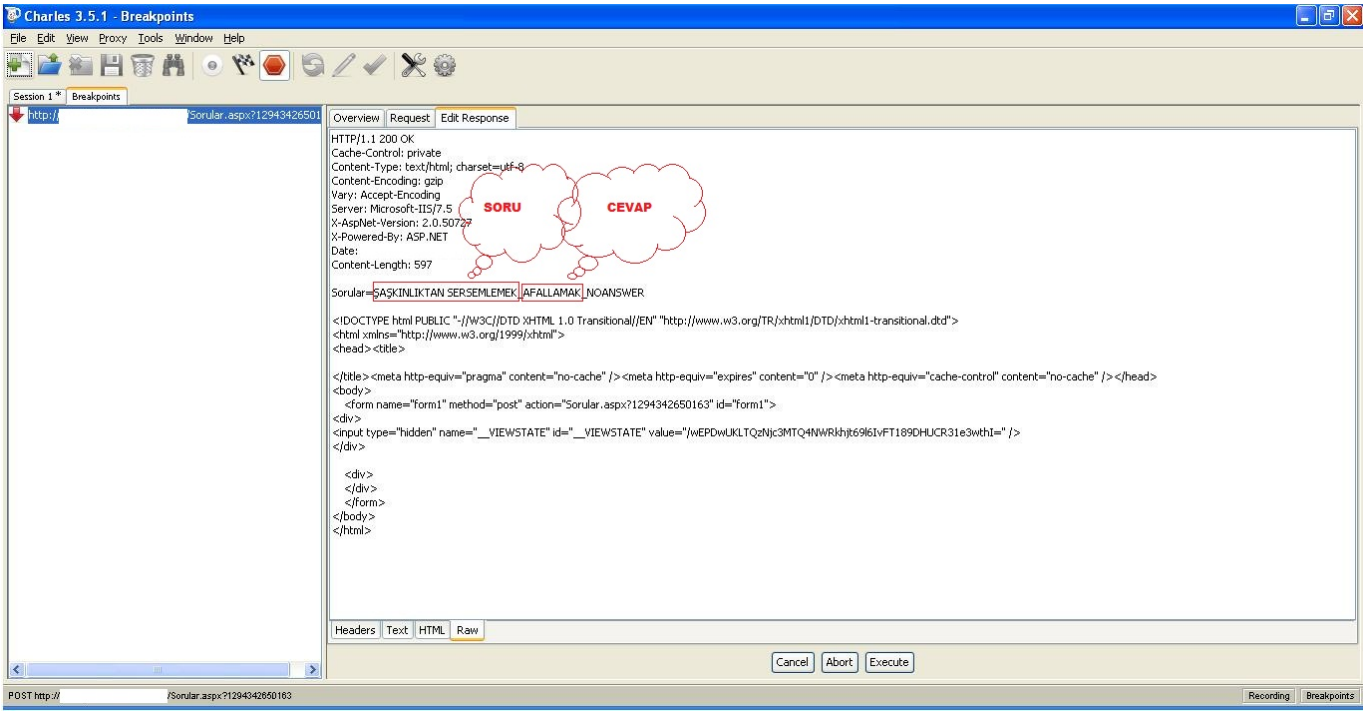
Örnek olarak Flash ile geliştirilmiş oyunları ele alarak art niyetli kişilerin çoğunlukla yoğunlaştığı noktalara kısa göz atalım;

- Flash oynatıcı ile sunucu arasında gerçekleşen trafiğin manipüle edilmesi: Özellikle Flash ile geliştirilmiş olan oyunlarda istemci tarafına güvenilerek kontrollerin istemci tarafında gerçekleştirilmesi sağlanmakta ve istemci tarafında işlenen veri sorgusuz sualsiz sunucu

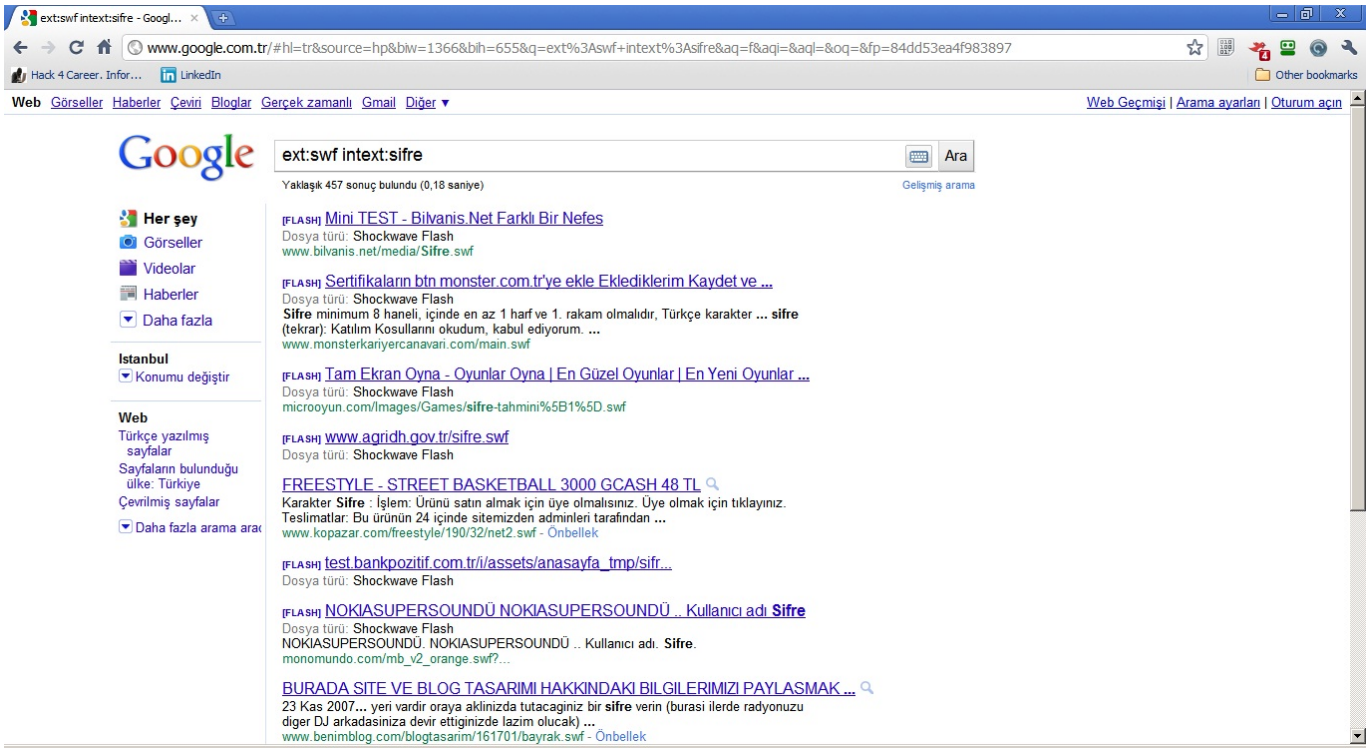
tarafında işleme alınmaktadır. Durum böyle oluncada ödüllü oyunlarda ve yarışmalarda bu durumu istismar eden hileciler ortaya çıkmakta ve haksız kazanç sağlamaktadırlar. Örnek olarak aşağıdaki ekran görüntüsünde yer alan oyunu inceleyecek olursanız sunucudan istemci tarafına sorulara ilave olarak yanıtların da gönderildiğini görebilirsiniz. Bu trafiği görebilmek ve gerekirse manipüle edebilmek için yapmanız gereken Burp, Paros ve benzer proxy araçları ile internet tarayıcısı ile sunucusu arasına girmektir.

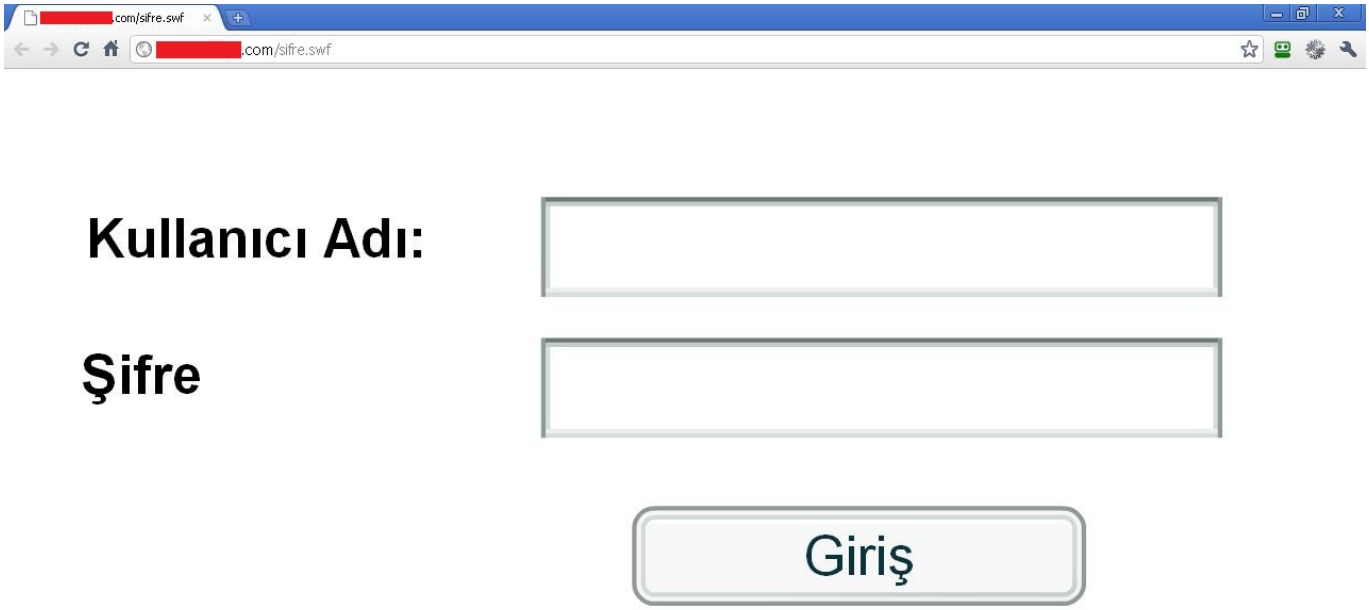


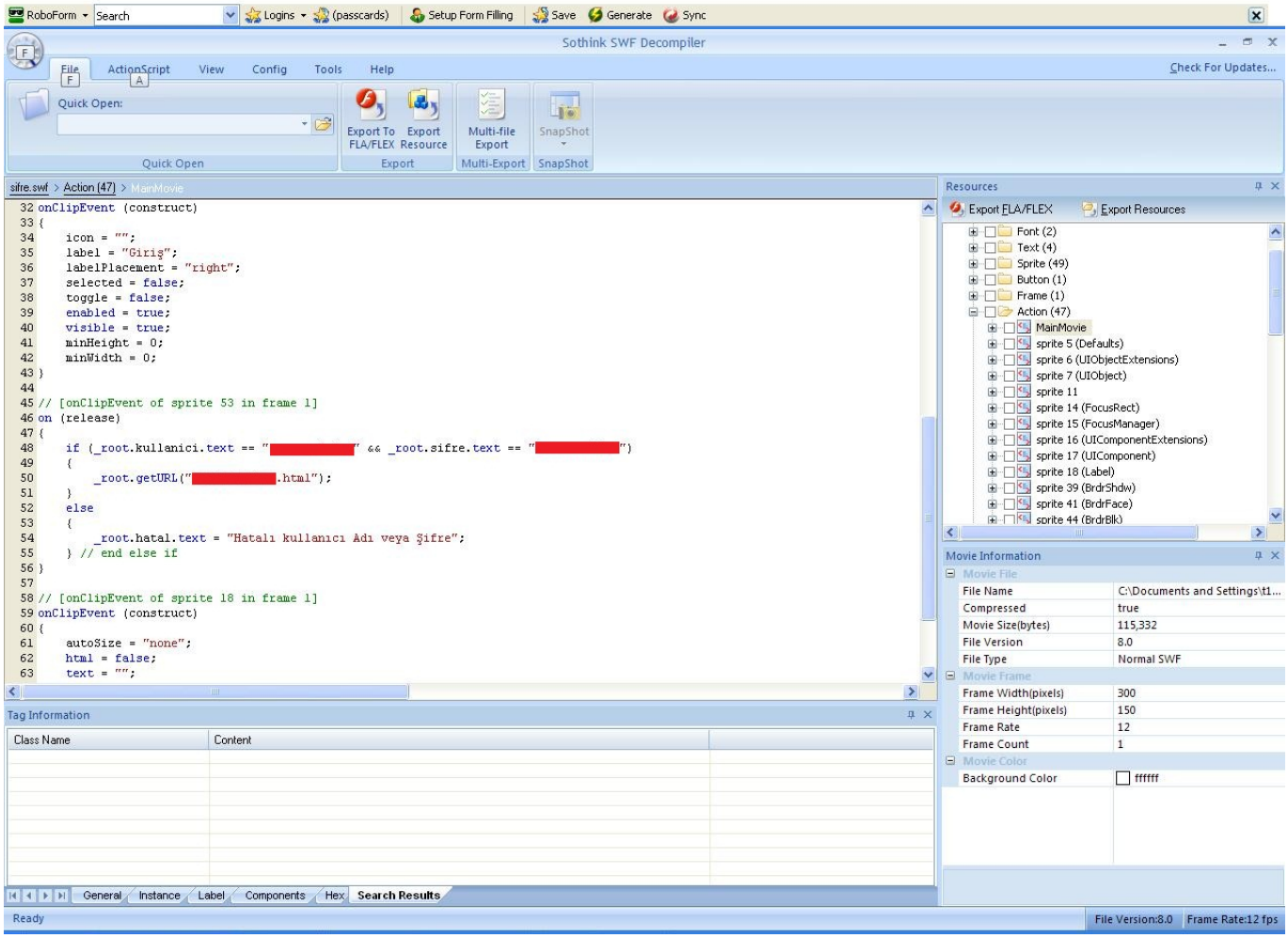




- Kaynak koduna çevirme: Az öncede bahsettiğim gibi baytkod olmasından ötürü Flash uygulamalarını kaynak koduna 3. parti bir araç ile çevirmek oldukça kolaydır bu nedenle uygulama içine statik kullanıcı adı ve şifre koymak doğru bir yaklaşım olmaz. Aşağıdaki ekran görüntüsü bu hatayı gözler önüne seren güzel bir örnek olabilir.

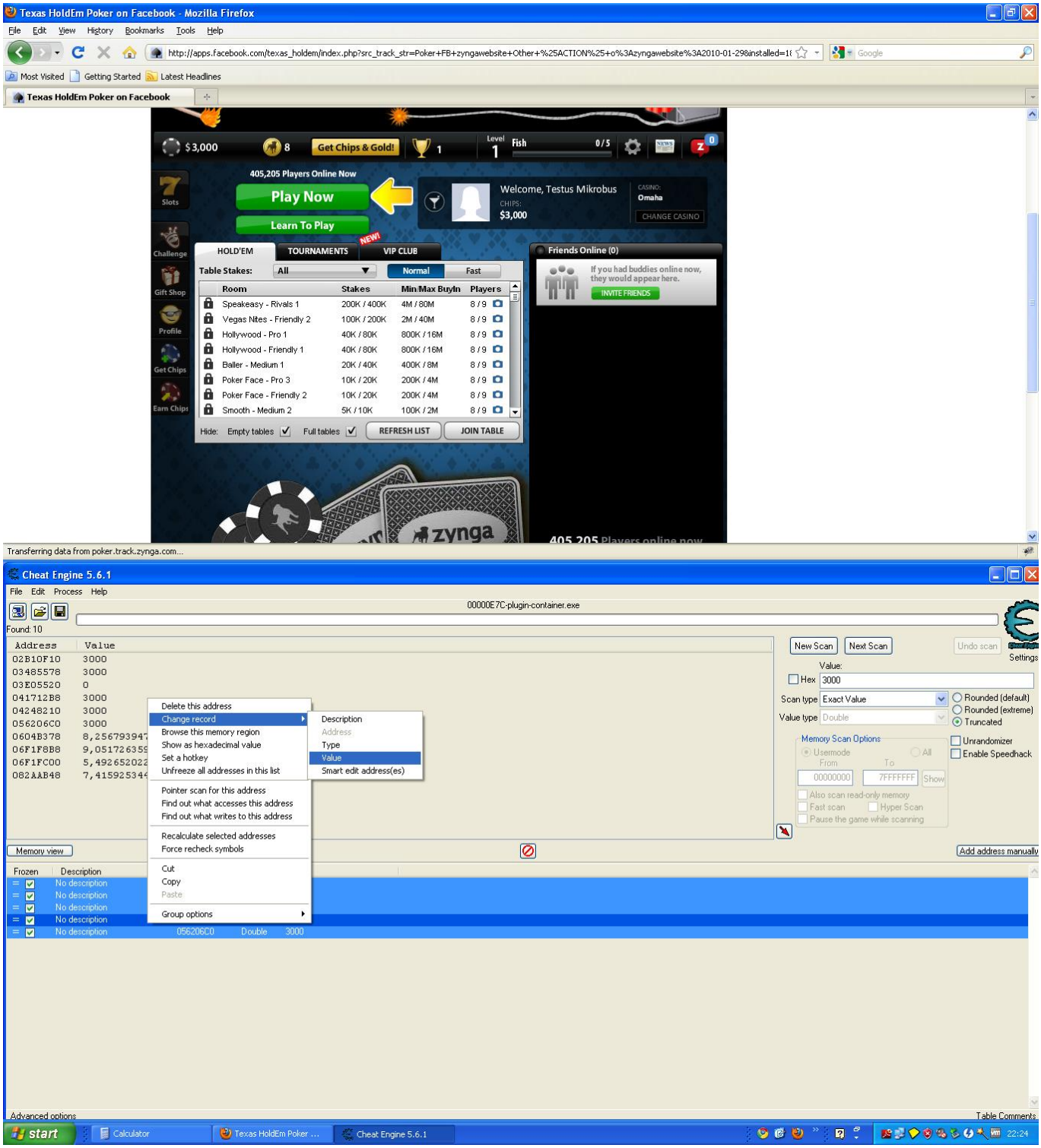


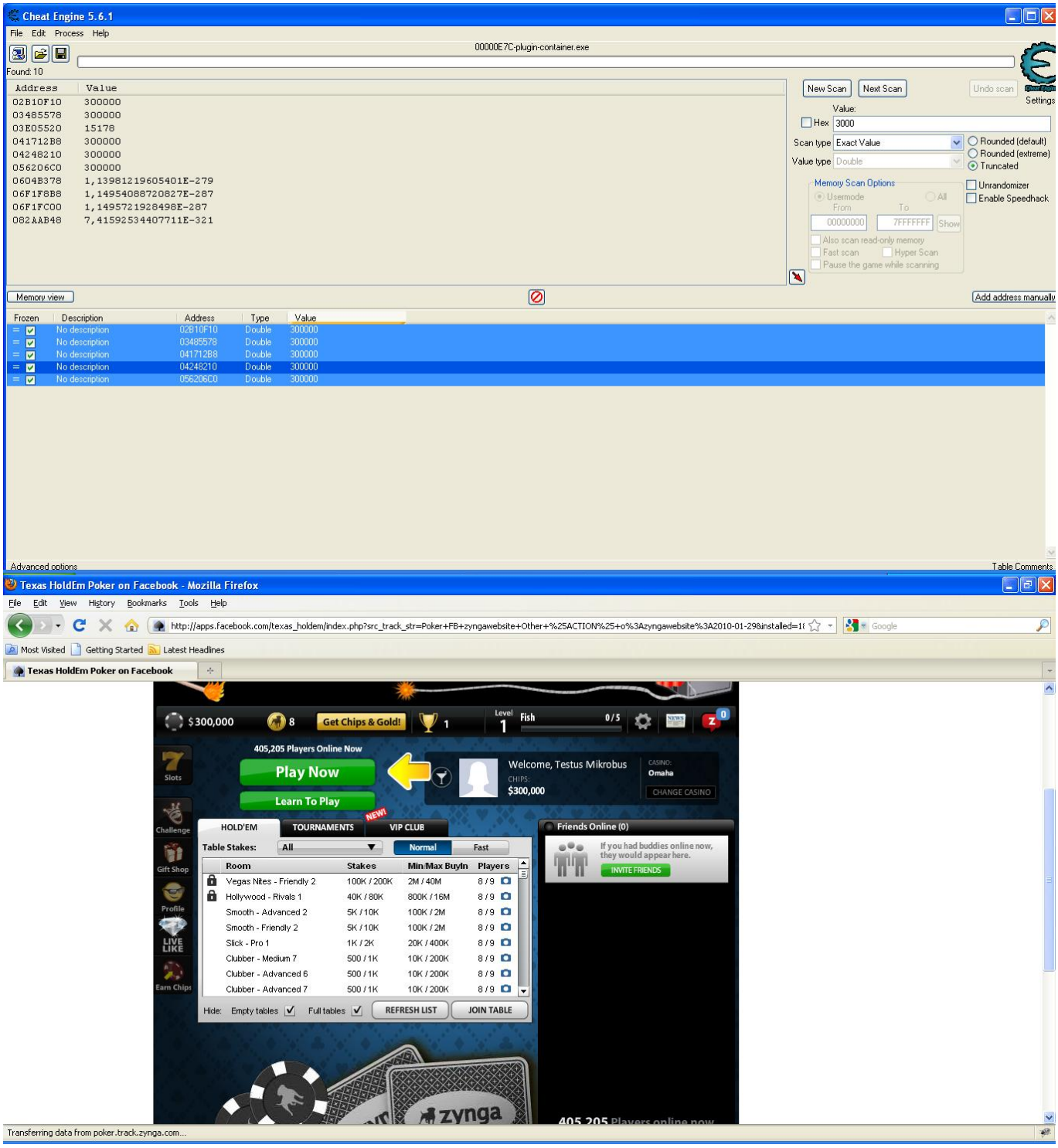




- Hafızaya müdahale etme: Diğer tüm uygulamalarda olduğu gibi Flash

uygulamaları tarafından kullanılan verilerin bir kısmıda hafızada saklanmaktadır. Hafızaya müdahale ederek uygulamanın akışını değiştirmek, sahip olmadığınız bir yetkiye sahip olabilmek mümkün olabilir. Özellikle oyunlarda hafızaya müdahale ederek gücünüzü yükseltmek veya sanal paranızı arttırmak haksız kazanca yol açabilir. Aşağıdaki ekran görüntüsünde bu amaçla kullanılan Cheat Engine aracı ile bir Poker oyununda sahip olunan paranın nasıl yükseltilebildiğini görebilirsiniz. Bunun için yapmanız gereken o an sahip olduğunuz paranın karşılığını hafızada bulmak ve istediğiniz değer ile değiştirmektir.

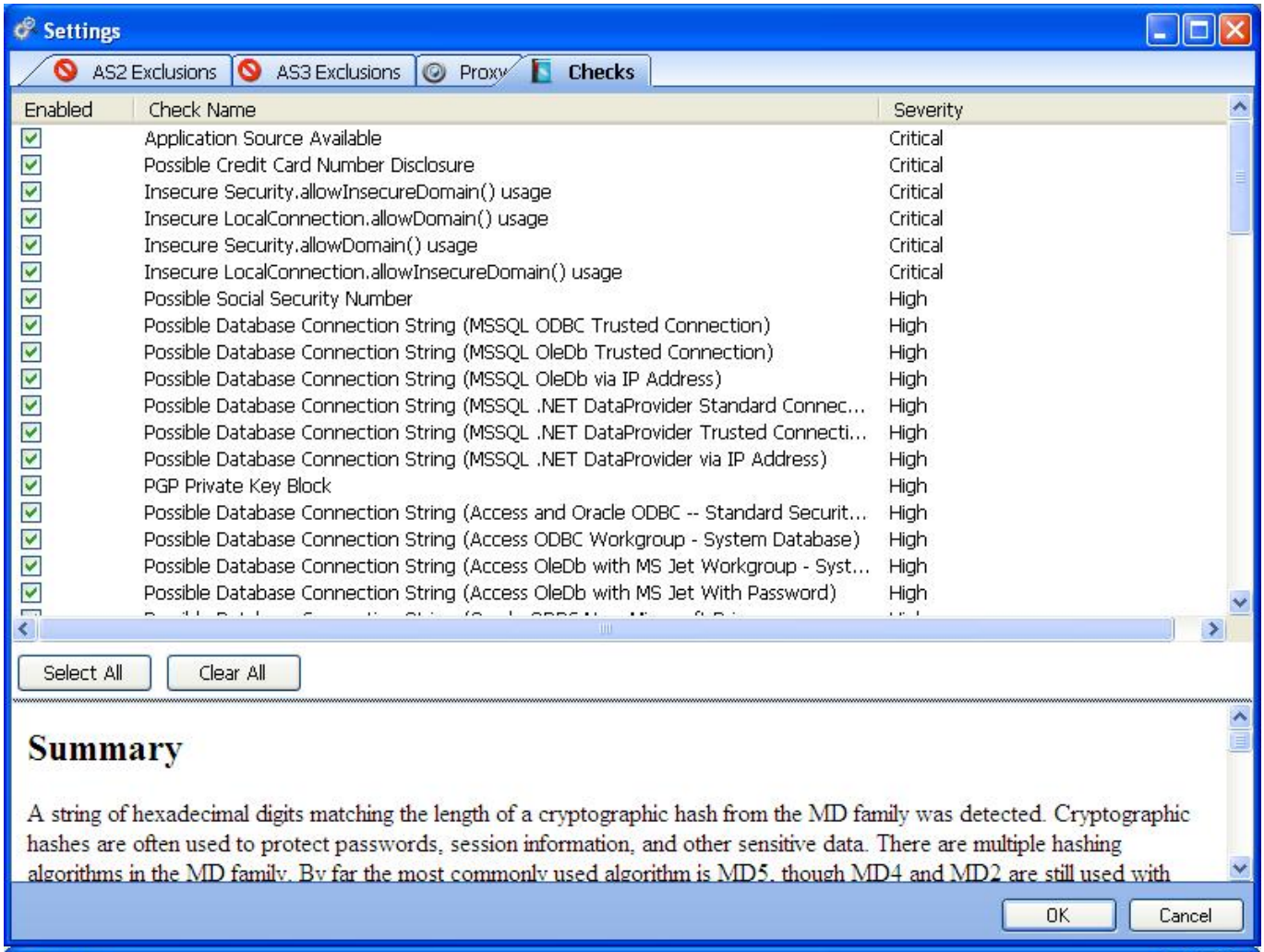


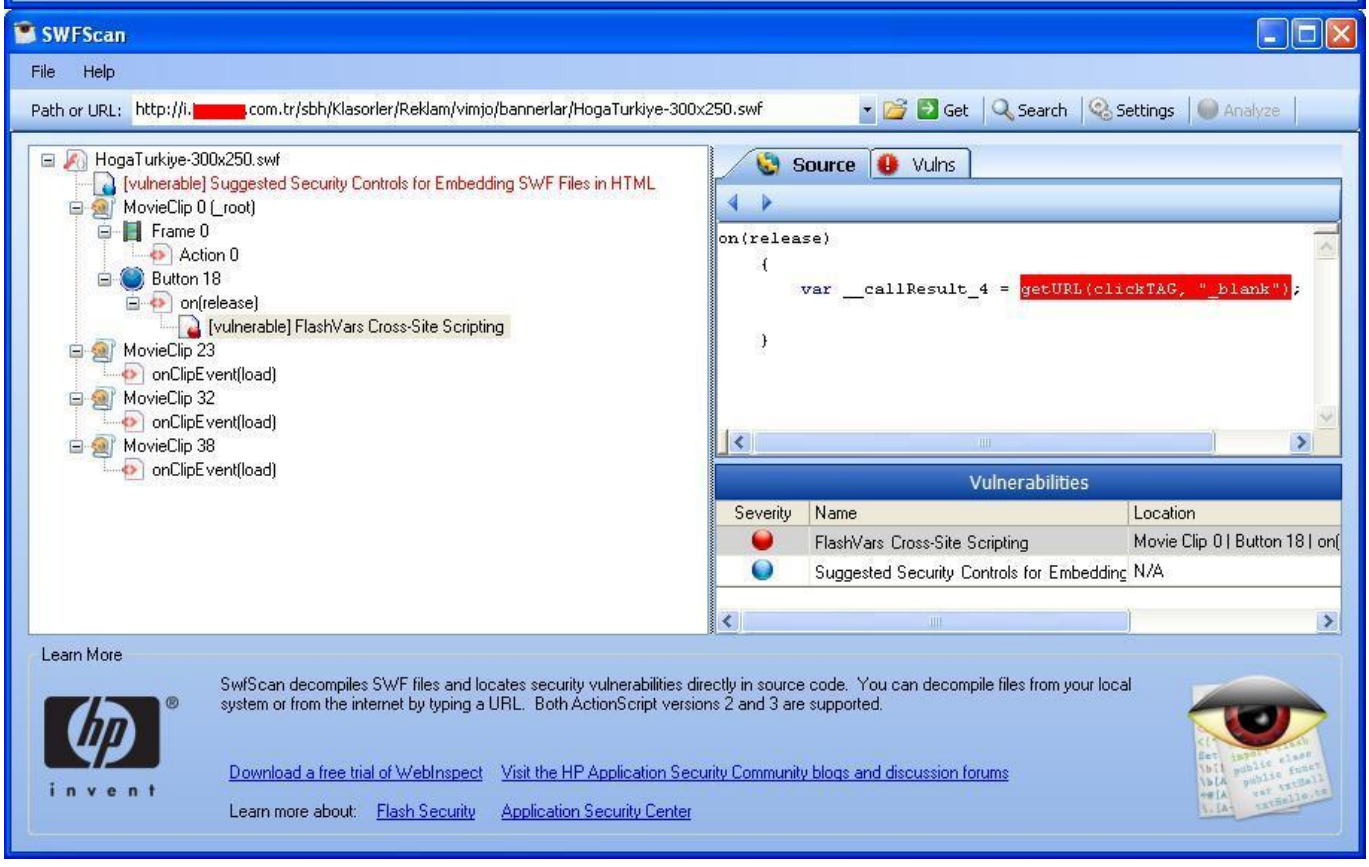


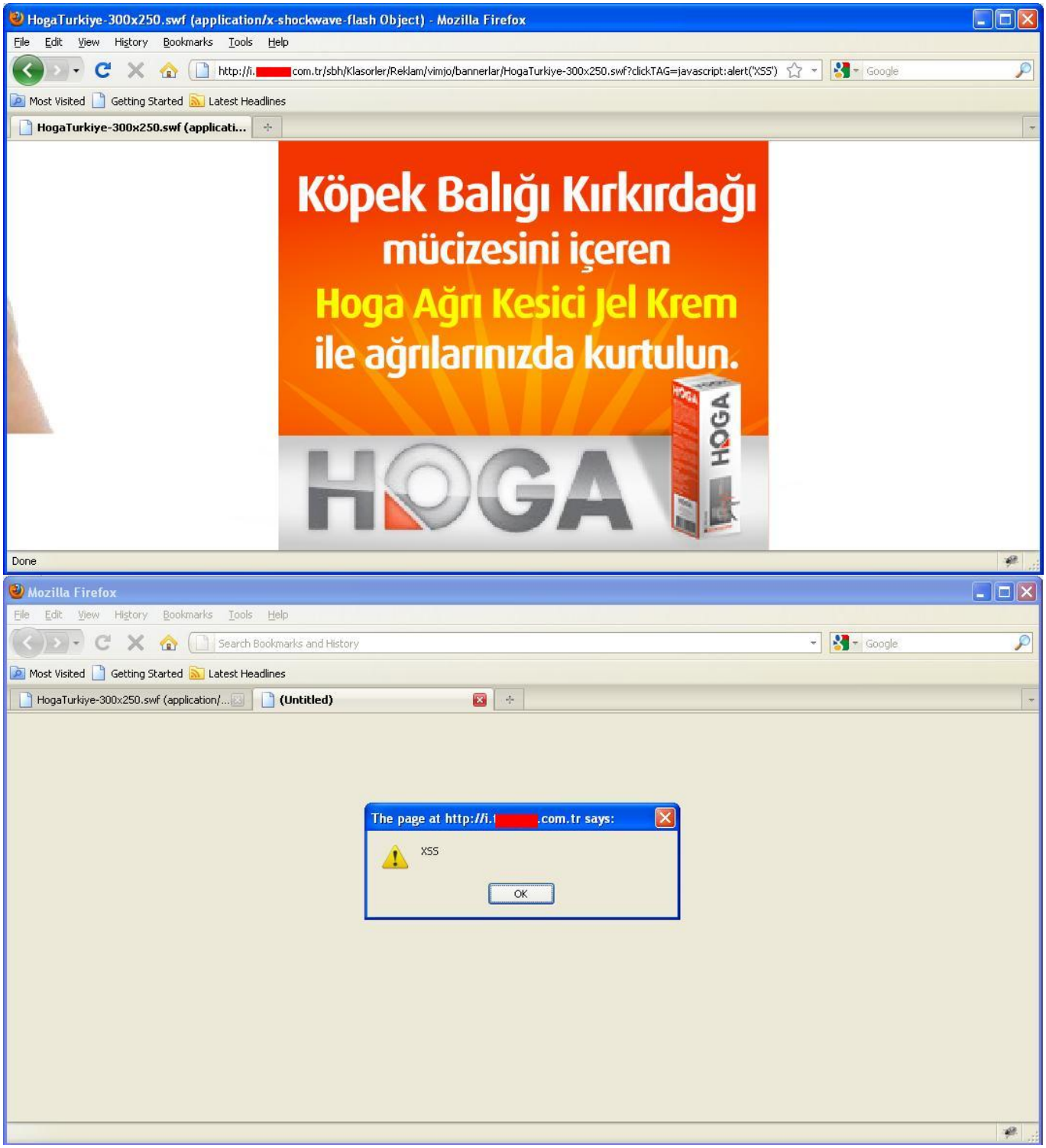
- Tersine çevirme(disassembling): Flash uygulamasına ait SWF dosyasını analiz etmek için kaynak koduna çeviremediğimiz durumlarda baytkodu okunabilir hale çevirebilir ve analizimizi gerçekleştirebiliriz. Analizle yetinmeyerek baytkoda müdahale edebilir ve SWF dosyasını yamayabiliriz. Kaynak koduna çevirdiğimiz ancak tekrar derleyemediğimiz durumlarda da bu yola başvurabiliriz. Bu iki durumda da hem tersine çevirme hem de yamama için RABCDasm aracından faydalanabilirsiniz. Örnek olarak bir oyun düşünün, kaynak koduna çevirmek mümkün ve analiz neticesinde yönetim paneli SWF dosyasının içinde yer alıyor ancak

uygulamayı derleyenler tarafından bu yönetim paneline ulaşmak mümkün değil çünkü bu actionscriptte yer alan ve bu panel ile ilgili olan fonksiyon oyunun yüklenmesi esnasında görünür değil. Ancak bu dosyayı tersine çevirerek (disassembling) müdahale edebilirseniz (patching) bu panelin yüklenme esnasında görünür hale gelmesini sağlayabilir ve yönetici paneline erişebilirsiniz. İşte tam olarak bu durumu konu alan bir zafiyeti geçtiğimiz aylarda kaşfederek oyunu geliştiren firma ile paylaştım ve düzeltilmesini sağladım. (Firma çalışanlarının samimi ve profesyönelce yaklaşımından dolayı kendilerini tebrik etmeden geçmeyeceğim. Farkındalığın arttırılması adına firma adını gizleyerek videoyu yayınlamamı sağladıkları içinde kendilerine ayrıca teşekkür etmek isterim.

- Zafiyet tarama araçları: Actionscript programlama dilide güvenli bir şekilde kullanılmadığı taktirde XSS, XSRF gibi zafiyetlere yol açabilmektedir. Özellikle URL kabul eden, işleyen fonksiyonlarda ve HTML kullanılan parametrelerde bu zafiyetlere sıkça rastlayabiliriz. Örnek olarak Flash ile hazırlanmış olan reklamlarda kullanılan clickTAG değişkeni güvenli kullanılmadığı taktirde XSS zafiyetine yol açabilmektedir. Bu ve benzer sorunları tespit etmek için Actionscript kodunu detaylı olarak analiz etmek gerekir ancak bu zaman alıcı bir iş ve çoğu kimse için uzmanlık gerektirebildiği için bunu gerçekleştiren programlardan faydalanabiliriz. HP SWFScan bu amaçla geliştirilmiş, hedef SWF dosyasını tersine çevirerek analiz eden ve 60’dan fazla güvenlik zafiyetini tespit edebilen ve raporlayabilen faydalı bir araçtır. Aşağıdaki ekran görüntüsüne bakacak olursanız rastgele olarak seçilmiş örnek bir sitedeki SWF dosyasında yer alan XSS (cross-site scripting) güvenlik zafiyetini başarıyla tespit edebildiğini görebilirsiniz. (SWFScan Actionscript 2 ve 3 sürümlerini desteklemektedir. 2 sürümü için ayrıca SWFIntruder aracınıda kullanabilirsiniz.) Bu tür araçlar kimi zaman güvenlik zafiyetlerini tespit edemeyebilirler bu nedenle her ihtimale karşı actionscripti analiz etmekte yarar olduğunu söyleyebilirim.


Settings
AS2 Exclusions
AS3 Exclusions
Proxy
Checks
Enabled
Check Name
Severity
Application Source Available
Critical
Possible Credit Card Number Disclosure
Critical
Insecure Security.allowInsecureDomain() usage
Critical
Insecure LocalConnection.allowDomain() usage
Critical
Insecure Security.allowDomain() usage
Critical
Insecure LocalConnection.allowInsecureDomain() usage
Critical
Possible Social Security Number
High
Possible Database Connection String (MSSQL ODBC Trusted Connection)
High
Possible Database Connection String (MSSQL OleDb Trusted Connection)
High
Possible Database Connection String (MSSQL OleDb via IP Address)
High
Possible Database Connection String (MSSQL .NET DataProvider Standard Connec...
High
Possible Database Connection String (MSSQL .NET DataProvider Trusted Connecti...
High
Possible Database Connection String (MSSQL .NET DataProvider via IP Address)
High
PGP Private Key Block
High
Possible Database Connection String (Access and Oracle ODBC -- Standard Securit...
High
Possible Database Connection String (Access ODBC Workgroup - System Database)
High
Possible Database Connection String (Access OleDb with MS Jet Workgroup - Syst...
High
Possible Database Connection String (Access OleDb with MS Jet With Password)
High
Select All
Clear All
Summary
A string of hexadecimal digits matching the length of a cryptographic hash from the MD family was detected. Cryptographic hashes are often used to protect passwords, session information, and other sensitive data. There are multiple hashing algorithms in the MD family. By far the most commonly used algorithm is MD5, though MD4 and MD2 are still used with
OK
Cancel


SWFScan
File
Help
Path or URL:
http://i.[redacted].com.tr/sbh/Klasorler/Reklam/vimjo/bannerlar/HogaTurkiye-300x250.swf
Get
Search
Settings
Analyze
HogaTurkiye-300x250.swf
[vulnerable] Suggested Security Controls for Embedding SWF Files in HTML
MovieClip 0 (_root)
Frame 0
Action 0
Button 18
on(release)
[vulnerable] FlashVars Cross-Site Scripting
MovieClip 23
onClipEvent(load)
MovieClip 32
onClipEvent(load)
MovieClip 38
onClipEvent(load)
Source
Vulns
on(release)
{
var __callResult_4 = getURL(clickTAG, "_blank");
}
Vulnerabilities
Severity
Name
Location
FlashVars Cross-Site Scripting
Movie Clip 0 | Button 18 | on(
Suggested Security Controls for Embedding
N/A
Learn More
SwfScan decompiles SWF files and locates security vulnerabilities directly in source code. You can decompile files from your local system or from the internet by typing a URL. Both ActionScript versions 2 and 3 are supported.
Download a free trial of WebInspect
Visit the HP Application Security Community blogs and discussion forums
Learn more about:
Flash Security
Application Security Center



Art niyetli kişilerin Flash uygulamalarınızı istismar etmesini zorlaştırmak için mutlaka action scriptinizi gizlemeli (obfuscation), Adobe tarafından güvenli uygulama geliştirme önerilerini dikkate almalı, hafızaya müdahale için saklanan değerleri kullanım sonrasında hemen değiştirmeli ve trafiğe müdahaleyi zorlaştırma adına sunucu ile uygulama arasındaki değerleri hashlemenizi tavsiye ederim.

Bir sonraki yazıda görüşmek dileğiyle…

Sunum dosyası: Powerpoint sürümü