

ENINE BOYUNA SIBER GÜVENLİK

Hasan Emre Özer

30 Ocak 2016 Cumartesi

hasanemre@invictuseurope.com

- Siber Güvenlik Araştırmacısı (ProDAFT)
- Siber güvenlik meraklısı, Linux sevdalısı, Bug Hunter
- Web uygulama güvenliği, Zararlı yazılımlar, Scada Sistemleri
- Nku IEEE Cs, Superbug üyesi
- Profesyonel hentbolcu (idi)
- @liselibeyy

- Hacker nedir, Hacker çeşitleri, farkları, ortak yönleri
- DeepWeb ve Tor ağı yapısı
- Kriptoloji
- Stegonografi
- Pentest
- Tempest
- Sosyal Mühendislik
- Bug Bounty Bug Hunter
- Güncel Olaylar
- Final

HACKERS

HACKER KIMDIR?

A close-up portrait of a man with light-colored eyes and a serious expression, looking directly at the camera. The lighting is dramatic, with one side of his face in shadow. The text "MR. ROBOT" is overlaid in a bold, red, stylized font across the lower half of his face.

MR. ROBOT

- Hacker, herhangi bir sistemi kullanım amacı dışında kullanan kişiye denir. (Can Yıldızlı)
- Hackerlar kendi içlerinde dil, din, ırk, yaş gözetmeksizin herkese eşit olarak yaklaşmaktadır.
- Statü olarak belirleyici etken tamamen bilgi seviyesidir.
- Hacker Etiği ve Hacker Manifestosu düşünce yapılarını özetlemektedir.
- Hackerlar farklı motivasyonlara sahip olabilmektedirler. Bu motivasyonlarından dolayı kendi aralarında gruplanmalar yaşanmıştır.

- Hacker
- Script kiddie
- Hacktivist
- Cracker
- Phreaker
- Penetration Tester
- Malware Analysist
- Reverse Engineer
- Cyber Crime Responser
- 0day Researcher

HEYKIRO

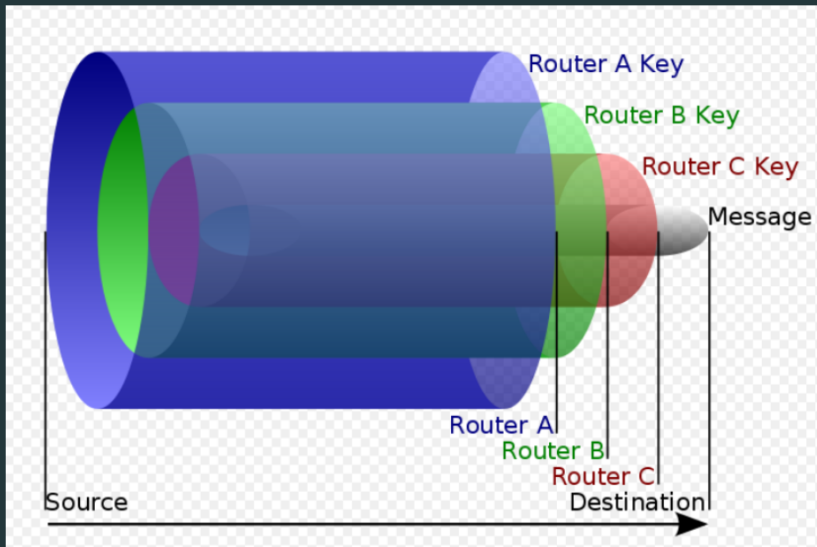


DEEPWEB VE TOR AĞI

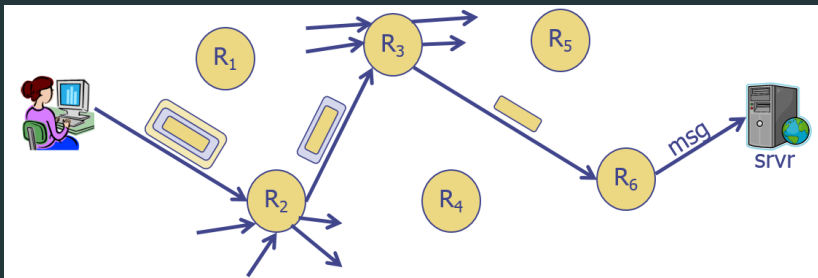
- Deep Web standart web tarayıcılarıyla ulaşılamayan, arama motorlarında listelenmeyen internet sitelerine verilen genel bir isimdir.
- İnternet sitelerinin isimleri anlamsızdır ve .onion gibi uzantıları vardır. Örnek: <http://3g2upl4pq6kufc4m.onion/>
- Tor ağına bağlanmak için firefox'un modifiye edilmiş hali olan tor browser kullanılabilir.

- Bağlantı sırasında giden veriler her node üzerinden geçerken şifreli bir şekilde iletilir.
- Her node'un kendine ait private ve public keyi mevcuttur. Tor algoritması bu paketi her bilgisayarın public keyiyle şifreler, sonrasında yollanan her bilgisayarda bu dosyanın katman katman şifreleri çözülür.
- Bağlantı tüneli oluşturulurken tüneldeki her bir node ile ortak bir anahtar belirlenir. Bu anahtar 'Diffie-Hellman Key Exchange' algoritmasına göre belirlenir ve tor network içinde gezinen verilerin şifrelenmesini sağlar.
- Veri sırayla tünel içindeki nodelar üzerinde ilerlerken bir soğanın katmanlarının içeri doğru açılması gibi her Tor unsurunda şifreli verinin bir katmanı açılır.
- Bağlantı sırasında giden veriler her node üzerinden geçerken şifreli bir şekilde iletilir.

DEEPWEB VE TOR AĞI



DEEPWEB VE TOR AĞI



packet =

$E_{pk_2}(R_3, \dots)$

$E_{pk_3}(R_6, \dots)$

$E_{pk_6}(svr, msg)$

- NoScript ile JavaScript/Flash/Java'yı devre dışı bırakmak.
- HTTPS Everywhere ile sadece HTTPS sayfalara bağlanmak.
- Firewall kuralları ile TOR'suz bağlantıları izin vermemek.
- Sanal makine kullanmak.

KRIPTOLOJI

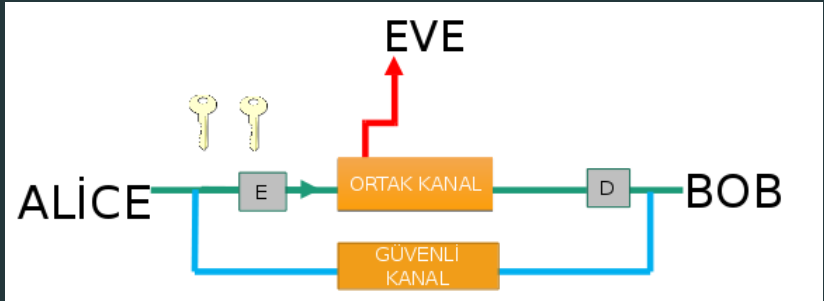
- Kriptoloji temelde, bilginin “şifrelenmesi” yöntemiyle tarafların bilgi alışverişi sırasında gelebilecek herhangi pasif veya aktif saldırıların bilgi güvenliğine, gizliliğine ve bütünlüğüne zarar vermesini veya erişmesini engellemektir.
- Eski örneklerden enigma verilebilir ,yeni olarak TrueCrypt, Kindle, Banka Kartları, telefonlar örnek olarak ele alınabilir.

- II. Dünya Savaşı sırasında Nazi Almanyası tarafından gizli mesajların şifrelenmesi ve tekrar çözülmesi amacı ile kullanılan bir şifre makinesi
- Savaş Nazi Almanyası tarafından üstünlükle giderken müttefikler gizli mesajları okuyabilmek için kriptocu ekipler toplamaya başladı. İngiliz kriptolog Alan Turing bu şifrelemenin üstesinden geldi ve savaş bu olaydan sonra yön değiştirdi. Müttefikler kazandı.

ENIGMA



SİMETRİK ŞİFRELEME



SIZCE ALGORITMA GIZLENMELİ MİDİR?

STEGANOGRAFI

- Steganografi, eski Yunanca'da "gizlenmiş yazı" anlamına gelir ve bilgiyi gizleme bilimine verilen addır. Steganografi'nin şifrelemeye göre en büyük avantajı bilgiyi gören bir kimsenin gördüğü şeyin içinde önemli bir bilgi olduğunu farkedemiyor olmasıdır, böylece içinde bir bilgi aramaz.
- Steganografi için kullanılan toollardan en bilineni steghide'dir.

STEGANOGRAFI DEMO

PENTEST

- Açılımı Penetration Testing, türkçesi sızma testi.
- Tam türkçe meali, gelin beni izinli, ahlaklı, namuslu bir şekilde hackleyin ve bana bunu nasıl yaptığınıza dair bir rapor yazın.
- Genel olarak sızma testleri web ve network uygulamalarına yönelik olarak yapılmaktadır.
- Türkiyede sızma testi uzmanlığı belgesi TSE tarafından verilmektedir.
- CEH, OSCP, ESCA, MBA , LPT, ISO 27001

- WhiteBox Testing
- BlackBox Testing

- Bilgi Toplama (Pasif/Aktif)
- Zafiyet Taraması
- Erişim kazanma
- Erişimden faydalanma
- İzleri yok etme

TEMPEST

- TEMPEST, cihazlardan yayılan ve cihazların işlediği bilgilerin ele geçirilebilmesine neden olabilecek elektromanyetik sinyallerin takip edilmesi ve engellenmesini kapsayan bir teknolojidir.
- Elektronik cihazlar çalışırken etrafa elektromanyetik enerji yayar. Yayılan enerji analiz edilerek o cihazın o an ne yaptığı hakkında fikir edinilebilir.
- Cihazlar etraftaki elektromanyetik enerjiden etkilenebilirler. Bu şekilde bir cihazı uzaktan yönetmek mümkün olabilir.

- Ofis ortamında monitörlerden sızan radyo sinyallerini oksiloskop, anten ve spectrum analiz cihazları ile inceleyerek görüntüyü elde etmek mümkündür.

ÖRNEK TEMPEST - EKRAN GÖRÜNTÜSÜ DİNLEME SALDIRILARI

The quick brown fox jumps over THE LAZY DOG

The quick brown fox jumps over THE LAZY DOG

The quick brown fox jumps over THE LAZY DOG

The quick brown fox jumps over THE LAZY DOG

The quick brown fox jumps over THE LAZY DOG

The quick brown fox jumps over THE LAZY DOG

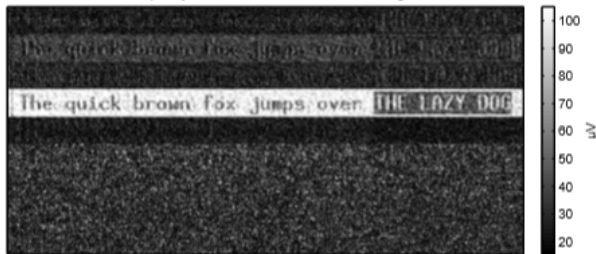
The quick brown fox jumps over THE LAZY DOG

The quick brown fox jumps over THE LAZY DOG

The quick brown fox jumps over THE LAZY DOG

ÖRNEK TEMPEST - EKRAN GÖRÜNTÜSÜ DİNLEME SALDIRILARI

324 MHz center frequency, 50 MHz bandwidth, 5 frames averaged, 3 m distance



648 MHz center frequency, 100 MHz bandwidth, 5 frames averaged, 3 m distance



SOSYAL MÜHENDISLIK

- Türkçe tabiri insan kandırma sanatı olarak nitelendirilebilir.
- Her sistem hacklenmeyebilir, fakat her insan hacklenir.
- En ünlü sosyal mühendisler Kevin Mitnick (The Condor), Christopher Hadnagy (HumanHacker)
- Zararsız görünen bilgiler zararlı olabilir
- Sosyal Medya hesapları bir tehdittir.
- Bana yardımcı olabilir misiniz/Size yardımcı olabilirim gibi sözler en etkilileridir.
-

- Telefonla görüşüyorsanız, yüz yüze görüşmeyi teklif edin. Bir takım hareketlerinden bazı şeyleri anlayabilirsiniz.
- Sürekli yetkili birisi olduğunu söylemesi
- Teklifinin yerine getirilmemesi dahilinde kötü sonuçlar doğuracağı.
- Aciliyetin üzerine vurgu yapılması.

Çoğu zararlı yazılım ve saldırı türünde kötü adamlar erişim sağlamak için sosyal mühendislik tekniklerinden faydalanırlar. Teknik zafiyetleri yamalamak mümkün olsa da, insan aptallığı ve saflığı için bir yama yoktur. Chris, günümüzün sosyal mühendislik saldırılarını ortaya koyarak, bu tekniklerin nasıl işlediğini gösteriyor. Bu kitap, sosyal mühendislik saldırılarının nasıl fark edilebileceği ve önlenebileceğine ilişkin daha iyi bir içgörü kazanmanıza yardım edecek.

KEVIN MITNICK, Yazar, Konuşmacı ve Danışman



BUG BOUNTY BUG HUNTER

- Bug Bounty, web, mobil, masaüstü ve bunlar gibi yazılımlarında gözden kaçırdıkları hataları hackerlar aracılığıyla tespit etmek, aynı zamanda hackerların bu zafiyeti kötüye kullanmasını önlemek amacıyla çeşitlik ödüller sundukları projedir.
- Bug bounty programlarına katılan, bu yazılımlarda zafiyet bulan kişilere Bug Hunter denir.
- Scope, mail yazma ve raporlama teknikleri çok önemlidir.
- Bug bounty programlarında en fazla bilinen kurumlar: Google, microsoft,yandex, facebook,apple,twitter gibi dünyaca ünlü firmalardır.

the unofficial **HackerOne** disclosure timeline.

text to filter reports

ownCloud disclosed a bug submitted by **ashesh** 27 Jan 2016 ☹
[s2.owncloud.com: SSL Session cookie without secure flag set](#)

ownCloud disclosed a bug submitted by **d0znpp** 27 Jan 2016 ☹
[XXE at host vpn.owncloud.com](#)

HackerOne disclosed a bug submitted by **00day** 27 Jan 2016 ☹
[Team Member\(s\) associated with a Group have Read-only permission \(Post internal comments\) can post comment to all the participants](#)

Mail.Ru disclosed a bug submitted by **harry_mg** 27 Jan 2016 ☹
[Multiple vulnerabilities in mail.ru subdomains](#)

HackerOne disclosed a bug submitted by **intidc** 26 Jan 2016 ☹
[HTML injection can lead to data theft](#)

Twitter disclosed a bug submitted by **wesecureapp** 25 Jan 2016 ☹
[IDOR- Activate Mopub on different organizations- steal api token- Fabric.io](#)

Square Open Source disclosed a bug submitted by **bburky** 25 Jan 2016 ☹
[git-fastclone allows arbitrary command execution through usage of ext remote URLs in submodules](#)

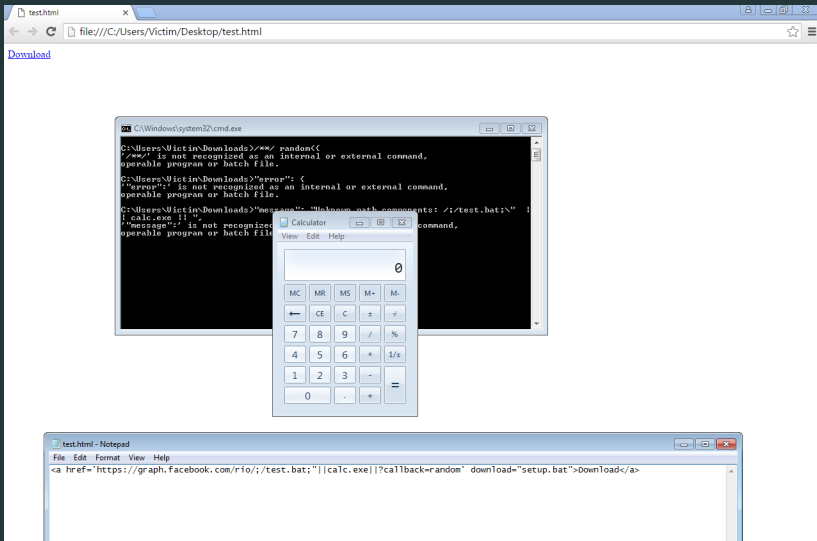
Square Open Source disclosed a bug submitted by **bburky** 25 Jan 2016 ☹
[Unsafe usage of Ruby string interpolation enabling command injection in git-fastclone](#)

ownCloud disclosed a bug submitted by **haiderkamal** 23 Jan 2016 ☹
[owncloud.help: Text Injection](#)

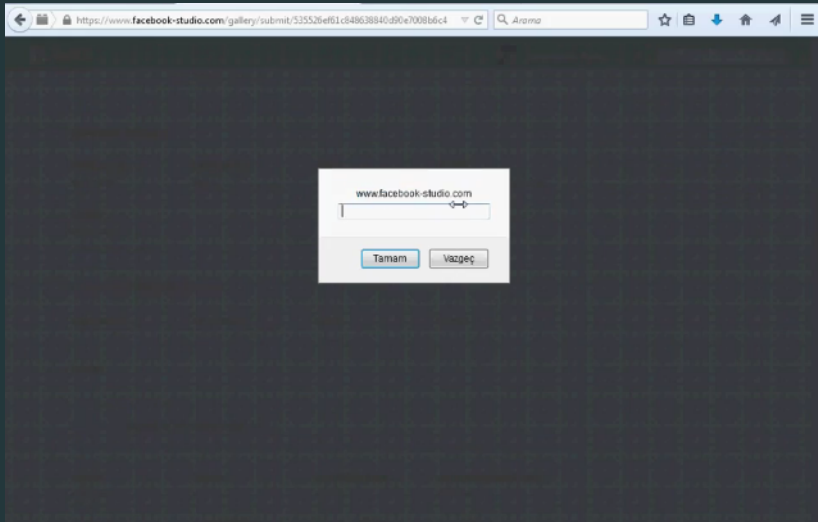
TWITTER ÖDÜL

Vulnerability	Core Twitter [1]	All Other
Remote Code Execution	\$15,000	\$10,000
Significant Authentication Bypass	\$7,500	\$5,000
Cross Site Scripting that can perform critical actions [2] [3]	\$2,500	\$1,500
Cross Site Request Forgery on critical actions [2]	\$2,500	\$1,500
All other Cross Site Scripting [3]	\$1,000	\$500
All other Cross Site Request Forgery	\$250	\$140

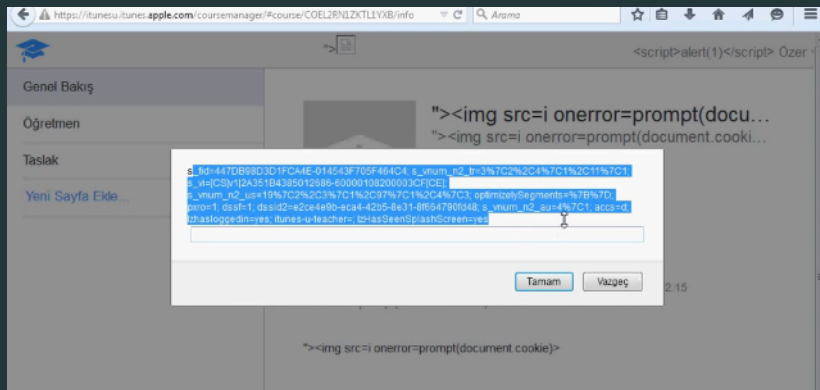
FACEBOOK REFLECTED FILE DOWNLOAD



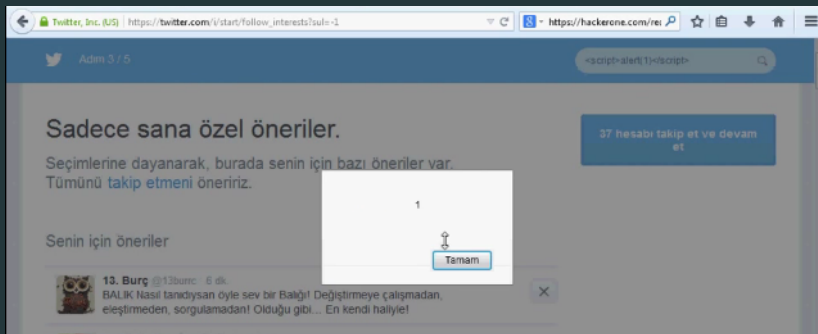
FACEBOOK STUDIO XSS



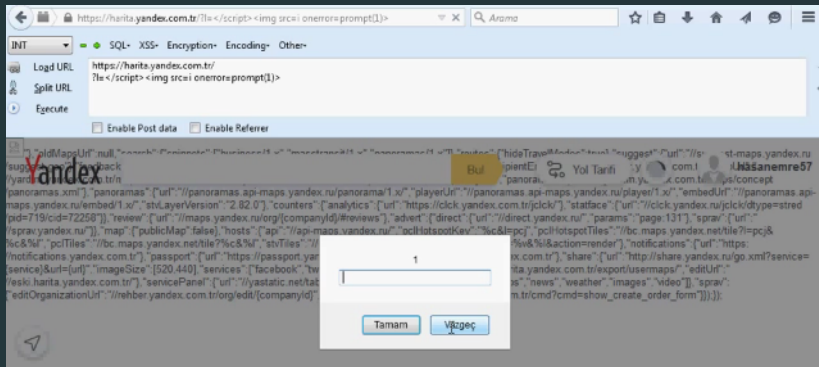
APPLE XSS



TWITTER XSS



YANDEX XSS




DRUPAL 7 SQL INJECTION

#31756

Drupal 7 pre auth sql injection and remote code execution

Share:      

State ● Resolved (Closed)

Participants  

Disclosed publicly **April 6, 2015 12:40pm +0300**

Types Remote Code Execution, SQL Injection

Bounty **\$3,000**

[Collapse](#)

GÜNCEL OLAYLAR

- SHELLSHOCK

- ISIS Siber Halifeleri

- Adobe'un Flash'tan desteğini çekmesi

- Cryptolocker Analizi

SORULAR?