HIGHLIGHTS DER APPSECEU UND HACK IN THE BOX

62. MÜNCHNER OWASP STAMMTISCH


OWASP AppSecEU 2015
Amsterdam, The Netherlands
19-22 May 2015

ÜBERBLICK

- Agenda
  - Trainings
    - 2015-05-19 – 2015-05-20
  - Tracks
    - 2015-05-19 – 2015-05-20
    - DEV,OPS,HACK,CISO,HACKPRA
  - Social Event
    - Dinner@Nemo
- Rates
  - 75/350/400
  - 75/500/550

MY SCHEDULE

- 50 Shades of AppSec
  - Troy Hunt
- Hard knock lessons on bug bounties
  - Jonathan Cran
- Rise of the Machines
  - Yossif Daya
- Server-side browsing considered harmful
  - Nicolas Grégoire

MY SCHEDULE

- Dark Fairytales from a Phisherman
  - Michele Orrù
- Security and Insecurity of HTTP Headers
  - Dirk Wetter
- PDF – Mess with the Web
  - Alex Infuhr

50 SHADES OF APPSEC

Troy Hunt

- „Everybody can become a hacker“
  - LOIC
- Security Fails
- Educating developers
  - Stackoverflow
  - Insecure Code Samples

HARD KNOCK LESSONS ON BUG BOUNTIES

Jonathan Cran

- Bugcrowd Erfahrungen
  - Can I start a bug bounty program?
  - What is the scope?
  - How do you handle reports?
  - Rewards?

RISE OF THE MACHINES

Yossif Daya

- Akamai experience with Crawlers/Scraper
- Detection
  - Signatures
  - Profiling
- Mitigation/Management
  - Block
  - Throttle
  - Allow

SERVER-SIDE BROWSING CONSIDERED HARMFUL

Nicolas Grégoire

- Server-side attacks
- Bug Bounty examples

DARK FAIRYTALES FROM A PHISHERMAN

Michele Orrù

- Presentation of PhishLulz
  - PhishingFrenzy
  - BeEF
- Phishing Fairytales

SECURITY AND INSECURITY OF HTTP HEADERS

Dirk Wetter

- Information Disclosure
- HSTS
- Public-Key-Pins
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection
- Content-Security-Policy

PDF – MESS WITH THE WEB

Alex Infuhr

- PDF Specs
- Protection
- Attack Vectors
  - No bug = no fix

PRESERVING ARCADE GAMES

Ange Albertini

- Erhaltung von Oldie-Games
- Kopierschutz 80er
  - Hardwareschutz


HITB
HITBSecConf
AMSTERDAM // MALAYSIA

ÜBERBLICK

- Agenda
  - Trainings
    - 2015-05-26 – 2015-05-27
  - Tracks
    - 2015-05-28 – 2015-05-29
    - Track1, Track2, Labs
- Rates
  - 299/999
  - 299/1499

MY SCHEDULE

- Illusory TLS: Impersonate, Tamper, and Exploit
  - Alfonso de Gregorio
- How many Million BIOSes would you like to exploit
  - Corey Kallenberg, Xeno Kovah
- Exploiting Browsers the Logical Way
  - Bas Venis

MY SCHEDULE

- Stegosploit: Hacking with Pictures
  - Saumil Shah
- Powershell for Penetration Testers
  - Nikhil Mittal
- Mozilla InvestiGator
  - Julien Vehent

ILLUSORY TLS: IMPERSONATE, TAMPER, AND EXPLOIT

Alfonso de Gregorio

- Underhanded Crypto Contest entry
- Young and Yung elliptic curve asymmetric backdoor in RSA key generation
- Attacker controlled PRNG seed
  - „The upper order bits of the RSA modulus encode the asymmetric encryption of a seed generated at random“

HOW MANY MILLION BIOSES WOULD YOU LIKE TO EXPLOIT

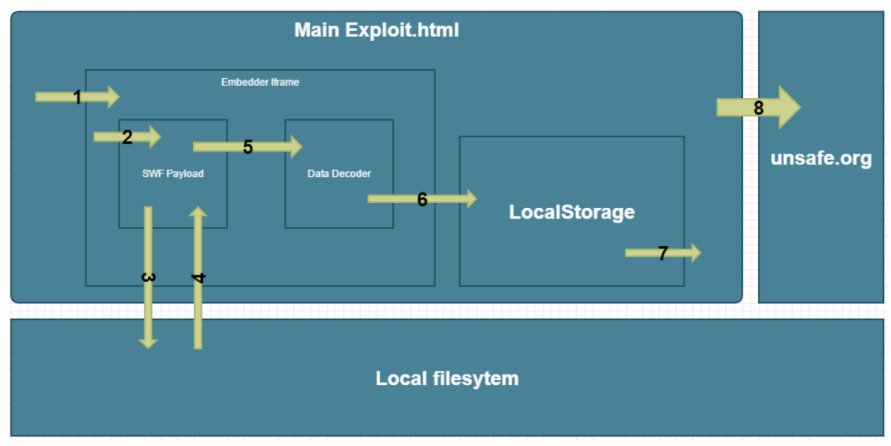
Corey Kallenberg, Xeno Kovah

- BIOS-Rootkit LightEater
- Infect System Firmware
  - System Management Mode

EXPLOITING BROWSERS THE LOGICAL WAY

Bas Venis

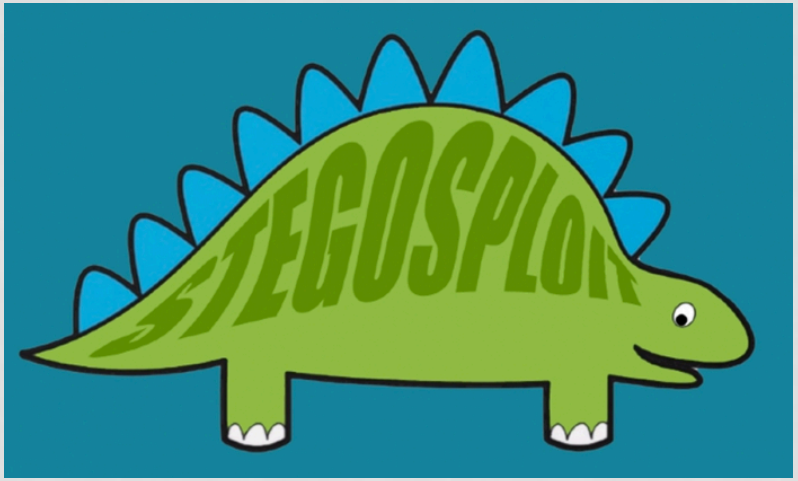
- Samples of Logic Bugs
- CVE-2014-0508
  - Read local file and send
- CVE-2014-0535
  - Now with access to remote files
- CVE-2014-0554
  - Recycled CVE-2014-0508



STEGOSPLOIT: HACKING WITH PICTURES

Saumil Shah

- Deliver Browser Exploit using pictures
  - Stylish
  - Undetected
- CANVAS+JS
  - Polyglot (image/js)
- Time-shifted delivery



POWERSHELL FOR PENETRATION TESTERS

Nikhil Mittal

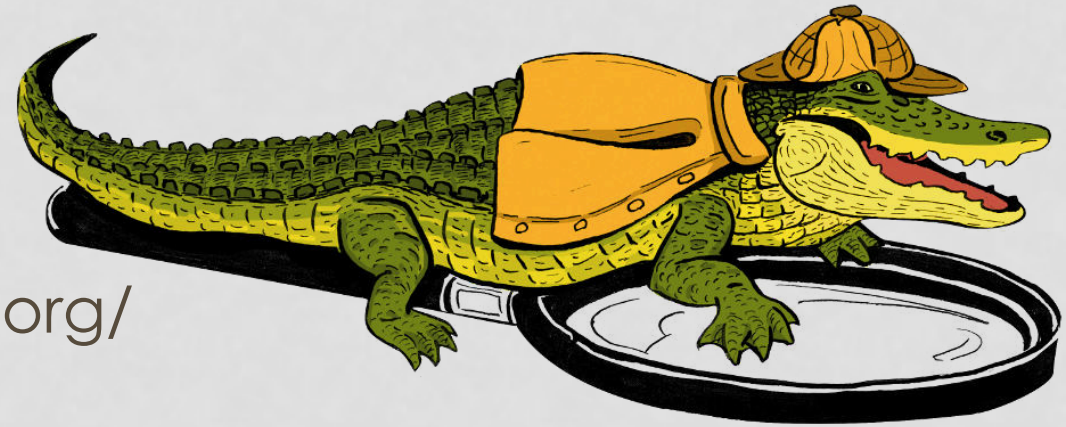
- This workshop would help anyone who wants to know more about PowerShell from a security perspective

- https://github.com/samratashok/nishang

MOZILLA INVESTIGATOR

Julien Vehent

- Forensics framework built by OpSec
  - „Query a pool of endpoints to verify the presence of a specific indicators“
  - „Provide strong authentication of investigators“
- http://mig.mozilla.org/



HITBHaxpo

ÜBERBLICK

- Agenda
  - Briefings
    - 2015-05-26 – 2015-05-27
  - CTF
- No charge

HIGHLIGHTS

- Minix 3 - A Reliable and Secure Operating System
  - Andrew S. Tanenbaum
- The A-to-Z of CyberSecurity – as a Kid Understands It
  - Reuben Paul