HackMiami

HTML5 Threat Landscape: Past, Present, and Future
Prepared for Devcon5 LA - December 2013
Alexander Heid - @alexheid

About Me

Alexander Heid

President, CEO of HackMiami

Fmr. Chair of S. FL OWASP

I break stuff and steal online things.

I like to computers and internet.

@alexheid & @hackmiami on

“Internet is srs bizns.” - Me.

About HackMiami

These are our most common engagements, things stay interesting and busy - www.hackmiami.org/services/

- Web/Mobile/**HTML5** Vulnerability Assessments
- Training Seminars
- Speaking Engagements
- Capture the Flag Tournaments & other real life manifestations of digital entertainment
- Website and social network optimization
- Server configuration hardening
- Annual conference

What we will discuss...

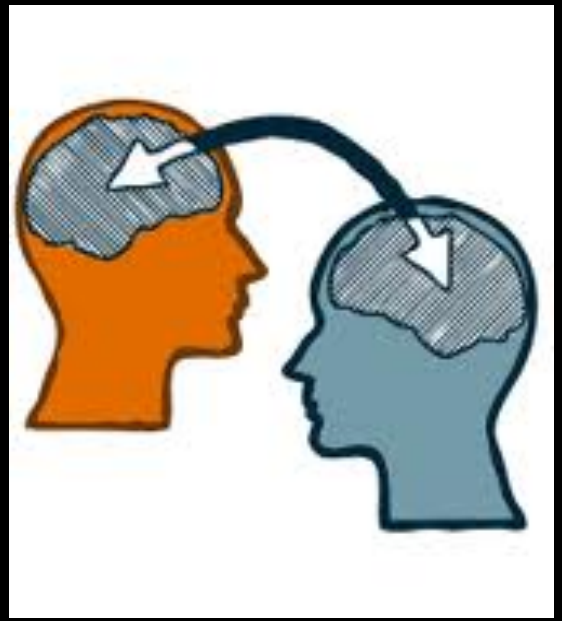
Improvements & Backpedals

Underground Attack Methods

Common Attack Tools & Techniques

Emerging Technologies & Threats

Solutions to identified security risks

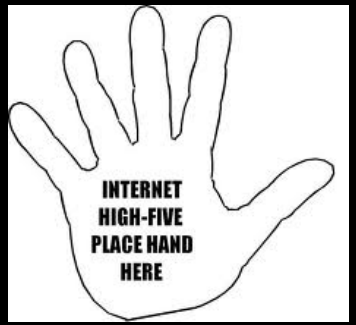


Improvements over the years...

Awareness of vulnerable functions is more commonplace among developers

Awareness has increased about the need for application security and 3rd party vulnerability assessments.

Cryptocurrency technology has emerged as a way to engage in e-commerce while avoiding the risks of credit cards such as chargebacks.



Things also got worse...

Things that stayed the same... or got worse…

- Larger user base means a larger need for security awareness and practices.
- More nulled scripts, more insecure proprietary plugins for open source frameworks.
- More abandoned small websites online from all over the world providing opportunities for attackers to harvest botnets made of servers and VPS.
- More new ways to steal things and more new things to be stolen.
- All this is bad.

Underground Attack Methods

Reconnaissance / Information Gathering – Attackers use OSINT methods
Gain access – SQL injection, RFI, LFI, weak pws, reused pws, etc.
Maintain Access – Backdoor the target for persistence, PHP shells
Identify Valuables - Attackers just want valuables: Billing info, email/passwords, and server resources
Escalate Privileges – Use local exploit to get root/admin access
Ex-filtrate Data – Transfer the database, source code and other valuables
Cover Your Tracks – Remove all logs and traces of activity, if possible.

New Vectors of Attack

Technologies that were previously experimental are now being widely deployed

Mobile everything / tablet everything

HTTP based APIs – Everything can talk to everything

Web apps for physical security controls

Virtualization (teh cloud)

Attacks against hypervisors and VM management CMS will lead to bulk compromises

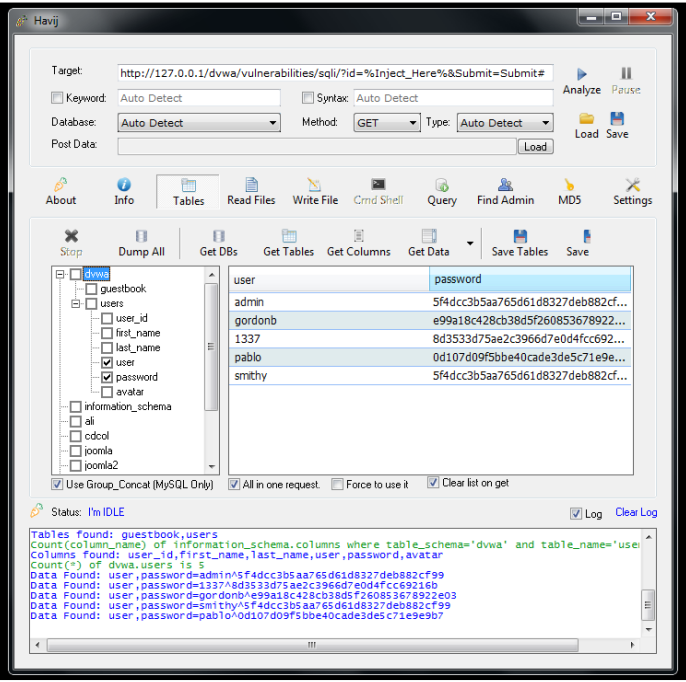
Cryptocurrency theft (Bitcoin, Litecoin)

New complex technology with API support and diverse user base

Server Side Attack Tool (SQLi)

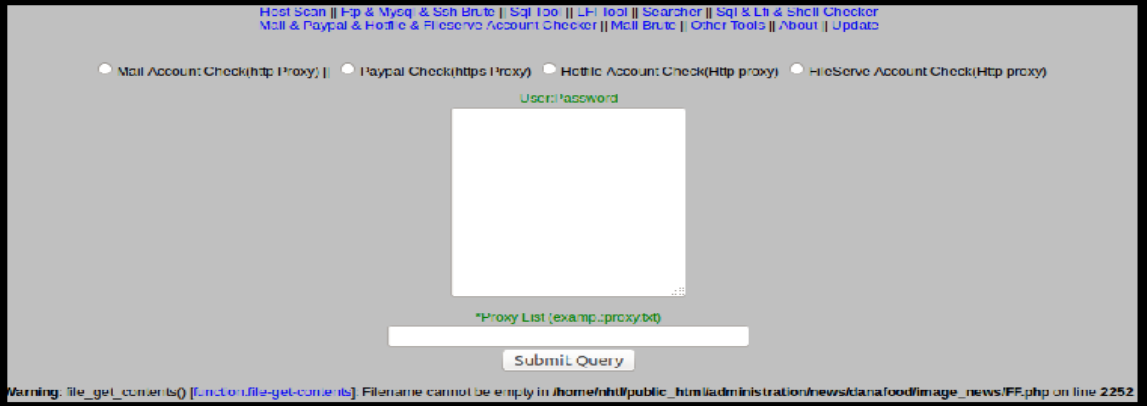
Havij SQL Injection Tool

Script kiddie tool with great powers to unearth admin creds and dump SQL dbs on poorly configured applications.



Credential Attack Tool (Checkers)

* Checkers are used by fraudsters to check the valid rates on compromised email:passwords, credit cards, and other account logins of value.



HTML5 Attack Vectors

HTML5 extended functionalities create new vectors of attack

- New vectors of XSS
- Client Side SQLi
- Proliferation of third party libraries
- SSO/OAuth

Technology moves forward, as it also moves backwards

Bank Wire Fraud

Bank wire fraud is made simpler by mobile devices, which rely on lightweight HTML5 apps

Old methods of CSRF style wire fraud made difficult by improved session handling and multi factor authentication implementations, such as SMS messaging

Infecting a mobile device allows for the defeat of multi factor authentication

Infecting a device and obtaining OAuth/SSO credentials allows for takeovers as valuable as taking over an e-mail address.

Zeus for Android?

Zeus has been used in conjunction with SMS malware and observed in the wild as a multidevice infection that seeks to engage in wire transfers of targets.

Old tools, new method

http://blogs.mcafee.com/mcafee-labs/dissecting-zeus-for-android-or-is-it-just-an-sms-spyware

Client Side Attack - XSS

Cross Site Scripting and Cross Site Sharing (XSS)

New functionalites of HTML5 and heavy reliance of javascript presents new vectors of client side code execution.

Do not trust an applications to pass safe input to each other. One app talking to another app without being sanitized can still cause problems.

Cross Site Sharing Attack

Client Side Attack - SQLi

HTML5 can use of client side SQL databases to store application data

Traditional SQL injection attacks focus on attacking the back end SQL server through the application. The goal is to be able to read/write data from nonpublic SQL tables and columns through the web application vulnerability.

Client side SQL injection attacks the dynamic database that is stored on the user machine.

In mobile applications this can include user credentials.

DO NOT STORE USER CREDENTIALS IN PLAINTEXT IN THE DATABASE.

Webservice/API/Attack Vectors

Authentication Bypass
If a backend service is only making use of basic authentication, improper configuration of .htaccess could allow for authentication bypass with tools like HTExploit.

CSRF Attacks

For Improper authentication or use of GET/POST or excessive HTTP methods can lead to compromise via web service/API

DDoS Attacks

Webservices and the servers that house them may not be hardened to anticipate large amounts of traffic. Mobile devices are lightweight, and the server may experience a large attack in the form of a different kind of traffic flood.

Old Vectors, More Targets

Old Attack Vectors Being Used in New Ways, en masse

Joomla, Wordpress, Drupal, Everything else too: Plugin Exploitation

Attackers able to take advantage of plugins such as Timthumb, JCE, and other vulnerable libraries as well as abandoned VPS providers.

```
#############################################################
# Description : Wordpress Plugins - HTML5 AV Manager for WordPress Shell
Upload Vulnerability
# Version : 0.2.7
# Link : http://wordpress.org/extend/plugins/html5avmanager/
# Plugins : http://downloads.wordpress.org/plugin/html5avmanager.0.2.7.zip
# Date : 26-05-2012
# Google Dork : inurl:/wp-content/plugins/html5avmanager/
# Author : Sammy FORGIT - sam at opensyscom dot fr -
http://www.opensyscom.fr
#############################################################
```

Cryptocurrencies

Bitcoin, Litecoin, *coin

Bitcoin and Litecoin has revolutionized global payment processing. Torrents, but for money.

HackMiami whitepaper on the topic:

'Analysis of the Cryptocurrency Marketplace' – http://www.hackmiami.org/whitepapers/HackMiami-Analysis_of_the_Cryptocurrency_Marketplace.pdf

New things to steal, new ways to steal them. Mostly application level attacks.

http://www.extremetech.com/computing/164134-how-bitcoin-thieves-used-an-android-flaw-to-steal-money-and-how-it-affects-everyone-else

Solutions to Vulnerable Code?

SDLC – Secure Development Life Cycle + ongoing assessments

Ongoing vulnerability assessments throughout the product development life cycle can go a a long way to prevent vulnerabilities from cropping up unexpectedly at the end of a project, right before it is deployed into production. These delays can make or break a release.

Break it early on, so you don't have to rebuild it later.

OWASP Source Code Analysis Tools

https://www.owasp.org/index.php/Source_Code_Analysis_Tools

Solution to MFA Problem?

OAuth and SSO functionalities create vulnerabilities where a compromised social networking account is as valueable as a compromised e-mail, and visa versa

The Yubikey is an open source 'something you have' solution that is nullifies the security issue of compromised user credentials, as users must fall prey to a social engineering attack to be fully compromised.

Yubikey.org

Solutions?

Fully understand functionality capabilities before deployment – intended functionality does not limit possible functionality (i.e., eval(); and exec();)

Have trusted 3rd party do a comprehensive vulnerability assessments on production applications.

Harden server configurations - .htaccess and index.html is ur friend

Research the latest public application threats by following security and exploitation mailing lists

Participate in your local hackerspaces and **OWASP** groups to meet talented like minded people who are open to trade information about programming and exploitation research.

Resources

OWASP - http://www.owasp.org

HTML5 Cheat Sheet - https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet

HTML5 Exploits - http://www.html5exploits.com

OWASP XSS Filter Evasion Cheat Sheet - https://www.owasp.org/index.
php/XSS_Filter_Evasion_Cheat_Sheet

OWASP SDLC Cheat Sheet (needs your contributions) - https://www.owasp.
php/Secure_SDLC_Cheat_Sheet

Yubikey – http://www.yubikey.org

OWASP Source Code Analysis Tools - https://www.owasp.org/index.
php/Source_Code_Analysis_Tools

Thanks!

Thanks to CrossFire Media and DevCon5 for bringing me out here!

If you are interested in having HackMiami take a look at your webapp or server, hit me up alex@hackmiami.org

Any questions?

Hack Miami CONFERENCE 2014 MAY 09-11, 2014 Miami Beach, Florida

Email me: alex@hackmiami.org
Twitter: @alexheid && @hackmiami
Websites: http://www.alexanderheid.com | http://www.hackmiami.org