An approach to Web Application Penetration Testing

By: Whiskah

- #whiskah
- Security enthusiast
- NOT a CI$$P, CIS*, GIAC, MCS*, CCN*
- NOT Lulzsec or Anonymous :)

Don’t be confused

Vulnerability assessment – identify, verify and rank vulnerabilities

Penetration testing – identify, analyze and exploit vulnerabilities to prove that systems can be compromised. (Result: Fail or Succeed)

Agenda

- An approach to web application penetration testing
- NOT a technical discussion about webappsec f00
- Buy me a beer later to discuss webapp kungfu

So?

- You are tasked to pentest a webapp?
  - What do you do?
  - Where do you begin?

Common Approach

- Immediately bang a web app scanner against the target and generate a report

- Use checklists only without exploiting issues identified

Issues: Web App Scanners

- Are good at finding technical vulnerabilities (sqli, xss, LFI, RFI etc…) but they don't understand business context or logic flaws
- In short...they lack the human creativity of an experienced pentester

Issues: Checklists

- Can be used as baseline for checking for missing controls but it cannot simulate a real attacker or adversary

- Missing controls (e.g Lack of encryption, lack of session timeout etc…)

Recommended Approach

- Create a threat profile for the target application
- Create a test plan
- Perform the test
- Prepare the report

I. Threat Profiling

- Think of what an adversary want to achieve by attacking the application (Think in terms of C.I.A.)

- As the owner of the application, what are you worried about

- A threat profile is the set of all threats the application should protect against

Why Threat Profile?

- Allows the tester to design test cases that achieve the adversary’s goals

- Allows the tester to focus on interesting variables quickly

E.g. file.php?lang=en

Sample Threat Profile/Attacker Goals: Online Banking

- Unauthorized fund transfers
- Unauthorized bills payment
- Unauthorized access to SOA
- Gain access to customer data
- Etc …

II. Create a test plan

- Map the threat profile to the relevant pages in the application.

- Determine what attacks to perform to realize the threat profile (hacker creativity)

  - Web app attacks (logic flaws, xss, sqli, lfi, rfi, csrf etc..)

Sample Test Plan: Online Banking

- Unauthorized fund transfer – maps to the funds transfer page(s)

Example attack:

- Parameter manipulation – manipulate the source or target accounts

  fundtransfer.php?src=acntA&target=acntB

- Attempt to transfer funds even if the source accounts have zero balance
- Attempt negative values

Sample Test Plan: Online Banking

- Unauthorized bills payment – maps to the bills payment page(s)

Example attack:

- Parameter manipulation – manipulate the source or target accounts
- Attempt to pay bills even if the source accounts have zero balance
- Use negative values

Sample Test Plan: Online Banking

- Gain access to customer data – identify page(s) that can be SQL injected

Example attack:

- SQL Injection

III. Perform the Test

- Execute the approved test plan
- New ideas may come up during this phase. Update the test plan as needed
- Combine both automated scanners with manual tests
- When a vulnerability is found, take a step-by-step screen capture of the attack

IV. Prepare the report

- Include an Executive Summary for top management & a more detailed Technical Report for I.T. Personnel/Staff

(*Prepare a DRAFT report and send to the client for review) Why?

Reporting: Executive Summary

- A high level overview of the test. Who?, What? When?, Scope, Purpose, Methodology, Limitations.
- A summary of key findings that would affect business along with recommendations
- Use non-technical language. Relate how the findings can affect busine$$

Reporting: Executive Summary

Which do you think would have more impact to a CEO?

“Pentest Co. was able to identify xss,sqli in ACME Bank application”

or

“Pentest Co. was able to transfer $100000 from CEO’s account to a dummy account”

Reporting: Technical Report

- More Detailed findings suitable for IT managers/staff
- Include references to web application research papers or OWASP
- Step-by-step of the attack even my grandma can reproduce :-D
  - educate developers into developing secure code
  - educate client

Recommended Approach

- Create a threat profile for the target application
- Create a test plan
- Perform the test
- Prepare the report

KTnxBye!

Questions?

Credits:

www.ivizsecurity.com
www.plynt.com