



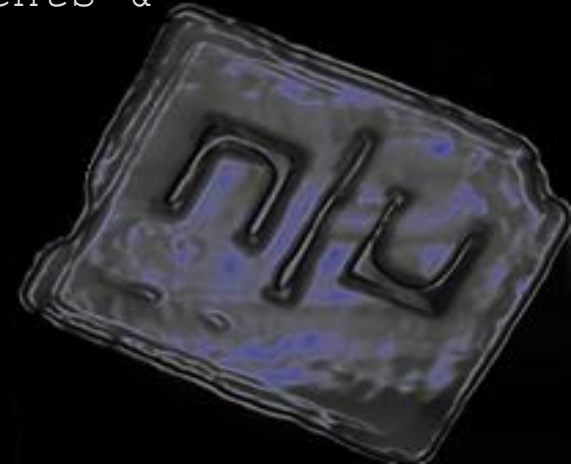
Penetration Testing versus Source Code Review

-Nikhil Waghlikar

Practice Lead | Security Assessments &
Digital Forensics

www.niiconsulting.com

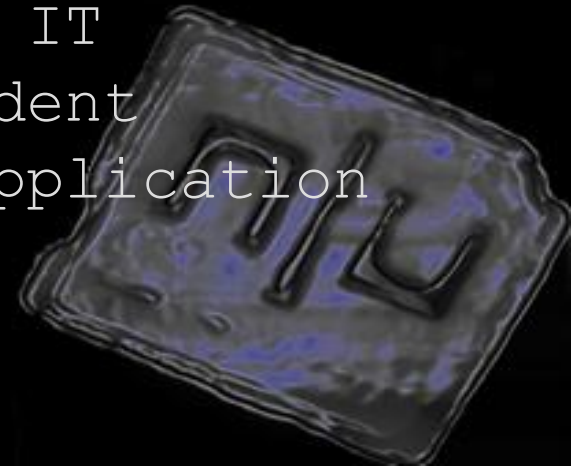
nikhil@niiconsulting.com





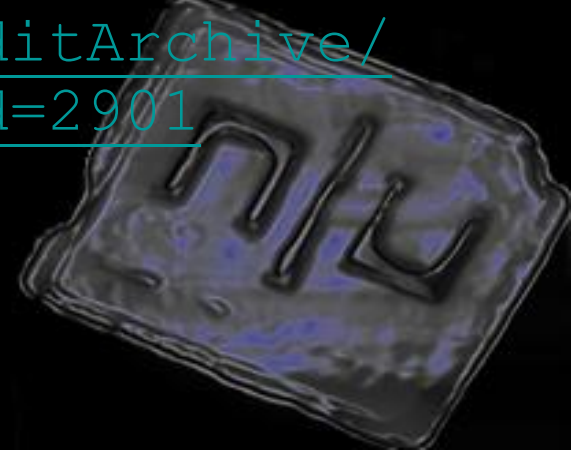
Nikhil Waghlikar- Speaker Profile

- CEH, ISO 27001|LA
- Penetration testing, Security Auditing, Digital Forensics, GRC, Solutions, Performance Auditing
- Numerous India and Middle East based clients
- Conducted training on various fields of Information security like GRC, IT Security, Green IT, VAPT, Incident Response, Digital Forensics, Application Security



Articles

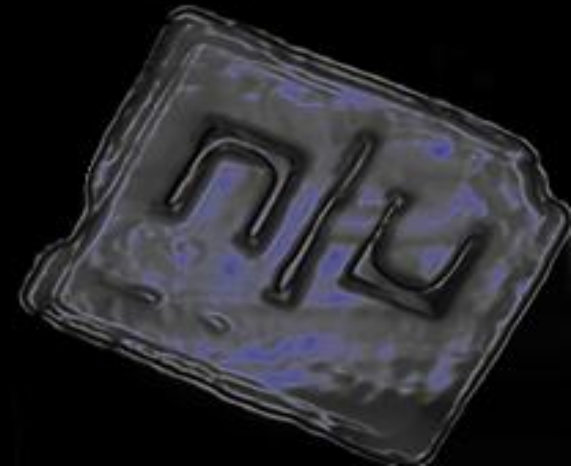
- ▶ Dare to Delete my files – Checkmate
- ▶ Universal Extractor – Checkmate
<http://www.niiconsulting.com/checkmate/>
- ▶ Assessing Bandwidth Use as a Function
Network Performance – ITAudit
<http://www.theia.org/ITAuditArchive/index.cfm?catid=21&iid=571>
- ▶ Essential Aspects of an Effective
Network Performance Audit – ITAudit
<http://www.theia.org/ITAuditArchive/index.cfm?iid=575&catid=21&aid=2901>





Agenda

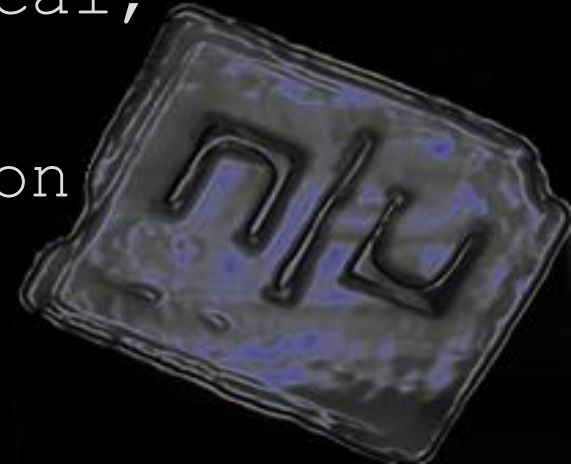
- ⊕ Security Assessment
- ⊕ Debate: PT vs. SCR
- ⊕ Penetration Testing Cons
- ⊕ Source Code Review Cons
- ⊕ PT vs. SCR
- ⊕ Conclusion





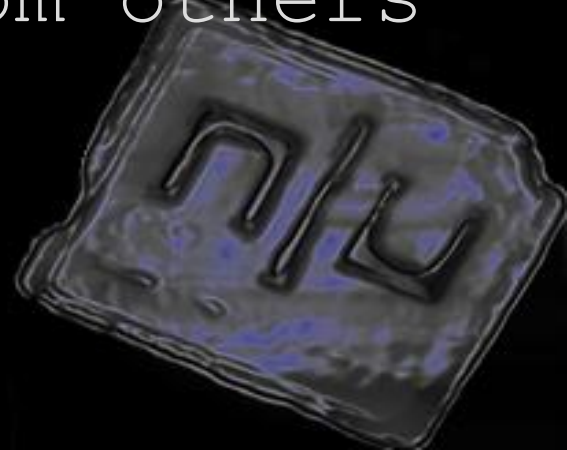
Security Assessment

- Explicit study to locate IT Security vulnerabilities and Risks (wikipedia)
- Methodologies
 - Penetration Testing
 - Source Code Review (SCR)
 - Reverse Engineering
 - Audits (compliance, technical, process etc)
- Lets concentrate on two common approaches: PT & SCR



Debate: PT vs. SCR

- Which approach is better?
 - Mixed responses
- Confident biased responses only from product vendors or domain specific experts
- Diffident responses from others

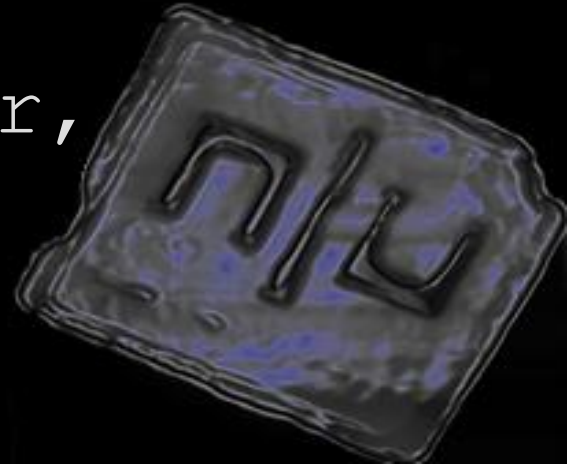




Popular Quote

"Penetration testing is dead.
The concept as we know it is on
its death bed, waiting to die
and come back as something
else."

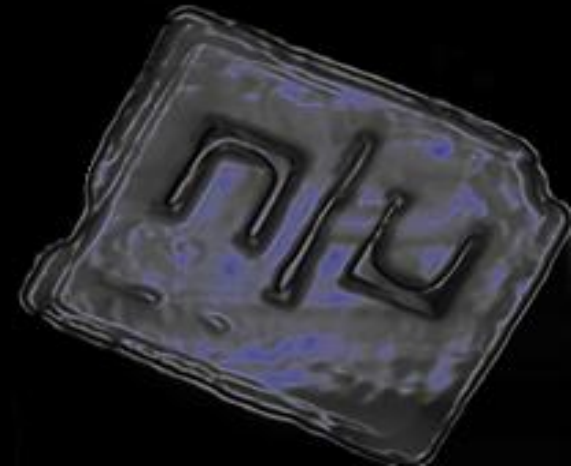
- Brian Chess, Co-Founder,
Fortify Software





Penetration Testing - *Cons*

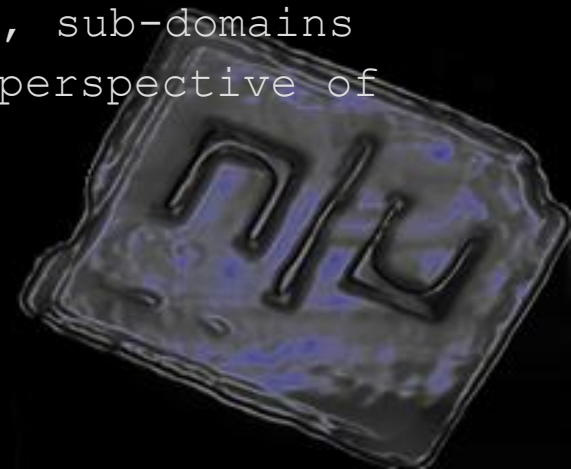
- ⊕ Risk based Penetration testing
 - ⊕ Test cases
 - ⊕ Business Logic
 - ⊕ Risk consideration
 - ⊕ Technical issues





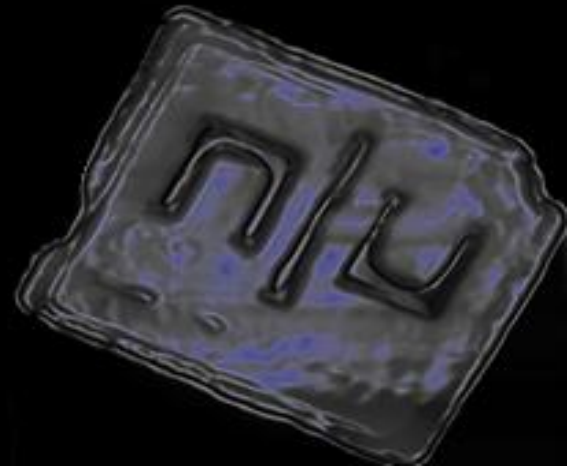
Data mining – scraping deep

- ⊕ A local search engine with millions of hits on the website
- ⊕ Key concerns are:
 - ⊕ Growing competition
 - ⊕ Need to expand rapidly through resellers and franchisee model
 - ⊕ Threat of exposure of data to unscrupulous elements
 - ⊕ Low competitive entry barrier – biggest threat of corporate espionage
- ⊕ External web application test
 - ⊕ Running repeated search queries – changing session IDs, changing source IP addresses
 - ⊕ Exploiting other channels – WAP, Toolbar, sub-domains
- ⊕ Internal business applications tested from perspective of a:
 - ⊕ Tele-caller
 - ⊕ Marketing agent
 - ⊕ Developer



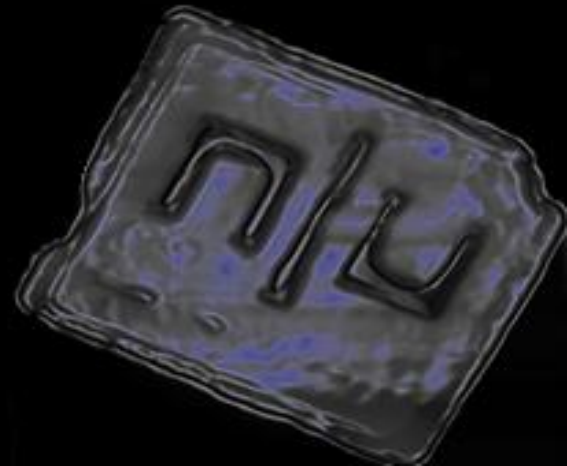


WAP request counter modified



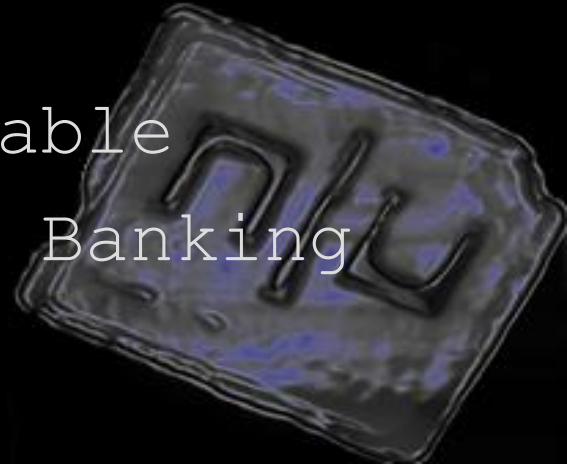


Search Engine Indexing Fault



Other Possibilities

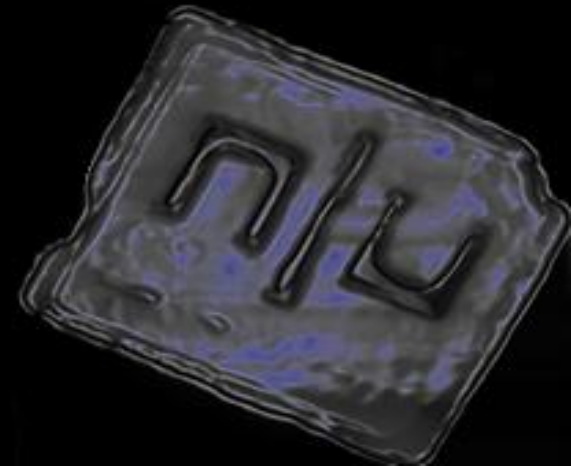
- Specific issues in Authentication
 - Weak CAPTCHA implementation
 - Enumeration based on Error messages
 - Username Enumeration
- Configuration issues with web server, OS or Firewall
- Source Code not made available
- Regulation - NIC, Internet Banking





Source Code Review - *Cons*

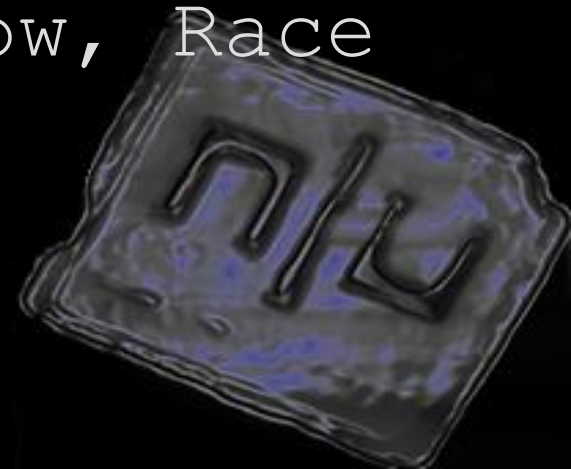
- Systematic examination of computer source code intended to find and fix mistakes and security vulnerabilities
- Typically addresses:
 - Implementation Errors
 - Design Errors





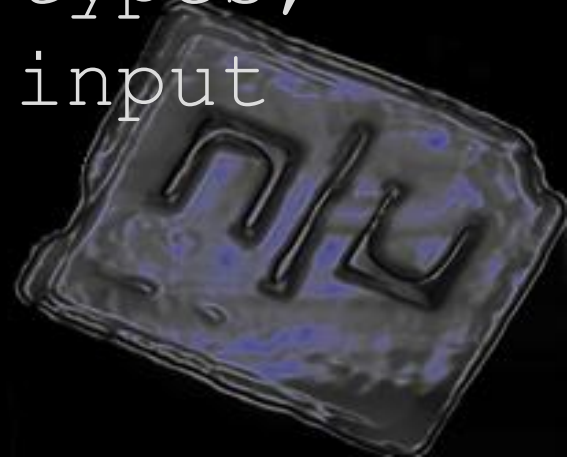
Implementation Errors

- Quality style defects in code
- Typically stand-alone when identified
- Generally bad or 'scratch-pad' types programming practices
- Example: Buffer Overflow, Race conditions



Design Errors

- ✦ Failure to utilize or adequately implement security related functions
- ✦ Includes authentication, encryption and the use of insecure external code types, and validation of data input and application output



Penetration Testing v/s Source Code Review

Penetration Testing

More of Black Box approach

May not always find all vulnerabilities

Can identify vulnerabilities max to a level of web pages or forms

Thorough, time effective and non-expensive

Well defined methodologies (OWASP, OSSTMM)

Source Code Review

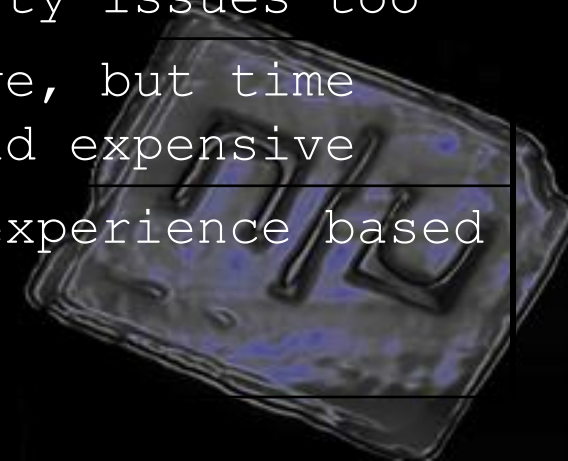
More of White Box Approach

A complete set of vulnerabilities can be discovered

Can get down to the root cause of the vulnerability that would end up fixing other security issues too

Comprehensive, but time consuming and expensive

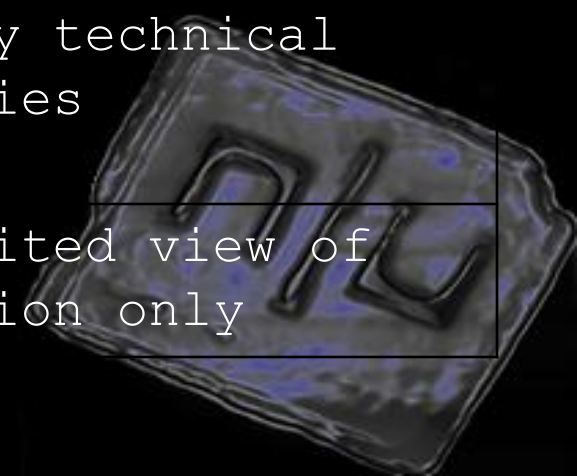
Ad-hoc and experience based methodology





Penetration Testing v/s Source Code Review

Penetration Testing	Source Code Review
Indirectly contributes to SDLC	Directly contributes to SDLC
Emulates real world hacking scenarios	Emulates backend, restricted and hypothetical scenarios
Gives more assurance from hacking perspective to clients	Gives more assurance from secure development perspective to clients
Can find both technical vulnerabilities and business risks	Can find only technical vulnerabilities
Provide holistic view of application deployment	Provides limited view of the application only



Conclusion

- ⊕ Each approach has its own perspective
- ⊕ Not a good idea to compare and debate
- ⊕ A well-timed combination of both approaches can be extremely beneficial in identifying and fixing security issues at the earliest





Thank you!

Questions and feedback

Nikhil Waghlikar

*Practice Lead | Security Assessments & Digital
Forensics*



nikhil@niiconsulting.com

www.niiconsulting.com

