Risk-based Penetration Testing

What is on your mind, is on your body

Nikhil Wagholikar
Practice Lead | Security Assessments & Digital Forensics
Member, Mumbai OWASP Chapter
www.niiconsulting.com
nikhil@niiconsulting.com

Nikhil Wagholikar– 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 of Network Performance – ITAudit http://www.theiia.org/ITAuditArchive/index.cfm?catid=21&iid=571
- Essential Aspects of an Effective Network Performance Audit – ITAudit http://www.theiia.org/ITAuditArchive/index.cfm?iid=575&catid=21&aid=2901

Agenda

- Regular pen-testing vs. Risk-based pentesting
- The process of risk-based testing
  - Understanding the business
  - Legal & regulatory requirements
  - Understanding the risks
  - Examples
  - Client-side attacks
  - Beyond hacking technology
- Conclusion

Table Editor - "EIP"."[redacted]_PAYSLIP_MAR_[redacted]_EXEC"
EMPLOYEE...
ELEMENT_...
ELEMENT_...
CLASSIFICA...
VALUE
SALARY_M...
029371 Basic Salary Earnings
029371 Dom Training A... Earnings
029371 Employee GOS... Statutory Deduc...
029371 GOSI Statutory Deduc...
029371 Housing allowa... Earnings
029371 Net Amount Net Amount
029371 Transport allow... Earnings
029371 XX Recovery Ca... Involuntary Ded...
037656 Basic Salary Earnings
037656 Employee GOS... Statutory Deduc...
037656 GOSI Statutory Deduc...
037656 Housing allowa... Earnings
037656 Net Amount Net Amount
037656 Transport allow... Earnings
037656 XX Recovery Ca... Involuntary Ded...
037745 Basic Salary Earnings
037745 Employee GOS... Statutory Deduc...
037745 GOSI Statutory Deduc...
037745 Housing allowa... Earnings
037745 Net Amount Net Amount
037745 Transport allow... Earnings
037745 XX Recovery Ca... Involuntary Ded...
038516 Basic Salary Earnings
038516 Domestic Seco... Earnings
038516 Employee GOS... Statutory Deduc...
038516 GOSI Statutory Deduc...

Problem Background

Lack of Business Risk Perspective – US Department of Homeland Security:

"Most penetration testing processes and tools do little, if anything, to substantively address the business risks…

This is largely due to the fact that the tools and the testers view the target systems with "technology blinders" on…

Although many testing tools and services claim to rank vulnerabilities in terms of technical severity, they do not typically take business risk into account in any significant sense.

At best, the test teams conduct interviews with the business owners of the applications and the application architects in an attempt to ascertain some degree of business impact, but that connection is tenuous.

…the business perspectives, however limited, that these processes can determine are all post facto. That is, they make their business impact rankings after the test is completed…*This is a key shortcoming of penetration testing practices today."*

https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/penetration/655-BSI.html

Software Security – building security in, Chapter 6 on "Penetration Testing Today"

"**The problem? No clue about security risk. No idea whether the most critical security risks have been identified**, how much more risk remains in the system, and how many bugs are lurking in the zillions of lines of code"

The challenge

“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

Let's start at the beginning

- Some theory

Pre-sales Approach

- Client: “Please provide quote for black-box penetration test”
- SP: “Please provide list of IP addresses and URLs, and application test IDs”

Pre-sales Approach - Evolved

- Client: “Please provide quote for black-box penetration test”
- SP: “Hang on…”
- SP: “I’d first like to know…”

Traditional vs. Risk-based Pentesting

Traditional Pentesting	Risk-based Pentesting
Focus is on technical vulnerabilities	Focus is on business risks
Requires strong technical know-how	Requires both technical and business process know-how
Having the right set of tools is critical	Understanding the workings of the business and applications is critical
Is usually zero-knowledge	Requires a person who understands the business process to play a significant role – usually an insider
Understanding the regulatory environment is good	Understanding the regulatory environment is mandatory

Traditional vs. Risk-based Pentesting

Traditional Pentesting	Risk-based Pentesting
Severity levels are based on technical parameters	Severity levels are based on risk to the business
Risk levels in report are assigned post facto	Risk levels in report reflect the levels assigned prior to testing
Test cases are build based on testing methodologies or generic testing processes	Tests cases additionally build on risk scenarios
Audience for the report is usually the IT and Security teams	Audience for the report also includes the business process owners and heads of departments

Case study

- Corporate Banking Platform – allows 3 logins
  - Maker who enters the transaction into the system
  - Verifier who checks the transaction data
  - Authorizer who authorizes the final payment
- Each screen in the web application is different based on privilege level of logged in user
- Security implemented by:
  - Restricting access to URLs that allow certain transactions
  - Parameters that trigger certain transactions

Case study

- RA Phase
  - Understand business process
  - Understand business risks
  - Define test cases
    - Can maker do what verifier does
    - Can verifier do what authorizer does
    - Can client's admin do what bank's admin does
    - So forth
- Pentesting discovers
  - http://www.bankPay.co.in/BankPayApp/authorizePaymentAction.action is available only to Authorizer
  - But what if Maker puts it in his browser?
  - Transaction still doesn't get authorized
  - Further investigation reveals a parameter:
    - Filter='block'
  - When this value is changed to:
    - Filter='submitToPay'

Understanding the business

- Who are the key actors – employees, departments, customers, partners, vendors, investors, brokers, franchisees, resellers?
- What applications do they use?
- What data do they access through these applications?
- What are the risks if any of these actors turns bad?
- What possibilities exist if an actor should decide to misuse the data – building fraud scenarios?

Regulations that drive webapp testing

- PCI DSS
  - For all credit card processing merchants
  - Quarterly, semi-annual, annual network scans and penetration tests
  - Focus on web application security
  - Requires high-level of protection of credit card data
  - There are no fines for non-compliance but breaches of security could put you out of business
- HIPAA
  - For healthcare and pharma providers
  - Requires high-level of protection for patient records and medical history
  - Fines for non-compliance are usually high
  - Breaches could put you out of practice/business

Other regulations

- FDA
- FFIEC
- SOX
- Indian IT Act 2008
- RBI / Other Central Bank
- Others

A6 – Information Leakage and Improper Error Handling

CWE 717

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

Publications website

Internationally acclaimed publications website

- Earns income via paid subscription to researched publications
- Publications are key intellectual property
- Membership levels and subscription values differ based on sensitivity and type of information accessible
- Use of the Google Search appliance leads to indexing of all data
- While members only data is not accessible directly, it is accessible via the ‘Text Version’ link from the Google search results!

Leading stock exchange

- Investors use the stock exchange via brokers
- However, direct interactions with exchange include:
  - Registering with the exchange to obtain investor IDs
  - Modifying investor personal data
  - Nominating others to trade on their behalf
  - Obtaining trade summaries
  - Obtaining research reports
- One of the key risks identified:
  - Violation of privacy

Gaining the business perspective

- Website analysis reveals two areas of interest
  - A local search functionality
  - Online access to personal trading history and balance sheets
- Each investor has a personal investor number – National Investor ID (NID)
- Website also offers educational games and documents on how to trade
- Guessing passwords for user IDs gives access to complete trade history and balance sheets
- Entering interesting search terms results in personal details of investors being revealed

A9 – Insecure Communications – CWE 720

- Driven by business risks and regulatory requirements
- Identify all sensitive data, not just authentication credentials
- PCI DSS requires encryption of credit card data
  - Between the client and the web server
  - When stored in the database
  - Between the web application server and the database server
- HIPAA requires securing of all patient data
  - Prescriptions
  - Medical history
  - Diagnostic results
  - Transcriptions

Abuse of business functionality

Taking it further – Pentesting ERP

Fraud scenarios for a P2P Webapp

For a procure-2-pay cycle, possible fraud scenarios could include?

- Adding a vendor without proper approval
- Changing the banking data of a vendor so that payments go into the wrong bank account
- Approving a quote by violating access rights
- Approving an invoice without a goods-received-note being present
- Colluding with another user to perpetrate a fraud
- Violating maker-checker controls

Fraud scenarios for an online share trading platform

- Main actors involved are:
  - Brokers
  - Franchisees
  - Investors
- Possible frauds could occur as follows:
  - Attacker gathers enough data to social engineer a broker
  - Attacker places trades on behalf of investors by violating web application security – jacking up share prices
  - Attacker is able to determine trading patterns of HNIs – High Networth Individuals
  - Attacker violates payment gateway controls to channel money into his/her own account
  - Attacker impersonates a broker/franchisee and social engineers the share trading company

Buy goods for free!

- Internal audit of a Southern India-based retail store contracts us to do a 'tiger team' attack
- Objective of the exercise is to determine controls over financial information
- Risks identified:
  - Access sensitive financial information?
  - Modify goods prices and accounts information significantly?
  - Change tags on goods to buy them at lower price?

Master Data is uploaded from flat files

A5 – Cross Site Request Forgery

CWE – 352

Posting ghost messages

Social networking website

- Value of website derives from focus on privacy and ease-of-use
- Peer-feedback is the key to the popularity
- Messages posted privately and on public ‘walls’, ‘scrapbooks’, ‘blogs’
- Integrity of messages is key
- Social engineering can be used to trigger CSRF and XSS attacks

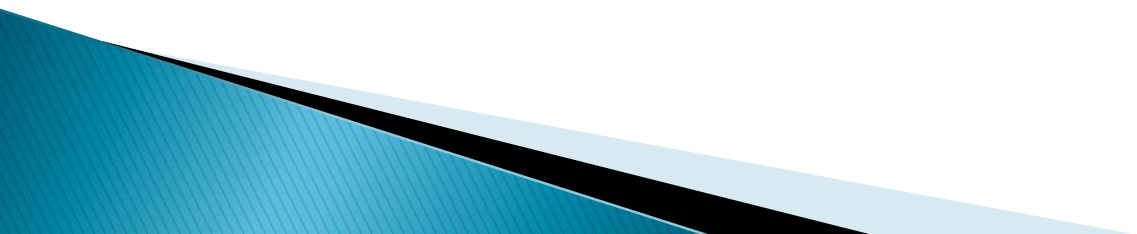
A1 – Cross site scripting

Or HTML Injection?

Challenges with XSS

- Explaining the technicality of the issue to developers and management
- Explaining exploitability and impact of the issue
- Demonstrating practical risk from it
- In some situations, explaining it additionally as HTML injection may help

Option 1 – show it as XSS



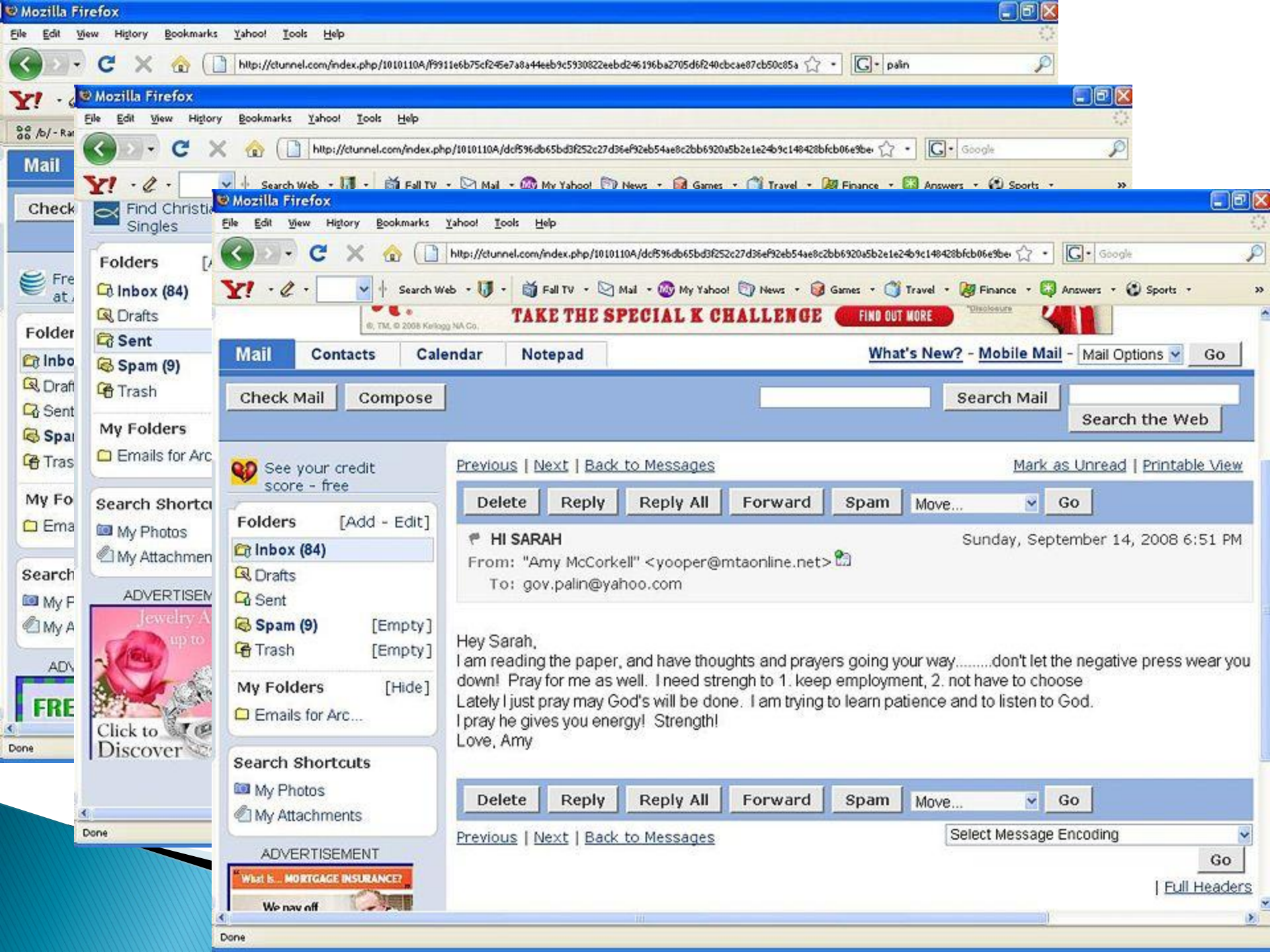
Option 2 – show it as HTML injection

Attacking the End-user

- And other techniques

Client-side attacks

- Vote for Cyber Security!


Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://ctunnel.com/index.php/1010110A/f9911e6b75cf245e7a8a44eeb9c5930822eebd246196ba2705d6f240cbcae87cb50c85a
palin
Mozilla Firefox
http://ctunnel.com/index.php/1010110A/dcf596db65bd3f252c27d36ef92eb54ae8c2bb6920a5b2e1e24b9c148428bfcb06e9be
Google
Search Web Fall TV Mail My Yahoo! News Games Travel Finance Answers Sports
Mail
Check
Find Christian Singles
Folders
Inbox (84)
Drafts
Sent
Spam (9)
Trash
My Folders
Emails for Arc
Search Shortcuts
My Photos
My Attachments
ADVERTISEMENT
Jewelry
up to
Click to Discover
Done
Mozilla Firefox
File Edit View History Bookmarks Yahoo! Tools Help
http://ctunnel.com/index.php/1010110A/dcf596db65bd3f252c27d36ef92eb54ae8c2bb6920a5b2e1e24b9c148428bfcb06e9be
Google
Search Web Fall TV Mail My Yahoo! News Games Travel Finance Answers Sports
TAKE THE SPECIAL K CHALLENGE
FIND OUT MORE
Disclosure
Mail
Contacts
Calendar
Notepad
What's New? - Mobile Mail - Mail Options
Go
Check Mail
Compose
Search Mail
Search the Web
See your credit score - free
Folders [Add - Edit]
Inbox (84)
Drafts
Sent
Spam (9) [Empty]
Trash [Empty]
My Folders [Hide]
Emails for Arc...
Search Shortcuts
My Photos
My Attachments
ADVERTISEMENT
What is... MORTGAGE INSURANCE?
We pay off
Previous | Next | Back to Messages
Mark as Unread | Printable View
Delete
Reply
Reply All
Forward
Spam
Move...
Go
HI SARAH
Sunday, September 14, 2008 6:51 PM
From: "Amy McCorkell" <yooper@mtaonline.net>
To: gov.palin@yahoo.com
Hey Sarah,
I am reading the paper, and have thoughts and prayers going your way.....don't let the negative press wear you down! Pray for me as well. I need strengh to 1. keep employment, 2. not have to choose
Lately I just pray may God's will be done. I am trying to learn patience and to listen to God.
I pray he gives you energy! Strength!
Love, Amy
Delete
Reply
Reply All
Forward
Spam
Move...
Go
Previous | Next | Back to Messages
Select Message Encoding
Go
| Full Headers
Done

Hello, /b/ as many of you might already know, last night sarah palin's yahoo was "hacked" and caps were posted on /b/. i am the lurker who did it, and i would like to tell the story.

In the past couple days news had come to light about palin using a yahoo mail account, it was in news stories and such, a thread was started full of newfags trying to do something that would not get this off the ground, for the next 2 hours the acct was locked from password recovery presumably from all this bullshit spamming.

after the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from wasilla, and it only has 2 zip codes (thanks online postal service!)

the second was somewhat harder, the question was "where did you meet your spouse?" did some research, and apparently she had eloped with mister palin after college, if youll look on some of the screenshits that I took and other fellow anon have so graciously put on photobucket you will see the google search for "palin eloped" or some such in one of the tabs.

I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on "Wasilla high" I promptly changed the password to popcorn and took a cold shower...

>> rubico 09/17/08(Wed)12:58:04 No.85782727

this is all verifiable if some anal /b/tard wants to think Im a troll, and there isn't any hard proof to the contrary, but anyone who had followed the thread from the beginning to the 404 will know I probably am not, the picture I posted this topic with is the same one as the original thread.

I read though the emails... ALL OF THEM... before I posted, and what I concluded was anticlimactic, there was nothing there, nothing incriminating, nothing that would derail her campaign as I had hoped, all I saw was personal stuff, some clerical stuff from when she was governor.... And pictures of her family

Other client-side attacks

- Browser-based exploits
- Trojaned MS Office/PDF files
- Combine with SE on social networking sites
  - LinkedIn
  - Monster.com and job sites
  - Social networking sites
- Phishing attacks
- Evil maid attacks
- Windows Metafile-type exploits
- RSA (2-factor) hacks

Challenges

- Fear of the unknown
- Client resistance
- Simply a checklist item
- Cost
- Time

Conclusions

- Real-world hackers are hacking the business, not the technology – they always have been
- Penetration testers need to bring their approach up to speed – go beyond the norm
- Endeavor to obtain greater business know-how and a larger perspective than “technical blinkers”
- Cookie-cutter pen-testing methods don’t add value
- Technical testing needs to be combined with physical penetration testing and social engineering
- Reports and executive summaries should reflect this deeper understanding of the business perspective

Thank you!

Questions and feedback

Nikhil Wagholikar

Practice Lead | Security Assessments & Digital Forensics

NII Consulting

nikhil@niiconsulting.com

www.niiconsulting.com