Expertise or Incompetence?

Michael Barwise

The recent New York Times report on the May 2011 Citigroup data breach quotes some unnamed security experts describing the attack as "especially ingenious." So I braced myself for a description of some ultra-sophisticated attack vector, but this is what I found.

The attackers apparently logged in to the online cardholder interface and then tampered with the customer account number in the URL parameter set. However a security expert apparently said of the technique *"it would have been hard to prepare for this type of vulnerability,"* adding that he (assuming it was a he) *"wondered how the hackers could have known to breach security by focusing on the vulnerability in the browser."* According to "law enforcement officials" *"the expertise behind the attack ... is a sign of what is likely to be a wave of more and more sophisticated breaches by high-tech thieves..."*

When I read this I (briefly) rolled about laughing - before uttering a cry of despair. Because this is just about as daft as it gets, and it says a whole lot more about our supposed "security experts" than it does about the attackers. For a start, URL parameter tampering is as old as the hills (or at least, as old as the http GET method), and it's utterly trivial to execute - even to automate. But it's also incredibly easy to prevent it being abused - indeed you have to be exceptionally slack as a developer to deliver an interface vulnerable to such an attack. All you have to do to protect yourself are some basic authentication management and user input validation, plus - most importantly - *never use predictable sensitive data as publicly visible parameters*. These are such fundamental principles of online systems development that they should be second nature. So it's far from "hard to prepare for" unless you're a perfect idiot.

Nevertheless interfaces that can be attacked in this way are still extremely common, so there must be a lot of idiots out there developing them. And thus the attackers knew it was an option worth trying - it was probably very near the top of their list - because it's so ancient and obvious. But it's not a "vulnerability in the browser" - it's a flaw in the application on the server side. Anyone who thinks otherwise is a complete nincompoop. So who on Earth these supposed "security experts" are defies my understanding. At least one of them didn't want to be named, and in my books they're wise to remain anonymous - they deserve to be dragged through town on a hurdle with a firewall round their necks, the same as was done to dodgy grocers in the Middle Ages. And the site developers who left it wide open likewise. With incompetents like these on the side of law and order, the bad guys "don't need no steenkin' expertise."

Originally appeared on the Infosecurity Network, June 2011