

# Seven Business Logic Flaws That Put Your Website At Risk

October 2007  
Jeremiah Grossman  
Founder and CTO, WhiteHat Security

## Executive Summary

Session handling, credit card transactions, and password recovery are just a few examples of Web-enabled business logic processes that malicious hackers have abused to compromise major websites. There are many forms of business logic vulnerabilities commonly exploited by attackers. These vulnerabilities are routinely overlooked during QA because the process is intended to test what a piece of code is supposed to do and not what it can be made to do. The other problem(s) with business logic flaws is scanners can't identify them, IDS can't detect them, and Web application firewalls can't defend them. Hardly a winning trifecta. Plus, the more sophisticated and Web 2.0 feature rich a website, the more prone it is to have flaws in business logic due to the complexities involved.

As the number of common vulnerabilities such as SQL Injection and Cross-Site Scripting are reduced, the bad guys are increasing their attacks on business logic flaws. Following are real-world scenarios that demonstrate how pernicious and dangerous business logic flaws are to the security of a website. We'll also show how best to spot them and provide organizations with a simple and rational game plan to prevent them.

## Winning an Online Auction

### Class: Abuse of Functionality

An on-line auction website prevents attackers from guessing the passwords of users by temporarily locking accounts that receive too many failed attempts (5 tries) in a given amount of time. Once an account is locked, the attacker (or the user) must wait for a timeout to expire (1 hr) before attempting to login again. Account locking is one of several techniques used to slow down brute force attacks.

Once logged-in, users are able to browse items being auctioned and view who bid on what. To place a bid, a user is asked for their password to verify their intent, which prevent unintended bids and also stops Cross-Site Request Forgery attacks. The bidding process is tied into the login security system to deny password guessing in this area, as well.

### Can you spot the security problem?

If a malicious user wanted to place competing bidders at a disadvantage and improve their odds of winning an auction, they could, easily. To do so, they'd start by bidding on the item early and at a low price. When/if someone placed a higher bid, the malicious user would respond not only by bidding slightly higher, but also by running a sustained login brute force attack against that user's account. The result: The user would be unable to bid on the item because their account would be purposely locked by the attacker, since the bidding system is tied to the login security system. The malicious user would continue this attack for anyone who attempted to bid higher until the auction ends. The malicious user is not guaranteed to win, but locking out competitive bidders certainly improves the odds, while retaining their ability to drop out of the running at any time.

### Solution

- *Do not display user names on the website. This not only increases user privacy, but also prevents an attacker from knowing which bidder they need/want to lockout.*
- *As an alternative to an account lockout, a CAPTCHA system may be employed if an account has received too many failed login attempts. This method has the benefit of preventing brute force attacks, without the potential side effect of locking out legitimate users who are making bids.*
- *Online auctions may allow sellers to specify a minimum bid price before they must sell the item. So, if an attacker used the method described to get an unreasonable price, they are not guaranteed to get the item.*

## “Interactive” T.V.

### Class: Insufficient Process Validation

The website for Cable News 14 in North Carolina allowed registered users to submit weather related announcements for T.V., in order to alert local residents of school or business closures. The submissions are posted to the onscreen crawl during the newscast as a public service and periodically rotated. Think Web 2.0 for television.

To prevent abuse, such as users posting defamatory messages, station personnel must first review the submission's content before it's allowed to air. Afterward, users are free to edit the content to reflect any changes in status. For example, if a business or a school reopened or is to remain closed for an extended period, local residents can stay informed by monitoring the crawl.

### Can you spot the security problem?

Anytime user-supplied data is collected and redistributed for mass consumption online or via mainstream media, there is a risk that the content could be malicious or abusive. Spam, derogatory comments, pornography, or various forms of malware are all common examples. Moderators are typically present in online message boards, chatrooms, mailing list, etc. to remove any offensive material. On T.V. the familiar sound bleeps and blackout blocks provide roughly the equivalent function. In some particularly sensitive distribution outlets, such as public television, content should be carefully reviewed PRIOR to being aired or risk FCC fines. In the Cable News 14 below, this was done only partially.

One particular malicious user noticed the submission-editing feature of the system. They posted a nice informative message and then waited for the moderators to approve it for airing. Afterward, the malicious user edited the message with new bogus content. The content was allowed to air because the system did not require edited messages to undergo further moderator scrutiny. By the time the loophole was noticed by Cable News 14, the malicious user had shared his discovery with others on a public message board whose participants also got their 15 minutes of fame<sup>1</sup>.



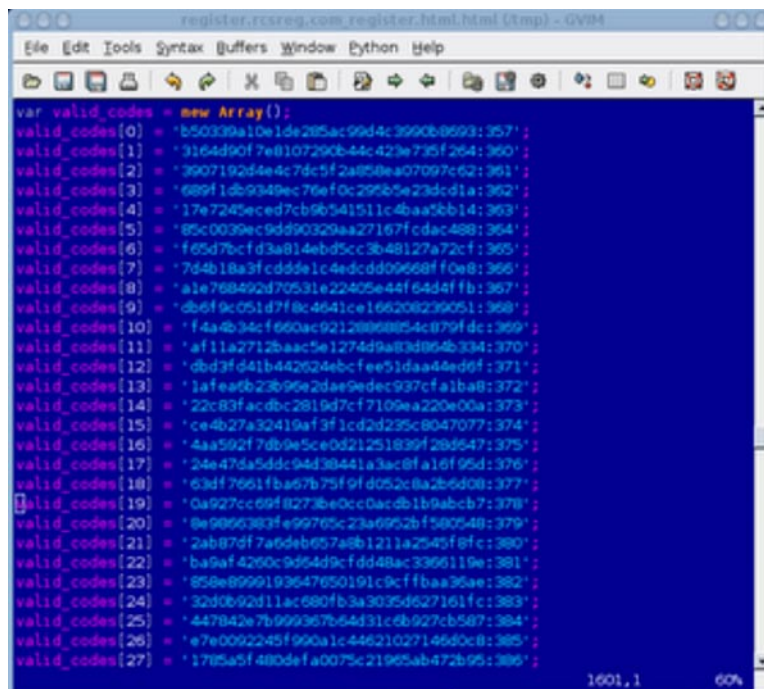
### Solution

In this case, the solution would have been easy: To not allow content edits or review each edit before airing. The downside is this requires additional human resources for screening.

## See Steve Jobs up Close

### Class: Information Leakage

During the MacWorld 2007 Expo, special Priority Codes (uppercase characters, digits, and 5 characters in length) could be used by VIPs to obtain free Platinum Passes with on-line registration. Platinum Passes were a \$1,695 value and came with a chance to see Apple CEO Steve Jobs up close. Hidden in the source code of the sign-up Web page was a list of available PCs encrypted with a one-way algorithm (MD5), which were used to ease Web server load. Before users submitted their order, any submitted PCs would be MD5'ed using JavaScript and then compared client-side against the hidden list. If the PC matched one on the list, the order would be sent to the server. If not, the user would receive an error message and the server would not need to be contacted.



```

var valid_codes = new Array();
valid_codes[0] = 'b50339a10e1de205ac99d4c3900b0593:357';
valid_codes[1] = '3164d90f7e8107290b44c423e735f264:360';
valid_codes[2] = '3907192d4e4c7dc5f2a850a07097c62:361';
valid_codes[3] = '689f1db9349ec76ef0c295b5e23dc1a:362';
valid_codes[4] = '17e7245eced7cb9b541511c4baa5bb14:363';
valid_codes[5] = '85c0039ec9dd90329aa27167fcdac488:364';
valid_codes[6] = 'f65d7b9cf3a814ebd5cc3b48127a72cf:365';
valid_codes[7] = '7d4b18a3fcdd6e1c4edcdd09668ff0e8:366';
valid_codes[8] = 'a1e788492d70531e22405e44f64d4fb:367';
valid_codes[9] = 'db6f9c051d7f8c4641ce166208239051:368';
valid_codes[10] = 'f4a4b34cf660ac92128868054c879fde:369';
valid_codes[11] = 'af11a2712baac5e1274d9a83d864b334:370';
valid_codes[12] = 'dbd3fd41b442624ebcf51daa44ed6f:371';
valid_codes[13] = '1afea6b23b96e2dae9edec937cf1a1ba8:372';
valid_codes[14] = '22c83facdb2819d7cf7109ea220e00a:373';
valid_codes[15] = 'ce4b27a32419af3f1cd2d235c8047077:374';
valid_codes[16] = '4aa592f7db9e5ce0d21251839f289647:375';
valid_codes[17] = '24e47da5ddc94d38441a3ac8f1a16f95d:376';
valid_codes[18] = '63df7661fba67b75f9fd052c8a2b6d08:377';
valid_codes[19] = '0a927cc69f8273be0cc0acdb1b9abc7:378';
valid_codes[20] = '8e986383fe99765c23a6952b1580548:379';
valid_codes[21] = '2ab87df7a5deb657a8b1211a2545f8fc:380';
valid_codes[22] = 'ba9af4290c9054d9cfd48ac3366119e:381';
valid_codes[23] = '858e8999193647650191c9c1fbaa36ae:382';
valid_codes[24] = '32d0b92d11ac680fb3a3035d627161fc:383';
valid_codes[25] = '447842e7b999367b64431c6b927cb587:384';
valid_codes[26] = 'e7e0092245f990a1c44621027146d0c8:385';
valid_codes[27] = '1785a5f480dfa0075c21965ab472b95:386';

```

### Can you spot the security problem?

Several people noticed the hidden list of MD5 PCs in the Web page source code and also that the key space was small - so small in fact that they could be easily brute-forced. Hackers quickly created programs for doing so; and, a few minutes later were cracking the PCs (usable during conference registration) to obtain free Platinum Passes<sup>2,3</sup>.

### Solution

There is a strong desire to have the web browser perform data input validation to ease Web server load, and often this can be done safely. In this case the developer chose to place sensitive data on the client, even encrypted, in such a way that cryptanalysis could be performed. It would have been better to let the server solely perform this process and preserve the security of the system.

## Day trading contest for \$1,000,000

### Class: Insufficient Process Validation

CNBC's Million Dollar Portfolio Challenge provided amateur traders a chance to match their skills against the portfolios of the Internet's best. 375,000 contestants competed in ten one-week challenges for a \$10,000 prize and a spot in the final round to go for the cool million. To win, all they had to do was make the most "funny" money.

### Placing stock trades is essentially a two-step process:

**Step 1.** Select the stocks you wish to purchase, enter the number of shares, and press the submit button. The back-end system calculates the total order using the current share price and waits for user confirmation before executing the trade.

**Step 2.** The user can either drop out of the transaction or confirm the order, which then executes the mock stock transaction to update their portfolio.

### Can you spot the security problem?

To make impossibly accurate picks, a malicious trader would select several stocks to buy (but NOT execute the order in step 2) with companies scheduled to post earnings after trading closes that day. After setting up the order, they'd leave their browser window open until after the closing bell. If the stock price rose by a significant percentage during after-hours trading, the trader would only then execute the transaction. Since their session contained the original stock price and did not recalculate using the current share price, the trader would be guaranteed huge portfolio gains and be well on their way to winning the million<sup>4,5,6</sup>.

### Solution

- *When executing the trade, the system should always calculate based upon the true current share price.*
- *The session for a pending trade should have an expiration time set; 20 minutes would be sufficient.*
- *Reject any incoming trades when the market is closed.*

## The House almost always Wins

### Class: Abuse of Functionality and Information Leakage

Blackjack is a simple card game where the player plays against the dealer and attempts to get closer than the dealer to 21 without going over (busting). When reduced to code, even simple games of chance tend to have complex trees of logic flows, which may take different amounts of time to execute. These logic flaws also dictate when cards are dealt, opportunities to bet, and when the dealer must hit or stand.

Blackjack rules say the dealer should offer a player an opportunity to buy insurance if the dealer's up card is an Ace, in case the hole card is a 10-value. In one published case, a Paradise Poker player noticed that when the dealer was showing an Ace and DID have a pocket 10-value card, there was a noticeable timing delay before the game offered insurance. Sort of a digital version of a poker player's "tell". This tell provided the player a slight edge over the house, providing them the advantage to make money<sup>7</sup>.

### Solution

Pad certain area of decision logic with extra time to smooth out timing nuances that can be fingerprinted. Or, optimize the code in areas to allow it to run with the same execution time as other areas of the system.

## Password Recovery

### Class: Weak Password Recovery Validation

The business owners of a website plan to reduce support costs by supplementing expensive customer support representatives with a Web-based customer self-service tool. One feature includes the ability to recover forgotten passwords. If a user wants to reset their password, they enter their email address and answer a previously defined secret question. The question is something personal, which makes it easy to remember, and in this case happens to be their favorite color. When the user correctly answers the question, they're presented with an HTML form to enter a brand new password.

#### 1. Can you spot the security problem?

There are very few available colors that the average user might choose, making it really easy for an attacker to guess all the common possibilities (red, blue, green, black, etc.). To compensate for the oversight, the business owners decide to introduce another secret question, but this time one that would be harder to guess. The date of birth (DOB) is decided upon, which includes the month, day and year, because it provides a significantly larger amount of possible answers. Should the user correctly answer both secret questions (color and DOB) they would be allowed to reset their password.

#### 2. Can you spot the security problem?

There are actually a few problems. While the DOB is harder to guess, the data isn't exactly confidential (besides the fact that it only has roughly 16,200 possible answers (12 x 30 x between the ages of 15 and 60)), based upon possible average user demographics. Attackers attempting to brute force the answer may easily do so at an average speed of 1 guess per second, taking only 4.5 hours to exhaust them all.

Which bring us to the next problem: There is no limit on the number of guesses an attacker may try before the account is locked for a period of time or protected with a CAPTCHA.

Undeterred, the business owners decide to add yet another secret question. But this time they pick the user's city of birth (COB). Certainly only the real user would be able to correctly answer all three answers, and no way an attacker could guess their way through. Also added was an image-based CAPTCHA system to prevent brute force attacks.

#### 3. Can you spot the security problem?

While the secret questions are steadily becoming harder for an attacker to guess, not to mention more of a burden on the users, the COB often doesn't scale internationally. For example in Mexico, home to 106 million people, 30% of the population is from one of five urban areas (Mexico City, Guadalajara, Monterrey, Puebla and Toluca)<sup>8</sup>.

Suddenly, what was a hard to guess secret question for a U.S. citizen has been greatly reduced to 1 in 5 for roughly 1/3 of Mexican users.

Next, the business owner decides that instead of fighting the cat and mouse game of secret questions, which negatively impact the user experience, they can utilize the user's email address. Certainly only the real user has access to their inbox, and email sniffing is considered an acceptable risk. When a user requests a password reset, the back-end system sends them an email containing the following link for them to click on:

[http://website/password\\_reset?account=user@email.tld](http://website/password_reset?account=user@email.tld)

When clicked, the user is presented with a password reset form.

#### 4. Can you spot the security problem?

The URL format is predictable. Attackers can easily brute force email addresses to reset user account passwords; that is, if they can't find valid addresses ahead of time. To improve the security of the system, the user's email address is removed and replaced with a session ID to track which account the request is tied to. To ensure uniqueness, the session ID uses a 12-digit number that increments each time a user requests a password reset. For example:

`http://website/password_reset?id=000000001000`

`http://website/password_reset?id=000000001001`

`http://website/password_reset?id=000000001002`

#### 5. Can you spot the security problem?

To reset another account password, a malicious user would first attempt to reset their own password a few times in order to analyze the new URL format. They would notice that the format uses a predictable incrementing number. In one attack they could decrement their session ID number manually to see if they can beat any users to resetting their passwords. Or, they could initiate an account password reset for a user and start incrementing the session ID in the URLs until they find the right number.

#### Solution

Password recovery systems are especially difficult to secure against abuse. The best way is to keep them as simple as possible and utilizing a user's email address provides a well-accepted form of authentication. Make sure the session identifiers are not predictable by an attacker.

## Making Millions by Trading on Semi-Public Information

### Class: Predictable Resource Location and Insufficient Authorization

Business Wire provides a service where registered website users are able to receive a steady stream of up-to-date press releases. Press releases are funneled to Business Wire by various organizations, which are sometimes embargoed temporarily because the information may affect the value of a stock. Press release files are uploaded to the Web server (Business Wire), but not linked, until the embargo is lifted. At such time, the press release Web pages are linked into the main website and users are notified with URLs similar to the following:

`http://website/press_release/08/29/2007/00001.html`

`http://website/press_release/08/29/2007/00002.html`

`http://website/press_release/08/29/2007/00003.html`

Before granting read access to the press release Web page, the back-end Business Wire system ensures the user is properly logged-in.

#### Can you spot the security problem?

An Estonian financial firm, Lohmus Haavel & Viisemann, discovered that the press release Web page URLs were named in a predictable fashion. And, while links might not yet exist because the embargo was in place, it didn't mean a user couldn't guess at the filename and gain access to the file. This method worked because the only security check Business Wire conducted was to ensure the user was properly logged-in, nothing more. According to the SEC, which began an investigation, Lohmus Haavel & Viisemann profited over \$8 million by trading on the information they obtained<sup>9</sup>.

## Solution

The system should ensure that press releases are only served to authorized users after the embargo date has been passed.

## Conclusion

Business logic flaws are pervasive and extremely diverse. It's easy to see why even the best QA processes overlook these issues because they typically don't check for what the system can be manipulated to do. And, vulnerability scanners, intrusion detection systems, and Web application firewalls would have an equally hard time, because the attacks look more or less like "normal" traffic. Data value requires knowledge of context and does not know what the website is supposed to do, or the path through the logic, so it can't tell if it did something wrong. To find these business logic issues, the pairing of experienced security experts with automated scanning is a best practice for achieving complete website vulnerability coverage.

## References

- <sup>1</sup> Pranksters bedevil TV weather announcement system: <http://www.securityfocus.com/news/8191>
- <sup>2</sup> Macworld crack offers VIP passes, hacker says: [http://www.news.com/Macworld+crack+offers+VIP+passes,+hacker+says/2100-1002\\_3-6149994.html](http://www.news.com/Macworld+crack+offers+VIP+passes,+hacker+says/2100-1002_3-6149994.html)
- <sup>3</sup> Your Free MacWorld Expo Platinum Pass (valued at \$1,695): [http://grutztopia.jingojango.net/2007/01/your-free-macworld-expo-platinum-pass\\_11.html](http://grutztopia.jingojango.net/2007/01/your-free-macworld-expo-platinum-pass_11.html)
- <sup>4</sup> \$1,000,000 CNBC stock trading contest hacked: <http://jeremiahgrossman.blogspot.com/2007/06/1000000-cnbc-stock-trading-contest.html>
- <sup>5</sup> CNBC's Easy Money: [http://www.businessweek.com/bwdaily/dnflash/content/jun2007/db20070607\\_007145.htm](http://www.businessweek.com/bwdaily/dnflash/content/jun2007/db20070607_007145.htm)
- <sup>6</sup> Finalists allege hacking in \$1 million stock contest: <http://www.securityfocus.com/brief/521>
- <sup>7</sup> Online Games Are Written By Humans: <http://haacked.com/archive/2005/08/29/9748.aspx>
- <sup>8</sup> Demographic Informaiton for Mexico: <http://en.wikipedia.org/wiki/Mexico#Demography>
- <sup>9</sup> SEC Vs. The Estonian Spiders: <http://www.webpronews.com/topnews/2005/11/02/sec-vs-the-estonian-spiders>

## The WhiteHat Sentinel Service – Complete Website Vulnerability Management

**Find Vulnerabilities, Protect Your Website** – The WhiteHat Sentinel Service is a unique combination of expert analysis and proprietary automated scanning technology that delivers the most comprehensive website vulnerability coverage available. Worried about the OWASP Top Ten vulnerabilities or the WASC Threat Classification? Scanners alone cannot identify all the vulnerabilities defined by these standards. WhiteHat Sentinel can. Many of the most dangerous vulnerabilities reside in the business logic of an application and are only uncovered through expert human analysis.

**Continuous Improvement and Refinement** – WhiteHat Sentinel stays one step ahead of the latest website attack vectors with persistent updates and refinements to its service. Updates are continuous – as often as one day to several weeks, versus up to six months or longer for traditional software tools. And, Sentinel uses its unique “Inspector” technology to apply identified vulnerabilities across every website it evaluates. Ultimately, each site benefits from the protection of others.

**Virtually Eliminate False Positives** – No busy security team has time to deal with false positives. That’s why the WhiteHat Sentinel Security Operations Team verifies the results of all scans. Customers see only real, actionable vulnerabilities, saving time and money.

**Total Control** – WhiteHat Sentinel runs on the customer’s schedule, not ours. Scans can be manually or automatically scheduled to run daily, weekly, and as often as websites change. Whenever required, WhiteHat Sentinel provides a comprehensive assessment, plus prioritization recommendations based on threat and severity levels, to better arm security professionals with the knowledge needed to secure them.

**Unlimited Assessments, Anytime Websites Change** – With WhiteHat Sentinel, customers pay a single annual fee, with unlimited assessments per year. And, the more applications under management with WhiteHat Sentinel, the lower the annual cost per application. High volume e-commerce sites may have weekly code changes, while others change monthly. WhiteHat Sentinel offers the flexibility to assess sites as frequent as necessary.

**Simplified Management** – There is no cumbersome software installation and configuration. Initial vulnerability assessments can often be up-and-running in a matter of hours. With WhiteHat Sentinel’s Web interface, vulnerability data can be easily accessed, scans or print reports can be scheduled at any time from any location. No outlays for software, hardware or an engineer to run the scanner and interpret results. With the WhiteHat Sentinel Service, website vulnerability management is simplified and under control.

### About the Author

Jeremiah Grossman is the founder and CTO of WhiteHat Security, a world-renowned expert in website vulnerability management, co-founder of the Web Application Security Consortium, and recently named to InfoWorld’s Top 25 CTOs for 2007. Mr. Grossman is a frequent speaker at industry events including the BlackHat Briefings, ISACA, CSI, OWASP, Vanguard, ISSA, OWASP, Defcon, etc. He has authored of dozens of articles and white papers, credited with the discovery of many cutting-edge attack and defensive techniques and is co-author of the book *XSS Exploits*. Mr. Grossman is frequently quoted in major media publications such as InfoWorld, USA Today, PCWorld, Dark Reading, SC Magazine, SecurityFocus, CNET, SC Magazine, CSO, and InformationWeek. Prior to WhiteHat he was an information security officer at Yahoo!

### About WhiteHat Security, Inc.

Headquartered in Santa Clara, California, WhiteHat Security is a leading provider of website vulnerability management services. WhiteHat delivers turnkey solutions that enable companies to secure valuable customer data, comply with industry standards and maintain brand integrity. WhiteHat Sentinel, the company’s flagship service, is the only solution that incorporates expert analysis and industry-leading technology to provide unparalleled coverage to protect critical data from attacks. For more information about WhiteHat Security, please visit [www.whitehatsec.com](http://www.whitehatsec.com).



WhiteHat Security, Inc. | 3003 Bunker Hill Lane, Suite 220 | Santa Clara, CA 95054 | 408.343.8300 | [www.whitehatsec.com](http://www.whitehatsec.com)

Copyright © 2007 WhiteHat Security, Inc. | Product names or brands used in this publication are for identification purposes only and may be trademarks or brands of their respective companies.

10.01.07