Security Analysis of Online Gambling Systems

Milad Mesbah (Student ID: 65658064) mesbah@interchange.ubc.ca, Nima Hosseinikhah (Student ID: 23917057) djnima@interchange.ubc.ca

***Abstract* — in recent times, many people around the world gamble on online casinos with peace of mind, as these online corporations promise alluring bonuses and promotions, and advertise their system as extremely secure and convenient for users. In this paper, we analyse security flaws of some online casinos, which we exploited through various security attacks. We will also present a risk analysis on online gambling and investigate assets, threats and threat agents involved as well as security design principles that are violated. Countermeasures will be proposed for all security problems discovered.**

I. Introduction

VARIOUS online gambling games have been developed in the recent years and have increasingly gained popularity around the globe. However, like any other web application, there are security risks involved in using online casinos. It should come as no surprise that without proper security measures, users' personal and banking information can be stolen by web attackers.

For the purpose of our security analysis, we selected a few popular online casinos, namely: Casino-On-Net (a brand of 888 group), Rushmore Online Casino, and PokerStars. We launched up to nine different types of attacks on each of these casinos, mostly with the intention of analysing the possibility of gaining access into user accounts. In particular we tried SQL injection, cross-site scripting, the Man in the Middle, session hijacking, Social Engineering, game fixing, brute force, online dictionary and denial of service attacks. As a result, we were able to analyse system designs, defence strategies, and security policies of these casinos, identify flaws, and suggest solutions for them.

In the next section of this report, we will present a brief threat analysis of online casinos. In sections III and IV we will elaborate on our unsuccessful and successful attacks, respectively. A number of countermeasures will be introduced in section V, before concluding the report in section VI.

II. Threat Analysis

As part of a security analysis, it is important to determine the assets, threats and threat agents for the subject at hand. Therefore, we identified the value of the assets at risk, the threats to which they are vulnerable, and the sources of these threats. Table I summarizes our threat analysis.

III. Failed Attacks

A. SQL Injection

SQL injection is one of the most commonly used attacks by hackers to modify or access resources. This attack can only be performed if the target website does not check form inputs submitted by the users. We performed this attack on Casino-On-Net, Rushmore and PokerStars websites. After trying all their forms and failing to get access or modify any of their resources we concluded that none of these websites is vulnerable to SQL injection.

TABLE I
Threat Analysis

Asset	Threat	Threat Agents
Personal information (e.g. Address, phone, etc)	personal information being viewed (Disclosure)	Hackers
Bank Account Information	Banking information being disclosed (Disclosure)	Hackers
Money in the account	Money transferred into another account or used up to place bets	Hackers, cheaters

Table I – Risk analysis

B. Cross-site Scripting (XSS)

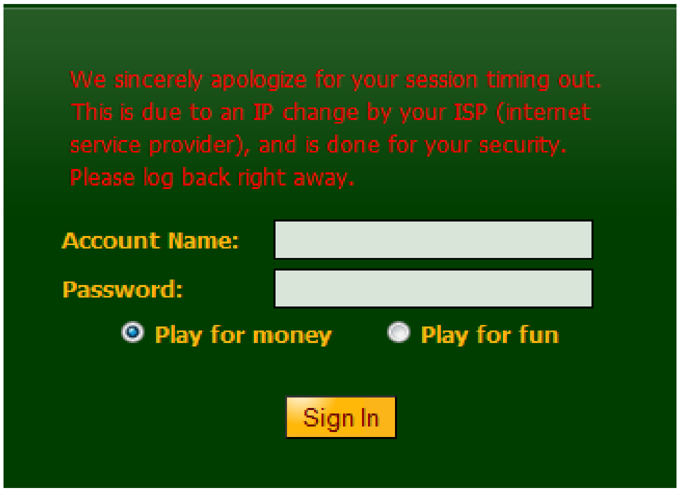
This is another form of an application layer attack which allows the attacker to embed malicious script into a page and gather information about the users of the website. This attack also relies on whether the inputs of a form on the website are correctly checked. We searched our target website to find vulnerable forms, but we were unable to find one. The fact that both SQL injection and XSS attacks failed indicates that these website are checking all the user inputs for any malicious content.

C. Session Hijacking

Session hijacking refers to stealing a valid session for another client and using that session to access the client's private data. This attack can either be performed by stealing a client's cookie, or finding a session ID that is valid. We knew that cookie stealing, which generally requires a script to be run on client's computer, is not possible in our case, since our XSS attacks failed.

Furthermore, we could not find a valid session ID in any way, because all of our target websites use random session IDs – making it infeasible to perform a brute force to find a working session ID.

We also decided to perform an experiment whereby we logged into an account we made on Rushmore, used its session IDs on a different computer (i.e. different IP address). However, we were immediately denied access by the server because of the change in IP address (See Fig. 1).



We sincerely apologize for your session timing out. This is due to an IP change by your ISP (internet service provider), and is done for your security. Please log back right away.

Fig. 1 The error message generated by Rushmore Online Casino when session-hijacking was attempted.

IV. Successful Attacks

A. Social Engineering

To explore security vulnerabilities of some online casinos, we conducted two types of Social Engineering attacks. The first one was a simple attack in which we took advantage of basic user information to obtain (through guessing) the password to their online casino accounts. The second attack was more advanced. It involved collecting usernames through brute force attack on user Email accounts at a particular online casino, as well as sending out fake Email messages to deceive users into visiting a phishing website we had set up.

Online Password Guessing

One of the online casinos we analysed was the popular Casino-On-Net. While we were analysing the security of their website, we came across their user registration form, in which they enforced users to choose passwords that are exactly eight characters long and consist only of English letters and digits. Later, we also realized that the passwords are not case-sensitive either. We recognized this as a fatal security flaw and a violation of "Defence in Depth" security design principle. Therefore, we decided to try a simple social engineering attack, as the limited password possibilities increased the chance of successfully guessing a password.

We sat a virtual Blackjack table on Casino-On-Net and only observed other players. At the table, players were identified and displayed by their usernames. We collected some of these usernames and, for the purpose of our attack, selected those that possibly revealed some user information, such as real name, birth year, phone number (e.g. John1965, Michael6045556767, DavidChung). Using this information, we made educated guesses at the password for each selected username.

We realized that Casino-On-Net does not impose any online password-guessing prevention mechanism. One can try entering as many passwords as he wants, without being blocked in any way. Therefore, shortly after the start of the attack, we happened to correctly guess the password of an account with a revealing username. In this case, the username included a birth year. Since we knew that the password must be eight characters long, and should only consist of letters and digits, we realized, at our third guess, that the password was simply the birth year repeated twice.

Phishing Attack

We tried another type of Social Engineering attack on a different online casino, namely: Rushmore Online Casino. Through our analysis, we noticed that Rushmore website provides a service, whereby one can claim a forgotten username and obtain it by providing the Email address with which the username was registered. To do so, anyone can simply click on "Forgot your Account Name" link (as illustrated in Fig. 2) and, once prompted, enter an Email address. If the Email address has been registered with the website, the username will be displayed immediately. However, if the Email address is not associated with any username in the database, the user will be notified that the "e-mail address does not match".

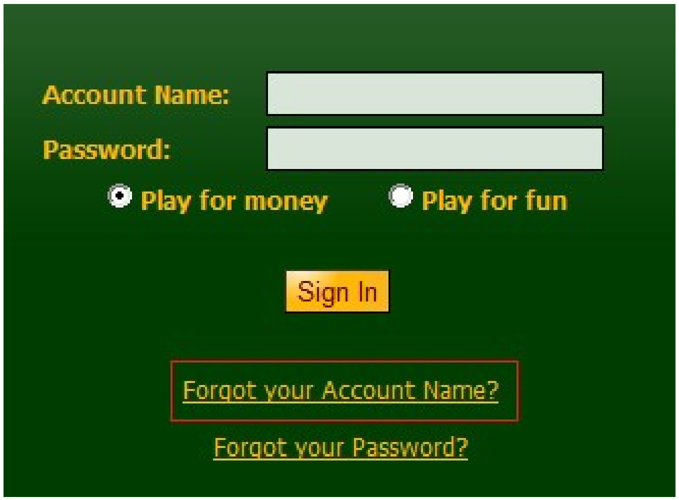


Fig. 2 Login window on Rushmoreonline.com – the link to username recovery service is outlined in red.

We can categorize this security flaw as a violation of the principle of Questioning Assumptions. Rushmore Online Casino failed to see the possibility that an attacker can obtain a list of Email addresses and their corresponding usernames at Rushmore very easily, and utilize them for various types of attacks on user accounts. We demonstrated how this service can be misused through our Social Engineering attack.

First, we extracted over one hundred usernames from Rushmore database by inputting a long list of random hotmail Email addresses to the website. We automated the procedure by modifying and adding JAVA code to HttpClient component.

The program tried an Email address from the list, every one second, against the username recovery service of Rushmore website. The delay would prevent us from being immediately blocked by Rushmore security service; though, we still got blocked after about 100 tries. Therefore, we also used a proxy list to change the IP address after a set of 80 tries to bypass the blocking. At the end, we managed to obtain a list of usernames and their corresponding Email addresses. Having this list, we could perform various types of attacks. At this section of the report, we will discuss our phishing attack.

We simulated a phishing attack by sending bogus Emails to the Email address that we found to be registered with Rushmore. The contents of this email can be found in the Appendix section at the end of this report. The Email would appear to be sent from Rushmore staff, since the sender address was forged using *deadfake*'s free service provided at deadfake.com.

Basically, the Email offered a bonus to the users on behalf of Rushmore Online Casino and directed them to our phishing website. The phishing website replicated Rushmore's web interface and allowed users to enter their usernames and passwords. We could potentially collect any username and password entered at our phishing web site, but, due to legal and ethical issues, we only collected statistics of the number of times people were deceived to log into the phishing website. We sent the Email to a total of 50 users and after one week, according to our page counter, the login window on the phishing site was used twice.

B. Online Dictionary Attack

This is an attack where the hacker uses brute force in order to find the password for an account, but instead of trying all possible password combinations, the attacker uses a dictionary of common passwords. To test whether any of our target websites were vulnerable to this attack, we wrote a java program that was capable of brute forcing html form-based login systems over an SSL connection. We soon discovered that one of our target websites is vulnerable to this attack (Rushmore Online Casino).

To launch the attack, we first created an account with the website and tried to see if our program is able to find the password we chose. After a few attempts we noticed that the website does not allow more that 10 login attempts in a short period of time from the same IP address. Thus, in order to bypass this problem, we introduced a one-second delay between our login requests, and instead of attacking one account, we optimized the program to attack multiple accounts by using a proxy list to mask our actual IP address.

The successful program used a list of user names and a small dictionary. It would try a password from the dictionary against all the usernames in the list. Once all the usernames were checked, the program would establish a new SSL connection to the server, using a new proxy (and therefore a different IP address from the server's point of view) and repeat the procedure. At the end, using a list of sixty usernames and a small password dictionary, we were able to find the password for 6 of the accounts.

C. Denial of Service Attack

The denial of service attack is an attempt to make the resources unavailable to its intended users. While we were performing our experiments during the online dictionary attack, we noticed that if the target server identifies us as an attacker, it locks the account corresponding to the username that we were attacking. Once the account is disabled the user cannot log in to his/her account.

At first, this may appear to be a fine defence against brute force attacks. In order to test it, we created an account and brute forced the password without any delays from one IP address. After the attack, we realized that the account was totally shut down – therefore denying login service even to the actual user. A problem with this strategy is that the user of the account is never notified of the incident. Once the user tries to sign in, he will only receive a generic error ("Incorrect Account Name or Password"). This strategy also violates the security principle of psychological acceptability, because the security mechanism utilized makes it difficult for the user to access the system.

D. Game Fixing

Game fixing attack can be defined as the act utilizing system vulnerabilities to change the outcome of the game that runs on the system. This type of attack (or cheat) is mostly performed on online poker games. To do so, a user manages to get on the same poker table using different User IDs, thus having the advantage of seeing the cards of multiple players (all of whom are the cheater itself) and make better decisions throughout the game than other users at the table.

We chose PokerStars, which is the largest online poker website with over 15 million users, as our target website [5]. To test whether game fixing is possible or not we used two user accounts and tried to play on the same table from the same internet connection. Though, the server only allowed one of usernames on the table since we were connecting from the same network. Therefore, we decided to use a proxy on one of the computers to mask our IP address. To do this we used the software called Proxifier to manually enforce the PokerStars software to use a proxy. We then used the Privoxy software in conjunction with the TorOnion software to use the anonymous Tor Network. With this setup (illustrated in Fig. 3) we were able to change the IP address of the machine; therefore, the PokerStars server was unable to detect that our computers were connecting from the same network. We then were able to sit on the same table, which gave us the advantage of seeing more cards than other players. It is clear that this design flaw violates the principle of questioning assumptions.

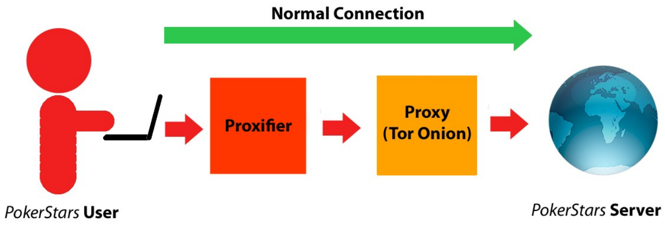


Fig. 3 Game-fixing connection setup

V. Proposed Countermeasures

After studying the design flaws and problems we identified with the online casinos discussed in this report and online gambling in general, we realized possible countermeasures that can eliminate and prevent some of these problems:

1) *Choose a strong password*

We recommend users of online casinos to choose a strong password. A strong password should consist of a combination of uppercase and lowercase letters, digits, and if possible, special ASCII characters. For users' convenience, the password can be selected such that it is pronounceable, yet random (or at least not a dictionary word). We also suggest users not to incorporate personal information (such as year of birth or place of residence) in their passwords.

2) Enforce secure passwords

Online casinos should inform users about weak and strong passwords, and guide them to choose a password that is secure. Users should be required to select secure passwords upon registration. To do so, IT specialists can integrate password strength checkers into the online registration forms and prevent users from choosing weak passwords.

3) Implement a secure username recovery service

One of the security flaws we mentioned in this report was the username recovery service on Rushmore Online Casino website. We recommend these services to be implemented in a more secure manner. For example, when one enters an email address to recover the username, the username should not be disclosed on the web page. Rather, it is better to send the username to the registered Email address and provide a notification of this action. This way, only the true owner of the account, who forgot his/her username, will be able to recover it. This will prevent attackers from extracting username and email address pairs.

4) Do not reveal registered Email addresses

Online casinos should treat Email addresses as private user information and prevent disclosing them to public. The login service or the username or password recovery services of online casinos may make use of the registered Email addresses as part of their designs (e.g. Rushmore Online Casino). Though, these services should not specify whether or not the provided Email address exists in the system. Such information makes the life of attackers much easier. For example, in the case of username recovery, an alternative approach would be to simply notify the user that the username has been sent to the registered Email address – regardless of whether or not the Email address exists in the database. This king of notification can act as a "white lie" in case the service is misused by attackers.

5) Prevent against online password-guessing, brute force or dictionary attacks

A common security flaw we detected in many online casinos was failure to prevent online password-guessing, as well as brute force and dictionary attacks. We could try, at a fairly quick rate, as many username/password combinations as we wanted on each of the online casinos we analysed throughout this project, without facing any kind of prevention. Techniques such as exponential back-off, disconnection, disabling and jailing should be implemented in the design login systems of online casinos.

6) Choose reasonable attack prevention techniques

As mentioned earlier, one of the design principles we found to be violated by some online casinos (Rushmore in particular) was the principle of Psychological Acceptability. The cause of this violation was improper attack prevention techniques. Rushmore defended against brute force attack by completely shutting down accounts on which too many incorrect username/passwords were tried within a very short amount of time. Although this prevented attackers from cracking the password, it also caused inconvenience for the actual account holder, because the real owner of the account could neither log in nor was he notified about the matter. A better strategy, we suggest, would be to prevent brute-forcing using other techniques, such as exponential back-off or image verification.

VI. Conclusion

Although online casinos have made gambling easier and more convenient, users should be aware that, despite all the advertised security, there is still a chance that their online accounts are compromised by attackers – especially when passwords are weak. Selecting an online casino that is provably secure in every aspect is the first step toward protecting personal information when gambling online. Users should also familiarize themselves with the concept of strong password, and choose their passwords with care and attention.

A secure online casino is not necessarily one that merely uses Secure Socket Layer or HTTPS protocols. It should also follow all principles of designing secure systems, effectively protect itself from all types of attack, and enforce its users to choose strong passwords.

VII. Appendix

The following is the header and body of the phishing Email that was sent as part of our social engineering attack:

From: offers@rushmorecasino.com
To: mesbah@interchange.ubc.ca
Date: Tue, 24 Nov 2009 02:15:55 +0000
Subject: Rushmorecasino $50 Bonus

Dear Player,

We are pleased to inform you and other Rushmore Casino members about our new Bonus!

The bonus amounts to $50 and is valid until January, 1, 2010. To redeem your bonus, you simply need to login to your account.

Here is a shortcut that navigates you to the login page:
http://www.rushmoreonline.com/login

Again, congratulations on your $50 bonus!

Best of luck and enjoy the Casino!

--
Rushmore Casino Customer Service
US Toll-free: 1-800-488-1746
UK Freephone: 0-800-047-0972

References

[1] K.D. Mitnick, W. L. Simon, *The Art of Deception: Controlling the Human Element of Security*. John Wiley, 2002, chapter 7.

[2] Online Casino Spotlight. (2009, Oct.) *Online Gambling Under Attack By Web Scrapers* [Online].
Available: http:// onlinecasinospotlight.com/2009/10/online-gambling-under-attack-by-web-scrapers/

[3] M. Shema. *Web Security Pocket Reference* .McGraw -Hill, 2003, pp. 23—72

[4] J. Erickson, *HACKING: The Art of Exploitation*, 2008, chapter 3

[5] E. Rogers (Sept, 2008) *Poker Stars Releases Mac Download Online Poker Room* [Online]. Available: http://onlinecasinosuite.com/casino-news/sept08/macdownload-onlinepokerroom-3175.html

[6] D. Stuttard, *The Web Application Hacker s Handbook: Discovering and Exploiting Security Flaws*. 2007, chapter 6