https://doi.org/10.48009/2_iis_2020_289-299

PHPBB3 BULLETIN BOARD SECURITY TESTING

Nishitkumar Patel, Georgia Southern University, np00573@georgiasouthern.edu
Hayden Wimmer, Georgia Southern University,hwimmer@georgiasouthern.edu
Loreen Marie Powell, Bloomsburg University, lpowell@bloomu.edu

ABSTRACT

Use of web applications and electronic bulletin board systems has become increasingly popular and plays an important role in our day to day life. Today, users want to read, post, and respond to just about everything they can on the Internet. The problem is that many web applications and bulletin board platforms contain sensitive data that hackers try to exploit and steal useful information. The applied research examines the security of the phpBB3 platform by performing five security attacks (packet sniffing, forum spamming, session hijacking, SQL injection, and XSS scripting). The results revealed successfully security breaches and vulnerabilities exists within the phpBB3 platform. Based upon these result, this research provided recommends and countermeasures to reduce the vulnerabilities and improve phpBB3 security.

Keywords: BBS, PhpBB3, PHP, Vulnerability, Security, Packet Sniffing, Forum Spamming, Session Hijacking, SQL Injection, XSS Scripting

INTRODUCTION

A computer bulletin board system (BBS) is an asynchronous electronic transmission of information to participating users. BBSs allow internet users to post information and respond (Tang, Kong, Song, & You, 2007). The use of BBSs is not a new topic as they have been around longer than the Internet (Long, Greenberg, Ismeurt, & McGrath, 2001; Makulowich, 1993; Alemi et al., 1996). Over the years, BBS have notably expanded the transfer of information among people and organizations (Huang & Leung, 2012). As a result, BBSs have been known to have many benefits such as teambuilding, knowledge interdependency, information dissemination, decision making, self-help, and collaboration (Bullen & Bennett, 1991; Chen, Du, Liu, Zhang, & Zhang, 2019; Huang, 2010; Jin, Cheung, Lee, & Chen, 2009; Malone & Rockart, 1993; Tillquist, 1996; Yates, 1989).

One of the most widely applied BBS software is phpBB3 (https://www.phpbb.com), which is free, open source software that has been developed by PHP. The popularity of the message boards or internet forums has been facilitated by the increased access to internet. Therefore, people join bulletin boards and engage in a discussion related to a particular (Huang & Leung, 2012). The bulletin board style interface is preferred because of its ease of use and the seamless connection that people have on the platform. The BBSs contain sensitive information that needs to be protected from unauthorized use or access by third parties. Some hackers may be attracted by the rich data and could attempt to exploit and steal the useful information. It is, thus, important to implement fixes that can help in preventing attacks and subsequent loss of information.

Currently, existing literature within the BBS are focuses on their use from a personal or organizational perspective (Huang, & Leung, 2012; Alemi et. al., 1996; Zhang & Zhang, 2019). There is a lack of research focusing on phpBB3 vulnerabilities and possible countermeasures. In a recent summary of the 2019 big and ugly breaches, Robinson (2019) stated that in the video game, Town of Salem, there were approximately seven million hacked accounts in which the hacker gained access to the users MD5 (phpBB3) username and password, and forum activity. He argues that the current status of cybersecurity is alarming and immediate attention is needed. To fill this research gap, this applied research paper focuses on highlighting the popularity of the phpBB3 among other BBSs. Specifically, this research performed the following attacks: packet sniffing, forum spamming, session hijacking, SQL injection, and XSS scripting. Vulnerabilities are identified and explained, as well as, recommended countermeasures to eliminate the vulnerabilities and to improve phpBB3 security are proposed.

This research has practical implications for the information technology professionals working with BBSs. The remaining structure of this paper is as follows: brief review of the literature, methodology, results, recommendations, and conclusion.

LITERATURE REVIEW

A number of studies that have been conducted on phpBB3 software indicate that its security can be easily compromised by the hackers who are targeting the rich information contained in the platforms (Robinson, 2019). The security of the software can be comprised at different levels that include compromising the user passwords and installing malwares to track the passwords stored on the databases. According to Zhang (2014), the security of phpBB3 software can easily be compromised due to the continued use of an earlier version of the software that has weak algorithms. The earlier version continues to be used as it helps in solving the compatibility issues that are associated with the modern software platform. Hackers are, thus, able to take advantage of the weaker versions to access the platforms and gain access to important user information.

PHP is the most utilized framework for offering web applications. It has grown to become a critical part of our culture as people utilize it in, basically, all forms of their life functions. Marashdih, Zaaba, and Suwais (2018), note that the framework is utilized by users in managing bank accounts, interacting with friends, educational services and for filling taxes. When hackers compromise the systems they gain access to important information that can be used to harm the users (Letsoalo & Ojo, 2017). For example, they can use banking information to manipulate the financial system and obtain funds from the users' accounts. The ease of compromising security of web applications is facilitated by the vast amount of servers that are used to run them throughout the world (Fong, Lee, Lin, & Yue, 2010). Therefore, they become a target for most hackers that are looking to gain access to user information.

The most common vulnerability on PHP web application is cross site scripting (XXS). According to Marashdih et. al. (2018), cross site scripting is an injection type of attack that introduces spamming tools into the user's device and, consequently, steals sensitive information, sessions, user accounts, and cookies. The attack is executed through introduction of malicious scripts into the source code (Prokhorenko, Choo, & Ashman, 2016). Cross site scripting also occurs in web applications that utilize user data without encoding or validating. It allows a hacker to execute a script in the browser of the user, thus, disfiguring the websites, taking command of user sessions, or direct the user to sites that are suspicious (Zhang & Fan, 2014). Despite the enhanced process of reducing the vulnerabilities of web applications, Gupta and Gupta (2018), note that approximately 65% of web application still contains vulnerabilities to cross site scripting. They are the most popular threats to web applications.

The advancement of technologies and increased accessibility to internet has enhanced the use of web applications to execute various functions in people's daily lives. However, as people continue to use the functions enabled by web applications, the threat of theft of information is enhanced (Sharma, Gupta, & Khanna, 2019). Cybersecurity has, thus become one of the most major topics in the modern online world. The threat is more advanced as virtually anything in the current world is connected to the internet network. Cyber-attacks can interfere with online business and shopping, banking, and interactions. When people are conducting online transactions, they pass on sensitive information that requires high levels of confidentiality and integrity (Kamal, 2016). However, the high amount of data that is passed through the internet has made it complex to protect sensitive data. Informational technology experts, thus, have a task of developing secure mechanisms that can handle large data and provide assurance of users' confidentiality and integrity.

Andrea, Wojciech, and Max (2018) provides an overview into various publicly available network vulnerabilities scanning tools, by identifying and classifying them and then showing their strengths, weaknesses, features and capabilities. These are the tools that can be used to execute attacks, defend against attacks or learn where an attacker may target. In this paper, they discussed the need for tools that allow us to perform white hat hacking and penetration testing for security purposes. Skipfish is one of the tools used to perform penetration testing in this work.

METHODOLOGY

The goal of this research paper is to conduct security testing on phpBB. For the scope of this research, the following attacks were performed: packet sniffing, forum spamming, session hijacking, SQL injection, and XSS scripting. The common tools used for this research were a Ubuntu server, Kali Linux operating system, switch, router, and default installation of phpBB3. PhpBB3 was selected for this research because it is free and the most common free BBS platform.

System Setup

For the system setup, Ubuntu version 18.04 Live was installed on a Lenovo tower and booted into an operating system from a 64GB USB. After installing Ubuntu, we installed Apache2, phpMyAdmin, MySQL and a default installation of phpBB3. Kali Linux is very resourceful and user-friendly, it is used to carry out effective penetration testing on systems, networks and web applications.

A TP-Link Router and Cisco catalyst 2960-S switch was used for the network setup. Figure 1 provides an outline of the network setup.

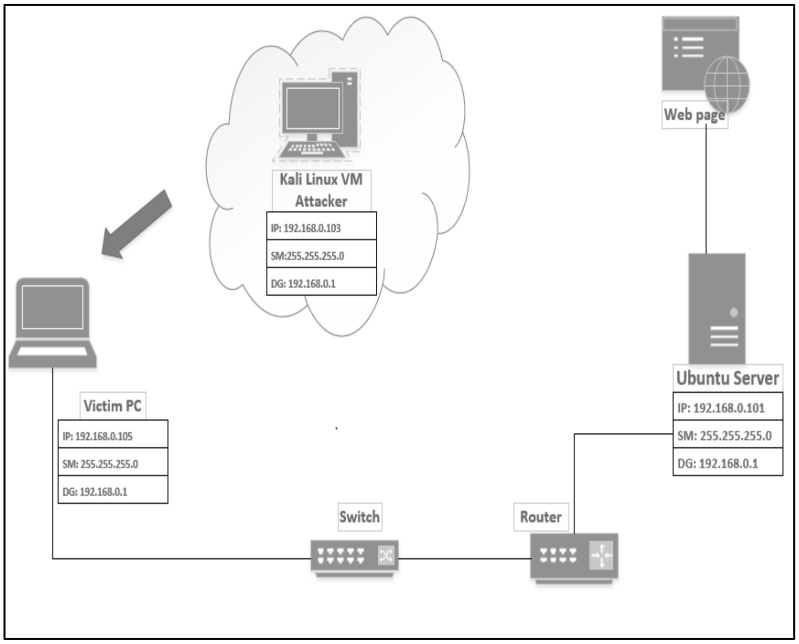
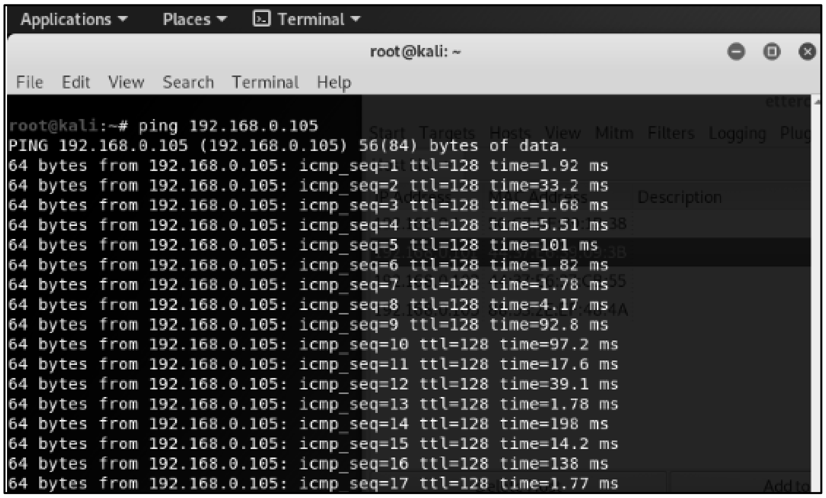


Figure 1: Configuration of the Network

Network scan and connectivity

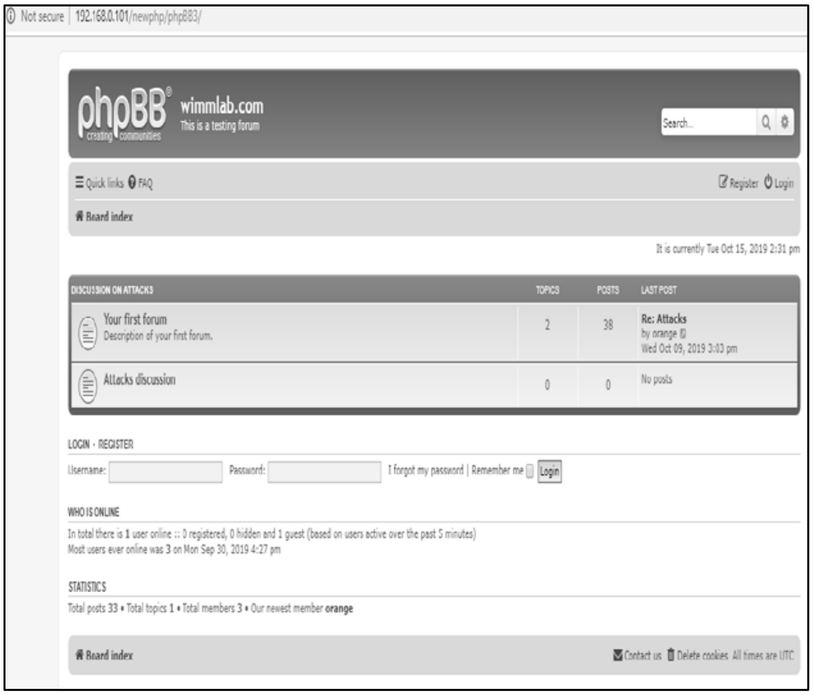
The first phase was to check connectivity between the Kali Linux machine, victim PC, and the localhost webpage (phpBB3). The "ping" command, was used to ping the Victim PC and access the web page using IP 192.168.0.101/newphp/phpBB3 from victim PC. Figure 2 and 3 show this phase.

In the next phase of the project, multiple user accounts were created for users to login to the forum with a username and password to participate in the discussion.



```
root@kali:~# ping 192.168.0.105
PING 192.168.0.105 (192.168.0.105) 56(84) bytes of data.
64 bytes from 192.168.0.105: icmp_seq=1 ttl=128 time=1.92 ms
64 bytes from 192.168.0.105: icmp_seq=2 ttl=128 time=33.2 ms
64 bytes from 192.168.0.105: icmp_seq=3 ttl=128 time=1.68 ms
64 bytes from 192.168.0.105: icmp_seq=4 ttl=128 time=5.51 ms
64 bytes from 192.168.0.105: icmp_seq=5 ttl=128 time=101 ms
64 bytes from 192.168.0.105: icmp_seq=6 ttl=128 time=1.82 ms
64 bytes from 192.168.0.105: icmp_seq=7 ttl=128 time=1.78 ms
64 bytes from 192.168.0.105: icmp_seq=8 ttl=128 time=4.17 ms
64 bytes from 192.168.0.105: icmp_seq=9 ttl=128 time=92.8 ms
64 bytes from 192.168.0.105: icmp_seq=10 ttl=128 time=97.2 ms
64 bytes from 192.168.0.105: icmp_seq=11 ttl=128 time=17.6 ms
64 bytes from 192.168.0.105: icmp_seq=12 ttl=128 time=39.1 ms
64 bytes from 192.168.0.105: icmp_seq=13 ttl=128 time=1.78 ms
64 bytes from 192.168.0.105: icmp_seq=14 ttl=128 time=198 ms
64 bytes from 192.168.0.105: icmp_seq=15 ttl=128 time=14.2 ms
64 bytes from 192.168.0.105: icmp_seq=16 ttl=128 time=138 ms
64 bytes from 192.168.0.105: icmp_seq=17 ttl=128 time=1.77 ms
```

Figure 2: Successful ping results to Victim PC



wimmlab.com
This is a testing forum

It is currently Tue Oct 15, 2019 2:31 pm

DISCUSSION ON ATTACKS	TOPICS	POSTS	LAST POST
Your first forum Description of your first forum.	2	38	Re: Attacks by orange Wed Oct 09, 2019 3:03 pm
Attacks discussion	0	0	No posts

LOGIN • REGISTER

Username: Password: I forgot my password | Remember me □

WHO IS ONLINE

In total there is 1 user online :: 0 registered, 0 hidden and 1 guest (based on users active over the past 5 minutes)
Most users ever online was 3 on Mon Sep 30, 2019 4:27 pm

STATISTICS

Total posts 33 • Total topics 1 • Total members 3 • Our newest member orange

All times are UTC

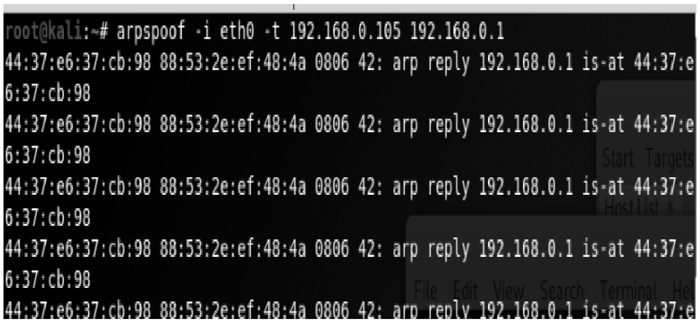
Figure 3: Successful connection to the webpage using IP 192.168.0.101

Attacks

Arp spoof attack

In this phase, different types of attacks in the phpBB3 platform. The first type of attack performed was Arp Spoof attack. For an Arp spoof attack, a malicious user sends unsolicited ARP replies to both the gateway and the target LAN user. Arp spoof attack attempts to divert traffic from its originally intended host to an attacker instead.

For an Arp Spoof attack, the Kali Linux attack machine was configured for IP forwarding and the command "echo 1 > /proc/sys/net/ipv4/ip_forward" was used. After enabling IP forwarding, we attacked the target IP (Victim PC) and default gateway of the network using arpspoof attack. Figure 4 displays the command used:



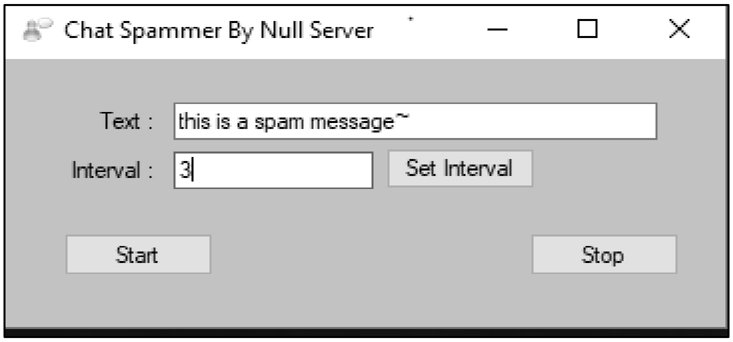
```
root@kali:~# arpspoof -i eth0 -t 192.168.0.105 192.168.0.1
44:37:e6:37:cb:98 88:53:2e:ef:48:4a 0806 42: arp reply 192.168.0.1 is-at 44:37:e
6:37:cb:98
44:37:e6:37:cb:98 88:53:2e:ef:48:4a 0806 42: arp reply 192.168.0.1 is-at 44:37:e
6:37:cb:98
44:37:e6:37:cb:98 88:53:2e:ef:48:4a 0806 42: arp reply 192.168.0.1 is-at 44:37:e
6:37:cb:98
44:37:e6:37:cb:98 88:53:2e:ef:48:4a 0806 42: arp reply 192.168.0.1 is-at 44:37:e
6:37:cb:98
44:37:e6:37:cb:98 88:53:2e:ef:48:4a 0806 42: arp reply 192.168.0.1 is-at 44:37:e
```

Figure 4: Arp spoofing attack

In the above command, the first IP was set as the target machine IP and the second IP as a default gateway IP address. This command kept sending ARP packets to the target IP and default gateway.

Forum Spam

Another attack performed was spamming the forum. Forum spamming repeatedly posted the messages in a discussion post. A chat spammer was used because it is a free open source tool, to spam the forum. This tool flooded the discussion forum with messages. Specifically, text was set to "this is a spam message". Figure 5 illustrates the Chat Spammer used.



Chat Spammer By Null Server

Text : this is a spam message~

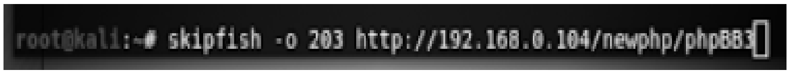
Interval : 3

Figure 5: Chat spammer tool

Session Hijacking

Session Hijacking is a method of taking over a web user session by stealing an active communication session from a legitimate user. Web applications keep track of logged in users through the use of sessions. With phpBB3, users are tracked using session identifier cookie (Sid) (Fong, Lee, Lin, & Yue, 2010). In this type of attack, if the attacker is on the same network, a valid session ID can be spoofed to get into the system to extract data.

For this type of attack, Skipfish, an open source tool in Kali Linux, was used. Skipfish is an active web application security reconnaissance tool that scans session IDs for applications that put session IDs in the URL. Figure 6 illustrates the command used to scan the web application for session ID.



```
root@kali:~# skipfish -o 203 http://192.168.0.104/newphp/phpBB3
```

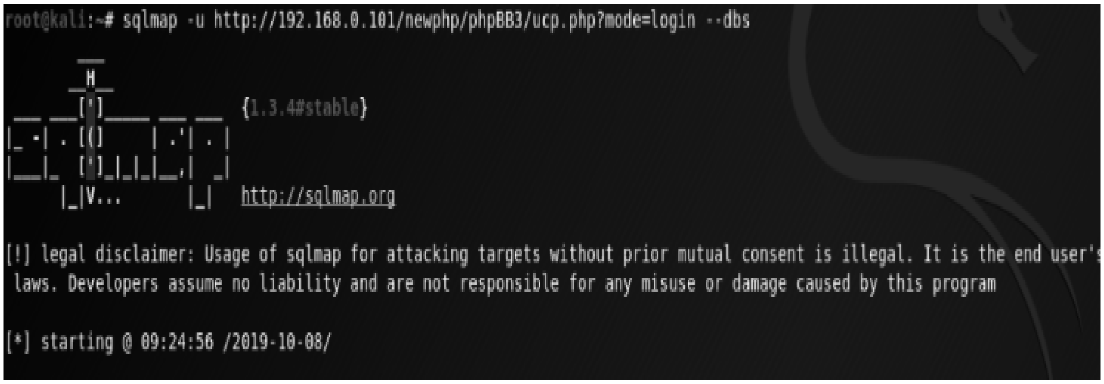
Figure 6: Skipfish tool for session hijacking

SQL Injection Attack

SQL injection attacks are a very common threat to websites that have their input validation poorly implemented; hence, making its database prone to attacks. SQL injection is a code injection technique used to attack database applications, in which an attacker inserts malicious SQL statement for execution to access data. A vulnerable website can easily lead a company to be hacked and their data stolen by malicious people. Any sort of hacking on a company can lead to massive losses of confidential data that can be used against the employees of the company or the company itself.

During implementation of this attack the common tools we used were Kali Linux and SQLmap tool. Once kali Linux was running, we opened the terminal and typed in SQLmap –h, which lists all the commands that can be used to execute further.

As shown in Figure 7, the "*SQLmap –u* *http://192.168.0.1/newphp/phpBB3/ucp.php?mode=login* *–dbs"* command was used. This command enabled the SQLmap to check for a vulnerability in the web application's database in different areas.

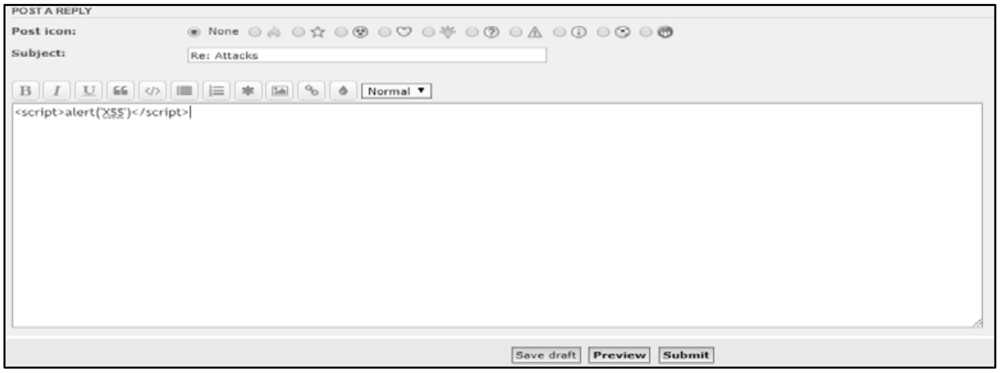


```
root@kali:~# sqlmap -u http://192.168.0.101/newphp/phpBB3/ucp.php?mode=login --dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.3.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's
 laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 09:24:56 /2019-10-08/
```

Figure 7: SQLmap tool used to inject the database.

Cross-site Scripting

Cross-site scripting attacks are malicious client-side code injection attack. For this attack, malicious java script was injected in the comment section of the web page. The main purpose of this attack was to steal a user's identity data – cookies, session ID and other information. As shown in figure 8, JavaScript was injected into the reply section of the forum. The malicious script used was "<script>alert('XSS')</script>".



POST A REPLY

Post icon: ● None ○ ○ ○ ○ ○ ○ ○ ○ ○ ○ ○

Subject: Re: Attacks

Normal ▼

```
<script>alert('XSS')</script>
```

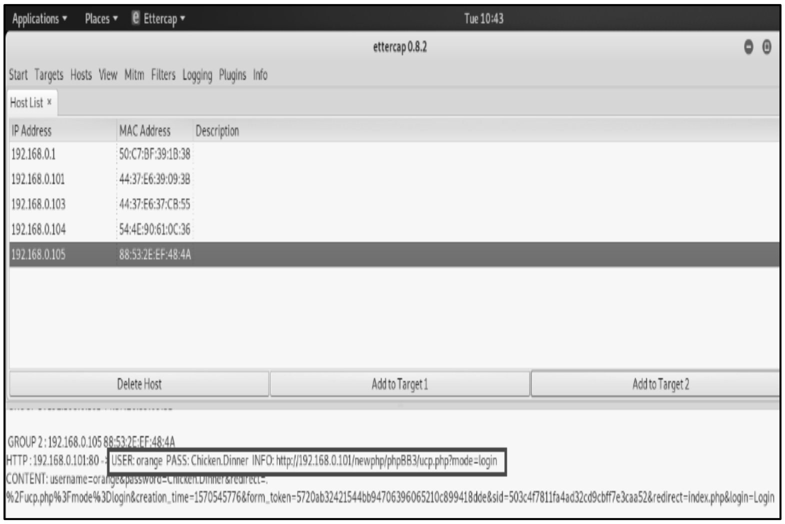
Figure 8: Malicious script injected in the reply section of the discussion post

RESULTS

This sections presents results that were obtained by the implementation of the five different types of attacks in the phpBB3 platform.

Arp Spoof Attack Results

Our results show Arp spoof attack was successful. Figure 9 shows the success Arp spoof attach. Specifically, we were able to obtain the username and password in the attacker machine using Ettercap when the victim logged into the phpBB3 discussion forum.



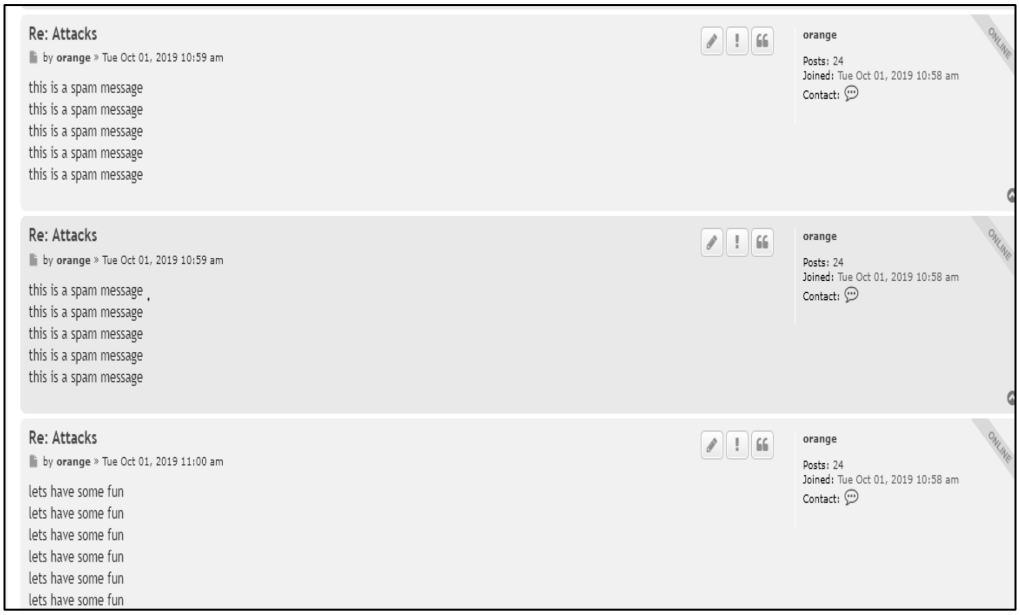
IP Address	MAC Address	Description
192.168.0.1	50:C7:BF:39:1B:38	
192.168.0.101	44:37:E6:39:09:3B	
192.168.0.103	44:37:E6:37:CB:55	
192.168.0.104	54:4E:90:61:0C:36	
192.168.0.105	88:53:2E:EF:48:4A	

```
GROUP 2 : 192.168.0.105 88:53:2E:EF:48:4A
HTTP : 192.168.0.101:80 -> USER: orange  PASS: Chicken.Dinner  INFO: http://192.168.0.101/newphp/phpBB3/ucp.php?mode=login
CONTENT: username=orange&password=Chicken.Dinner&redirect=.
%2Fucp.php%3Fmode%3Dlogin&creation_time=1570545776&form_token=5720ab32421544bb94706396065210c899418dde&sid=503c4f7811fa4ad32cd9cbff7e3caa52&redirect=index.php&login=Login
```

Figure 9: Successful Arp Spoof Attack that captures login credentials

Forum Spam Attack Results

Figure 10 shows the forum spam was successful and the discussion post was flooded with “this is a spam message” and “let’s have some fun” texts. These messages were flooded within minutes once the start button was pressed.



Re: Attacks
by **orange** » Tue Oct 01, 2019 10:59 am

this is a spam message
this is a spam message
this is a spam message
this is a spam message
this is a spam message

orange
Posts: 24
Joined: Tue Oct 01, 2019 10:58 am
Contact:

Re: Attacks
by **orange** » Tue Oct 01, 2019 10:59 am

this is a spam message
this is a spam message
this is a spam message
this is a spam message
this is a spam message

orange
Posts: 24
Joined: Tue Oct 01, 2019 10:58 am
Contact:

Re: Attacks
by **orange** » Tue Oct 01, 2019 11:00 am

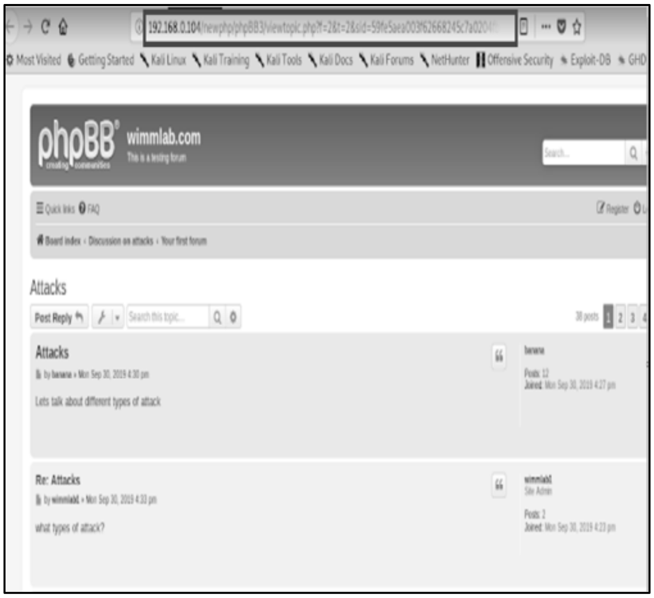
lets have some fun
lets have some fun
lets have some fun
lets have some fun
lets have some fun
lets have some fun

orange
Posts: 24
Joined: Tue Oct 01, 2019 10:58 am
Contact:

Figure 10: The forum after the spam attack

Session Hijacking Results

As illustrated in Figure 11, we were able to capture the session ID and gain unauthorized access to the web server.



192.168.0.104/newphp/phpBB3/viewtopic.php?f=2&t=2&sid=59fe5aea003f62668245c7a0204

Attacks

Attacks
by banana » Mon Sep 30, 2019 4:30 pm

Lets talk about different types of attack

banana
Posts: 12
Joined: Mon Sep 30, 2019 4:27 pm

Re: Attacks
by wimmlab1 » Mon Sep 30, 2019 4:33 pm

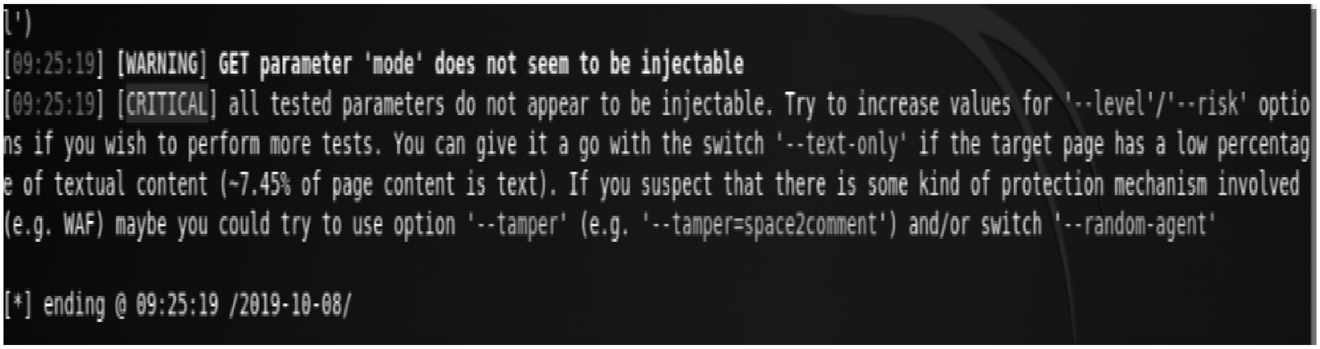
what types of attack?

wimmlab1
Site Admin
Posts: 2
Joined: Mon Sep 30, 2019 4:23 pm

Figure 11: Session hijacking results

SQL Injection Attack Results

Figure 12 shows the result of the SQL injection attack. It is important to note that we were unable to perform this attack as all the parameters that were tested did not appear to be injectable.

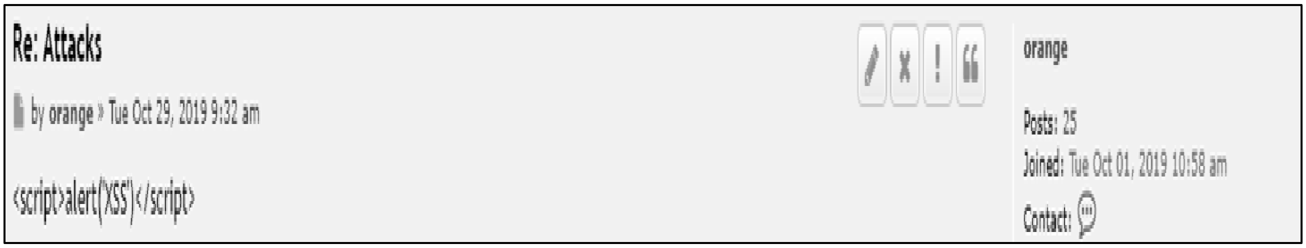


```
l')
[09:25:19] [WARNING] GET parameter 'mode' does not seem to be injectable
[09:25:19] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' optio
ns if you wish to perform more tests. You can give it a go with the switch '--text-only' if the target page has a low percentag
e of textual content (~7.45% of page content is text). If you suspect that there is some kind of protection mechanism involved
(e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 09:25:19 /2019-10-08/
```

Figure 12: SQL injection attack results

Cross-site Scripting Attack Results

Figure 13 shows the attack was not successful as it did not successfully activate the malicious script that was inserted in the reply section. The result depicted plain text that was printed out with no effects.



Re: Attacks

by orange » Tue Oct 29, 2019 9:32 am

<script>alert('XSS')</script>

orange

Posts: 25
Joined: Tue Oct 01, 2019 10:58 am
Contact:

Figure 13: Cross-Site scripting attack results

RECOMMENDATIONS & PROPOSED COUNTERMEASURES

One of the common ways of ensuring security of data and accounts is through password encryption, which involves application of a password processing function (Deepa & Thilagam, 2016). It secures the password information, thus, protecting it from hackers' activities. Users can also protect their data and accounts from threats of attack by enabling a two-step authentication process. Apart from the password provided when logging into an account, a verification code is sent to a user's mobile phone or email (Sharma, Gupta, & Khanna, 2019). They have to input the verification code for them to access the account. Web application users should also ensure that they use Hyper Text Transfer Protocol Secure (HTTPS) connection when they are logging in into any web server or while engaging in online shopping and online banking (Baitha & Vinod, 2018). Web application fora can further be protected through improved security protection of the database. It includes continuous update of patches in time and installation of intrusion detection system. Use of these security measures can help keep data shared in web applications secure.

CONCLUSION

Web applications enabled by phpBB3 software are widely used in various functions. As is indicated in the above demonstrations, users and technology experts can exploit the security vulnerabilities found on the phpBB3 platform and come up with possible fixes that could prevent the attack from happening in the future. The vulnerabilities posed to web applications mainly arise from cross site scripting capability that allows attackers to inject codes on the web browser of a victim and get access to his/her sensitive resources such as passwords, credit card information, and cookies among others. Such security threats can be limited through use of password encryption, two-step, authentication passwords, use of HTTPS connection, and improving security connection of the database.

It is important to note that this research is not without limitations. First, the research is limited phpBB3 platform. The research is also limited to free security tools selected. Future research should address these limitations and expand BBS security testing on different platforms. Additionally, future research should focus on examining additional security tests. In conclusion, this research provides an important foundation for additional research on BBS security testing.

REFERENCES

Alemi, F., Stephens, R. C., Muise, K., Dyches, H., Mosavel, M. & Butts, J. (1996). Educating Patients at Home: Community Health Rap. *Medical Care, 34*(10), OS21.

Baitha, A. K., & Vinod, S. (2018). Session Hijacking and Prevention Technique. *International Journal of Engineering & Technology*, *7*(2.6), 193-198.

Bullen, C, & Bennett, J. (1991). Groupware in practice; an interpretation of work practices. In Dunlop C. and Kling R. (eds.), *Computerization and Controversy: Value Conflicts and Social Choices*. Boston: Academic Press, 257-287.

Chen, J., Du, Y., Liu, L., Zhang, P., & Zhang, W. (2019). BBS Posts Time Series Analysis based on Sample Entropy and Deep Neural Networks. *ENTROPY*, *21*(1), 2-14.

Deepa, G., & Thilagam, P. S. (2016). Securing web applications from injection and logic vulnerabilities: Approaches and challenges. *Information and Software Technology*, *74*, 160-180.

Fong, M., Lee, H., Lin, C. H., & Yue, D. (2010). Security analysis of phpBB3 bulletin board software. *EECE 412 Term Project Report*. Vancouver: University of British Columbia.

Gupta, S., & Gupta, B. B. (2018). XSS-secure as a service for the platforms of online social network-based multimedia web applications in cloud. *Multimedia Tools and Applications*, *77*(4), 4829-4861.

Huang, H., & Leung, L. (2012). Gratification Opportunities, Self-Esteem, and Loneliness in Determining Usage Preference of BBS and Blogs Among Teenagers in China. *Atlantic Journal of Communication*, *20*(3), 141–157.

Huang, L. (2010). Social contagion effects in experiential information exchange on bulletin board systems. *Journal of Marketing Management*, *3–4*.

Jin, X.L.; Cheung, C.M.K.; Lee, M.K.O.; Chen, H.P. (2009). How to keep members using the information in a computer-supported social network. *Computer Human Behavior*, 25(1), 1172–1181.
Kamal, P. (2016). State of the Art Survey on Session Hijacking. *Global Journal of Computer Science and Technology*.

Letsoalo, E., & Ojo, S. (2017, May). Session hijacking attacks in wireless networks: A review of existing mitigation techniques. In *the Proceedings of the 2017 IST-Africa Week Conference (IST-Africa),* 1-9.

Long, C. O., Greenberg, E. A., Ismeurt, R. L., & McGrath, J. M. (2001). Web-Based Bulletin Boards, *Home Healthcare Nurse*. 19(3), 177-178.

Makulowich, J. S. (1993). The Use of Electronic Communications in Environmental Health Research. *Environmental Health Perspectives*, *101*(1), 34.

Malone, T., & Rockart, J. (1993). How will information technology reshape organizations? In Bradley, S., Hausman, J., and Nolan, R. (eds,), *Globalization, Technology and Competition*. Boston: Harvard Business School Press, 37—56.

Marashdih, A. W., Zaaba, Z. F., & Suwais, K. (2018, October). Cross Site Scripting: Investigations in PHP Web Application. In *the Proceedings of the 2018 International Conference on Promising Electronic Technologies (ICPET)*, 25-30.

Prokhorenko, V., Choo, K. K. R., & Ashman, H. (2016). Web application protection techniques: A taxonomy. *Journal of Network and Computer Applications*, *60*, 95-112.

Robinson, T. (2019). Reboot: cybersecurity takes the stage: No longer just the concern of it, cybersecurity is the bad boy headliner that dominates centerstage and all stages beyond." *SC Magazine: For IT Security Professionals (15476693)* 30 (6): 8–22.

Sharma, P., Gupta, D., & Khanna, A. (2019). e-Commerce Security: Threats, Issues, and Methods. *Cyber Security in Parallel and Distributed Computing: Concepts, Techniques, Applications and Case Studies*, 61-77.

Tillquist, J. (1996). Participation on Electronic Bulletin Board Systems: An Empirical Analysis of Work Value Congruency. *Journal of Management Information Systems*, *13*(1), 107.

Tundis, A., Mazurczyk, W., & Mühlhäuser, M. (2018, August). A review of network vulnerabilities scanning tools: types, capabilities and functioning. In *Proceedings of the 13th International Conference on Availability, Reliability and Security*. 1-10.

Yates, J. (1989). Control through Communication. Baltimore: Johns Hopkins University Press.

Zhang, L., & Fan, J. (2014). The security analysis of PhpBB forum. *International Conference on Cyberspace Technology*. DOI: 10.1049/cp.2014.1367