UPB 2.2.7 Zero-Day Vulnerability Report

I2Sec CO., LTD.

May 16, 2011

Gi beom Hong
hondle20@gmail.com

Proprietary & Confidential

INDEX

1. Introduction

1-1. OWASP Top 10

OWASP Top 10 from Open Web Application Security Project released 10 things that are most critical web application security risks. OWASP Top 10 2010 release of the 'top 10 most dangerous attack' of web application security vulnerability was introduced. And "Broken Authentication and Session Management" is found as a result of a UPB vulnerability analysis.

OWASP Top 10 -2010
A1 - Injection
A2 - Cross-site scripting (XSS)
A3 - Broken Authentication and Session
A4 - Insecure Direct Object References
A5 - Cross Site Request Forgery (CSRF)
A6 - Security Misconfiguration
A7 - Failure to Restrict URL Access
A8 - Unvalidated Redirects and Forwards
A9 - Insecure Cryptographic Storage
A10 - Insufficient Transport Layer Protection

1-2. Broken Authentication and Session Management Vulnerability

When developers are programming web application based solutions they rarely focus on how the user's session is managed. Failing to keep this in mind can lead developers to introduce session management vulnerabilities in their applications.

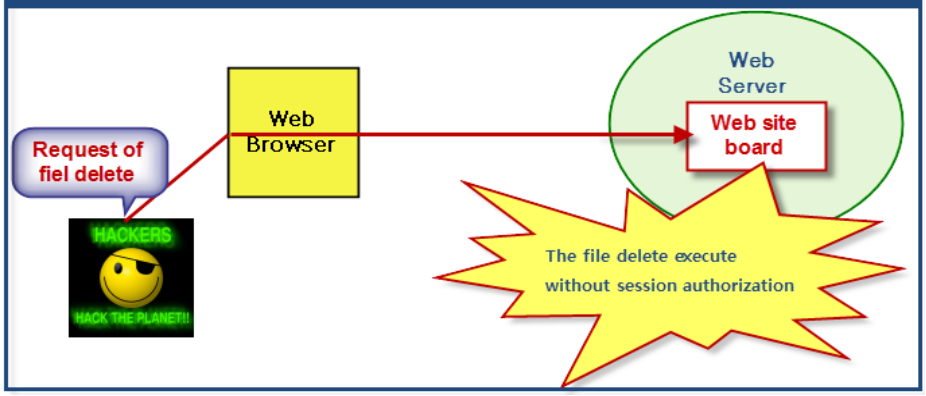
Session management vulnerabilities occur when developers fail to protect their users sensitive information such as user names, passwords, and session tokens.

Broken authentication vulnerabilities occur when developers fail to use authentication methods that have been adequately tested and rely on their own, often flawed, method for authenticating users.

These vulnerabilities are very hard for developers to identify on their own due to the far-reaching aspect of the code that handles session and authentication.

This vulnerability is occurred because there was no the file owner's authentication process ([Figure 1-1] reference). When a request of delete file to Bulletin board of the web site, values of Hidden Field were analyzed. The result, file was deleted post's ID, file's ID and file's name only. There was no certification process when delete file.

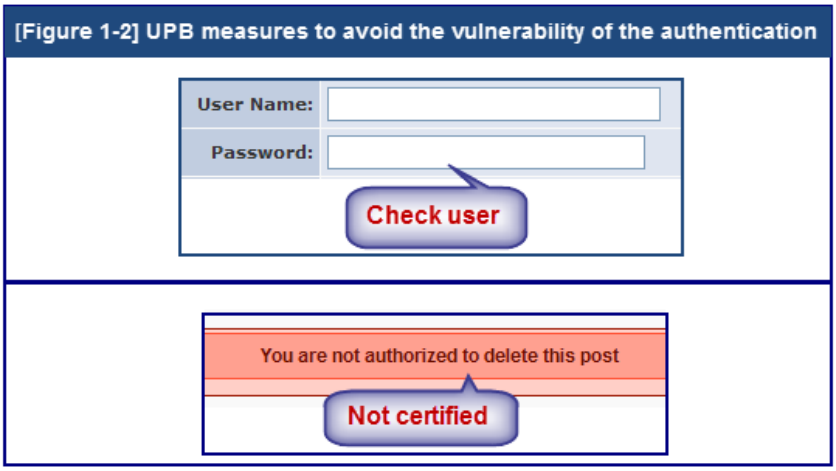
[Figure 1-1] Broken Authentication and Session Management



UPB approve the request to determine user's Session, Cookie information and Permission to protect Broken Authentication and Session Management. But the certification process did not set any application. So only correction in field of request message can delete the uploaded other user's file or admin's file.

To prevent this, Such as [Figure 1-2], when the request of delete file is made, authentication process is required owner of the file correct. In order to determine whether correct file's owner, verification code for Session and Cookie must be inserted.

[Figure 1-2] UPB measures to avoid the vulnerability of the authentication



UPB had inserted these preventive measures into application. However, request of the delete file didn't occur this verification.

Key point of "Broken Authentication and Session Management" attack were as follows.

Key points of Broken Authentication and Session Management attack

● Threat Agents(Attacker): Consider anonymous external attackers, as well as users with their own accounts, who may attempt to steal accounts from others. Also consider insiders wanting to disguise their actions.

● Attack Vectors(Attack path): Attacker uses leaks or flaws in the authentication or session management functions (exposed accounts, passwords, session IDs) to impersonate users.

● Security Weakness(Security Vulnerability): Developers frequently build custom authentication and session management schemes, but building these correctly is hard. As a result, these custom schemes frequently have flaws in areas such as logout, password management, timeouts, remember me, secret question, account update, etc. Finding such flaws can sometimes be difficult, as each implementation is unique.

● Technical Impacts(Technical Impact): Such flaws may allow some or even all accounts to be attacked. Once successful, the attacker can do anything the victim could do. Privileged accounts are frequently targeted.

● Business Impacts(Business): Consider the business value of the affected data or application functions. Also consider the business impact of public exposure of the vulnerability.

2. Main Subject

2-1. Analyzed & The analysis environment

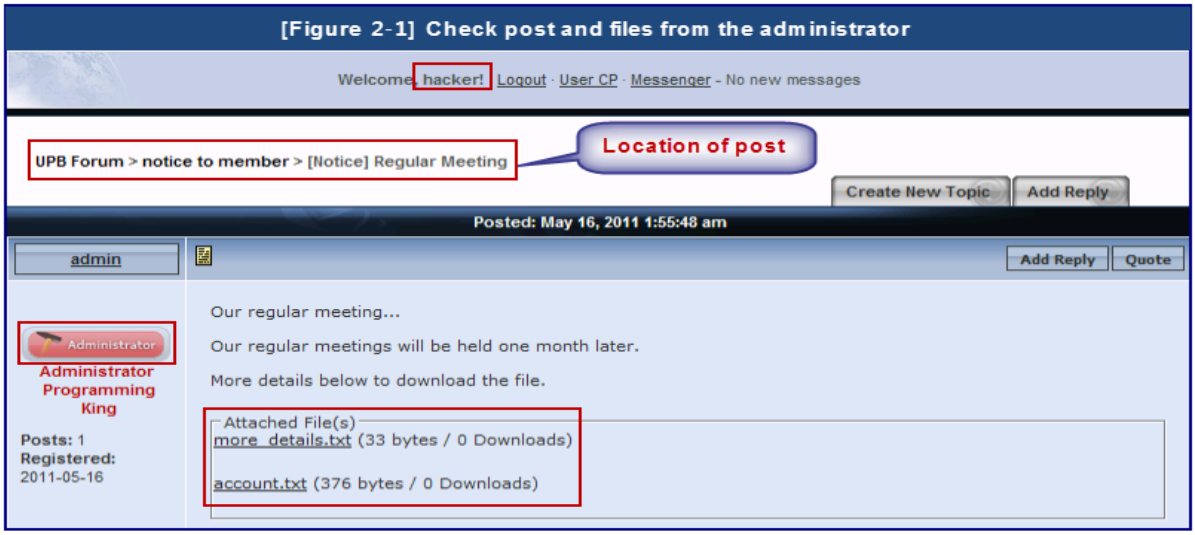
Environment for the analysis of UBP 2.2.7 zero-day vulnerabilities that have been organized as follows.

Vulnerability Analysis Environment	
Web Server	Apache 2.2.14
Database	My SQL 5.1.39
PHP	localhost
Host	PHP 5.2.12
Web Browser	IE 8
OS	Windows XP
UBP	UBP 2.2.7
Top manager id	admin
Attacker id	hacker

Let's verify that how delete the file from hacker's "Broken Authentication and Session Management" attack.

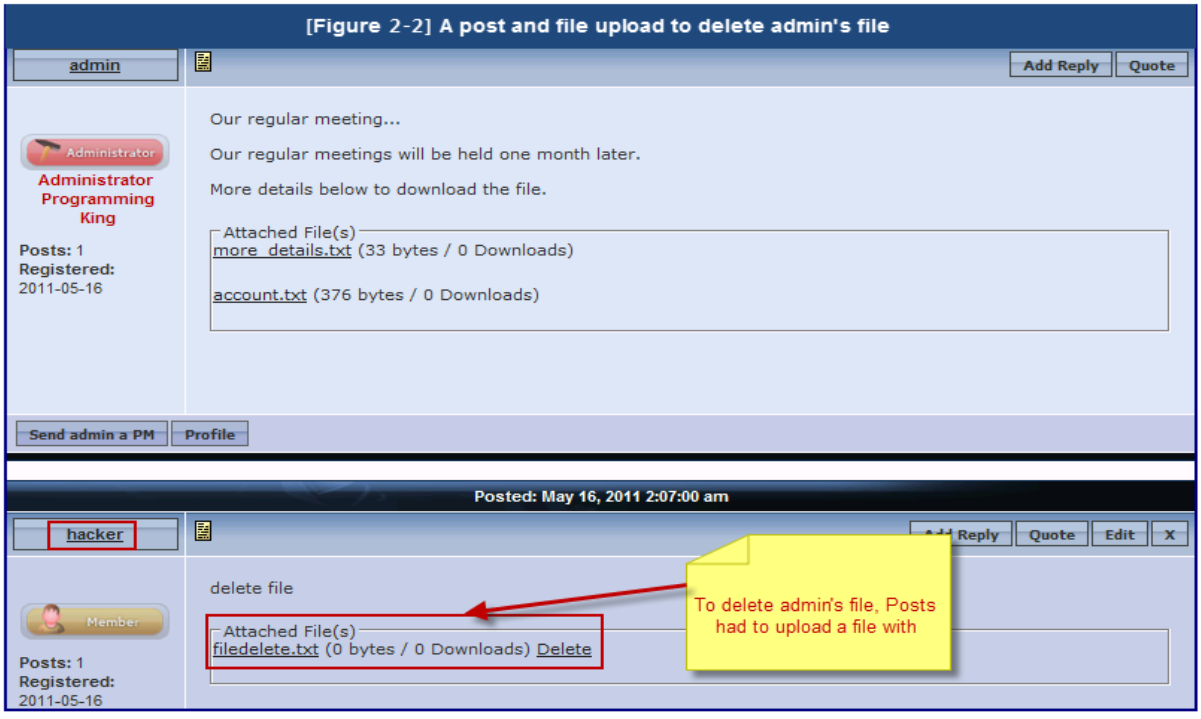
2-2. Penetration Testing

[Figure 2-1] Check post and files from the administrator



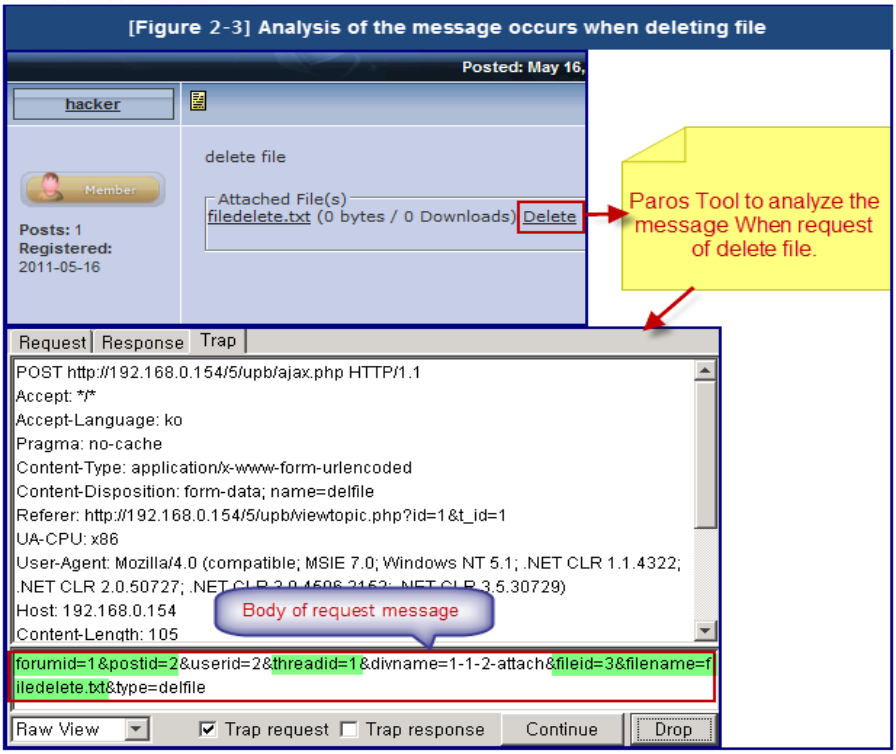
Hacker make sure the administrator's post position and the file.

[Figure 2-2] A post and file upload to delete admin's file



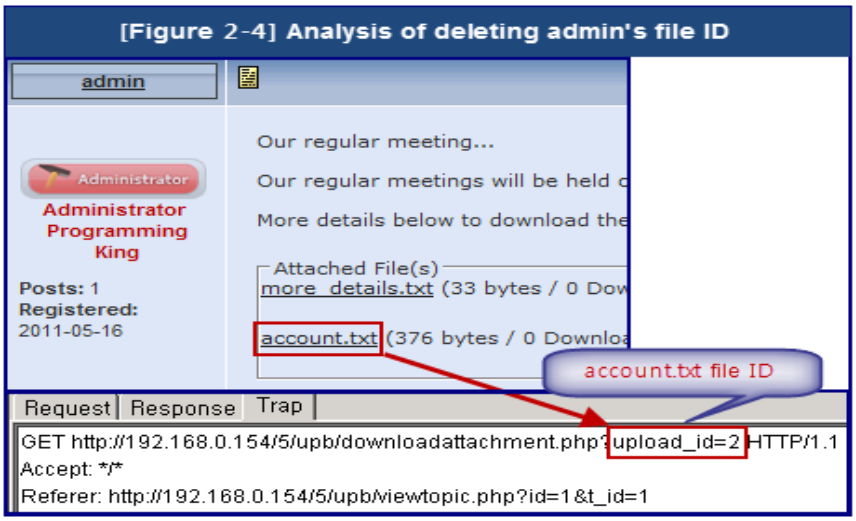
Hacker have uploaded a file and post to confirm the message occurs when a request to file delete.

[Figure 2-3] Analysis of the message occurs when deleting file

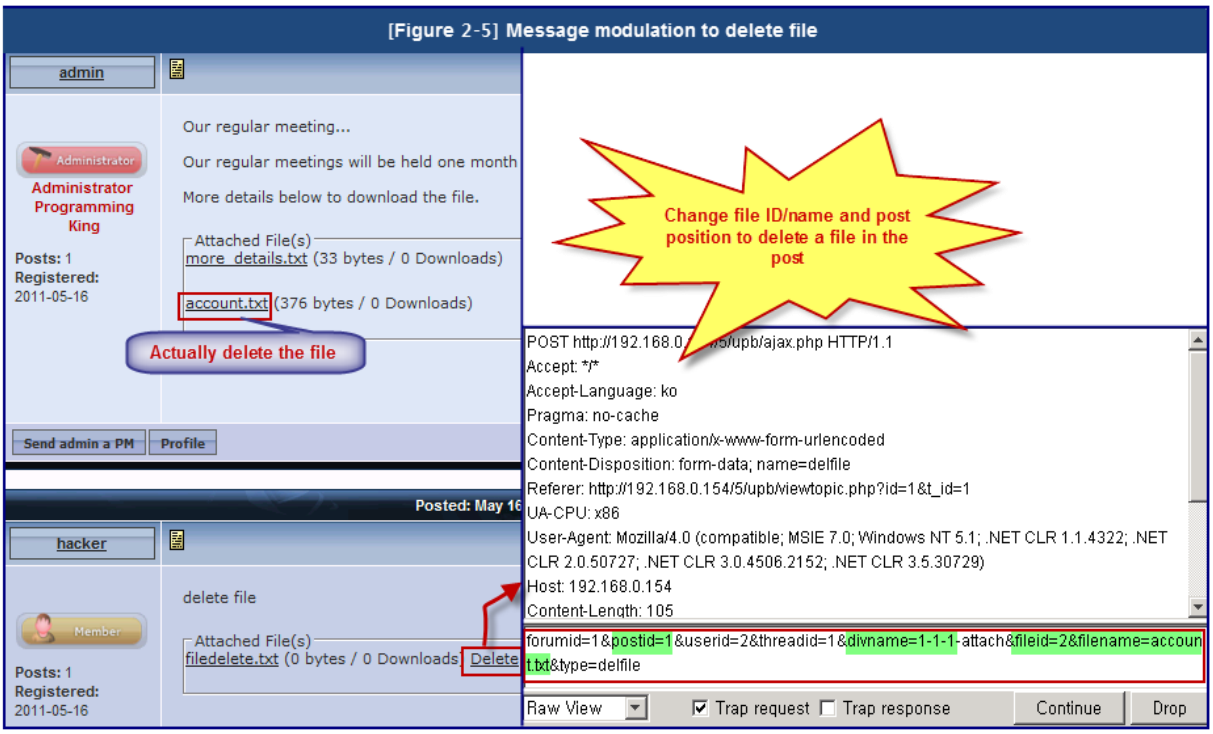


When a reuest to file delete, transmit post's position(forumid, posted, threadid) with file's id and file name(fileid, filename) to delete file through a request message by POST method. After seeing this message, the hacker assume that delete by id and name of the file when file delete.

[Figure 2-4] Analysis of deleting admin's file ID



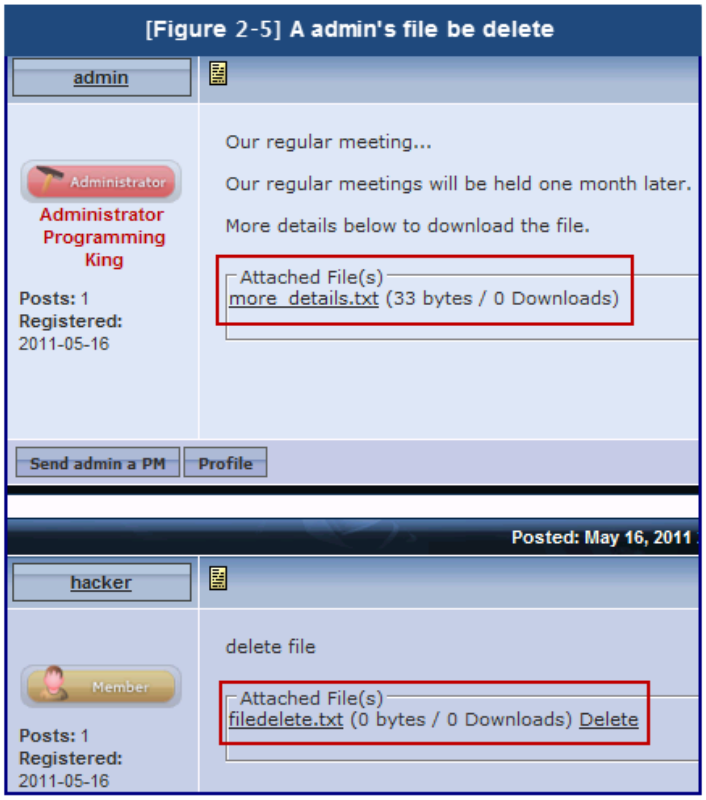
To investigate the ID of the deleteing file, click the file and can be found the file's ID through analysis of the request message.



[Figure 2-5] Message modulation to delete file

The location of the posts from Hacker is 'posted = 2'. therefore, admin's post's ID can be expect 1. This post's ID and file's ID/name is changed by uploaded a manager's file ID/name. And to server send change the delete file request message.

[Figure 2-5] A admin's file be delete



Delete file request message is modulated as admin's file. And send to server and acts without any message. Then comes back to the forum, admin's file is deleted. But hacker's file is remained.

3. Conclusion

3-1. Damage expected

Founded "Broken Authentication and Session Management" in UPB 2.2.7 can be cause great damaged to Integrity of three goals of information security (integrity, confidentiality, availability). Integrity means that the information should not be changes. As can be seen from the above penetration test, uploaded file by manager or account belonging to manager's gruop was deleted. Therefore, integrity is against.

If this file is informing recommendations to its members, or important file to user on use the Web site, the damage can greater than your expected. Dues account was changed and to inform it that the information posted on the bulletin board. And if hacker is deleting the information, users to use the Web site will be fallen into great confusion.

Furthermore if no definite prevention For "Broken Authentication and Session Management" vulnerability, sensitive information can be exposed to a malicious hacker. Therefore, 2nd damage can be expected.

3-2. Security Advisory

Discovered "Broken Authentication and Session Management" vulnerability to UPB 2.2.7 is occurred on execute request without the correct Authentication procedures. To prevent this, occur change message(delete, edit, etc) should be run authentication procedure once again

OWASP recommendations for Broken Authentication and Session management Vulnerabilities
1. A single set of strong authentication and session management controls.
2. Meet all the authentication and session management requirements defined in OWASP's Application Security Verification Standard (ASVS) areas V2 (Authentication) and V3 (Session Management).
3. Have a simple interface for developers. Consider the ESAPI Authenticator and User APIs as good examples to emulate, use, or build upon.
4. Strong efforts should also be made to avoid XSS flaws which can be used to steal session IDs.