


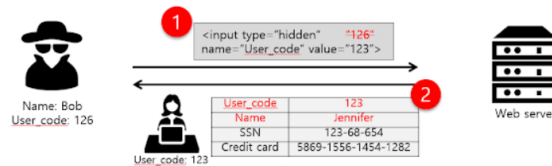


Written February 17, 2019 by
Debojyoti Chakraborty

 Blogs, Cyber News, Owasp

 No comments

OWASP Broken access control attack



source: <http://www.davidromerotrejo.com>

There are many applications available on the web which has role-based access control, which has different functionalities, based on that it determines what the user can do and see. For example, an education based user portal has mainly three roles Admin, Faculty, Student and if it is a healthcare portal the role list will be larger including Doctor, Patient, nurse, admin, Pharmacist, guest user etc.

Applications those are having multiple user access role model, they should implement proper access control policies so that the users can access own content. Any breach in this policy makes the application vulnerable to insufficient authorization.

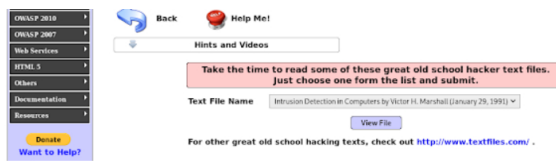
The vulnerability results when an application fails to check the user request to any content is authorized or not. Based on which level of functionality vulnerable it can be said there is a possibility to launch privilege escalation attack. For better understanding let's try this in a practical scenario.

Lunch the mutillidae web application



Goto Owasp 2017 > A5 - Broken Access Control > Insecure Direct Object Reference > Text File Viewer

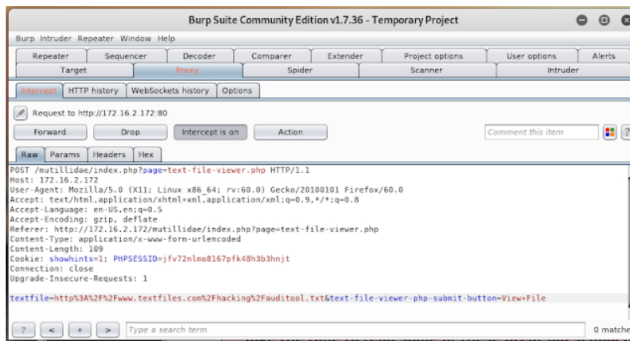




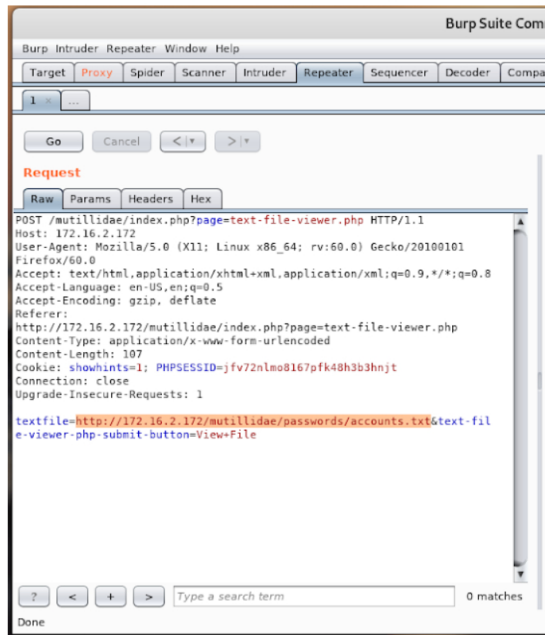
This page is made for reading some article, published by famous old school hacker. But the source of these files not belongs to the web application currently we are in. It is referring to those sources from <http://www.textfiles.com>. It means whenever we will click on the view by after the text file selection it will go to that URL and read from there to display the content.

In this article, we will temper the request using Burp suit and instead of sending the request to textfiles.com we will try to read our local robots.txt file.

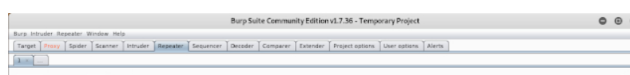
Launch the burp suite and configure it with the local proxy to intercept the web request. Now click on View File and come to burp suit.

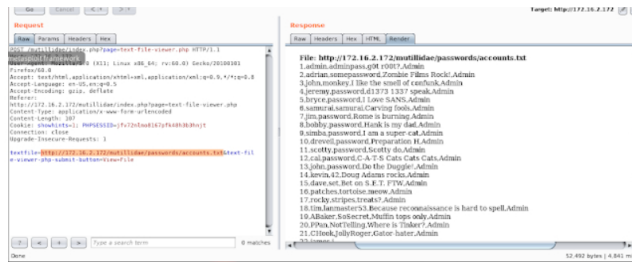


We will send this request to Repeater Tab, for doing so right click and select send to Repeater.



In the request tab, change the textfile value to <http://172.16.2.172/mutillidae/passwords/accounts.txt> and click on Go to see the output in Response tab.





Bingo!! Now we can see the output of the accounts.txt file in the response window. It means this file is not restricted to get access and view the content. Using this method a hacker can easily go through the directory and get access to other files too. So the best practice is, implement access control on server directories and files.

Please let me know if you have any further doubt on the same and give you valuable feedback in the comment section below. Thank you for reading my article we will see you soon. Happy hacking!!

☐ funny (0) ☐ interesting (0) ☐ cool (0)

Reactions:

[Newer Post](#)


[Home](#)

[Older Post](#)

0 comments:

[Post a Comment](#)

Enter your comment...



Comment as: [Google Account](#)

Publish

Preview

Pages

[Penetration Testing](#)
[Web-Penetration-Testing](#)
[CTF Challenges](#)
[Red Teaming](#)
[Tutorials and Others](#)
[Malware Research](#)
[About us](#)
[Contact us](#)
[Privacy Policies](#)

Labels

[Blogs \(17\)](#)
[CTF \(5\)](#)
[Cyber News \(29\)](#)
[Deep Web \(3\)](#)
[IoT \(3\)](#)
[Malware \(5\)](#)
[Owasp \(10\)](#)
[Tutorials \(5\)](#)
[Vulnerability \(3\)](#)

Popular Posts



[OWASP SQL Injection – Authentication bypass using BurpSuite](#)

SQL injection is a very common web application vulnerability, where hackers inject malicious SQL query to fetch sensitive information ...



[Cyber Threat Intelligence: weaponizing cyber defense](#)

The ability to dig in deep to understand what a person really cares about, who they are, without their knowledge, is a valuable skill set ...



[The Cybaze ZLab- Yoroi team spotted the latest version of APT28 Lojox rootkit aka Double-Agent](#)

A new type of the infamous APT28 Lojox (aka Double-Agent) has been spotted by Cybaze Z Lab – Yoroi team. APT28 is the latest vers...



[Hacking WPA2 Wi-Fi password using Evil Twin Attack | DNSMASQ and Hostapd](#)

Wireless protocols have drastically evolved since 2003 after the invention of WPA in terms of secured Wi-Fi access. These days , wireles...



[Mimikatz: Credential harvest, Pass the hash, Golden Ticket](#)

Mimikatz is a tool built in C

Facebook

Blog Archive

[February \(4\)](#)

Total Pageviews

Advertisement

mmikatz is a tool, built in C language and used to perform password harvesting in windows platform. It is very well known to ext...