Professor: Fabio Palomba

Coordinator:
Emanuele Iannone
Giammaria Giordano

SOFTWARE DEPENDABILITY'S PROJECT REPORT

AUTOMATED SOFTWARE VULNERABILITY TESTING

Muhammad Hamza Khan
Computer Science
University of Salerno
Salerno Italy
m.khan10@studenti.unisa.it

Areeb Ullah Khan
Computer Science
University of Salerno
Salerno Italy
a.khan4@studenti.unisa.it

Fahad Ahmed
Computer Science
University of Salerno
Salerno Italy
f.ahmed@studenti.unisa.it

ABSTRACT

The primary life cycle process includes acquisition, supply, development, operation, and maintenance. Dependability processes such as fault prevention, fault tolerance, fault removal and fault estimation must be executed over a software life cycle. There is need to develop and maintain the system continuously and consistently because no process cycle has been developed to engineer secured information system. Chosen OWASP as a testing tool to find weakness and vulnerabilities of application by users customize mode. Considering bypass authentication Schema as a testing approach which follows Black Box and Grey Box testing techniques which provide vulnerability assessment which follows four steps that are testing analysis assessment and remediation, we have examined authentication in adequacy that permits automated attacks such as credential stuffing where the attacker has a list of user name and password and apply step by step actions to find vulnerabilities of application.

To retain the system continuously there is a need to revise the tasks such as design, development, and test and maintain. Software market competition is increasing day by day all over the world.

INTRODUCTION

Vulnerability Testing is the process of identifying, quantifying, and prioritizing the vulnerabilities in a system. Examples of systems for which vulnerability assessments are performed include, but are not limited to, information technology systems, energy supply systems, water supply systems, transportation systems and communication systems.

Authentication is the process of attempting to verify the digital identity of the sender of a communication. A common example of such a process is the log on process. Testing the authentication schema means understanding how the authentication process works and using that information to circumvent the authentication mechanism. A good authentication method protects the sensitive information exchanged between the client and the server. That means any malicious attackers sniffing the messages must not be able to decrypt them and get the credential of the client.

In addition, it is often possible to bypass authentication measures by tampering with requests and tricking the application into thinking that the user is already authenticated. This can be accomplished either by modifying the given URL parameter, by manipulating the form, or by counterfeiting sessions.

METHODOLOGIES

There are several methods of bypassing the authentication schema that is used by a web application.

Black Box Testing is a software testing method in which the functionalities of software applications are tested without having knowledge of internal code structure, implementation details and internal paths. Black Box Testing mainly focuses on input and output of software applications and it is entirely based on software requirements and specifications. It is also known as Behavioral Testing.

Black Box Testing

*Article Title Footnote needs to be captured as Title Note

https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/04-Testing_for_Bypassing_Authentication_Schema.html

In **Direct Page Request,** a web application implements access control only on the log in page, the authentication schema could be bypassed. For example, if a user directly requests a different page via forced browsing, that page may not check the credentials of the user before granting access. Attempt to directly access a protected page through the address bar in your browser to test using this method.

SQL injection (Form Based Authentication) is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. It generally allows an attacker to view data that they are not normally able to retrieve. This might include data belonging to other users, or any other data that the application itself is able to access. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behavior.

A **session ID** is a unique number a server assigns to requesting clients. ID stands for identifier and is used to identify and track user activity. This unique ID can be a number code, numerical code, or alphanumeric code. In computer science, a session is a temporary connection between server and client. The short version SID (session ID) is also commonly used, for example in the context of web servers.

KEYWORDS

Vulnerabilty Testing, Software Tesing, Authentication Bypass, BlackBox Tesing, ZAP, OWASP.

RESULTS

The Open Web Application Security Project (**OWASP**) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted. OWASP tools, documents, videos, presentations, and chapters are free and open to anyone interested in improving application security and advocate approaching application security as a people, process, and technology problem, because the most effective approaches to application security require improvements in these areas. OWASP is a new kind of organization. Our freedom from commercial pressures allows us to provide unbiased, practical, and cost-effective information about application security.

Broken authentication is an umbrella term for several vulnerabilities that attackers exploit to impersonate legitimate users online. Broadly, broken authentication refers to weaknesses in two areas: session management and credential management. Both are classified as broken authentication because attackers can use either avenue to masquerade as a user: hijacked session IDs or stolen login credentials.

Attackers employ a wide variety of strategies to take advantage of these weaknesses, ranging from huge credential stuffing attacks to highly targeted schemes aimed at gaining access to a specific person's credentials.

In recent years, broken authentication attacks have accounted for many of the worst data breaches, and security experts sound the alarm about this underrecognized threat. The Open Web Application Security Project (OWASP) has included it in its "Top 10" list of the biggest web application security risks since 2017. By 2020, broken authentication had climbed to the number two spot.

Below, we'll explain what weaknesses are associated with broken authentication and how businesses can guard against them.

What Scenarios Can Cause Broken Authentication?
As mentioned earlier, the primary reasons for broken authentication. Let's understand them one by one.

a. Poor credential management
Consumer credentials can be hijacked to gain access to the system. There are various ways that the hacker can steal critical information, such as the following:

Weak passwords: The consumer creates a weak password like '12345' or 'pass123'. The hacker can use various password cracking techniques like rainbow tables and dictionaries to gain access to the system.

Weak cryptography: Using weak encryption techniques like base64 and weak hashing algorithms like SHA1 and MD5 make credentials vulnerable. Which is why they must be stored using strong hashing algorithms that make password cracking challenging.

b. Poor session management
Let's assume you like playing online games. You log in to the application and make several interactions with the network.

The application issues a session ID whenever you log in and records all your interactions. It is through this ID that the application communicates with you and responds to all your requests.

The OWASP broken authentication recommendations state that this session ID is equivalent to your original login credentials. If hackers steal your session ID, they can sign in by impersonating your identity. This is known as session hijacking.

The following points list the scenarios that can cause broken authentication.

- Weak usernames and passwords.
- Session fixation attacks.
- URL rewriting.
- Consumer identity details aren't protected when stored.
- Consumer identity details are transferred over unencrypted connections.

Tool

We used OWASP's Zed Attack Proxy (ZAP) tool to perform security testing, even if you don't have a background in security testing.

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of the Open Web Application Security Project (OWASP). ZAP is designed specifically for testing web applications and is both flexible and extensible. At its core, ZAP is what is known as a "man-in-the-middle proxy." It stands between the tester's browser and the web application so that it can intercept and inspect messages sent between browser and web application, modify the contents if needed, and then forward those packets on to the destination.

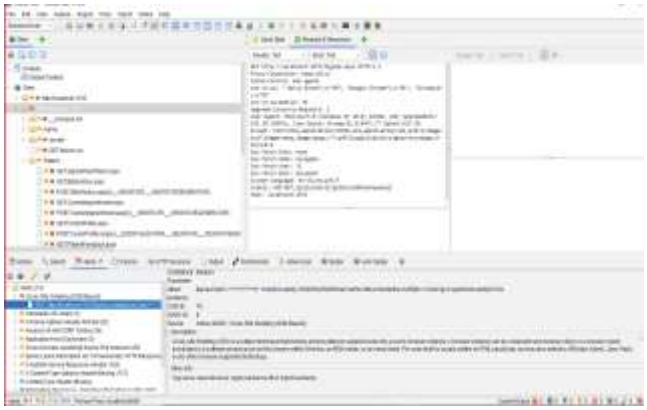


Figure: Using OWASP tool ZAP to find broken authentication flaws.

CONCLUSION

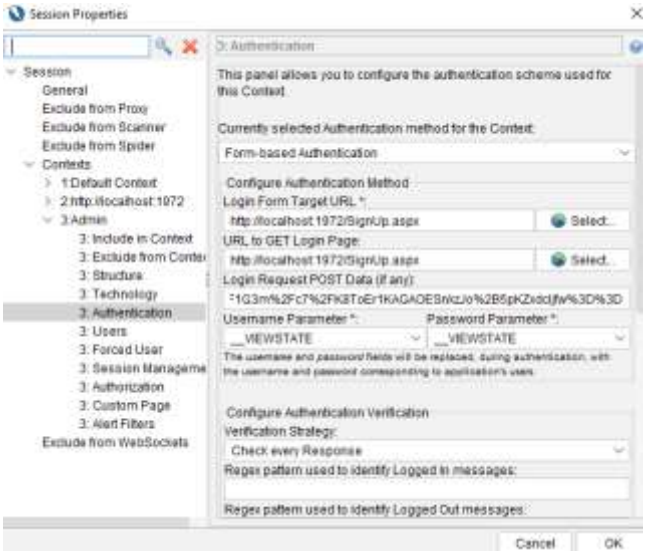
Consider security at all stages of development cycle by its customizing tools. Authentication security testing tool that scans through your web application to identity any security vulnerabilities as possible, ZAP generates the scan report in the form of Alerts that are marked with color coded flags which is helpful for identifying the weakness of authentication by its customize priorities. It is provide best approach to find application's bug by its selective testing type and then user can easily resolve bugs.

REFERENCES

[1] https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/04-Testing_for_Bypassing_Authentication_Schema.html

[2] https://www.zaproxy.org/docs/

[3] https://github.com/muhammadhamzakhan17/SWD-ClinicProject



Professor: Fabio Palomba

Coordinator:
Emanuele Iannone
Giammaria Giordano