

Security Misconfiguration

Overview

Security misconfiguration is one of the most commonly-seen security flaws in web applications. It refers to any security issue which is not a direct result of a programming error but rather a result of a configuration error. Security misconfiguration is usually a result of using default configurations or passwords, ad hoc or insufficient configurations, open cloud storage, poorly configured HTTP headers or use of detailed error messages containing sensitive information.

Security misconfigurations can occur at any level of the web application stack; from the web server or back-end database, to the platform or network services. These misconfigurations can be exploited by an attacker in order to gain unauthorized access to the system and in some cases can result in the attacker taking complete control over the system.

In this project, we will take advantage of security misconfigurations in the web app by exploiting a default account with a default password and inadvertently expose sensitive information via detailed error messages from the server.

Default Accounts with Default Passwords

One example of a security misconfiguration is use of default accounts with their default passwords still enabled and unchanged. These default passwords can be easily guessed by an attacker resulting in unauthorized system access; in fact, there are many websites which actually list default usernames and passwords for a number of different devices and applications. Common default username and password combinations include admin/admin, admin/password, root/root, user/user and user/password. In some cases, a password is not even set. It is evident how relatively simple it is for an attacker, by simply guessing the default password, can gain unauthorized access to a system.

Detailed Error Messages

Another example of a security misconfiguration is returning a detailed error message that exposes information about the underlying server. Any information revealing software or services, versions of software, directory structure, etc... may be used to search for known vulnerabilities of the server. If the server is running a software version that hasn't been updated and has a known vulnerability, bad actors could exploit the known vulnerabilities. This is why error messages should only be returned to the user when absolutely necessary. Messages should contain premade text that informs the user of the problem. They should NEVER contain unvalidated information that could be a security risk, such as error log data.

Attack Procedures

The screenshot below demonstrates the first step for all the Security Misconfiguration attack examples in this write-up. All remaining steps for each Security Misconfiguration attack can be found in their labeled sections.

The screenshot displays a web application titled "Website Security Research Project". It contains an introductory paragraph about web security, a goal statement, and a prompt to select an attack from a drop-down menu. The "Security Misconfiguration" option is selected. An orange callout box provides instructions: "Select 'Security Misconfiguration' from the drop down box to view a summary of this vulnerability. You may download the write-up for a more detailed explanation and then click 'Login' for a demonstration." Below the callout, the "Security Misconfiguration Overview" section is visible, followed by two buttons: "Download Writeup" and "Login". An orange arrow points to the "Login" button.

Website Security Research Project

According to Security Magazine, a study was conducted and found that there is an attack on the web every 39 seconds. Many of these attacks are made possible due to outdated technologies, or because developers aren't aware of standard security measures. Fortunately, many of these gaps in security can be mitigated through education and software updates.

Our goal is to educate by demonstrating how these top attacks on the web are performed. After each demonstration, a detailed write-up that explains how these attacks may be prevented will be provided.

Please select one of the top attacks from the drop-down box below to view more information.

Security Misconfiguration

Select "Security Misconfiguration" from the drop down box to view a summary of this vulnerability. You may download the write-up for a more detailed explanation and then click "Login" for a demonstration.

Security Misconfiguration Overview

Security misconfiguration is one of the most commonly-seen security flaws in web applications. It refers to any security issue which is not a direct result of a programming error but rather a result of a configuration error. Security misconfiguration is usually a result of using default configurations or passwords, ad hoc or insufficient configurations, open cloud storage, poorly configured HTTP headers or use of detailed error messages containing sensitive information.

Security misconfigurations can occur at any level of the web application stack; from the web server or back-end database, to the platform or network services. These misconfigurations can be exploited by an attacker in order to gain unauthorized access to the system and in some cases can result in the attacker taking complete control over the system.

In this project, we will take advantage of security misconfigurations in the web app by exploiting a default account with a default password and inadvertently expose sensitive information via detailed error messages from the server.

Download Writeup Login

Logging On With Default Credentials

Home Website Security Research Project

\$> Faulty Vault Bank

Warning! Vulnerability for Security Misconfiguration **on!** [Click here](#) to switch off

1) Click this button to pre-fill the Username and Password fields with default admin login credentials

2) Click Login button to test default admin credentials

User Login

[Login with Default Credentials](#) [Display Detailed Error Message](#)

Username

admin

Password

.....

[Login](#)

Don't have an account? [Create Account](#)

A common default password for admin accounts is 'admin', which we are testing here

Home Website Security Research Project

\$> Faulty Vault Bank

Welcome to the Administrator Dashboard!

Faulty Vault Bank Dashboard

Quick Stats

11 15,000 Bank Customers [Total Revenue \\$120,000,000](#) [Total Profit 5.3%](#)

Tasks
Calculated in last 7 days

■ This Week ■ This Month

Task	This Week	This Month
1	10	25
2	15	30
3	20	35
4	25	40
5	30	45
6	35	50
7	40	55
8	45	60
9	50	65
10	55	70

Project Monitor
Calculated in last 30 days

— Nov-18 — Nov-20

Day	Nov-18	Nov-20
1	2.0	4.0
2	1.0	4.0
3	3.0	3.0
4	3.0	4.0
5	2.0	3.0
6	1.0	6.0
7	3.0	4.0
8	2.0	5.0
9	4.0	2.0
10	1.0	2.0

Menu

[View User Account Details](#)

[Reset User Password](#)

[Disable User Account](#)

[Change User Credit Limit](#)

[Authorize Transactions](#)

[Logout](#)

3) You have successfully logged onto the admin console using the default login credentials assigned to the admin account

4) Once in the admin console, the attacker can take advantage of admin privileges and effectively take control of the bank

Returning Detailed Error Messages

Website Security Research Project

\$> Faulty Vault Bank

⚠ Warning! Vulnerability for Security Misconfiguration on! Click [here](#) to switch off

User Login

Login with Default Credentials Display Detailed Error Message

Username

fakeUsername

Password

Password

Login

Don't have an account? [Create Account](#)

1.) Click this button to fill in the "Username" field with an invalid username. 2.) Click "Login" (No need to fill in the "Password" field)

Upon an unsuccessful login attempt, a detailed error message is displayed revealing information about the underlying server. This information could provide a bad actor with the details needed to plan and carryout an attack on the web app.

faultyvault.com says

```
(datetime.datetime(2020, 11, 5, 9, 28, 17, 979961),  
&#39;hawkesc[hawkesc] @ localhost [127.0.0.1]&#39;; 37,  
1, &#39;Quit&#39;; b&#39;&#39;)  
(datetime.datetime(2020, 11, 5, 9, 28, 17, 976441),  
&#39;hawkesc[hawkesc] @ localhost [127.0.0.1]&#39;; 37,  
1, &#39;Query&#39;; b&#39;SELECT * FROM  
mysql.general_log a ORDER BY event_time desc LIMIT  
6&#39;))
```

OK

Website Hardening

Every piece of software that you install on your system requires manual security configuration, including the web server, application server and database server. To prevent unauthorized access, change every default password to something secure and not easily guessable by a would-be attacker. Furthermore, uninstall or disable any unused or unnecessary features or services from any new piece of software you install on your system. A minimal platform without any unnecessary components or features is much more secure and is less likely to have as many configuration issues.

Attempt at Logging On With Default Credentials After Website Hardening:

The screenshot displays a web application titled "Website Security Research Project" with a "Home" link in the top left. The main heading is "\$> Faulty Vault Bank". A green banner states "You are on a Safe Login Page" with a link to "Click here to Turn Vulnerability For Security Misconfiguration On". A red error message reads "Incorrect username/password! Please Try again!". Below this is a "User Login" section with two buttons: "Login with Default Credentials" and "Display Detailed Error Message". The "Username" field contains "admin" and the "Password" field contains ".....". A "Login" button is at the bottom, with a link "Don't have an account? Create Account" below it. Two callout boxes on the left provide context: an orange box notes that default admin credentials do not work, and a yellow box notes that the default password for the admin account was changed to a more secure password.

Home Website Security Research Project

\$> Faulty Vault Bank

🔒 You are on a Safe Login Page
[Click here to Turn Vulnerability For Security Misconfiguration On](#)

Incorrect username/password! Please Try again!

User Login

[Login with Default Credentials](#) [Display Detailed Error Message](#)

Username

admin

Password

.....

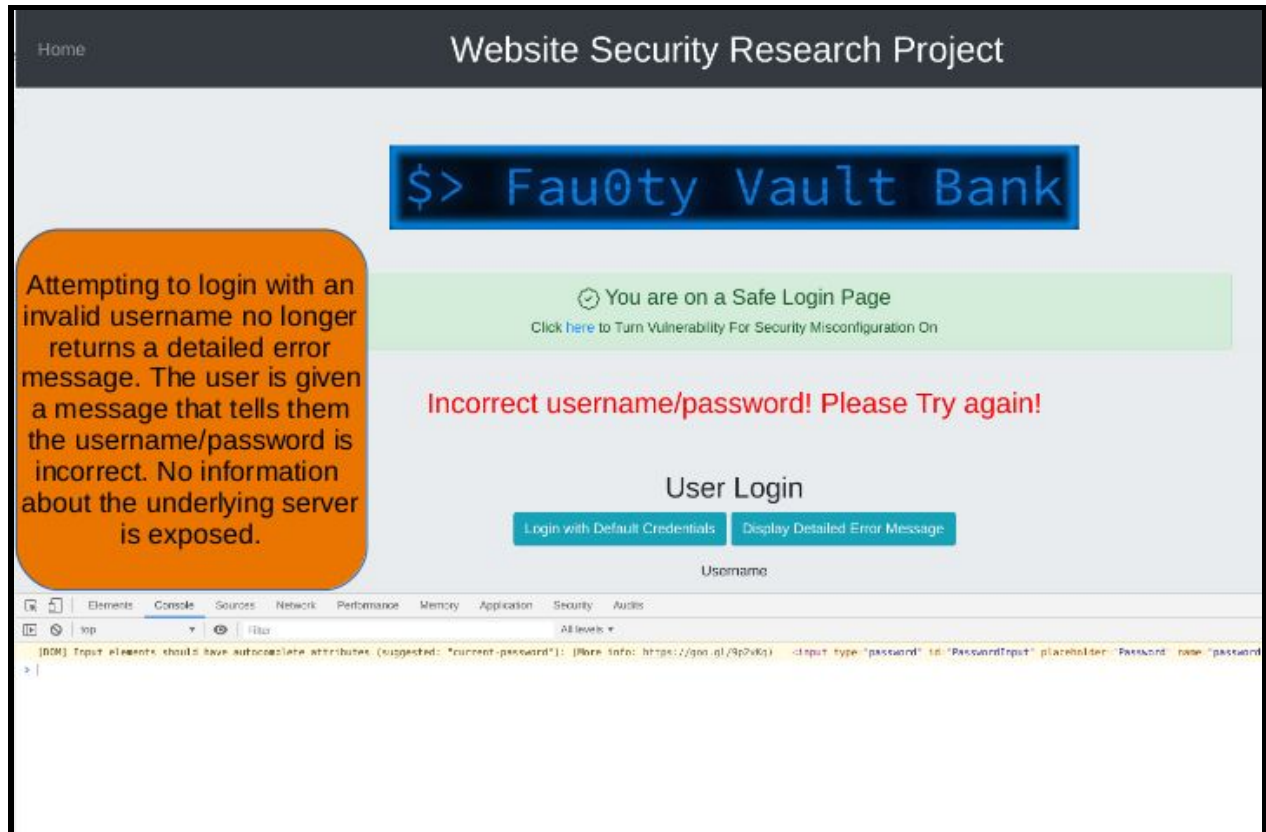
[Login](#)

Don't have an account? [Create Account](#)

Attempting to log on with default admin credentials does not work on the safe login page and an error message is displayed

The default password for the admin account was changed to a more secure password

Attempting To Login With Invalid Username After Website Hardening:



Resources

https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

<https://www.acunetix.com/blog/web-security-zone/security-misconfigurations/>

<https://datarecovery.com/rd/default-passwords/>

https://www.tutorialspoint.com/security_testing/testing_security_misconfiguration.htm