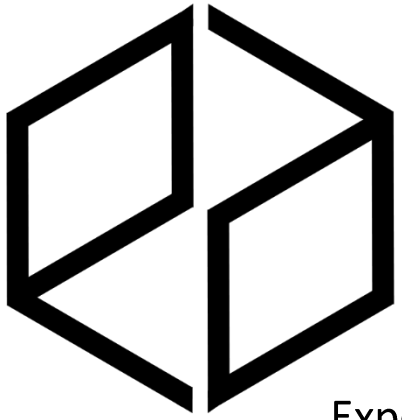
www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #5 Security Misconfiguration

By @isaacsabas



PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

www.pandoralabs.net

We are a Security-as-a-Service company

Providing businesses with on-demand IT security controls for them to meet their 24x7 security strategies & requirements.

We Make IT Secure

OWASP

Open Web Application Security Project


A1: Injection
A2: Broken Authentication and Session Management
A3: Cross-Site Scripting (XSS)
A4: Insecure Direct Object References
A5: Security Misconfiguration
A6: Sensitive Data Exposure
A7: Missing Function Level Access Controls
A8: Cross Site Request Forgery (CSRF)
A9: Using Components with Known Vulnerabilities
A10: Unvalidated Redirects and Forwards

OWASP #5

Security Misconfiguration

OWASP Top 10 Vulnerabilities

Improper server or web application configuration that can lead to various abuse.

Security Misconfiguration

What is it?

How is this vulnerability exploited?

- Debugging feature enabled
- Incorrect directory permissions
- Using default accounts or passwords
- Publicly available setup/configuration pages
- Remote administration ports and services are publicly available

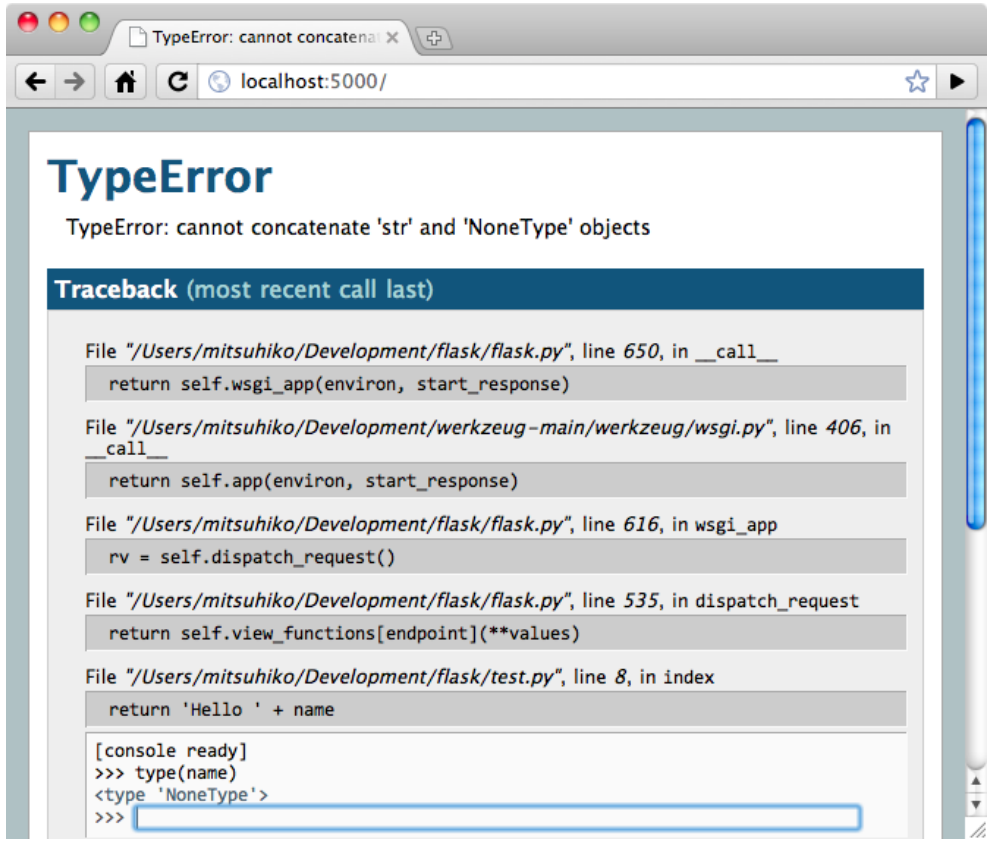
What are the Risks When Exploited?

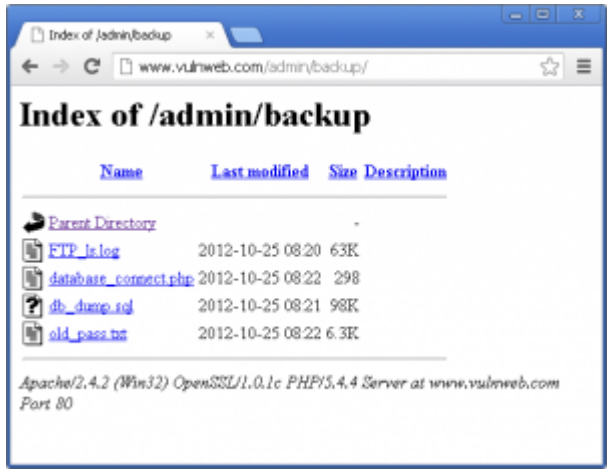
- Data leakage or theft
- Data manipulation
- Negative impact on reputation and income

How do I Prevent Such Vulnerability?

- Apply the concept of least privilege – **Everything off by default!**
- Ensure that the web server is configured according to the secure configuration guidelines
  1. Disable administration interfaces to public
  2. Disable debugging
  3. Disable use of default passwords/accounts
  4. Configure server to prevent unauthorized access and directory listing
  5. Only allow FTP and SSH ports to be access from management IP via firewall

Sample


TypeError: cannot concatena
localhost:5000/
TypeError
TypeError: cannot concatenate 'str' and 'NoneType' objects
Traceback (most recent call last)
File "/Users/mitsuhiko/Development/flask/flask.py", line 650, in __call__
return self.wsgi_app(environ, start_response)
File "/Users/mitsuhiko/Development/werkzeug-main/werkzeug/wsgi.py", line 406, in __call__
return self.app(environ, start_response)
File "/Users/mitsuhiko/Development/flask/flask.py", line 616, in wsgi_app
rv = self.dispatch_request()
File "/Users/mitsuhiko/Development/flask/flask.py", line 535, in dispatch_request
return self.view_functions[endpoint](**values)
File "/Users/mitsuhiko/Development/flask/test.py", line 8, in index
return 'Hello ' + name
[console ready]
>>> type(name)
<type 'NoneType'>
>>>


Index of /admin/backup
www.vulnweb.com/admin/backup/
Index of /admin/backup
Name Last modified Size Description
Parent Directory -
FTP_le.log 2012-10-25 08:20 63K
database_connect.php 2012-10-25 08:22 298
db_dump.sql 2012-10-25 08:21 98K
old_pass.txt 2012-10-25 08:22 6.3K
Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4 Server at www.vulnweb.com Port 80


500 - Internal server error.
127.0.0.2:81
Server Error
500 - Internal server error.
There is a problem with the resource you are looking for, and it cannot be displayed.

TIME FOR

Q&A

OWASP Top 10 – Security Misconfiguration

Go download WebGoat

https://github.com/WebGoat/WebGoat-Legacy

TRY IT YOURSELF

Some homework for you to learn a bit more.

WebGoat Installation How-To

1. Download Java VM, JDK 1.7
2. Download WebGoat: https://webgoat.atlassian.net/builds/browse/WEB-WGM/latestSuccessful/artifact/shared/WebGoat-Embedded-Tomcat/WebGoat-6.0.1-war-exec.jar
3. Run the .jar file:
    1. java -jar WebGoat-6.0-exec-war.jar
4. Then navigate in your browser to: (http://localhost:8080/WebGoat)
5. Login using guest account
6. Go to Insecure Configuration and complete the exercise

OWASP #5

Security Misconfiguration

OWASP Top 10 Vulnerabilities

www.pandoralabs.net

PANDORA
SECURITY LABS

Expert advice. Experience advantage.
Proactive Security Solutions Through Cutting-Edge Research.

OWASP TOP 10: #5 Security Misconfiguration

By @isaacsabas