https://www.vulnerable-site.com/images/filename?=‘%^&(#”%

An unknown error occurred while processing the request.:
com.fasterxml.jackson.databind.exc.InvalidTypeIdException: Could not resolve subtype of [simple type, class ClassB]: missing type id property 'type' at [Source: (io.undertow.servlet.spec.ServletInputStreamImpl); line: 67, column: 1] at com.fasterxml.jackson.databind.exc.InvalidTypeIdException.from(InvalidTypeIdException.java:43) at com.fasterxml.jackson.databind.DeserializationContext.missingTypeIdException(DeserializationContext.java:2083) at com.fasterxml.jackson.databind.DeserializationContext.handleMissingTypeId(DeserializationContext.java:1596) at com.fasterxml.jackson.databind.jsontype.impl.TypeDeserializerBase._handleMissingTypeId(TypeDeserializerBase.java:307) at com.fasterxml.jackson.databind.jsontype.impl.AsPropertyTypeDeserializer
...

Information Disclosure

Author: Rana Khalil (@rana__khalil)

Agenda

WHAT IS INFORMATION DISCLOSURE?

HOW DO YOU FIND IT?

HOW DO YOU EXPLOIT IT?

HOW DO YOU PREVENT IT?

WHAT IS INFORMATION DISCLOSURE?

Information Disclosure or also known as information leakage, is when a website unintentionally reveals sensitive information to its users.

Stack Trace Enabled

Improper error / exception handling with stack trace enabled.

```
at com.fasterxml.jackson.databind.jsontype.impl.AsPropertyTypeDeserializer.deserializeTypedFromObject(AsPropert
at com.fasterxml.jackson.databind.deser.BeanDeserializerBase.deserializeWithType(BeanDeserializerBase.java:1171
at com.fasterxml.jackson.databind.deser.SettableBeanProperty.deserialize(SettableBeanProperty.java:527)
at com.fasterxml.jackson.databind.deser.std.ThrowableDeserializer.deserializeFromObject(ThrowableDeserializer.j
at com.fasterxml.jackson.databind.deser.BeanDeserializer._deserializeOther(BeanDeserializer.java:194)
at com.fasterxml.jackson.databind.deser.BeanDeserializer.deserialize(BeanDeserializer.java:161)
at com.fasterxml.jackson.databind.jsontype.impl.AsPropertyTypeDeserializer._deserializeTypedForId(AsPropertyTyp
at com.fasterxml.jackson.databind.jsontype.impl.AsPropertyTypeDeserializer.deserializeTypedFromObject(AsPropert
at com.fasterxml.jackson.databind.deser.BeanDeserializerBase.deserializeWithType(BeanDeserializerBase.java:1171
```

Verbose Headers

When configured insecurely, response headers may leak information about the backend technologies used by the application.

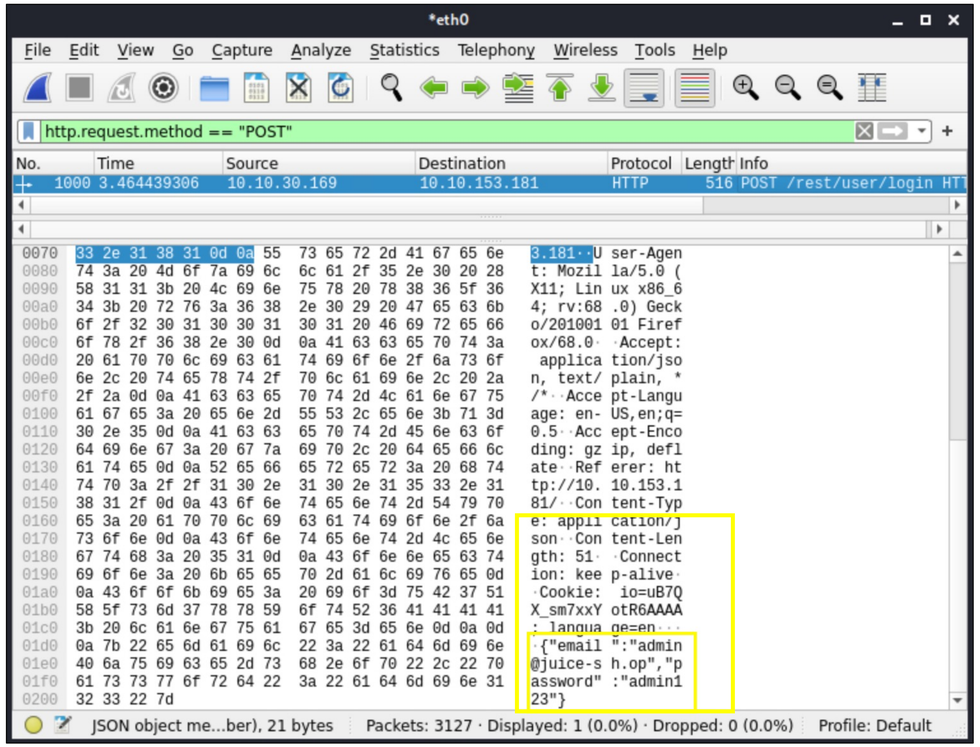
```
HTTP/2 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
X-Aspnetmvc-Version: 5.2
X-Aspnet-Version: 4.0.30319
X-Powered-By: ASP.NET
```

The following information can be deduced from the above example:

- The web server software used is Microsoft-IIS version 10.0
- The collect of application frameworks being run by the site is ASP.NET
- The ASP.NET version is 4.0.30319

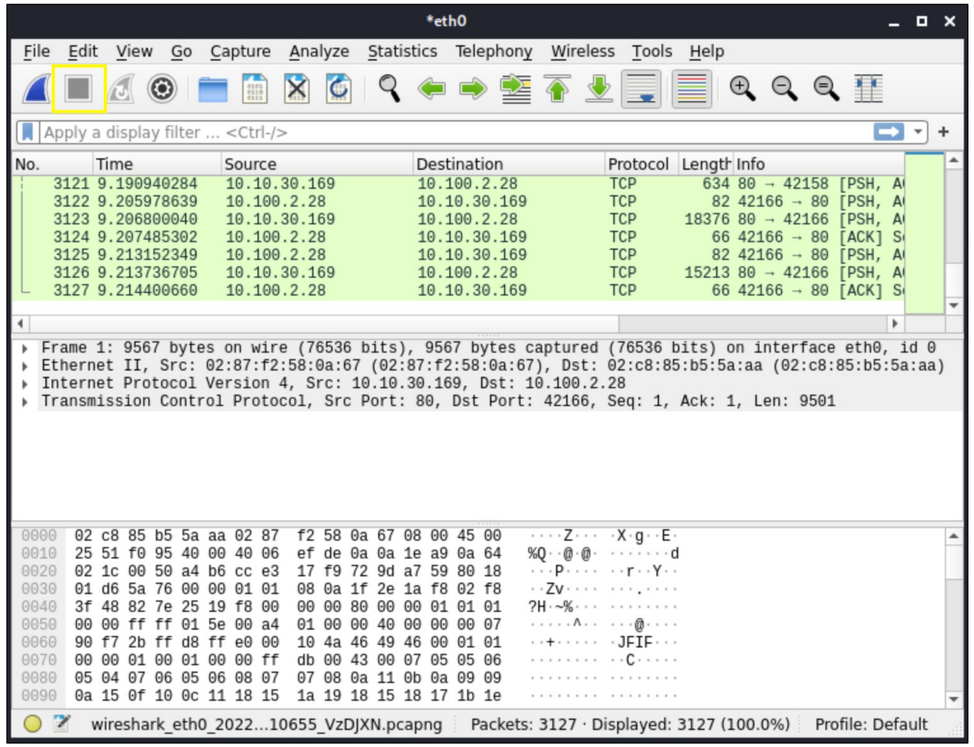
Use of Unencrypted Channel

HTTP

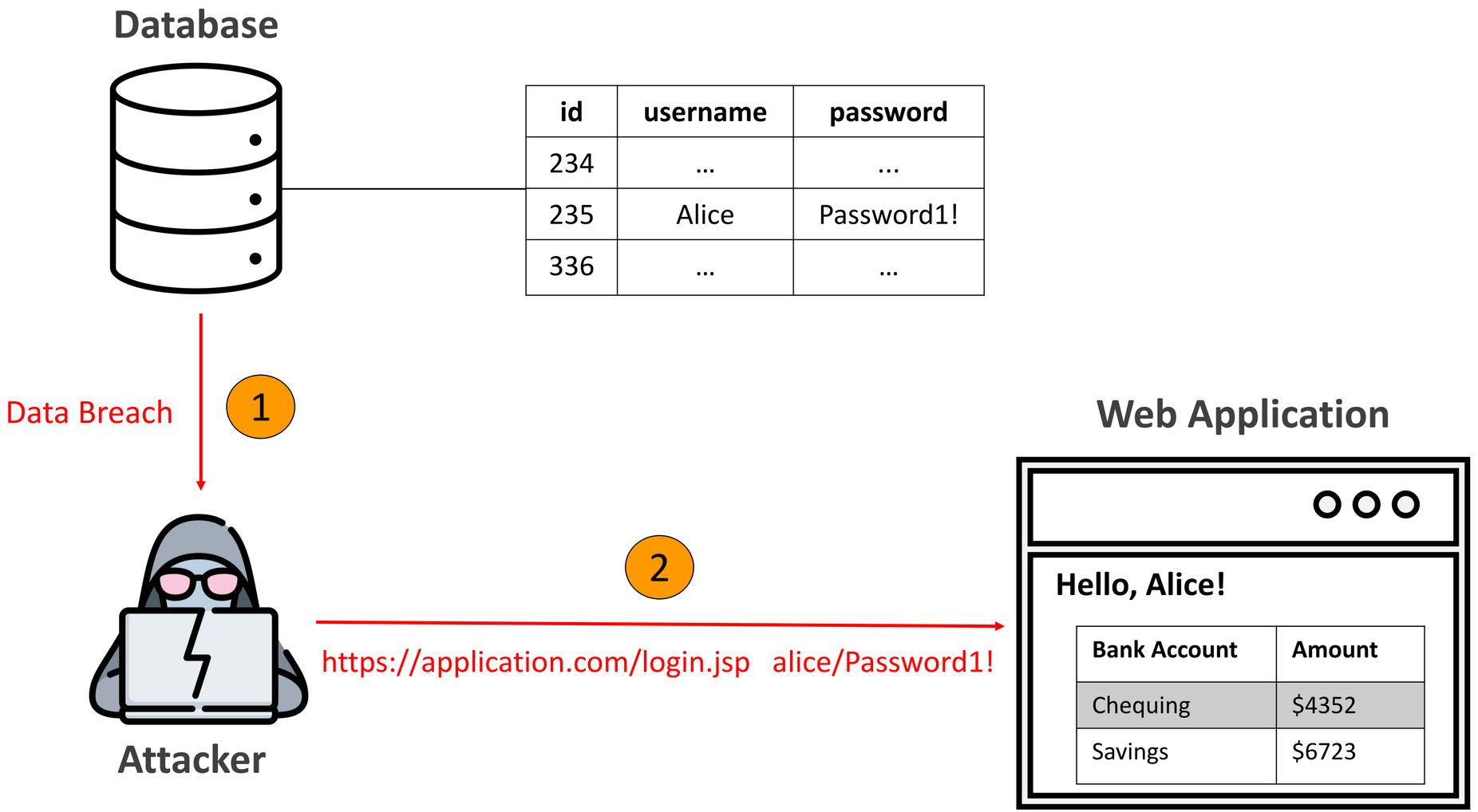


VS

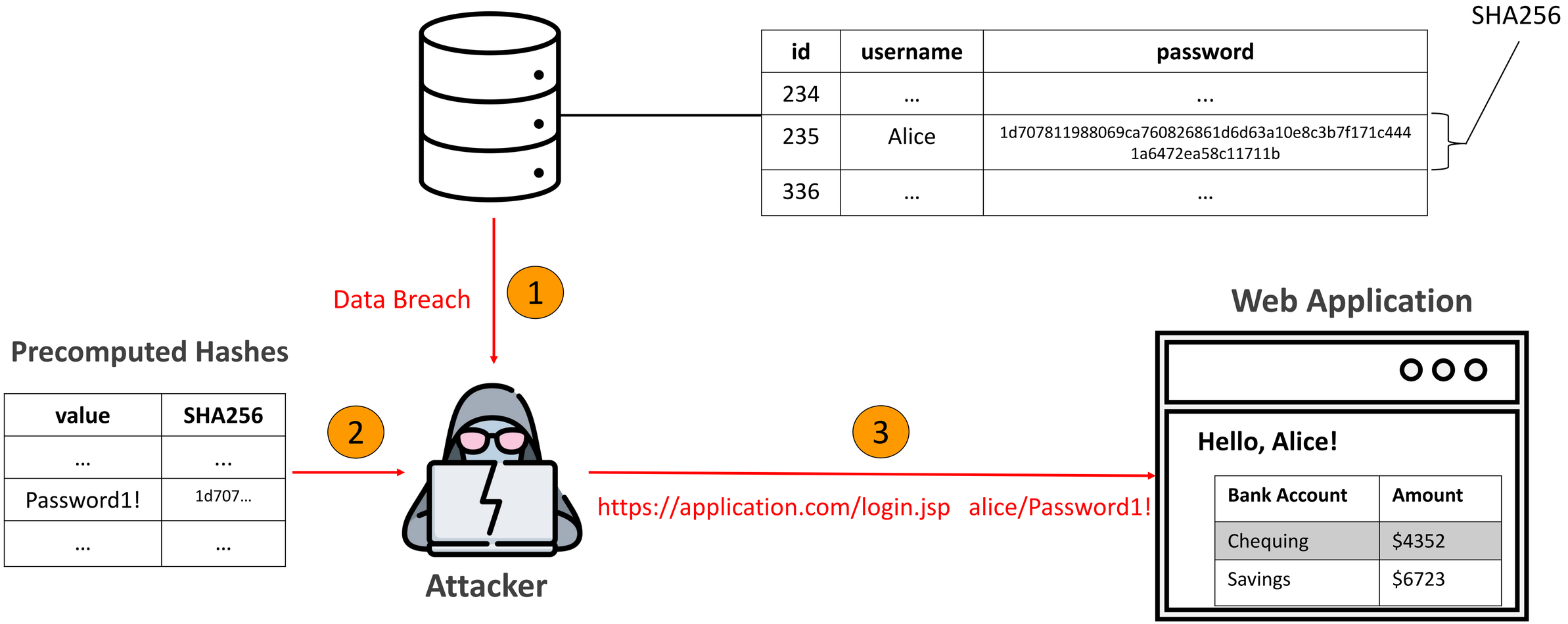
HTTPS



Storage of Credentials in Cleartext



Use of One-Way Hash Without Salt



Other Information Disclosure Examples

- Obscuring passwords or sensitive information using trivial encoding algorithms.
- Transmitting sensitive information in cleartext over a communication channel that can be sniffed by unauthorized actors.
- Hard-coding credentials, such as passwords or cryptographic keys, in the application code.
- Using insecure hashing or cryptographic algorithms.
- Improper verification of cryptographic signatures.
- Verbose error message or business design
- ....

Impact of Information Disclosure Vulnerabilities

- Unauthorized access to the application and host operating system.
  - **C**onfidentiality – Information disclosure vulnerabilities are usually used to view sensitive information.
  - **I**ntegrity – Information disclosure vulnerabilities in rare cases can be used to alter content in the application.
  - **A**vailability – Information disclosure vulnerabilities in rare cases can be used to delete content in the application.
- Remote code execution on the operating system

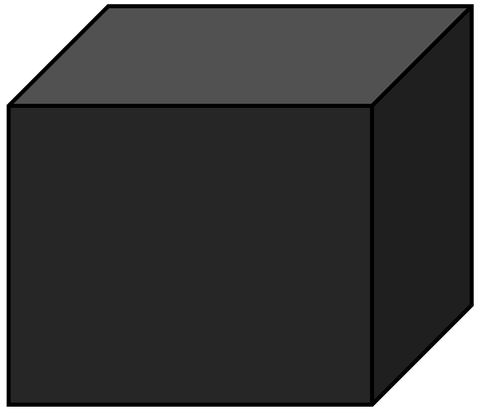
OWASP Top 10

OWASP Top 10 - 2013	OWASP Top 10 - 2017	OWASP Top 10 - 2021
A1 – Injection	A1 – Injection	A1 – Broken Access Control
A2 – Broken Authentication and Session Management	A2 – Broken Authentication	A2 – Cryptographic Failures
A3 – Cross-Site Scripting (XSS)	A3 – Sensitive Data Exposure	A3 - Injection
A4 – Insecure Direct Object References	A4 – XML External Entities (XXE)	A4 – Insecure Design
A5 – Security Misconfiguration	A5 – Broken Access Control	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Security Misconfiguration	A6 – Vulnerable and Outdated Components
A7 – Missing Function Level Access Control	A7 – Cross-Site Scripting (XSS)	A7 – Identification and Authentication Failures
A8 – Cross-Site Request Forgery (CSRF)	A8 – Insecure Deserialization	A8 – Software and Data Integrity Failures
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities	A9 – Security Logging and Monitoring Failures
A10 – Unvalidated Redirects and Forwards	A10 – Insufficient Logging & Monitoring	A10 – Server-Side Request Forgery (SSRF)

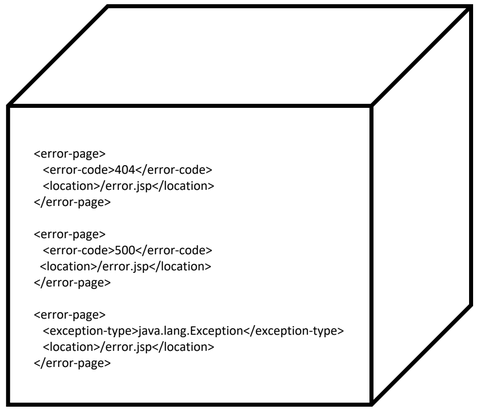
HOW TO FIND INFORMATION DISCLOSURE VULNERABILITIES?

Finding Information Disclosure Vulnerabilities

Depends on the perspective of testing.



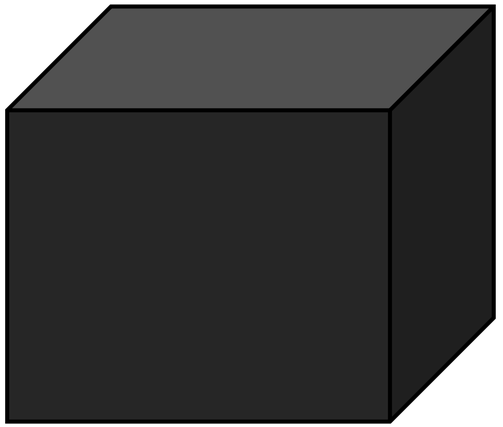
Black Box Testing



White Box Testing

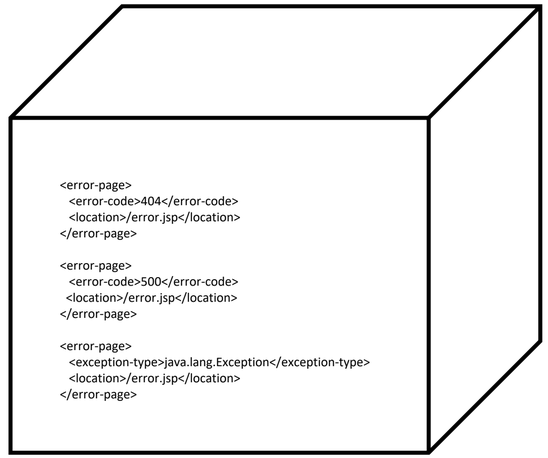
Black-Box Testing

- Understand and be able to recognize sensitive data.
- Map the application.
- Fuzz the application.
- Brute force or enumerate directories.
- …



White-Box Testing

- Review the server and application configuration for any debugging or diagnostic features that are enabled in the production environment.
- Review all error messages to determine if they leak sensitive information.
- Audit code to identify potential information disclosure in the code.
- If the application integrates with any third-party technologies, review the configuration for insecure or relaxed security features.



HOW TO EXPLOIT INFORMATION DISCLOSURE VULNERABILITIES?

Information Disclosure Labs

LAB
APPRENTICE
Information disclosure in error messages »

LAB
APPRENTICE
Information disclosure on debug page »

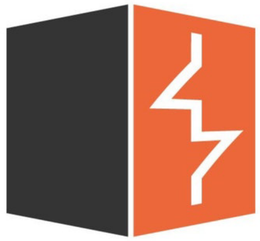
LAB
APPRENTICE
Source code disclosure via backup files »

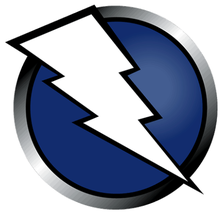
LAB
APPRENTICE
Authentication bypass via information disclosure »

LAB
PRACTITIONER
Information disclosure in version control history »

Automated Exploitation Tools

Web Application Vulnerability Scanners (WAVS).





HOW TO PREVENT INFORMATION DISCLOSURE?

Preventing Information Disclosure

- Ensure that all the teams involved in producing the application are aware of what information is considered sensitive.
- Audit code for potential information disclosure as part of the QA or build processes.
- Wherever possible, use generic error messages.
- Double-check that any debugging or diagnostic features are disabled in the production environment.
- Review all configuration settings for any third-party technology that you implement. Make sure to disable any features and settings that you don't actually need.

Resources

- Web Security Academy – Information Disclosure
  - *https://portswigger.net/web-security/information-disclosure*
- Web Application Hacker's Handbook
  - *Chapter 15 – Exploiting Information Disclosure*
- OWASP A02:2021 - Cryptographic Failures
  - *https://owasp.org/Top10/A02_2021-Cryptographic_Failures/*
- Shhh… don't let your response headers talk too loudly
  - *https://www.troyhunt.com/shhh-dont-let-your-response-headers/*