

COMMUNS WEB ATTACKS REFERENCES PT.1

JOAS ANTONIO

<https://www.linkedin.com/in/joas-antonio-dos-santos>

XSS

<https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting>

<https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/server-side-xss-dynamic-pdf>

<https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/dom-xss>

[Testing for Reflected Cross site scripting](#)
[Testing for Stored Cross site scripting](#)
[Testing for DOM-based Cross site scripting](#)

[https://cheatsheetseries.owasp.org/cheatsheets/Cross Site Scripting Prevention Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

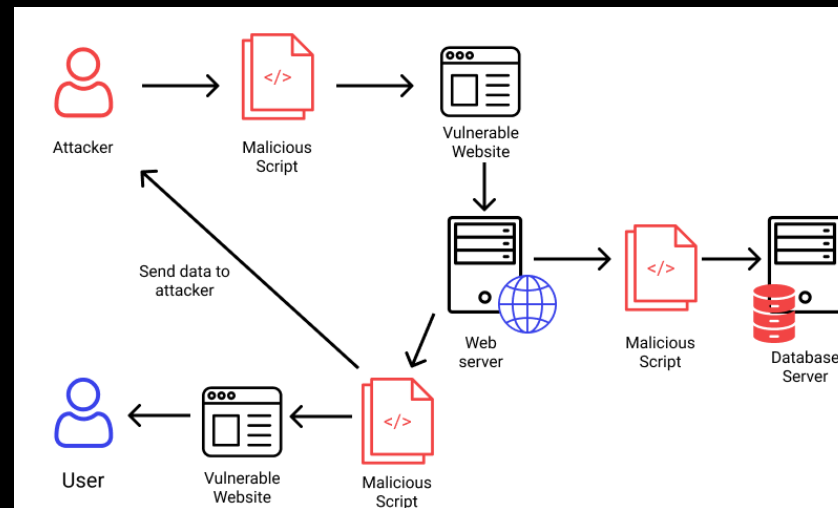
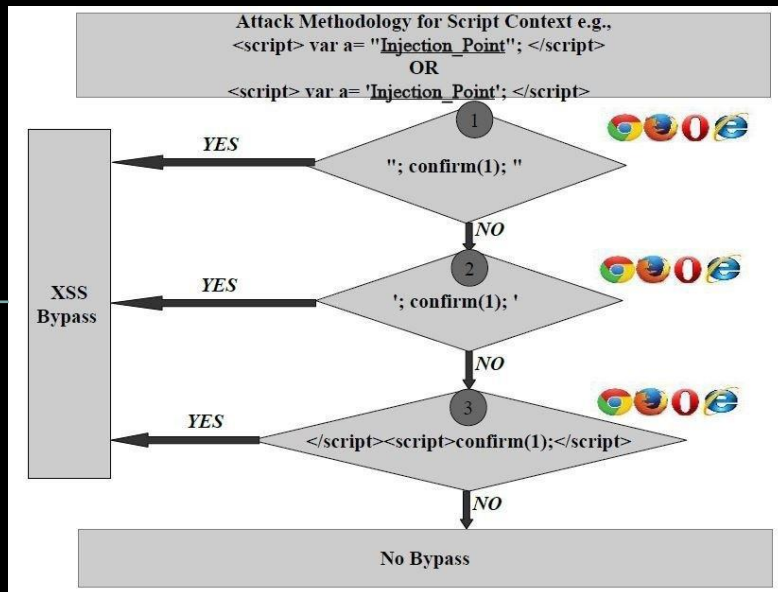
<https://github.com/payloadbox/xss-payload-list>

<https://portswigger.net/web-security/cross-site-scripting>

<https://blog.intigriti.com/hackademy/xss-challenges/>

<https://xss-game.appspot.com/>

<https://xsslabs.com/>



IDOR

<https://book.hacktricks.xyz/pentesting-web/idor>

https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

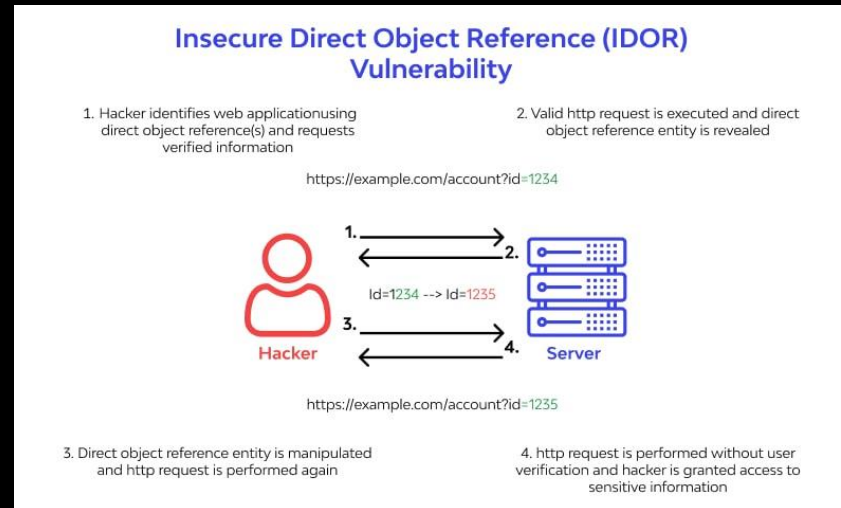
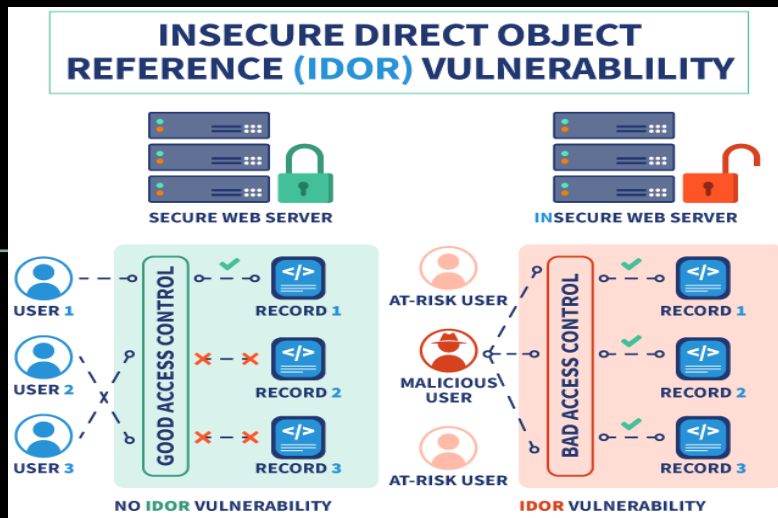
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/05-Authorization_Testing/04-Testing_for_Insecure_Direct_Object_References

<https://portswigger.net/web-security/access-control/idor>

<https://portswigger.net/web-security/cross-site-scripting>

<https://github.com/bm402/apidor>

<https://github.com/daffainfo/AllAboutBugBounty/blob/master/Insecure%20Direct%20Object%20References.md>



SQLi

<https://book.hacktricks.xyz/pentesting-web/sql-injection>

<https://book.hacktricks.xyz/pentesting-web/sql-injection/mysql-injection>

<https://book.hacktricks.xyz/pentesting-web/sql-injection/mssql-injection>

<https://book.hacktricks.xyz/pentesting-web/sql-injection/postgresql-injection>

<https://github.com/payloadbox/sql-injection-payload-list>

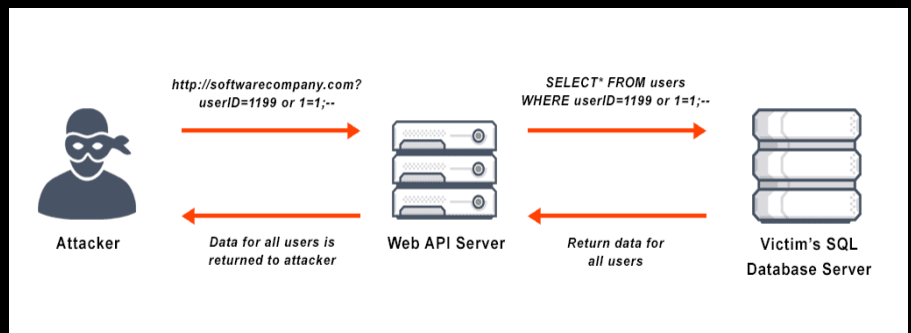
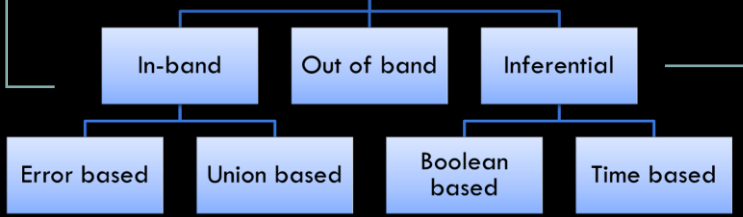
<https://www.soapui.org/docs/soap-and-wsdl/tips-tricks/web-service-hacking/>

<https://www.invicti.com/blog/web-security/sql-injection-cheat-sheet/>

<https://tryhackme.com/room/sqlilab>

<https://portswigger.net/web-security/sql-injection>

Types of SQL Injection



```
root@kali:~# sqlmap -u "http://192.168.10.111/checklogin.php"
```



```
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent :
they all applicable local, state and federal laws. Developers assume no liability and are not
responsible for any damages caused by the usage of the provided data (e.g. GET parameters)

[*] starting at 20:44:25

[20:44:25] [INFO] testing connection to the target URL
[20:44:25] [INFO] heuristics detected web page charset 'ascii'
[20:44:25] [INFO] checking if the target is protected by some kind of WAF/IPS/IDS
[20:44:26] [INFO] testing if the target URL content is stable
[20:44:26] [INFO] target URL content is stable
[20:44:26] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET pa
[*] shutting down at 20:44:26
```

XXE

<https://book.hacktricks.xyz/pentesting-web/xxe-xee-xml-external-entity>

<https://portswigger.net/web-security/xxe>

<https://xmind.app/m/eh9r7x/>

<https://github.com/payloadbox/xxe-injection-payload-list>

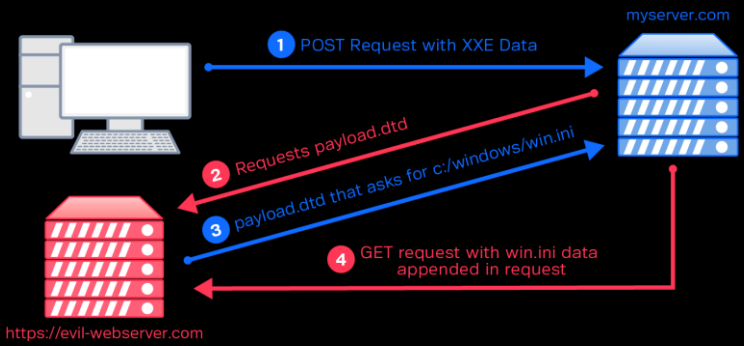
<https://github.com/HLOverflow/XXE-study>

<https://github.com/luisfontesl9/xxexploiter>

<https://github.com/jbarone/xxelab>

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/XXE%20Injection/README.md>

https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html



```
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
<!ELEMENT foo ANY >
<!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<foo>&xxe;</foo>
```

SSRF

<https://hacktricks.boititech.com.br/pentesting-web/ssrf-server-side-request-forgery>

<https://book.hacktricks.xyz/pentesting-web/ssrf-server-side-request-forgery>

<https://github.com/carlospolop/hacktricks/blob/master/pentesting-web/ssrf-server-side-request-forgery/README.md>

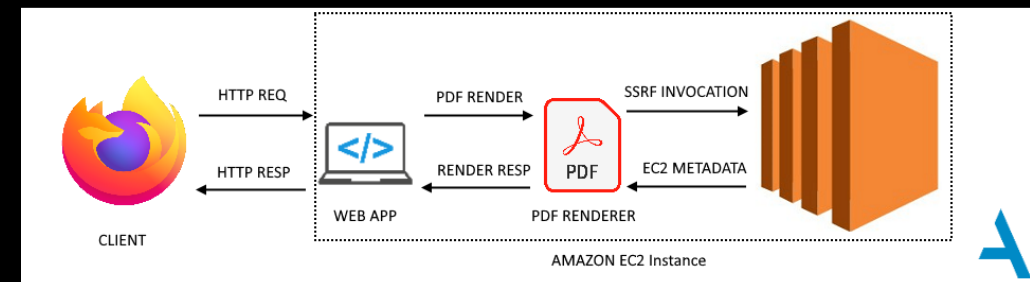
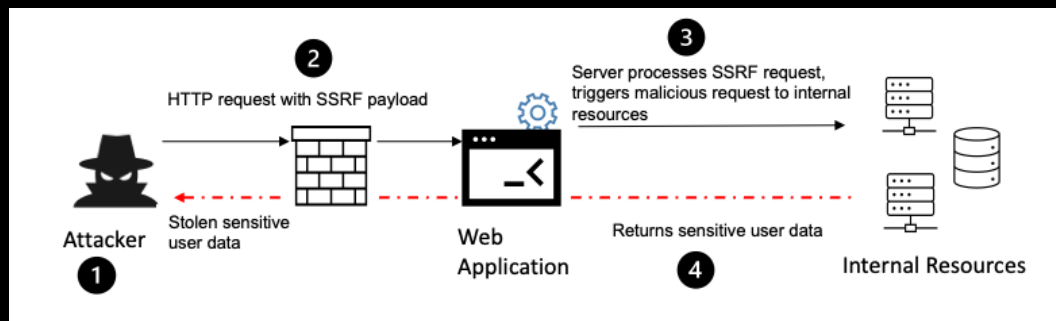
[https://owasp.org/www-community/attacks/Server Side Request Forgery](https://owasp.org/www-community/attacks/Server_Side_Request_Forgery)

<https://portswigger.net/web-security/ssrf>

<https://github.com/swisskyrepo/SSRFmap>

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Server%20Side%20Request%20Forgery/README.md>

[https://cheatsheetseries.owasp.org/cheatsheets/Server Side Request Forgery Prevention Cheat Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html)



Checklist:

<https://pentestbook.six2dez.com/others/web-checklist>

[https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP Web Application Penetration Checklist v1.1.pdf](https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Web_Application_Penetration_Checklist_v1.1.pdf)

<https://github.com/harshinsecurity/web-pentesting-checklist>

<https://github.com/Hari-prasaanth/Web-App-Pentest-Checklist>

WSTG:

<https://owasp.org/www-project-web-security-testing-guide/v42/>