Web Pentest 101

from abrasax to /dev/null

0x05: Uncovered Topics

Some content that you should see in this module

- XXE
- Admin Bypass
- Questions
- Challenge

XXE

A little bit about XML

- XML is a way of represent data, like HTML do with pages, but not necessarily pages, XML describe what you want to describe
- A type of XML data is called Entity. An Entity is like a shortcut to some information: <!ENTITY entity-name "entity-value">
- So, you can write XML information with it

```
<!ENTITY writer "Donald Duck.">
<!ENTITY copyright "Copyright W3Schools.">

XML example:

<author>&writer;&copyright;</author>
```

- Also, this entities can be loaded in external resources: <!ENTITY entity-name SYSTEM "URI/URL">
- So we get:

```
DTD Example:

<!ENTITY writer SYSTEM "https://www.w3schools.com/entities.dtd">
<!ENTITY copyright SYSTEM "https://www.w3schools.com/entities.dtd">

XML example:

<author>&writer;&copyright;</author>
```

- DTD means Document Type Definition

XML External Entity Injection

- When a external entity is requested, some application parse it's values and treat them
- If the parser is not securely configured, the hacker can request for the content of system files
- Let's go to explore WebGoat XXE Injection and see what happens
- This isn't a very common attack, but it's one that you should know
- Useful link: https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20injection

```
<?xml version="1.0"?>
<!DOCTYPE data [
<!ELEMENT data (#ANY)>
<!ENTITY file SYSTEM "file:///etc/passwd">
]>
<data>&file;</data>
```

Admin Bypass

That’s a ridiculous thing

- Some websites protect admin area with a login page, but not the other administratives pages, so, instead of login as admin, you just has to access directly the admin dashboard
- Some sites use client side protections against hackers, so you just has to change code, or even only read it
- Sometimes, you only has to change parameters or remove them

- In many sites you could even try a bruteforce
- Some password reset can be broken
- If the site is HTTP and NOT HTTPS anyone on your wifi can get your passwords
- Sometimes, actions that you doesn’t has permission to do are not visible in the panel, but if you try it directly you can just execute it.

Questions?

Challenge

Pretty easy

Finish the WebGoat challenges (including their CTF) and see you in the next module