WackoPicko App:

URL: https://www.aldeid.com/wiki/WackoPicko

Vulnerabilities

- Reflected XSS: In the search form, the query parameter is vulnerable.
- Stored XSS: The comment field is vulnerable to a persistent XSS attack.
- SessionID vulnerability: The session cookie value used for the administration authentication is based on a weak and guessable implementation (auto-incremental value).
- Stored SQL Injection: The first name field of the register users form contains a stored SQL injection which is then used unsanitized on the similar users page.
- Reflected SQL Injection: The username field is vulnerable.
- Directory Traversal: The tag field has a directory traversal vulnerability enabling a malicious users to overwrite any file the web server uses has access to.
- Multi-Step Stored XSS: The comment field is vulnerable to XSS, however must go through a preview form.
- Forceful Browsing: The user doesn't have to purchase the picture to see the high quality version.
- Command-line Injection: The password field is vulnerable to command line injections.
- File Inclusion: The /admin/index.php page is vulnerable to a file inclusion vulnerability, however you have to include %00 at the end.

- Parameter Manipulation: The userid parameter can be manipulated to see any user's page when you need to be logged in otherwise.
- Reflected XSS Behind JavaScript: The name parameter is vulnerable.
- Logic Flaw: A coupon can be applied multiple times reducing the price of an order to zero. The coupon in the initial data is SUPERYOU21.
- Reflected XSS Behind a Flash Form: The value parameter is vulnerable.
- Weak username/password: There is a default username/password combination of admin/admin.

Valid credentials

Priv	Username	Password
Standard	scanner1	scanner1
Standard	scanner2	scanner2
Standard	bryce	bryce
Admin	admin	admin
Admin	adamd	adamd