SY306 Team Project 3

Message Board Attack

Setup:

1. Save the current state of your database, so you can later restore it if needed.

    a. From the command line (as the team lead):

        i. ssh into `midn.cyber.usna.edu`

        ii. in the shell on `MIDN`, execute the following commands (replace **m21xxxx** with your alpha):

```
cd /project02
```

```
mysqldump -u m21xxxx -p -h midn m21xxxx > project02_backup.
```

    b. Check that the file `project02_backup.sql` was created in your `project02` folder

2. **Copy** - do not move - your files from `project02` to `project03`.

    Tip: an *easy* way to copy your `project02` files to `project03` is to run the following command from the team lead's `~/public_html$` directory:

```
cp -p -r project02 project03
```

3. Create a duplicate set of SQL tables for `projec03` as necessary (i.e. create users3, messages3, etc. in your MySQL database) **TIP!** Make sure to also update your Foreign Key constraints!

4. Verify functionality of `Project 03` before moving on...

Attack Instructions:

You and your teammates will attack `project03` of the **previous** team in your section (team 6 attacks team 5, team 5 attacks team 4, ...team 1 attacks team 6) as well as a sample project provided by your instructor. Click here to find the link to your team's specific sample project.

All attacks, successful or not, must be documented in such a way that the instructor can reproduce them. Download sy306_project3_SecurityEval.docx (right-click and "Save link as...") and store it in your `project03` directory. Record all attacks and their results in this document. Include screenshots if needed.

Try the various attacks we discussed in class (**HTML/CSS injections**, **JavaScript injection – XSS attacks**, **CSRF**, **SQL Injection**), and anything else that you can think of. The attacks can attempt to create unexpected behavior for the application – provoke error messages that reveal source code, change the display, get access to protected pages without providing a valid password, gather usernames and passwords, try cross site request forgery attacks to post messages as another user, steal cookies, elevate user privileges, etc. You must document all your work in the sy306_project3_SecurityEval.docx file that you will turn in for grading. Use additional sheets as needed to document attacks.

IMPORTANT! If your team is unable to perform successful attacks against your target team by 16:00 on Friday April 26th, please let your instructor know via e-mail.

Ground Rules:

1. Confirm your target team has copied their message board from `project02` to `project03` and verified proper functionality **before** beginning your attacks. Get the 'Green Light' from them before starting.
2. No DOS against any target message boards.
3. Attempts to guess server side (Python & MySQL) as well as client side credentials (HTML & JavaScript) are fair game.
4. No JavaScript redirects (Note: A valid JavaScript inject can be demonstrated with a simple alert box: `<script>alert("XSS!")</script>`)
5. Absolutely no automated vulnerability scanning tools such as NMAP, SQLMAP, Burp Suite, ZAP, etc. are to be used. Their use is prohibited on the USNA network!

Grading:

NOTE: The majority of project 3 will not be graded on the success or failure of the specific attacks, but rather the robustness/completeness of the attacks used, the comprehensiveness of the documentation provided, the ability to reproduce the attacks, the understanding of expected results and valid suggestions of proper defenses. ...That being said, additional points will be given for particularly well crafted or clever attacks!

Deliverables:

Electronic submission

One member of the team should submit the completed `sy306_project3_SecurityEval.docx` report to `submit.cs.usna.edu` under the "Project03" assignment by **23:59 on Tuesday April 30th**.