Intro to Web Application

...

Client side validation

Getting Started with Natas

http://overthewire.org/wargames/natas/

Username : natas0
Password : natas0
URL : http://natas0.natas.labs.overthewire.org

All passwords are also stored in /etc/natas_webpass/. E.g. the password for natas5 is stored in the file /etc/natas_webpass/natas5 and only readable by natas4 and natas5.

Level 0

- Right click!

Level 1

- Keyboard shortcut!

Level 2

- What resources were requested by your browser to the server?
- Anything suspicious?

Level 3

- Inspect the page
- How do you prevent Google from indexing pages?
- r/totallynotrobots

Level 4

- How can a site know where you came from?
- Can you fool the site?

Level 5

- How do sites know whether you’re logged in or not?
- How does “Remember me” feature works?

Level 6

- Read the source code carefully!
- How does the website store the password?
- Is the password located on a separate file?
- What is the password stored as? A plaintext? A variable?

Level 7

- Always remember the basic: inspect the page!
- How can the site figure out which page you are asking for?
- Can you manipulate the site to give you the page you want?

Level 8

- base64
- strrev
- bin2hex
- Reverse the obfuscation

Level 9

- Understand the source code
- Did they perform input sanitization?
- Can you inject a script?

Level 10

- What characters are filtered now?
- Can you avoid using those characters? Or maybe encode them?

Level 11

- XOR encryptions are easily reversible
- If “A” XOR “B” = “C”, then “C” XOR “B” = “A”

Level 12

- How does the site determine what kind of extension the file will have?
- Can we manipulate the site to upload our file as a script?
- Again, remember the basic: inspect the page!

Level 13

- How does the site figure out the type of our file?
  (Hint: Magic number)

Level 14

- Just like last time, does the site perform input sanitization?
- Can the site be injected with a script?
- Something to consider: can you input the username and password without using the HTML form provided?

Level 15

- Can you inject the site with a more sophisticated script?
- Read blind SQL injection?
- How can you automate the process of brute-forcing for a password?