Information System Security

Security Audit

ECE PARIS
ÉCOLE D'INGÉNIEURS

Warning

- Reminder: it is forbidden by law to make any intrusion into information systems (2 to 7 years imprisonment and 60,000 to 300,000 € fine). The attempt is punished by the same penalties as the offense (Articles 323-1 to 323-7 of the Penal Code)
- The techniques you learn in this lab are intended to make you aware of the vulnerabilities of information systems
- You should never use these techniques outside this lab

Details

- **Use the Vulnerable Debian server imported in the previous project**
- **IP address of vulnerable website is http://192.168.10.100 (after starting the server "Vulnerable Debian")**
  - Please do not use "Edge" browser
  - Do not look at the source code in the server
- **IDs for the application : admin/ecesecurity**
- **Exploit the vulnerabilities and answer the following questions.**
- **Don't forget to add some screenshots of the exploitation of each vulnerability**

Questions

- Command Injection

1. Indicate the command to enter in the form to extract the hostname and version number of the OS.
   Do you think that the PHP filtering function “htmlspecialchars” completely correct this vulnerability? Justify.

- CSRF

Describe how to exploit this vulnerability.

2. Does changing the method of submitting the form to POST correct the vulnerability? Justify.

3. What is the solution to avoid this vulnerability? Explain in detail how it works.

Questions

- File Inclusion

4. Include the file hackable/flags/fi.php and find sentences 4 and 5 in the page. Indicate how to avoid this vulnerability.

- File Upload

5. Upload and execute a script in order to get the php.ini from the website.

- SQL injection

6. Retrieve all user passwords and find their equivalent in clear.

7. What is your recommendation to avoid this vulnerability?

Questions

- SQL blind injection

8. Determine the version number of this Mysql database. Explain how you do it.

- Cross Site Scripting -> do not use “Google Chrome” for this attack

9. Give the malicious link allowing the hacker’s website (for instance evil.com) to get the session cookie of the victim.

10. Is it better to use the “htmlspecialchars” escape function before inserting data in database or when generating the page? Why?