به نام خدا

تمرین‌ها را فقط به صورت فایل pdf در سایت درس تحویل دهید.

تمرین چهارم – تست نفوذ (مهلت تحویل ۲۹ آذر)

هدف از این تمرین ارائه یک گزارش کامل با توجه به مواردی که در کلاس (TA)گفته شده، در رابطه با ارزیابی امنیتی یک وبسایت می باشد. باید در گزارش بصورت مختصر تست‌های انجام شده را به همراه نتیجه آن شرح دهید. و حاوی حداقل ۱۵ مورد از موارد گفته شده در زیر که در OWASP[1] منتشر شده است باشد.

- Testing for Credentials Transported over an Encrypted Channel (OTG-AUTHN-001)
- Testing for Weak lock out mechanism (OTG-AUTHN-003)
- Testing for weak password change or reset functionalities (OTG-AUTHN-009)
- Testing Directory traversal/file include (OTG-AUTHZ-001)
- Testing for Bypassing Authorization Schema (OTG-AUTHZ-002)
- Testing for Privilege escalation (OTG-AUTHZ-003)
- Testing for Insecure Direct Object References (OTG-AUTHZ-004)
- Testing for Session Management Schema (OTG-SESS-001)
- Testing for cookies attributes (OTG-SESS-002)
- Testing for Session Fixation (OTG-SESS-003)
- Testing for CSRF (OTG-SESS-005)
- Testing for logout functionality (OTG-SESS-006)
- Testing for Reflected Cross site scripting (OTG-INPVAL-001)
- Testing for Stored Cross site scripting (OTG-INPVAL-002)
- Testing for HTTP Parameter pollution (OTG-INPVAL-004)
- Testing for SQL Injection (OTG-INPVAL-005)
- Testing for XML Injection(TG-INPVAL-008)
- Testing for HTTP Splitting/Smuggling (OTG-INPVAL-016)

همان‌طور که می دانید انجام پروژه های دانشجویی تحت عنوان تست نفوذ و شناسایی حفره های امنیتی سایت ها جرم است. لذا از اجرای تست‌ها بر روی وبسایت هایی که اجازه این کار را نداده‌اند **خودداری** کنید. در این پروژه فقط مجاز هستید که وبسایت دانشکده (ceit.aut.ac.ir) را مورد بررسی قراردهید.

موفق باشید

[1] https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents