به نام خدا

تمرین سری دوم- درس توسعه امن نرم افزار

مهلت ارسال: ۱۴ خردادماه

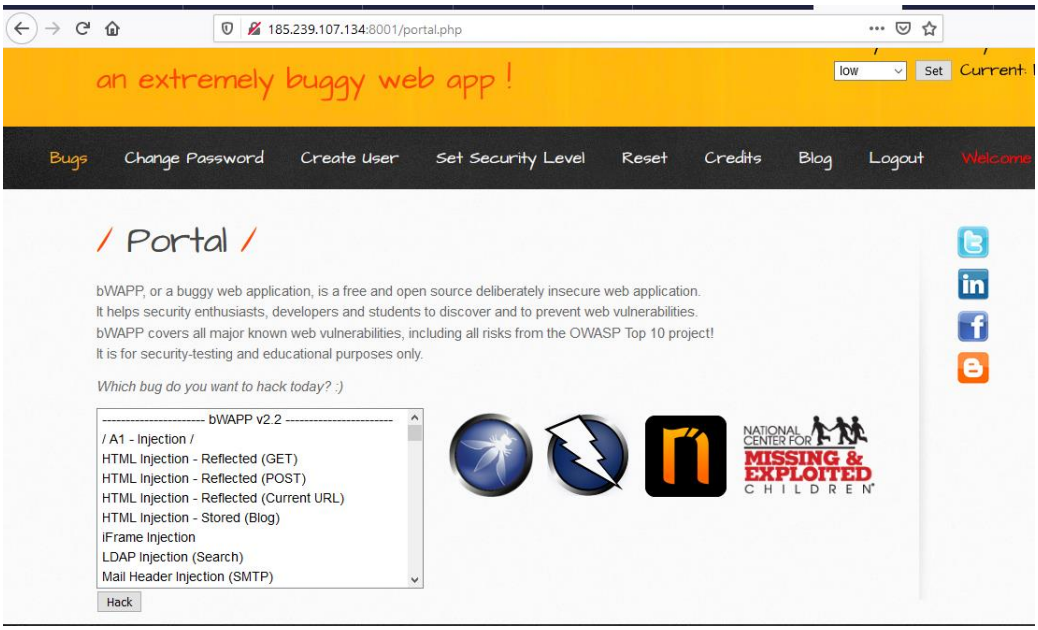
جهت انجام این تکلیف نیاز به نصب نرم‌افزار bwapp دارید. این نرم‌افزار یک نرم‌افزار opensource مشابه Dvwa است که برای آموزش امنیت صفحات وب و آسیب‌پذیری‌ها مناسب می‌باشد. برای نصب این نرم‌افزار می‌توان از Docker استفاده کرد. به اینصورت که ابتدا docker را روی سیستم عامل kali، ubuntu و .. نصب کنید. سپس در سایت https://hub.docker.com/ نسخه های آماده و open source نرم افزار bwapp را جستجو کرده و bwapp را روی port مشخصی مطابق با روش‌های گفته شده نصب کنید. برای مثال پس از نصب docker، با دستورات زیر bwapp روی port:8001 قابل مشاهده است. (لازم به ذکر است برای نصب می‌توان از روش‌های دیگری استفاده کرد.)

```
docker pull moeinfatehi/bwapp
docker run -d -p 8001:80 moeinfatehi/bwapp
```

پس از اجرا با لینک http://(ip_kali,ubuntu,..):8001/install.php نرم افزارbwapp را نصب کرده و با تنظیم سطح امنیتی low وارد سایت شوید (username:bee, pass: bug) سپس چالش های زیر را **حل** کرده و **راهکارهایی** جهت رفع آسیب‌پذیری موجود در چالش‌ها ارائه دهید:

- تمامی چالش‌های HTML Injection
- SQL Injection(GET/Search)
- SQL Injection(GET/Select)
- SQL Injection(POST/Select)
- SQL Injection(POST/Search)
- SQL Injection-Blind-Boolean-Based
- Cross-Site Scriptiong-Reflected(GET)
- Cross-Site Scriptiong-Reflected(Post)
- Cross-Site Scriptiong-Reflected(Cookies)
- تمامی چالش های Cross-Site Request Forgery
- Buffer Overflow(local)
- Buffer Overflow(Remote)
- OS Command Injection
- OS Command Injection(Blind)
- Session Management- Cookies(HTTP only)

فایل نهایی تکلیف شامل راه‌حل‌های حل چالش‌ها با ذکر جزییات دقیق، به همراه روش‌های پیشنهادی برای رفع آسیب پذیری‌های موجود در کد چالش‌ها می‌باشد.


185.239.107.134:8001/portal.php
an extremely buggy web app !
low
Set
Current:
Bugs
Change Password
Create User
Set Security Level
Reset
Credits
Blog
Logout
Welcome
/ Portal /
bWAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bWAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.
Which bug do you want to hack today? :)
---------- bWAPP v2.2 ----------
/ A1 - Injection /
HTML Injection - Reflected (GET)
HTML Injection - Reflected (POST)
HTML Injection - Reflected (Current URL)
HTML Injection - Stored (Blog)
iFrame Injection
LDAP Injection (Search)
Mail Header Injection (SMTP)
Hack
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

موفق باشید