Ph//shh/bin Attack&Defense 報告会

@elliptic_shiho

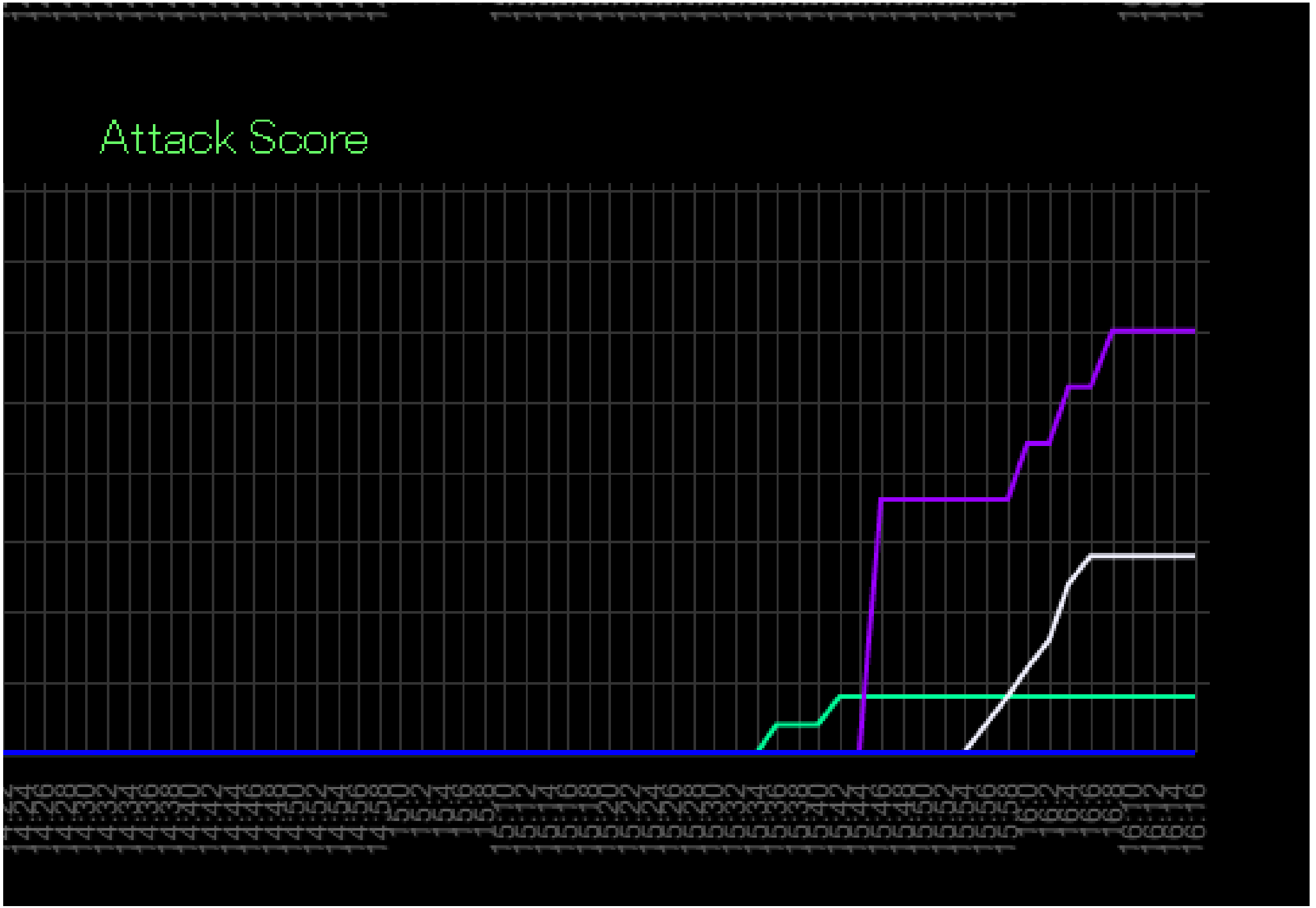
自己紹介

- 緑川 志穂(@elliptic_shiho)
- 暗号とレムニスケートが好物の高校1年生
- vuls, scryptos, Ph//shh/bin
- seccamp 2015参加します

さて

Ranking

Rank	Team	Attack Score	Defense Score	Damage
1	Ph//shh/bin	150	680	0
2	KenzenLab	70	700	0
3	smkwlab A	0	700	0
4	SayashiSayumi	0	700	0
5	satao	20	700	20


Attack Score

CTF for Beginners in Hakata (Attack&Defense)で優勝してきました

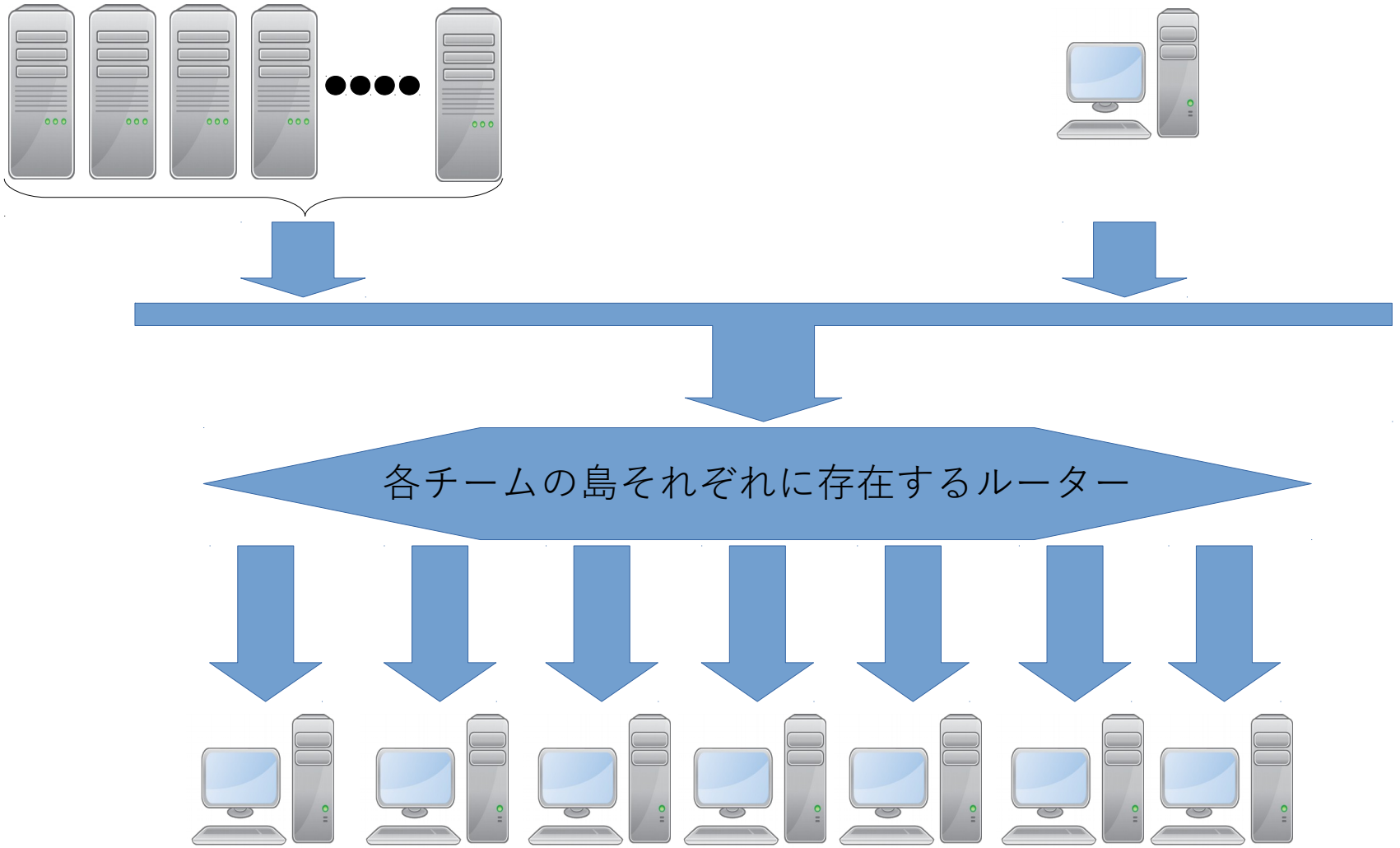
Attack & Defenseとは?

- CTFのスタイルの一つ
- 多分一番実践的
- DEFCONなんかがこの形式

Attack & Defenseとは?

- 各チームにサーバーが与えられる
  - 今回はRaspberry Piだった
- 各サーバーでは脆弱性のあるサービスが稼働している
  - 全てのサーバーで同じものが稼働している

各チーム一台ずつサーバー([0-9][1-9].ad.seccon)　スコアサーバー(ad.seccon)



Attack & Defenseとは?

- 他チームのサーバーを攻撃する(Attack)
  - 何をするかは場合による
  - シェルを取る、情報スティール、どこかに書き込む、...
- 同時に自分のチームのサーバー上で動くサービスの脆弱性を修正する(Defense)
  - 攻撃されないように

Attack & Defenseとは?

- ポイント計算
  - これも場合によります
  - 今回は(Attack Point + Defense Point) - Damageで計算された

Attack & Defenseとは?

- Attack Point
  - 攻撃して得られたポイント
  - 今回は情報スティールが目的だったので、スティールした情報1件に付き10pt

Attack & Defenseとは?

- Defense Point
  - 場合に(ry
  - 2分に一度「サービスが正常に稼働しているかどうか」のSLAチェックがあり、それに通ると10pt加算

Attack & Defenseとは?

- Damage
  - 他ではあるのかな?
  - 他チームに情報スティールされて取られた Attack Pointの分だけ加算される

Attack & Defenseとは?

- 今回は2つのサービスが動いていました
  - 擬似ECサイト
  - カスタムtelnetサーバー
  - 謎のftpサーバー

Attack & Defenseとは?

- Attack PointはECサイトからの擬似個人情報スティールで得られるようになっていました
  - 各チームに別々の情報がある
- カスタムtelnet問題はこの後チームメンバーが解説します

Web編

- いかにもなECサイト
- 攻撃できそうなポイントは?
  - コンタクトフォーム
  - 検索フォーム

Web編

- コンタクトフォームにXSSがあるらしい?
  - 送信確認時にalertを出せた
  - どうやらSQLインジェクションも可能

    → Blind SQL injectionで取れるのでは?

Web編

- 無理でした
  - データ量が多すぎる
  - 意味不明なエラー
  - 方法に無理がある

Web編

- ここまでで半分ほど時間を使ってしまった
- ちょろちょろtelnetのコードを読んでたりアクセスしている先のDBを少し読んでみたり
- そういえばユーザー登録ページもあるなぁ...

- なんか忘れてるな?

Web編

- 検索フォームがあるじゃないか
  - 早速SQLi発見
  - どうやら普通に値が見えるのでユーザー一覧を取得して整形して持ってくれば良さそう?

Web編

- DBのスキーマはこんなかんじだった

  id, email, password, last_login,
  deleted_at, group_id, name, kana, tel,
  zip_code, prefecture_id, address,
  created_at, updated_at

Web編

- しかし
  - この時スコアを得るためには次の形でフラグ文字列を作る必要があった

```
name,kana,email,tel,
zip_code,prefecture_id,address,password
```

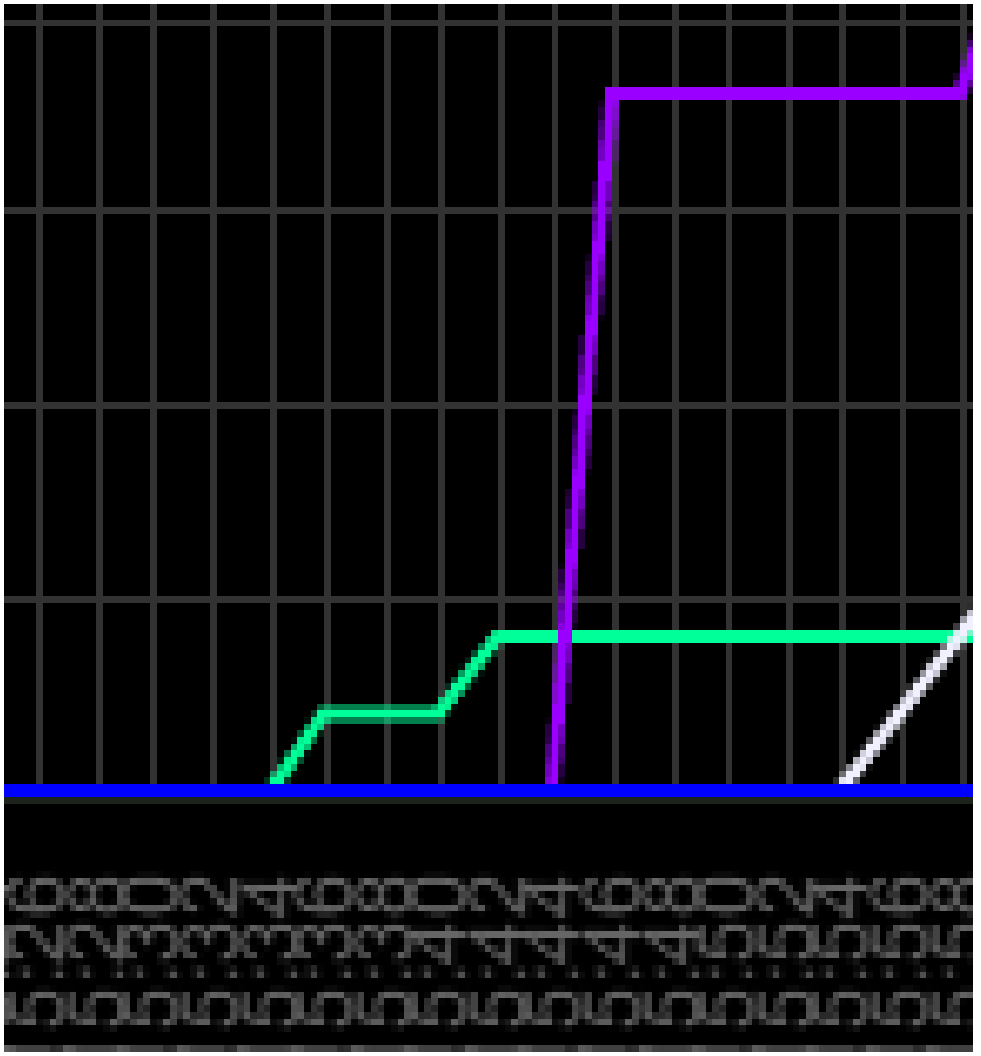
Web編

- 一度目の攻撃

```
' union select 1, (select group_concat(name separator
':') from users), 1,1,1,1,1,1,1,1;--
```

  - nameの部分を変えて色々試した
  - データが必要量集まったのでPythonで整形してフラグを作成
  - 一度に9件のACを得た

Web編



Web編

- 2回目以降

  - 流石に毎回pythonで整形し直すのは非効率的

  →SQLで整形しよう

  →それだ

Web編

- ということで書いた

```
' union select 1,(select
group_concat(concat(name,',',kana,',',emai
l,',',tel,',',zip_code,
',',prefecture_id,',',address,',',password
) separator ':') from
users),1,1,1,1,1,1,1,1;--
```

Web編

- うまくいったかに見えた

Web編

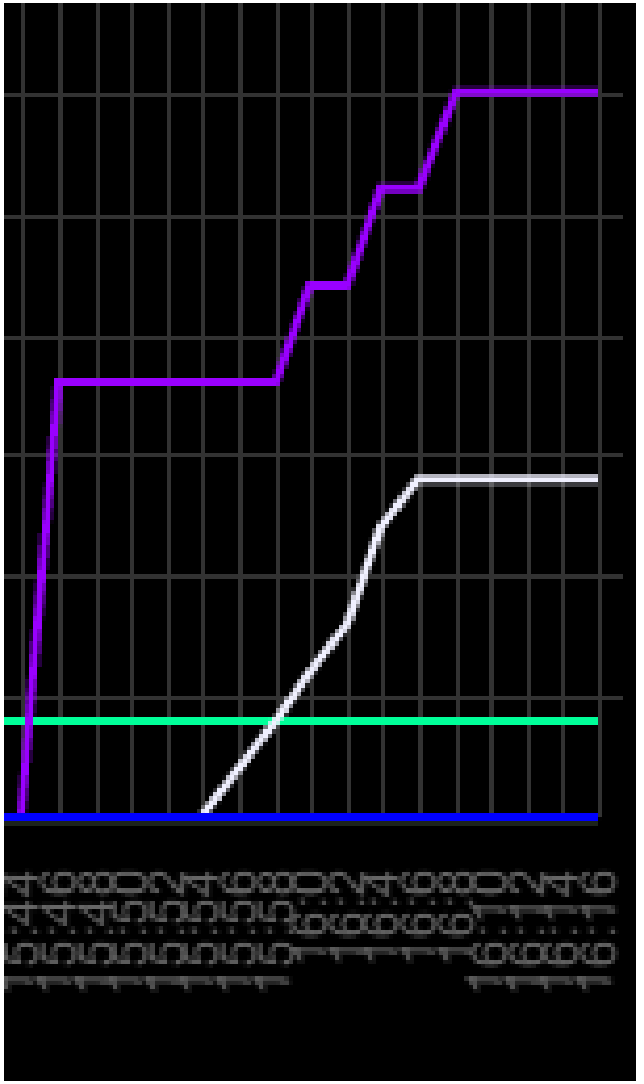
- うまくいったかに見えた

!!!! 文字数制限で一部しか見えない !!!!

Web編

- とりあえず2件は確実に取れるのでそれはそれで
  - 20ptずついくつかのチームから貰った

Web編



Web編

- こうして優勝しました
- telnet部分についてはこの後チームメンバーからLTします

telnet

Web編後日談

- union selectでわざわざgroup_concat使わなくても良かったのでは?

  → ....

Web編後日談

- ' union select 1, concat(name,',',kana,',',email,',',tel,',',zip_code, ',',prefecture_id,',',address,',',password),1,1,1,1,1,1,1,1 from users;--

Web問後日談

>>> 全てのレコードが文字数制限無しに取得できる <<<

Web問後日談

- 完全に盲点だった
  - やり方に固執したのが問題

Web問後日談

- その他について
  - ソースコードがあったにも関わらず殆ど読まなかった
    - 普段のオンラインCTFの悪癖
  - Adminページの存在にすら気づいていなかった

総括

- 良かった点
  - 最初に自分のPCでpython -m SimpleHTTPServer 8080をしてファイル配布サーバーを作った
  - SQLiコードを配布するのに役に立った

総括

- 良かった点
  - 情報共有が素早い
    - Skypeを利用していました
  - 互いの知識をうまく活用できた場面もあった

総括

- 反省点
  - 正直舐めてたと言わざるをえない
    - かなり奥深い競技形態
    - ARPスプーフィングで他チームのSLA落とせたんじゃ?等も考えられた
  - 通常のJeperdy形式CTFの癖が出てしまった

総括

- 反省点
  - 役割分担ができていなかった
  - 情報共有IMにSkypeを利用していたため、PC1台のみの参加だったメンバーには少しきつかった
  - もう一つRedmineのようなサービスを中で構築しておくべきだった

総括

- 最終的には優勝という形で終わることができてよかったです
- 自分に足りない点も見つかった上にチーム戦の意味を感じられた
- 実際にこのような攻撃をされているのかなという感覚を持つこともできた

余談

- SECCONの九州予選もAttack&Defenseらしいですね?
  - 学生限定らしいので学生の方々是非行きましょう
  - もちろん私達も参加します

余談

- 今回のAttack&Defenseで使われたECサイトのソースコードを使ったCTF問題が某某某某某氏によってアレされて自分のCTFサイトに投稿されています

  - Web自信あるぜ!って方は挑戦してみると良いかもしれません

http://s01.elliptic-shiho.xyz/ctf/problem/37

参考

- Web問題のソースコード

  https://github.com/Eidwinds/a_and_d_vulnerable_web

- telnet問題のソースコード

  https://github.com/koide55/yarareTelnet

ありがとうございました