Bezpieczeństwo usług sieciowych
— laboratorium 2 —
Rozwal.to

Adrian Frydmański

20 listopada 2017

1 Zerówka

1.1 Jak tego nie rozwalisz – usuń konto

Flaga ukryta w kodzie strony (w komentarzu).

Flaga: `DontMessWithZohan`

1.2 Typowa flaga za 1p.

Zarówno hasło do wpisania w pole jak i flaga widoczna w kodzie strony (w polu `script`).

Flaga: `ILikeBiscuits`

2 Crypto

2.1 Bob uwielbia xorować

Wiadomość zaszyfrowana przez xor na każdym bajcie tym samym kluczem, dodatkowo zakodowana w base64.

Program `Bob_uwielbia_xorowac.py` odkodowuje, a nastepnie sprawdza po kolei znaki zaszyfrowanej wiadomości. Zakładając, że testowany znak to zaszyfrowane „R" oblicza klucz i sprawdza, czy kolejne znaki po odszyfrowaniu tym kluczem to „OZWAL_{". Po znalezieniu pasującego ciągu uznaje, że klucz jest właściwy i odszyfrowuje całą wiadomość.

Flaga: `SingleXorByteCipher`

2.2 Alicja też xoruje

Wiadomość zaszyfrowana przez xor na każdym bajcie innym kluczem, dodatkowo zakodowana w base64.

Program `Alicja_tez_xoruje.py` odkodowuje, a następnie szuka możliwych fragmentów kluczy. Po kolei szuka fragmentu hasła, xorując 6-znakowe „ROZWAL" na każdym fragmencie zdekodowanego tekstu. Odważnie założyłem, że hasło będzie miało tyle, bądź mniej znaków i będzie hasłem słownikowym, czyli będzie zawierać znaki alfanumeryczne. „Przyjaźnie" wyglądającym okazał się fragment „kkotek", na podstawie którego wywnioskowałem, że hasło to „kotek". Nim odszyfrowałem cały tekst.

Flaga: `AliceIsImpressed`

2.3 Cweyk funcbjqlsiluqe

Tekst jest w języku angielskim. Próbuję znaleźć pojedyncze wielkie litery, które mogą być „I", pary liter po nich, które mogą być „am". Zamienione są tylko litery. Na podstawie tego, co otrzymuję próbuję szukać kolejnych słów, które mogą pasować i uzupełniam słownik z każdym uruchomieniem programu.

Flaga: `SubStitutionCipherIsWeak`

2.4 Nie kłam

Odczytałem ciacho po wpisaniu „xxxxxxxxxxlogin=admin" w formularzu „VxudCsIeS5e0MLhUIVh3C%2Bl3%2FvQKcTTGP49fRXSFRcA%3D".

Zdekodowałem je jako url, zdekodowałem jako base64, uciąłem pierwszy blok zawierający zaszyfrowaną frazę „login=xxxxxxxxxx" dzięki czemu pozostał mi tylko blok z zaszyfrowanym „login=admin" i zakodowałem z powrotem na base64 i na url za pomocą php sandboxa.

Podmieniłem ciacho na to, które otrzymałem. Ustawiłem na tylko do odczytu, dzięki czemu nie mogło ulec zmianie. Odświezyłem stronę i ~~na horyzoncie~~ zobaczyłem flagę:

Flaga: `SoYouDidCopyAndPaste`

2.5 Mieszkam w bloku

Jako, że kolejne bloki są szyfrowane takim samym kluczem (AES w trybie ECB), mogę dopasowywać blok wygenerowany przeze mnie z otrzymanym.

```
query=AAAAAAAAAA AAAA&f=ROZWAL_{X AAAAAAAAAAAAAAAA AAAA&f=ROZWAL_{?
query=AAAAAAAAAA AAA&f=ROZWAL_{XX AAAAAAAAAAAAAAAA AAA&f=ROZWAL_{??
query=AAAAAAAAAA AA&f=ROZWAL_{XXX AAAAAAAAAAAAAAAA AA&f=ROZWAL_{???
query=AAAAAAAAAA A&f=ROZWAL_{XXXX AAAAAAAAAAAAAAAA A&f=ROZWAL_{????
```

`query=AAAAAAAAAA &f=ROZWAL_{XXXXX AAAAAAAAAAAAAAA &f=ROZWAL_{?????`
`...`

X to podstawiane przeze mnie znaki, ? to fragmenty flagi. Całość jest oczywiście zaszyfrowana, ale porównywanie zaszyfrowanych bloków daje ten sam oczekiwany efekt. Jeśli drugi i czwarty blok ciacha się zgadzają, sprawdzana przeze mnie litera jest właściwa.

Flaga: `ECBisNotSoGreat`

3 Podsumowanie

Zdobyte punkty:

Zadanie	**Liczba punktów**
Jak tego nie rozwalisz - usuń konto	1
Typowa flaga za 1p.	1
Bob uwielbia xorować	20
Alicja też xoruje	125
Cweyk funcbjqlsiluqe	20
Nie kłam	100
Mieszkam w bloku	100
Suma	**367**