APACHE LOG

SQL Injection, XSS, and Brute Force Analysis

Computer Forensic | Apache Log Analysis

SQL INJECTION

```
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>64 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>96 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>112 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>104 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>108 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>106 HTTP/1.1" 200 75 "-" "Python-urllib/2.7"
```

Source: https://www.semanticscholar.org/paper/Inferential-SQL-Injection-Attacks-Stampar/ac062f5f4ad1af43a6d963b419835b936dd87728

SQL INJECTION

```
172.16.93.1 - - [03/Nov/2013:18:25:07 +0000] "GET /vuln.php?id=1%20AND%20ORD(MID((SELECT
%20IFNULL(CAST(surname%20AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id%20LIMIT%
200,1),3,1))>64 HTTP/1.1" 200 127 "-" "Python-urllib/2.7"
```

APACHE LOG INFORMATION

Client IP address: 172.16.93.1
Timestamp: 3 November 2013 18:25:07 +0000
Request line: GET /vuln.php?
id=1%20AND20ORD(MID((SELECT%20IFNULL(CAST(surname%20
AS%20CHAR),0x20)%20FROM%20users%20ORDER%20BY%20id
%20LIMIT%200,1)3,1)) HTTP/1.1
Status code: 200
Requested file size: 127
Referring link: Python-urllib/2.7

PENJELASAN

Pada log tersebut, diketahui bahwa pada tanggal 3 November 2013 dengan IP address 172.16.93.1 mencoba merequest GET method ke /vuln.php dengan id=1 dan mencoba melakukan SQL Injection. SQL Injection tersebut mencoba menampilkan code atau ascii paling kanan dari character pada string atau kata yang didapatkan dari character ke-3 surname di table users atau 0x20 (decimal: 32).

XSS

```
217.160.165.173 - - [12/Mar/2004:22:31:12 -0500] "GET /foo.jsp?<SCRIPT>foo</SCRIPT>.jsp HTTP/1.1" 200 578 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
217.160.165.173 - - [12/Mar/2004:22:37:17 -0500] "GET /cgibin/cvslog.cgi?file=<SCRIPT>window.alert</SCRIPT> HTTP/1.1" 403 302 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
```

APACHE LOG INFORMATION

Client IP address: 217.160.165.173
Timestamp: 12 March 2004 22:31:12 -0500
Request line: GET /foo.jsp?<SCRIPT>foo</SCRIPT>.jsp HTTP/1.1 & GET /cgibin/cvslog.cgi?file=<SCRIPT>window.alert</SCRIPT> HTTP/1.1
Status code: 200
Requested file size: 578 & 302
Referring link: Mozilla/4.75 [en] (X11, U; Nessus)

PENJELASAN

Pada log tersebut, diketahui bahwa pada tanggal 12 Maret 2004 jam 22.31 dengan IP address 217.160.165.173 mencoba merequest GET method ke GET /foo.jsp dan /cgibin/cvslog.cgi. Pada request itu ditemukan percobaan penggunaan kode scripting

Source: https://www.giac.org/paper/gcia/1996/detecting-attacks-web-applications-log-files/106864

BRUTE FORCE

```
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:45 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:45 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:45 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:45 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
192.168.86.99 - - [15/May/2019:10:45:45 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
```

Source: https://sevenlayers.com/index.php/191-pentesting-101-brute-force-attack

ANALYSIS

```
192.168.86.99 - - [15/May/2019:10:45:44 -0700] "POST /administrator/index.php HTTP/1.1" 200 5735
```

APACHE LOG INFORMATION

Client IP address: 192.168.86.99
Timestamp: 15 May 2019:10:45:44 -0700
Request line: POST /administrator/index.php HTTP/1.1
Status code: 200
Requested file size: 5735

PENJELASAN

Pada log tersebut, diketahui bahwa pada tanggal 15 May 2019 pukul 10.45 dengan IP address 192.168.86.99 mencoba merequest POST method ke /administrator/index.php. Dengan status code 200 yang menunjukkan bahwa request tersebut berhasil diterima server. Bisa disimpulkan log tersebut adalah brute force karena log request dilakukan berkali-kali, dalam bentuk banyak, dan dilakukan pada menit dan detik yang berdekatan.

THANK YOU