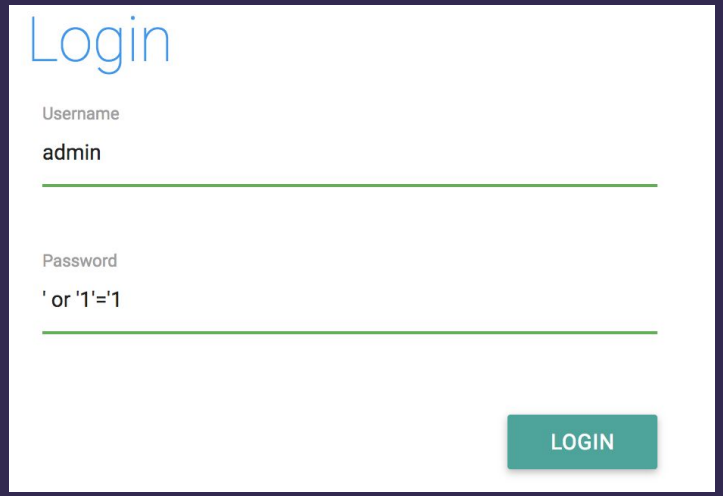
Hakkarar Sigraðir

```
username = request.form["username"]
password = request.form["password"]
query = f"SELECT * FROM users WHERE username='{username}' AND password='{password}'"
```




```
SELECT *
    FROM users
    WHERE username='admin'
      AND password='' or '1'='1';
```

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=sql+injection

There are 7495 CVE entries that match your search

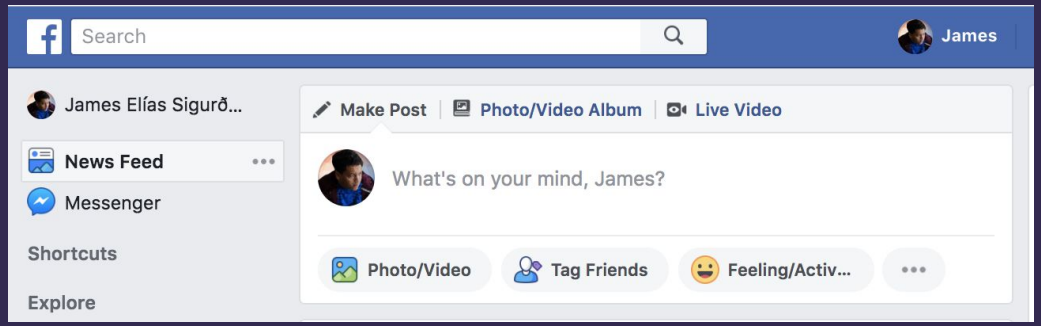
```
---[  Phrack Magazine   Volume 8, Issue 54 Dec 25th, 1998, article 08 of 12

-------------------------[  NT Web Technology Vulnerabilities
```

http://phrack.org/issues/54/8.html#article


03
59


Microsoft
Windows98


Search
James
James Elías Sigurð...
News Feed
Messenger
Shortcuts
Explore
Make Post
Photo/Video Album
Live Video
What's on your mind, James?
Photo/Video
Tag Friends
Feeling/Activ...

A1 - Injection

A2 - Broken Authentication

A3 - Sensitive Data Exposure

A4 - XML External Entities (XXE)

A5 - Broken Access Control

A6 - Security Misconfiguration

A7 - Cross-Site Scripting (XSS)

A8 - Insecure Deserialization

A9 - Using Components with Known Vulnerabilities

A10 - Insufficient Logging & Monitoring

2003

2003

2003

2017

XXE (Xml eXternal Entity) attack Oct 29 2002 11:23PM
Gregory Steuck (greg-xxe nest cx) (1 replies)

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Gregory Steuck security advisory #1, 2002

Overview:
XXE (Xml eXternal Entity) attack is an attack on an application that parses
XML input from untrusted sources using incorrectly configured XML parser.
The application may be coerced to open arbitrary files and/or TCP connections.

https://www.securityfocus.com/archive/1/297714/2002-10-27/2002-11-02/0


wat

Af hverju erum við ekki *enn* búin að stöðva þessa galla?

Fischer, Felix, et al. "Stack Overflow Considered Harmful?." The Impact of Copy & Paste on Android Application Security. CoRR abs/1710.03135 (2017).


ÖKUKENNSLA

Data Breach Costs

$7.2M average cost of a data breach

80 days to detect and **123 days** (4+ months) to resolve

Remediation Costs *(at each stage in the lifecycle)*

Sources: National Institute of Standards and Technology; Ponemon Institute

https://picoctf.com

Hack. Win.

icectf

SEPT. 6 - 13, 2018


SILVER SHINE

Lærið að brjótast inn í ykkar eigin kerfi
Áður en tölvuþrjótarnir gera það

Spurningar

james@adversary.io