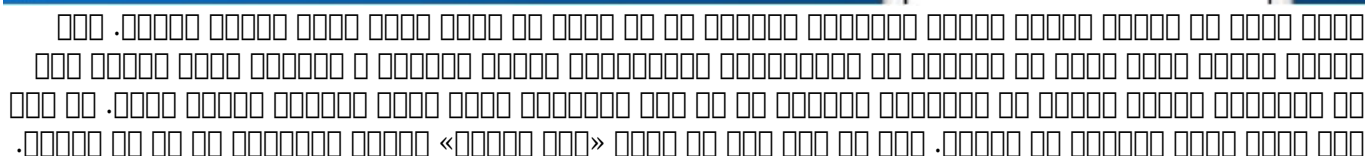


□□□ □□□□□ □□□ □□□□□□ □□ □□□□ □□ □□ □□ □□□□ □□□□□□

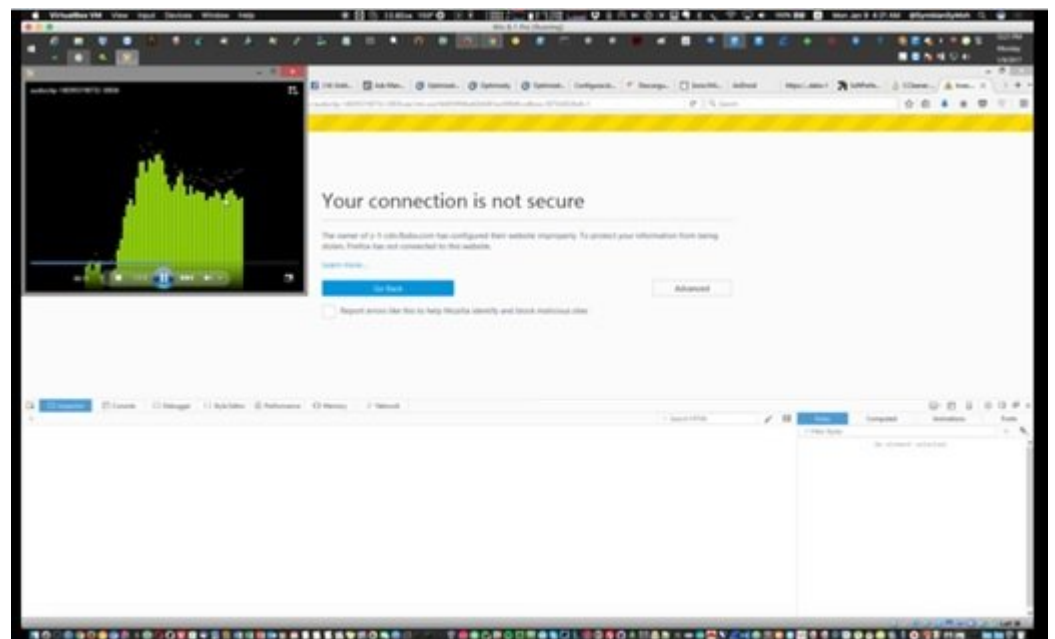
[illegible]

□□□□□□ □□ □□□□□□ □□□□□□ □□□□

[illegible]



이러한 공격은 SSL Strip 공격이라고 하며, 이는 HTTPS 통신을 HTTP로 강제로 변환시키는 공격입니다. 공격자는 중간에 끼어들어 통신을 가로채고, SSL 인증서를 발급받아 공격자의 IP로 통신을 유도합니다. 이 공격을 방지하기 위해서는 SSL Strip 공격을 탐지하고 차단하는 도구를 사용하는 것이 좋습니다. 예를 들어, SSL Strip 공격을 탐지하고 차단하는 도구를 사용하면, 공격자가 HTTPS 통신을 HTTP로 강제로 변환시키려는 시도를 탐지하고, 이를 차단하여 공격을 방지할 수 있습니다.



이러한 공격을 방지하기 위해서는

HTTP Strict Transport Security (HSTS) 정책을 적용하는 것이 중요합니다. HSTS는 웹 브라우저에 특정 웹사이트를 항상 HTTPS로만 접근해야 한다는 정보를 저장하는 정책입니다. 이를 통해 공격자가 SSL Strip 공격을 시도하더라도, 브라우저는 해당 웹사이트를 HTTPS로만 접근하려고 시도할 것입니다. 또한, Transport Security Headers (TSH)를 사용하여 통신을 암호화하고, CSRF 공격을 방지하기 위해 POST 요청을 검증하는 것도 중요합니다. GET 요청은 일반적으로 CSRF 공격의 대상이 되지 않지만, POST 요청은 CSRF 공격의 주요 대상입니다. 따라서, POST 요청을 검증하는 것은 CSRF 공격을 방지하는 데 매우 중요합니다.

00000000 00 000000 0000 00 00000000 00000000 000000 000 00 00000000 00000000 00000000 000 0000000000
 .000 00000 00000000 00000000 (downgrade attacks) 000000 000000 00000000 00 00000000 000 000000 00 000000

: □ □ □ □ □ □

: □□□□ □□□□

Page 10

• □ □ □ □ □ □ □ □ □ □ □

02:36 - 02/11/1395

•

MITM - 0000000000000000 - 0000 - 000 - 000000000000 - 00 - 000000 - 000000

<https://www.shabakeh-mag.com/security/6450>: █████ █████