



---

Second order mitigations against attackers tampering the app to disable or bypass the certificate pinning should be considered in cases where attackers can also control the device execution environment; i.e., where it is straightforward for attackers to execute the target app in their own emulation environment. e.g., an android application or a Linux userspace application.

## Alternatives & Related Technologies

Related: Browser Certificate Pinning, *HSTS*.

## References & Additional Reading

### *Attacker Tools*

- mitmproxy  
<https://mitmproxy.org/>
- burp  
<https://portswigger.net/burp>
- OWASP Zap  
[https://www.owasp.org/index.php/OWASP\\_Zed\\_Attack\\_Proxy\\_Project](https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project)
- JustTrustMe (Fuzion24/JustTrustMe)
- Frida universal (pcipolloni/universal-android-ssl-pinning-bypass-with-Frida)

### *Certificate Pinning Example Implementations*

[ikust/hello-pinnedcerts](#)

### *Certificate Pinning Testing*

OWASP MSTG Section

<https://github.com/OWASP/owasp-mstg/blob/master/Document/0x05g-Testing-Network-Communication.md#testing-custom-certificate-stores-and-certificate-pinning>

## Authors

Ben Gardiner, Irdeto

[ben.gardiner@irdeto.com](mailto:ben.gardiner@irdeto.com)