Einfuehrung in Web Security.

Die ueblichen Verdaechtigen.

Agenda

- Wie arbeiten Pentester
- OWASP Top 10
- Die alte Schule

Wie testen Pentester

- Web Proxy
- Scripting
- Debugger
- Action Script Extractor

Burp

(Live Demo)

OWASP Top 10

https://www.owasp.org/
images/b/b8/
OWASPTop10_DE_Version_1_0.pdf

Haeufigsten Sicherheitsluecken im Bereich Web.

Diese Top 10 sind aber nicht alles, was man testen muss.

Injection

Beispiel:

http://example.com/userView?id='+or+'1'='1

- SQL Injection
- Command Injection
- XPATH Injection

Cross Site Scripting (XSS)

Beispiel:

```
'><script>alert(document.cookie)</script>'
```

- Persistent oder Reflektiert

Filterung auf Eingabe oder Ausgabe?

Authentifizierungs. oder Sessionfehler

Beispiel:

http://example.com/booking?
jsessionID=EE2A396642...&
dest=London

- Session Token Leak
- Cookies HTTPS only Flag

Unsichere Objektreferenzierung

Beispiel:

http://example.com/person/123/view

- Direkte Referenzierung

Cross Site Request Forgery (CSRF)

Beispiel:

```
<img src=
"http://example.com/transferMoney?
amount=1500&
destinationAccount=12“
width="0" height="0" />
```

GET und POST

Fehlkonfiguration

- Update nicht eingespielt
- Directory Listing nicht deaktiviert
- Debug/Stacktrace Option an

Kryptografisch unsichere Speicherung

- Passwoerter (Hash ohne Salt)
- Kreditkartendaten

Mangelhafter URL Zugriffsschutz

Beipiel:

http://example.com/adminInfo/

- Admin Interfaces
- Intranet

Unsichere Transportschicht

- HTTP(S)
- schwache Zertifikate
- unsichere Datenbankverbindungen

Ungepruefte Um- oder Weiterleitung

Beispiel:

http://www.example.com/booking.php?
fwd=admin.php

- Interne Weiterleitung
- Extern auf Phishing oder Schadcode Seite

Click Jacking

Transparente IFrames

Die alte Schule

- Buffer Overflow
- Directory Traversal
- File Upload

Danke

Noch Fragen?

jens@nons.de /
jens.muecke@nruns.com