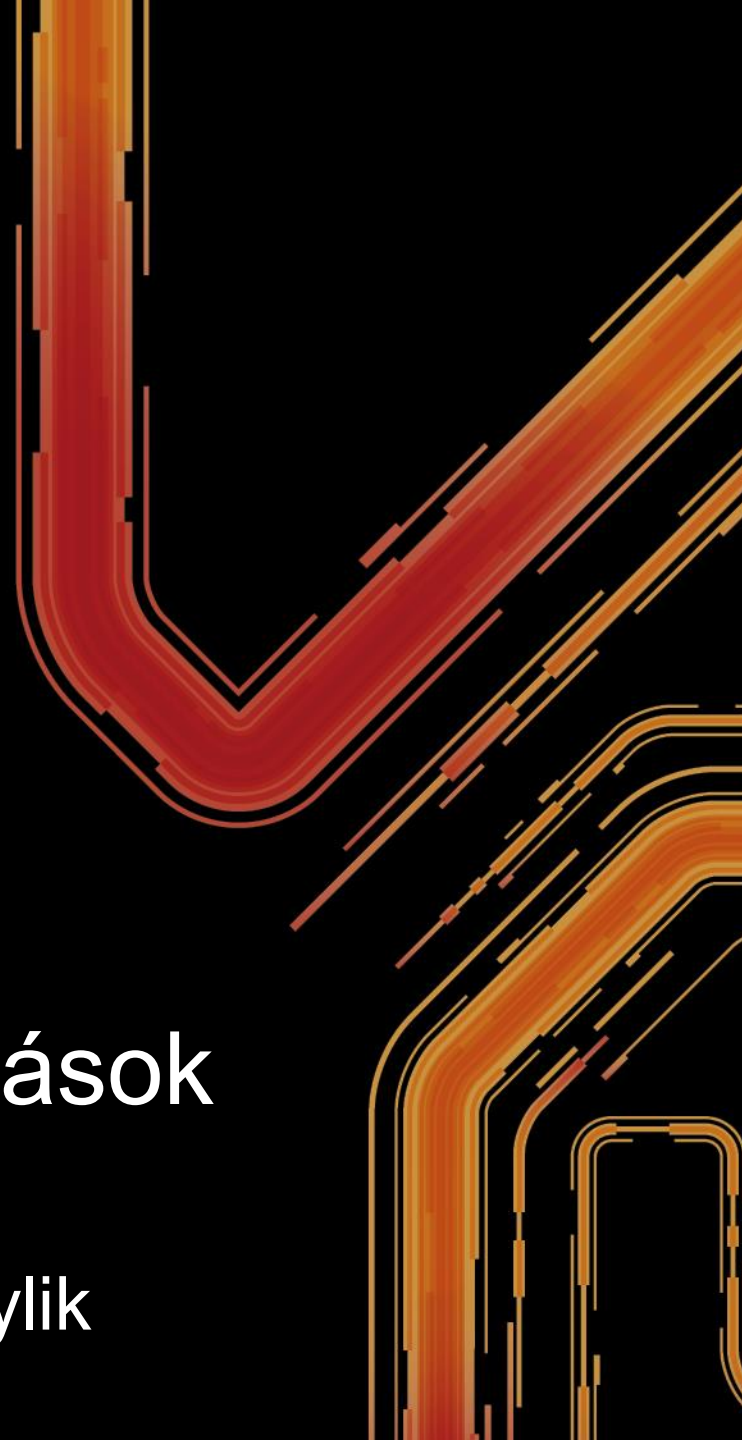




Egzotikus webalkalmazások
tesztelése,
avagy nem mind arany, ami fénylik



Bemutakozás

Veres-Szentkirályi András

Silent Signal

IT biztonsági szakértő

OSCP GWAPT

vsza@silentsignal.hu



Webalkalmazások



<http://xkcd.com/934>

- Nem mobil, BYOD, trendi
 - Engesztelő buzzword: cloud
 - ~15 év kitermelt néhány fejlesztőcsapatot
- Nem látni, mitől tűnnének el

Google Web Toolkit

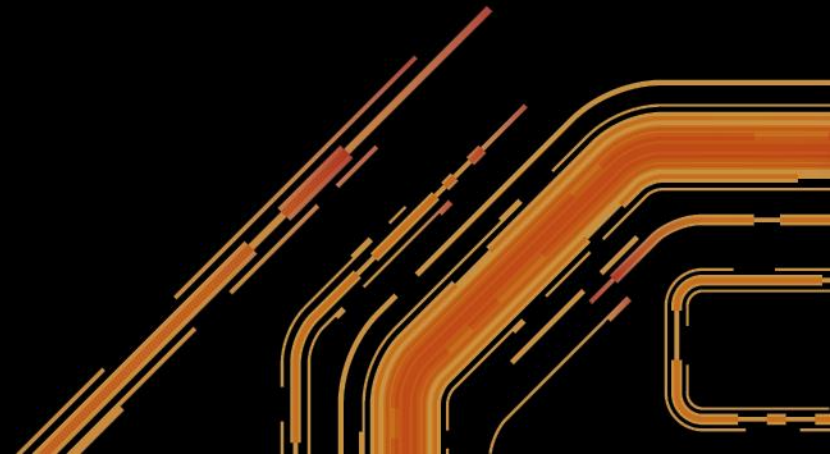
- Rich Internet Application
 - Blogger, Wallet, AdWords, Groups
- Java + AJAX
- Obfuszkált és optimalizált JS kód
- XSRF kivédve saját HTTP fejléccel
- Saját sorosítási formátum
 - Toolok nem ismerik
 - Verziók között vannak eltérések

DEMO



Google Web Toolkit hackelés

- Már a metódusok felsoroltatása is gond
 - Buherátor ki is adott pár toolt, lásd GitHub
 - Ez különösen verziófüggő
- Sérülékenységekre nincs kész scanner
 - „Nulláról” írni erőforrás-igényes
 - Írjunk proxy-t!



Flask

- Python web mikro-keretrendszer
- Jó alap egy ilyen eszközhöz
 - Egyszerű felépítés
 - Kevés zavaró elem
 - Beépített fejlesztői webszerver
- Kettőt egy csapásra
 - Proxy
 - Kézi tesztfelület

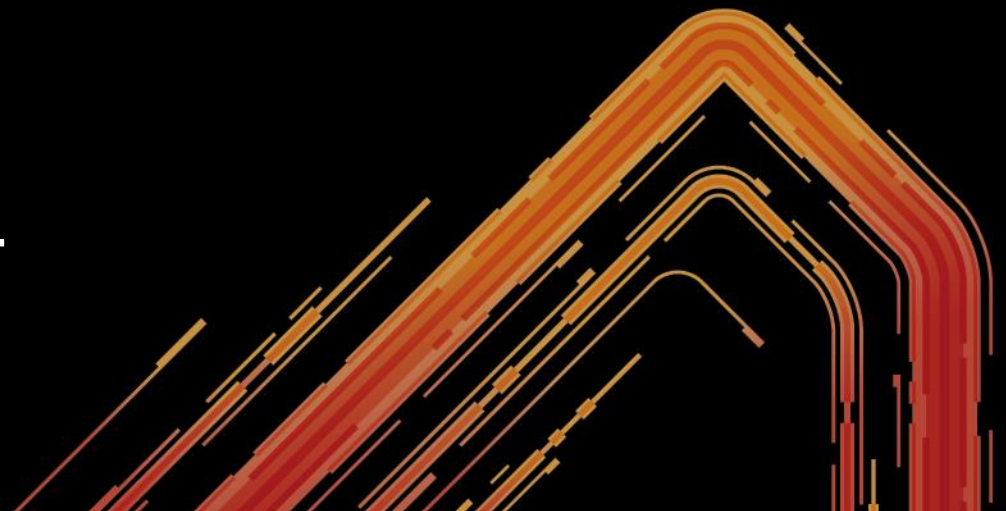


DEMO



SOAP

- Tudom, nem webalkalmazás
- Léteznek toolok, de...
 - Bitrot
 - Összetett objektumok kezelése
 - Ékezetek kezelése
- Megoldás?
 - Még egy proxy...



Intermezzo

TargetProxySpiderScannerIntruderRepeaterSequencerDecoderComparerExtenderOptionsAlertsWsdler

Binding	Operation	Port
InstantOrderSoap	OrderItem	http://10.2.9.105/InstantOrder.asmx
InstantOrderSoap	CheckStatus	http://10.2.9.105/InstantOrder.asmx
InstantOrderSoap12	OrderItem	http://10.2.9.105/InstantOrder.asmx
InstantOrderSoap12	CheckStatus	http://10.2.9.105/InstantOrder.asmx

Request

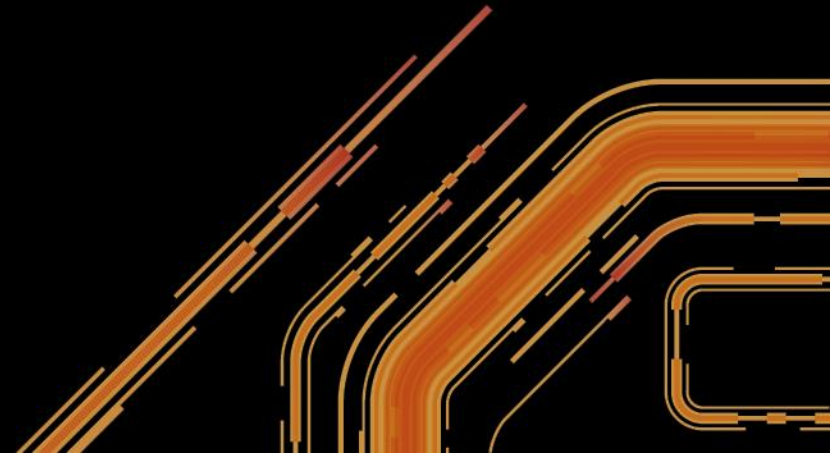
RawParamsHeadersHexXML

```
POST /InstantOrder.asmx HTTP/1.1
Accept-Encoding: gzip,deflate
Content-Type: text/xml; charset=UTF-8
SOAPAction: http://schemas.microsoft.com/samples/sqlserver/storefront/2005/3/OrderItem
Host: 10.2.9.105
Content-Length: 778

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://schemas.microsoft.com/samples/sqlserver/storefront/2005/3/">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:OrderItem>
      <ns:userName>gero et</ns:userName>
      <ns:password>sonoras imperio</ns:password>
      <ns:productID>3</ns:productID>
      <ns:quantity>3</ns:quantity>
      <ns:addressLine1>quae divum incedo</ns:addressLine1>
      <ns:addressLine2>verrantque per auras</ns:addressLine2>
      <ns:addressCity>per auras</ns:addressCity>
      <ns:addressStateProvinceID>3</ns:addressStateProvinceID>
      <ns:addressPostalCode>circum claustra</ns:addressPostalCode>
    </ns:OrderItem>
  </soapenv:Body>
</soapenv:Envelope>
```

SOAP vs. Python

- Használható kliens implementáció: SUDS
- WSDL feldolgozás
- Proxy objektum
- Factory pattern



DEMO



Tanulság

- Attól, hogy az infrastruktúrához nincs (még) tool, lehet a kódban hiba, sőt!
- Nem mindig kell nulláról kezdeni, a kerék újra feltalálása ritkán vezet jóra.
- Share the software: <http://git.io/s2>



The background features a complex pattern of glowing, multi-colored lines in shades of red, orange, and yellow. These lines are arranged in a way that suggests a circuit board or a network of data paths, with some lines forming large, rounded shapes and others branching out. The overall effect is a high-tech, digital aesthetic.

Köszönöm a figyelmet!