

Aplikacje webowe

Bezpieczeństwo systemów komputerowych
semestr zimowy, 2020/21

Przypomnieć - jak ktoś nie rozumie,
niech pinguje, bo nie widzę twarzy

Directory Traversal - co robić?

- opcja 1: whitelist znaków ([a-ZA-Z0-9]*)
- opcja 2: czy_plik_jest_w_katalogu()
- opcja 3: nie trzymać plików w systemie plików
 - dygresja: inne zalety, np. skalowalność

Directory Traversal - co robić?

```
File file = new File(BASE_DIRECTORY, userInput);  
  
if (file.getCanonicalPath().startsWith(BASE_DIRECTORY)) {  
  
    ...  
  
}
```

<https://portswigger.net/web-security/file-path-traversal>

Rozgrzewka

<http://bsk2020.kazet.cc:8018/post/1137>

Zadanie 6

...

```
if (isset($_GET['manpage'])) {  
    echo(system("man " . $_GET['manpage']));  
}
```

...

<http://bsk2020.kazet.cc:8006/>

Gra w banowanie

Blacklist nie działa
(i to jest dość ogólna zasada security)

Command Injection - co robić?

- opcja 0: biblioteka zamiast poleceń shellowych
- opcja 1: własne nazwy plików
- opcja 2: whitelist znaków ([a-ZA-Z0-9]*)
- opcja 3 wbudowane w język programowania mechanizmy zabezpieczeń (typu `subprocess.call(['ls', ...])`)

opinia (<https://portswigger.net/web-security/os-command-injection>): “Never attempt to sanitize input by escaping shell metacharacters. In practice, this is just too error-prone and vulnerable to being bypassed by a skilled attacker.”

Bazy danych

```
if (isset($_GET['username']) and isset($_GET['password'])) {  
    $username = (string) $_GET['username'];  
    $password = (string) $_GET['password'];  
    $result = mysqli_query(  
        $link,  
        "SELECT * FROM users WHERE username='" .  
            $username . "' AND password='" .  
            $password . "';";  
    );  
    if (mysqli_num_rows($result) > 0) {  
        echo "Logged in successfully. Flag is: (...)" ;  
    }  
}
```

<http://bsk2020.kazet.cc:8008/>

SQL Injection

- Występuje coraz rzadziej
 - Nie trzeba pisać ręcznie zapytań żeby zbudować formularz logowania...
 - ...albo dowolny inny kawałek aplikacji webowej
-
- Ale nadal czasem trzeba napisać skomplikowane, ręcznie zoptymalizowane zapytanie do bazy na kilkadziesiąt liniiek - i wtedy już SQLi jest możliwe

Te same problemy co przy command injection - nie pisać samemu filtrowania, wykorzystać wbudowane w framework.

Bazy danych - co robić?

- używać ochrony zapewnianej przez framework
- google: prepared statements/parameter binding

Bazy danych - co robić?

```
query = "INSERT INTO user (Id, Name) VALUES (%s, %s)"
```

```
record = (id, name)
```

```
cursor.execute(query, record)
```

```
connection.commit()
```

Rekonesans: Google Dork

- site:strona.com
- “index of” site:strona.com
- error site:strona.com
- warning site:strona.com
- warning site:strona.com -falsepositive1 -falsepositive2

Rekonesans: ciąg dalszy / OSINT

- crt.sh (co to jest? jak to działa? zadanie z mimuw.edu.pl)
- dnsdumpster.com (również - zadanie z mimuw.edu.pl)
- inne strony pod tym samym adresem IP? Shared hosting albo powiązane?
- Github
- ...

Z innej beczki: CEIDG, dokumenty spółek, PDFy w internecie, archive.org, ...

Rekonesans: ciąg dalszy

Dlaczego należy minimalizować ekspozycję na zewnątrz

(historia o Kibanie, kiedyś Jenkinsie)

Bonus

Plik o numerze 1 możecie odpakować wchodząc na:

<http://bsk2020.kazet.cc:8022/unpack/1/>

Zadanie to odpakowanie treści pliku nr 2.

Kod źródłowy: <http://bsk2020.kazet.cc:8022/source>

Zadania nie było na zajęciach - w razie czego, proszę pisać z pytaniami na krzysztof.zajac2@gmail.com.

XML External Entities (XXE)

Co to jest XML?

```
<people>
  <person>
    <first_name>Jan</first_name>
    <last_name>Nowak</last_name>
  </person>
  <person>
    <first_name>Jan</first_name>
    <last_name>Kowalski</last_name>
  </person>
</people>
```

XML External Entities (XXE)

Gdzie jest używany XML?

- EPUB
- RSS
- Office Open XML (.docx)

XML External Entities (XXE)

Gdzie jest używany XML?

AdsML, aecXML, Agricultural Ontology Service, AIML, AnIML, Atom, Attention Profiling Mark-up Language (APML), Automated Test Markup Language (ATML), Attention.xml, Auto-lead Data Format, BeerXML, Binary Format Description language, Biological Dynamics Markup Language (BDML), Business Intelligence Markup Language (BIML), Business Process Execution Language, Call Control eXtensible Markup Language, CCTRL, CellML, Channel Definition Format, Chemical Markup Language, ClaML, Clinical Data Interchange Standards Consortium, Clinical Document Architecture, COLLADA, Common Alerting Protocol (CAP), CXML, Darwin Information Typing Architecture (DITA), Data center markup language, Digital Forensics XML, Dimensional Markup Language, Directory Service Markup Language, DisplayML, DocBook...

Źródło: https://en.wikipedia.org/wiki/List_of_XML_markup_languages

AdsML, aecXML, Agricultural Ontology Service, AIML, AnIML, Atom, Attention Profiling Mark-up Language (APML), Automated Test Markup Language (ATML), Attention.xml, Auto-lead Data Format, BeerXML, Binary Format Description language, Biological Dynamics Markup Language (BDML), Business Intelligence Markup Language (BIML), Business Process Execution Language, Call Control eXtensible Markup Language, CCTRL, CellML, Channel Definition Format, Chemical Markup Language, ClaML , Clinical Data Interchange Standards Consortium, Clinical Document Architecture, COLLADA, Common Alerting Protocol (CAP), CXML, Darwin Information Typing Architecture (DITA), Data center markup language, Digital Forensics XML, Dimensional Markup Language, Directory Service Markup Language, DisplayML, DocBook, Document Schema Definition Languages, Document Structure Description, EAC, EAD, ebXML, eLML, EMMML Enterprise Mashup Markup Language, EPPML, EPUB, Extensible Application Markup Language, Extensible Data Format, Extensible Messaging and Presence Protocol, Extensible Provisioning Protocol, Extensible Resource Identifier, Extensible Stylesheet Language, Facelets VDL, FicML, FictionBook, FIXatdl, FIXML, FleXML, FpML, FXT, Geography Markup Language, GeoSciML, GJXDM, GPX, GraphML, Green Building XML, GuideML, GXA, GXL, HumanML, Industry Foundation Classes, Information and Content Exchange, IO-Link Device Description (IODD), JATS, Java Speech Markup Language, Job Definition Format, Job Submission Description Language, Keyhole Markup Language, Link contract, LOGML, MARCXML, MathML, Medical Reality Markup Language (MRML), Metadata Object Description Schema, Microformats, MOWL, Music Encoding Initiative (MEI), Music Markup Language, MusicXML, MXML, Namespace-based Validation Dispatching Language, National Information Exchange Model, Nested Context Language, NewsML, NewsML-G2, NeXML, NeuroML, ODD, ODRL, Office Open XML, OFX, OIOXML, Open Mathematical Documents (OMDoc), OML, Open eBook, Open Scripture Information Standard (OSIS), OpenDocument (ODF), OpenMath, OPML, phyloXML, PMML, PNML, PDBML, RailML, RDFa, RecipeML, Regular Language description for XML, RELAX NG, Remote Telescope Markup Language, Resource Description Framework, RoadXML, RSS (file format), RSS enclosure, RuleML, S5 file format, SAML, SBML, SBGN, Schematron, SCORM, SCXML, Simple Sharing Extensions, SMIL, SOAP, SOAP with Attachments, Speech Application Language Tags, Speech Synthesis Markup Language, SPML, Strategy Markup Language (StratML), Streaming Transformations for XML, SVG, SXBL, Text Encoding Initiative, ThML, Topicmaps, TransducerML, Translation Memory eXchange (TMX), TREX, Unified XUL Platform, Universal Description Discovery and Integration, Vector Markup Language, Vexi, VoiceXML, W3C MMI, WDDX, WaterML, Web feed, Web Ontology Language, Web Services Description Language, Web Services Dynamic Discovery, Wellsite information transfer standard markup language, WML Wireless Markup Language, WiX, WordprocessingML, WS-Policy, X3D, XAML, XACML, XBEL , XBL, XBRL, xCBL, xCal, XCES, XDI, XDuce, XDXF, XFA, XForms, XHTML, XHTML Basic, XHTML Friends Network, XHTML Modularization, XidML, XInclude, XLIFF, XLink, XMI, XML Encryption, XML Information Set, XML Interface for Network Services, XML Resource, XML Schema, XML Script, XML Signature, XML for Analysis, XML pipeline, XML-RPC, XMLTerm, XMLTV, XOMGL, XOXO, XPD, XPath (or XPath 1.0), XPath 2.0, XPointer, XProc , XQuery, XrML, XSIL, XSL Formatting Objects, XSL Transformations, XSPF, XTCE, XUL, XUpdate

Źródło: https://en.wikipedia.org/wiki/List_of_XML_markup_languages

XML External Entities (XXE)

XML ma możliwość zagnieżdżania również zewnętrznych plików.

Częścią zadania jest znalezienie jak się te zewnętrzne pliki zagnieżdża. Luka ma nazwę XML External Entities.

<http://bsk2020.kazet.cc:8011/>

Odczytajcie plik /flag.txt

Co robić?

- wniosek bezpośredni:
 - parsery XML mają *tryb bezpieczny*. Nie, nie jest zawsze włączony.
- wniosek ogólny:
 - czytać ostrzeżenia w dokumentacji (jeśli są. PHP SimpleXMLElement nie ma).
 - jeśli biblioteka - przetestować, spojrzeć w kod

Na następne zajęcia: Burp Suite Community

1. Co to jest?
2. <https://portswigger.net/burp>
3. Prośba o zainstalowanie.

(de)serializacja

Uwaga: tak, jak piszę na następnym slajdzie **nie należy** pisać w Django - celowo nie skorzystałem z mechanizmów wbudowanych we framework.

Zadania nie było na zajęciach - w razie czego, proszę pisać z pytaniami na krzysztof.zajac2@gmail.com.

```
if 'greeting' in request.GET:  
    response = HttpResponseRedirect('/')  
    response.set_cookie('greeting',  
        base64.b64encode(pickle.dumps('Hi, ' +  
            request.GET['greeting'])).decode('ascii'))  
    return response
```

```
context = {}
```

```
if 'greeting' in request.COOKIES:  
    context['greeting'] =  
        pickle.loads(base64.b64decode(request.COOKIES['greeting']))  
return TemplateResponse(request, 'main/homepage.html', context)
```

<http://bsk2020.kazet.cc:8014/>

(de)serializacja

Co robić? Otóż nie deserializować danych od użytkownika.