VULNERABILITIES IN .NET PLATFORM

MIKHAIL SHCHERBAKOV AT DOTNEXT CONFERENCE_

About me

- Independent developer and consultant
- Co-organizer of .NET meetups in Saint Petersburg and Moscow
- Former Product Manager at Cezurity, R&D Developer at Positive Technologies and Team Lead at Acronis, Luxoft, Boeing

About the talk

- CVE-2015-2526 ASP .NET MVC Regular Expression DoS
- CVE-2002-1145 MS SQL Server Elevation of Privilege
- CWE-264 ASP .NET Core Elevation of Privilege
- CVE-2016-3255 XXE Information Disclosure
- Deserializing Untrusted Binary Data

Why?

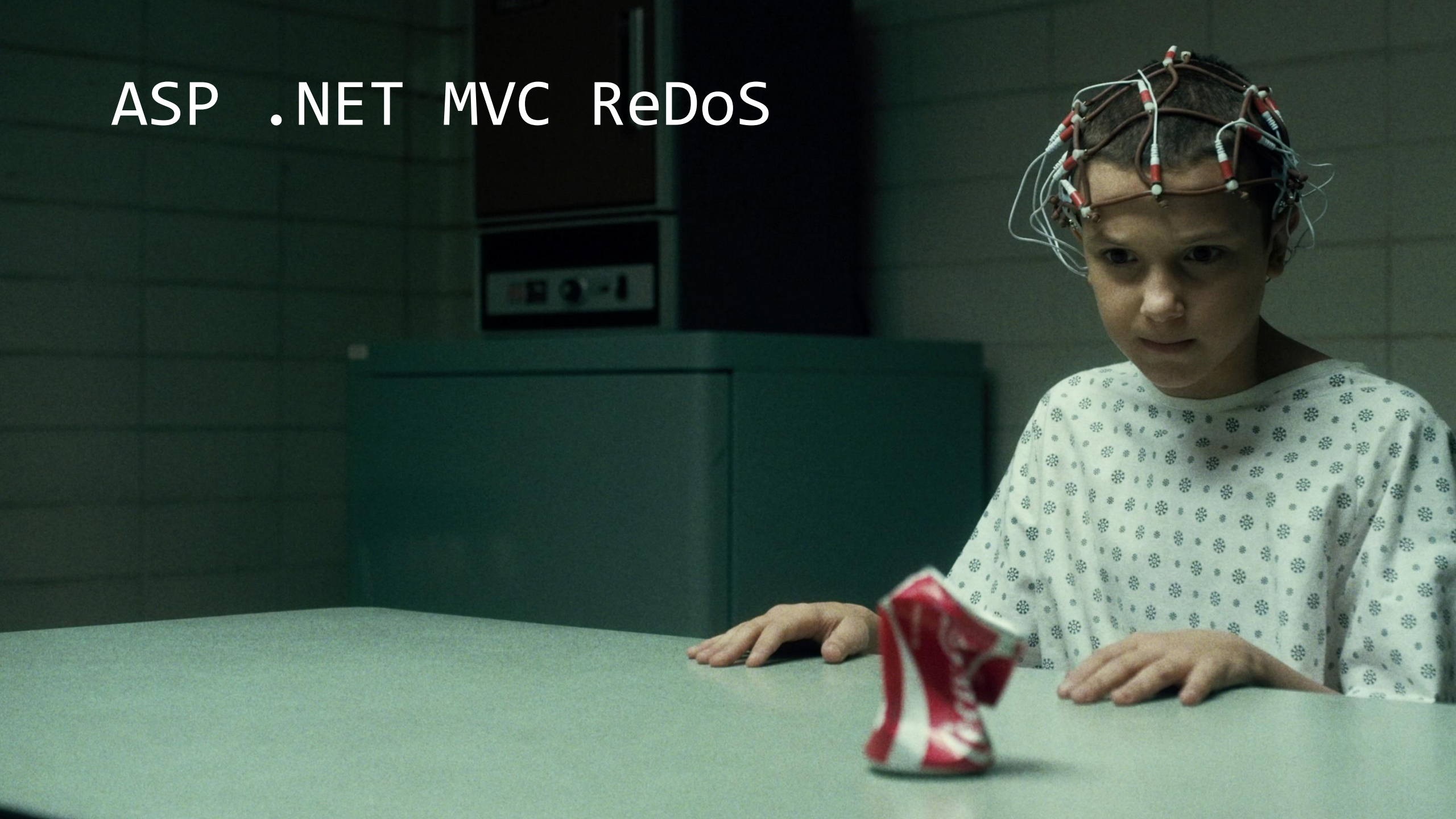
- Clean look at your code and… your life
- Do not make typical vulnerabilities


Fun and Hardcore!

ASP .NET MVC Regular Expression DoS

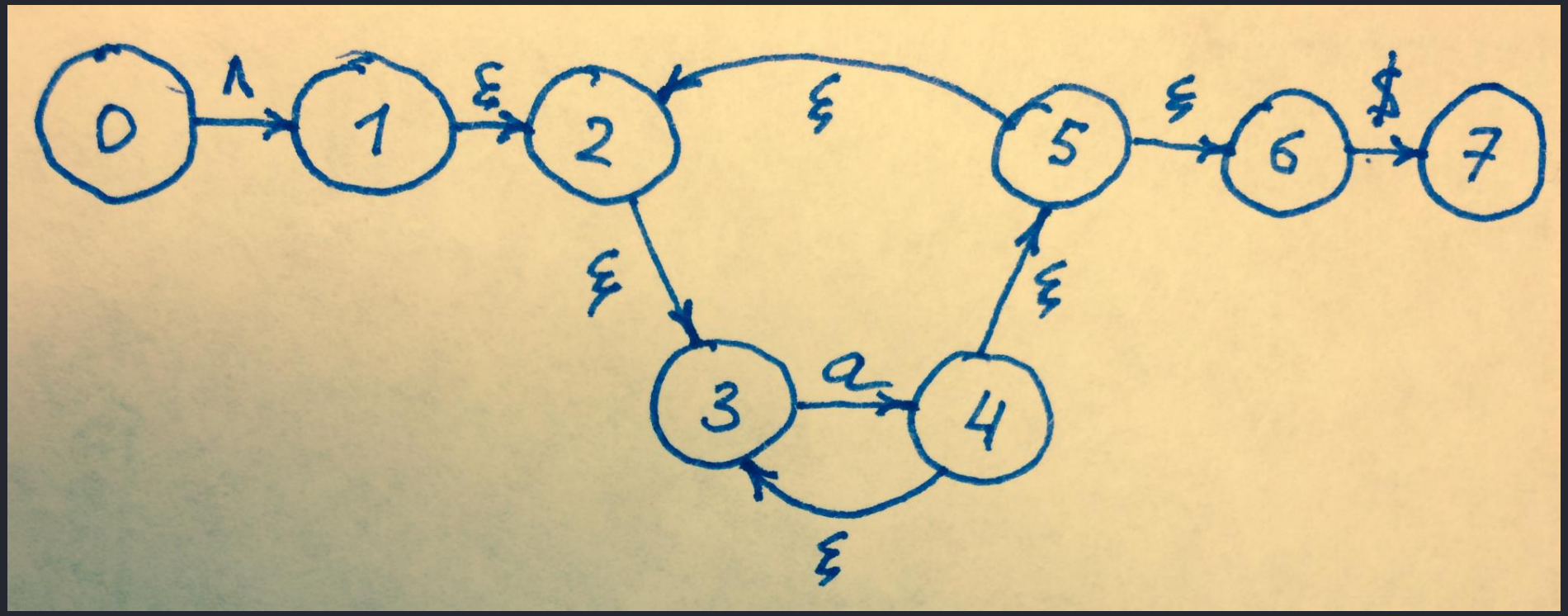
CVE-2015-2526

ASP .NET MVC ReDoS



The problematic Regex algorithm

^(a+)+$



Non-Deterministic Finite Automata

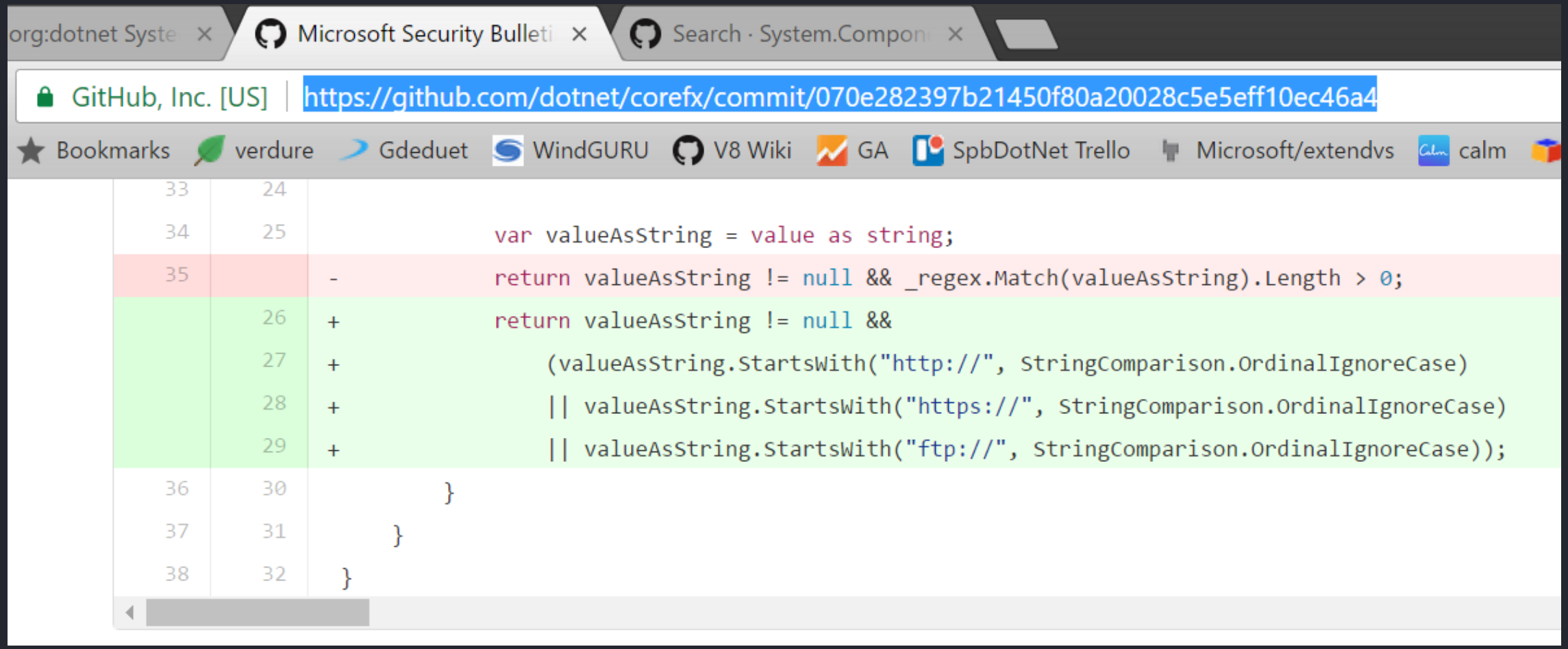
How to fix it

- Simplify RegExp
- Replace RegExp to a custom algorithm

How to fix it

```
^(https?|ftp):\/\/((((([a-z]|\d|-|\.|_|~|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-
\uFFEF])|(%[\da-f]{2})|[!\$&'\(\)\*\+,;=]|:)*@)?(((\d|[1-9]\d|1\d\d|2[0-4]\d|25[0-
5])\.(\d|[1-9]\d|1\d\d|2[0-4]\d|25[0-5])\.(\d|[1-9]\d|1\d\d|2[0-4]\d|25[0-
5])\.(\d|[1-9]\d|1\d\d|2[0-4]\d|25[0-5]))|((([a-z]|\d|[\u00A0-\uD7FF\uF900-
\uFDCF\uFDF0-\uFFEF])|(([a-z]|\d|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-\uFFEF])([a-
z]|\d|-|\.|_|~|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-\uFFEF])*([a-z]|\d|[\u00A0-
\uD7FF\uF900-\uFDCF\uFDF0-\uFFEF])))\.)+(([a-z]|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-
\uFFEF])|(([a-z]|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-\uFFEF])([a-z]|\d|-
|\.|_|~|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-\uFFEF])*([a-z]|[\u00A0-\uD7FF\uF900-
\uFDCF\uFDF0-\uFFEF])))\.?)(:\d*)?)(\/((([a-z]|\d|-|\.|_|~|[\u00A0-\uD7FF\uF900-
\uFDCF\uFDF0-\uFFEF])|(%[\da-f]{2})|[!\$&'\(\)\*\+,;=]|:|@)+(\/(([a-z]|\d|-
|\.|_|~|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-\uFFEF])|(%[\da-
f]{2})|[!\$&'\(\)\*\+,;=]|:|@)*)*)?)?(\?((([a-z]|\d|-|\.|_|~|[\u00A0-\uD7FF\uF900-
\uFDCF\uFDF0-\uFFEF])|(%[\da-f]{2})|[!\$&'\(\)\*\+,;=]|:|@)|[\uE000-
\uF8FF]|\/|\?)*)?(\#((([a-z]|\d|-|\.|_|~|[\u00A0-\uD7FF\uF900-\uFDCF\uFDF0-
\uFFEF])|(%[\da-f]{2})|[!\$&'\(\)\*\+,;=]|:|@)|\/|\?)*)?$
```

How to fix it


org:dotnet Syste
Microsoft Security Bulleti
Search · System.Compon
GitHub, Inc. [US]
https://github.com/dotnet/corefx/commit/070e282397b21450f80a20028c5e5eff10ec46a4
Bookmarks
verdure
Gdeduet
WindGURU
V8 Wiki
GA
SpbDotNet Trello
Microsoft/extendvs
calm
33 24
var valueAsString = value as string;
34 25
- return valueAsString != null && _regex.Match(valueAsString).Length > 0;
35
+ return valueAsString != null &&
26
+ (valueAsString.StartsWith("http://", StringComparison.OrdinalIgnoreCase)
27
+ || valueAsString.StartsWith("https://", StringComparison.OrdinalIgnoreCase)
28
+ || valueAsString.StartsWith("ftp://", StringComparison.OrdinalIgnoreCase));
29
}
36 30
}
37 31
}
38 32

How to fix it

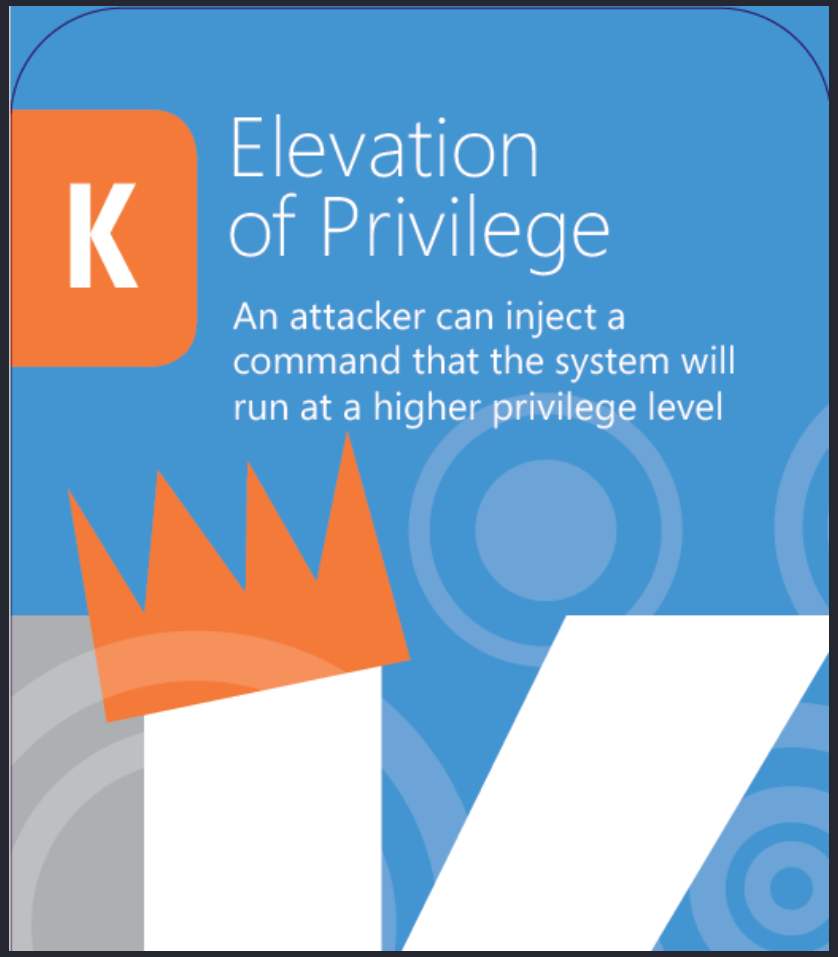
- Set a timeout in new Regex()
- Set a global timeout for all regular expressions

```
AppDomain.CurrentDomain.SetData(
    "REGEX_DEFAULT_MATCH_TIMEOUT",
    TimeSpan.FromSeconds(1));
```

MS SQL Server Elevation of Privilege

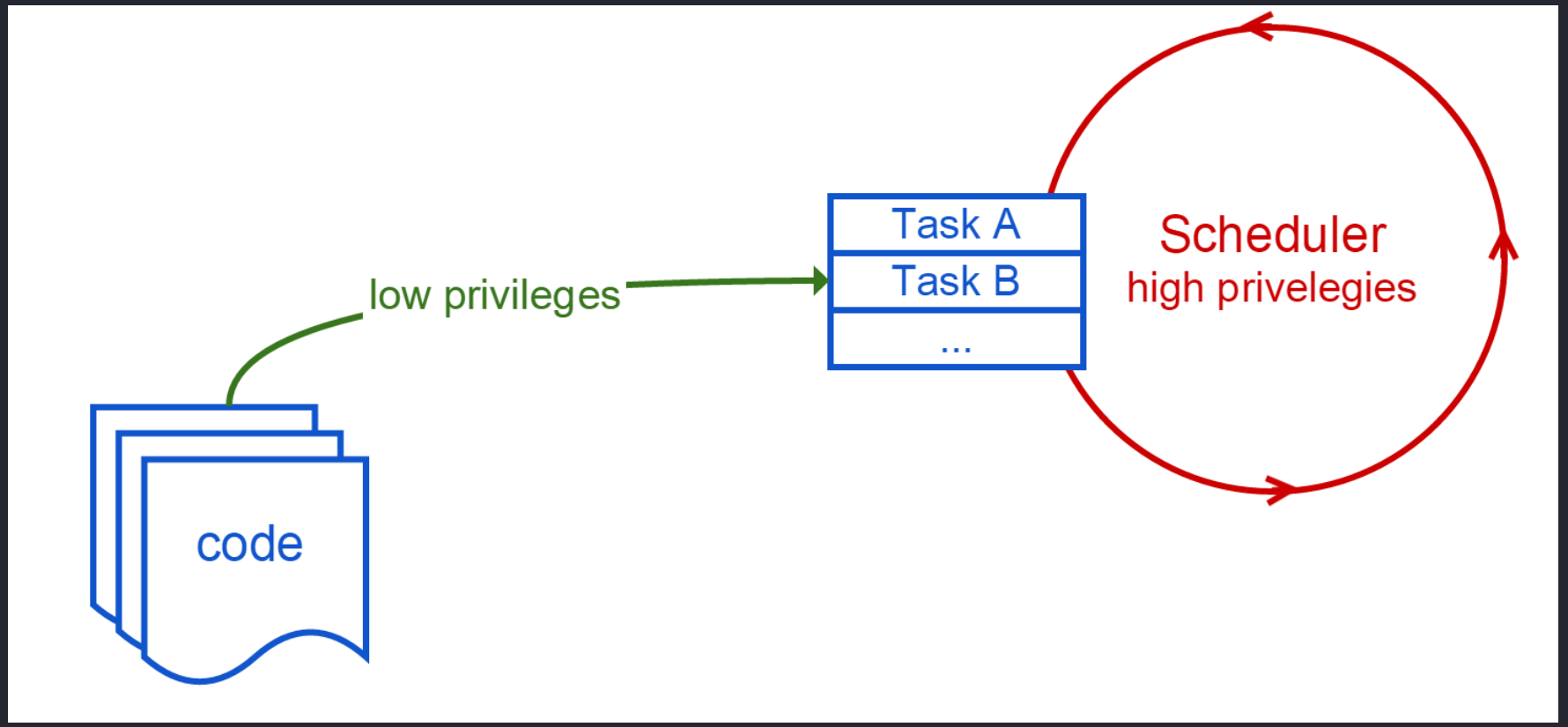
CVE-2002-1145

Elevation of Privilege (EoP)



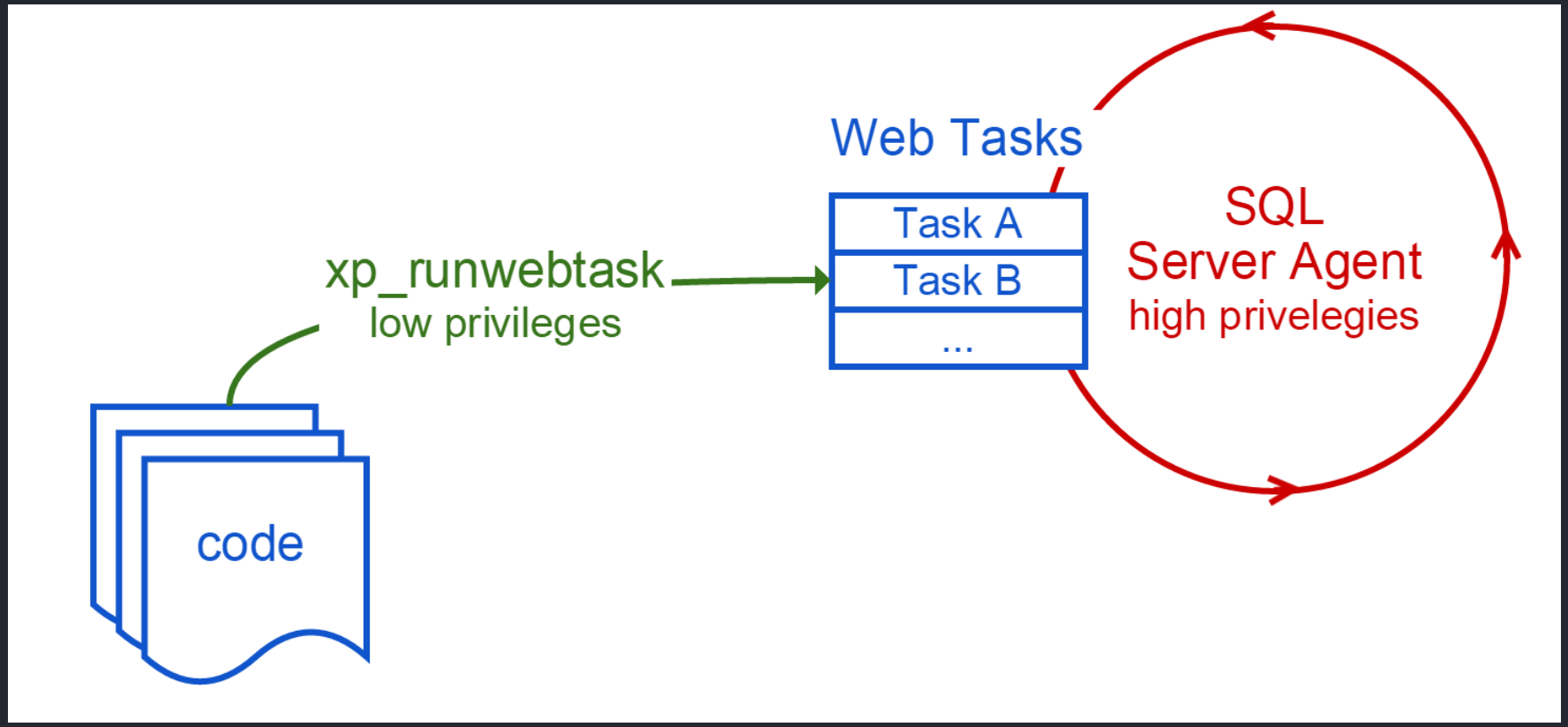
Have a fun with the EoP Card Game https://www.microsoft.com/en-us/sdl/adopt/eop.aspx

Luring Attack



Luring Attack

CVE-2002-1145 “EoP in SQL Server Web Tasks”



ASP .NET Core Elevation of Privilege

CWE-264

Using scoped services in ViewComponent

```
10      public interface IScopeService
11      {
12          string GuidTest { get; }
13
14          void FillGuid();
15      }
16
17      public static class ScopeServiceExtension
18      {
19          public static IServiceCollection AddScopeService(this IServiceCollection services)
20          {
21              services.AddScoped<IScopeService, ScopeService>();
22
23              return services;
24          }
25      }
```

https://github.com/gdegeneve/ViewComponentBug

How to fix it

2 ...spNetCore.Mvc.ViewFeatures/DependencyInjection/MvcViewFeaturesMvcCoreBuilderExtensions.cs

```
@@ -140,7 +140,7 @@ internal static void AddViewServices(IServiceCollection services)
140 140             services.TryAddSingleton<
141 141                 IViewComponentDescriptorCollectionProvider,
142 142                 DefaultViewComponentDescriptorCollectionProvider>();
143     -           services.TryAddSingleton<ViewComponentResultExecutor>();
    143 +           services.TryAddTransient<ViewComponentResultExecutor>();
144 144
145 145           services.TryAddSingleton<ViewComponentInvokerCache>();
146 146           services.TryAddTransient<IViewComponentDescriptorProvider, DefaultViewComponen
```

GitHub Commit http://bit.ly/2guXVMo
GitHub Issue http://bit.ly/2guOIUg
[Discussion] Microsoft Security Advisory 3181759 http://bit.ly/2fOJFiv

How to fix it

- Double check a security sensitive code: impersonation, scheduling tasks, sandboxing, modification data from low privileged user, introducing between low and high privileged code, lifetime of security sensitive objects
- Runtime check invariants of security sensitive data
- Everywhere minimal privileges by default

XXE Information Disclosure

CVE-2016-3255

Understanding XML Entity

```
1   <?xml version="1.0" encoding="utf-8" ?>
2   <!DOCTYPE catalog [
3     <!ENTITY msg "Hello Word">
4   ]>
5   <catalog>
6     <person>
7       <gAddress>&msg;</gAddress>
8       <gAge>18</gAge>
9       <gPhone>777-777-777</gPhone>
10    </person>
11  </catalog>
```

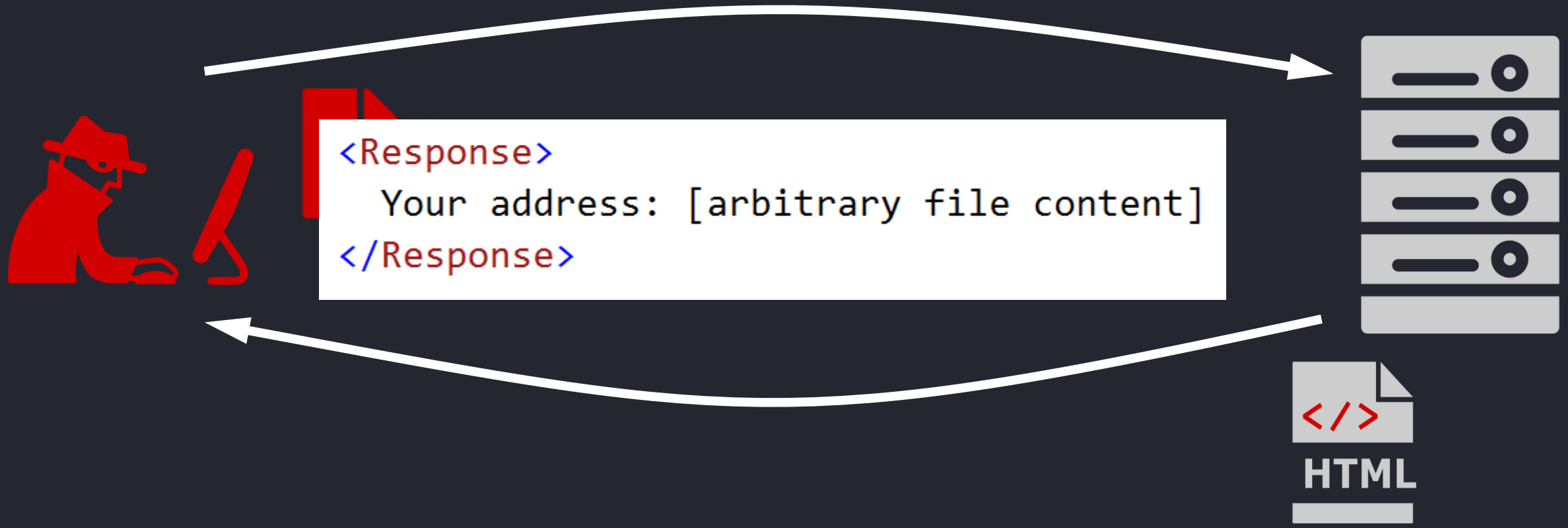
Billion Laughs Attack

```
1  <?xml version="1.0" encoding="utf-8" ?>
2  <!DOCTYPE catalog [
3    <!ENTITY a0 "dos" >
4    <!ENTITY a1 "&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;&a0;">
5    <!ENTITY a2 "&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;&a1;">
6    <!ENTITY a3 "&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;&a2;">
7    <!ENTITY a4 "&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;&a3;">
8  ]>
9  <catalog>
10   <person>
11     <gAddress>&a4;</gAddress>
12   </person>
13 </catalog>
```

Understanding XML External Entity

```
1   <?xml version="1.0" encoding="utf-8" ?>
2   <!DOCTYPE catalog [
3     <!ENTITY msg SYSTEM "file:///c:/inetpub/project/Web.config">
4   ]>
5   <catalog>
6     <person>
7       <gAddress>&msg;</gAddress>
8       <gAge>18</gAge>
9       <gPhone>777-777-777</gPhone>
10    </person>
11  </catalog>
```

Classic XXE Attack



Understanding XXE Attack

- No a direct feedback channel
- Get Web.config file
- Use XML parser settings by default

Understanding XXE Attack

237

It's very simple. I know these are standard methods, but you can create your own library to deal with that much better.

Here are some examples:

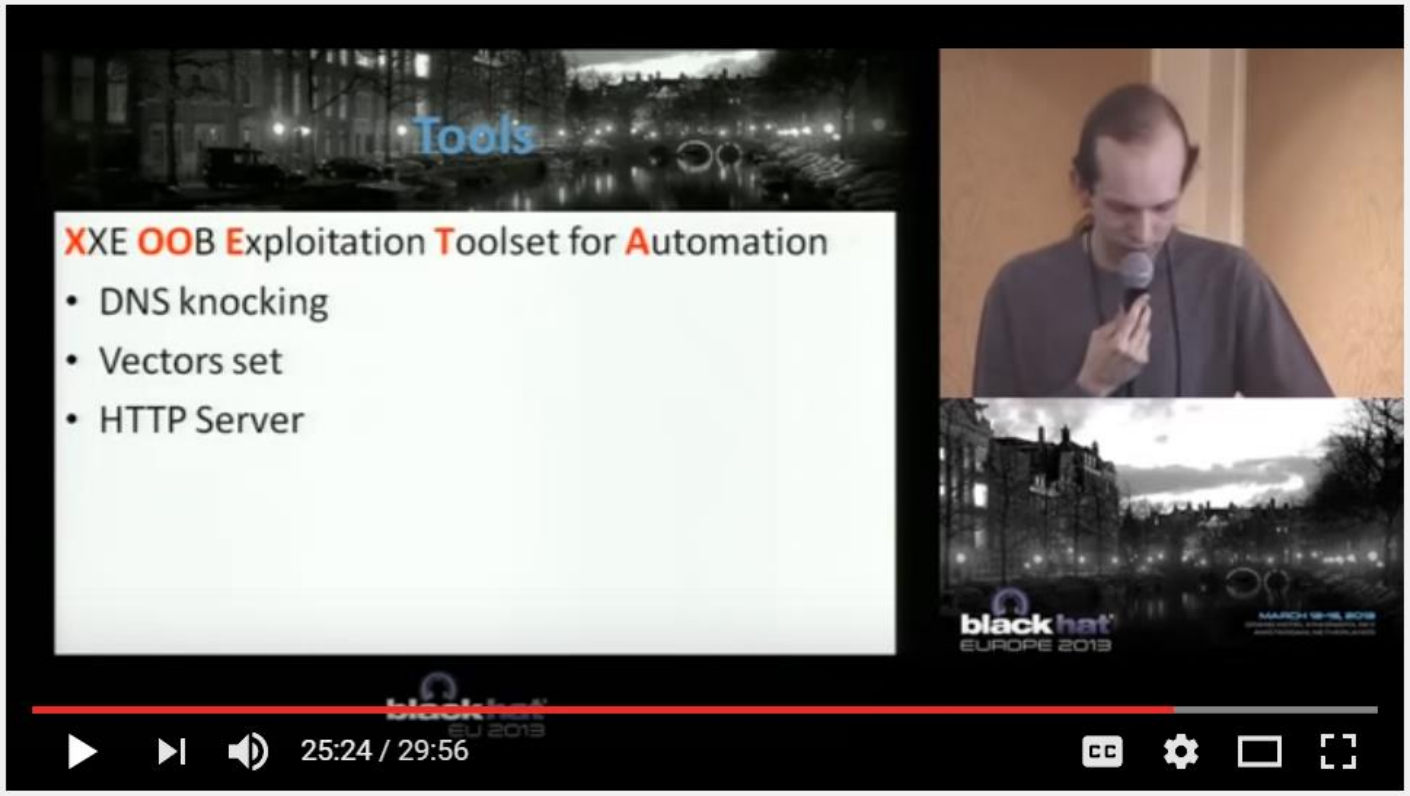
```
XmlDocument xmlDoc= new XmlDocument(); // Create an XML document object
xmlDoc.Load("yourXMLFile.xml"); // Load the XML document from the specified file

// Get elements
XmlNodeList girlAddress = xmlDoc.GetElementsByTagName("gAddress");
XmlNodeList girlAge = xmlDoc.GetElementsByTagName("gAge");
XmlNodeList girlCellPhoneNumber = xmlDoc.GetElementsByTagName("gPhone");

// Display the results
Console.WriteLine("Address: " + girlAddress[0].InnerText);
Console.WriteLine("Age: " + girlAge[0].InnerText);
Console.WriteLine("Phone Number: " + girlCellPhoneNumber[0].InnerText);
```

Also, there are some other methods to work with. For example, here. And I think there is no one best method to do this; you always need to choose it by yourself, what is most suitable for you.

http://stackoverflow.com/questions/55828/how-does-one-parse-xml-files

XXE Attack

XML Out-of-Band Data



A.Osipov, T.Yunusov 2013
“XML OOB Data Retrival”
https://youtu.be/eBm0YhBrT_c

T.Morgan 2014
“XML Schema, DTD, and Entity Attacks”
http://bit.ly/2h6wtTH

How to fix it

XML Object	Safe by Default?
XMLReader	
Prior to FW 4.0	Yes
FW 4.0+	Yes
XMLTextReader	
Prior to FW 4.0	No
FW 4.0+	No
XMLDocument	
Prior to 4.6	No
FW 4.6+	Yes

https://www.jardinesoftware.net/2016/05/26/xxe-and-net/

How to fix it

- Prohibit DTD processing
- Nullify references to resolvers
- Utilize a secure resolver
- Limit expansion size and set default timeouts

Deserializing Untrusted Binary Data

Binary Serializing

```
public class Hello : ICommand
{
    public string Execute()
    {
        return "Hello DotNext 2016!";
    }
}
```

Binary Serializing

```
[HttpPost]
public ActionResult Upload(HttpPostedFileBase file)
{
    var serializer = new BinaryFormatter();
    var command = (ICommand)serializer.Deserialize(file.InputStream);
    var result = command.Execute();

    return RedirectToAction(result);
}
```

Binary Serializing

```
public class Converter : ICommand
{
    private string converterName;
    private string arguments;

    public Converter(string converterName, string arguments)
    {
        if (converterName != "ConverterXML.exe" && converterName != "ConverterJSON.exe")
            throw new ArgumentException();

        this.converterName = converterName;
        this.arguments = arguments;
    }

    public string Execute()
    {
        Process.Start(converterName, arguments);
        return "OK";
    }
}
```

Binary Serializing

- Runtime Checks Bypass
- Unmanaged Data References
- Delegates and Events

Binary Serializing

```
[HttpPost]
public ActionResult Upload(HttpPostedFileBase file)
{
    var serializer = new BinaryFormatter();
    var command = (ICommand)serializer.Deserialize(file.InputStream);
    var result = command.Execute();

    return RedirectToAction(result);
}
```

Implicit Functionality

- ISerializable interface
- OnDeserialized or OnDeserializing attributes
- IDeserializationCallback interface
- IObjectReference interface
- Finalize method

.NET Remoting Binary Deserializing

```
if (this.TypeFilterLevel != TypeFilterLevel.Full)
{
    permissionSet = new PermissionSet(PermissionState.None);
    permissionSet.SetPermission(
        (IPermission)new SecurityPermission(SecurityPermissionFlag.SerializationFormatter));
}

try
{
    if (permissionSet != null)
        permissionSet.PermitOnly();
    requestMsg = CoreChannel.DeserializeBinaryRequestMessage(
        str, requestStream, _strictBinding, TypeFilterLevel);
}
finally
{
    if (permissionSet != null)
        CodeAccessPermission.RevertPermitOnly();
}
```

Deserializing Untrusted Binary Data

Binary Serializing

James Forshaw “Are you my Type? Breaking .NET Through Serialization”

https://media.blackhat.com/bh-us-12/Briefings/Forshaw/BH_US_12_Forshaw_Are_You_My_Type_WP.pdf

How to fix it

- Use custom serializer
- Use minimal privileges in serialization process

Summary

- OWASP Top Ten Project 2013 http://bit.ly/1OffewO
- OWASP Developer Guide http://bit.ly/1JcQLoh
- OWASP .NET Security Cheat Sheet http://bit.ly/2h2fDrQ
- Tom FitzMacken “What not to do in ASP.NET, and what to do instead” http://bit.ly/2h2sfyU

Thank you for your attention!

Mikhail Shcherbakov

Independent developer and consultant

linkedin.com/in/mikhailshcherbakov

spbdotnet.org

mskdotnet.org

@yu5k3