

In Secure Web Applications

Me



Denny Headrick

@dennythecoder

denny.headrick@gmail.com

Me

npm i denny




USAJOBS


 Sign In

 Help

 Search

 Keywords

2210

 Location

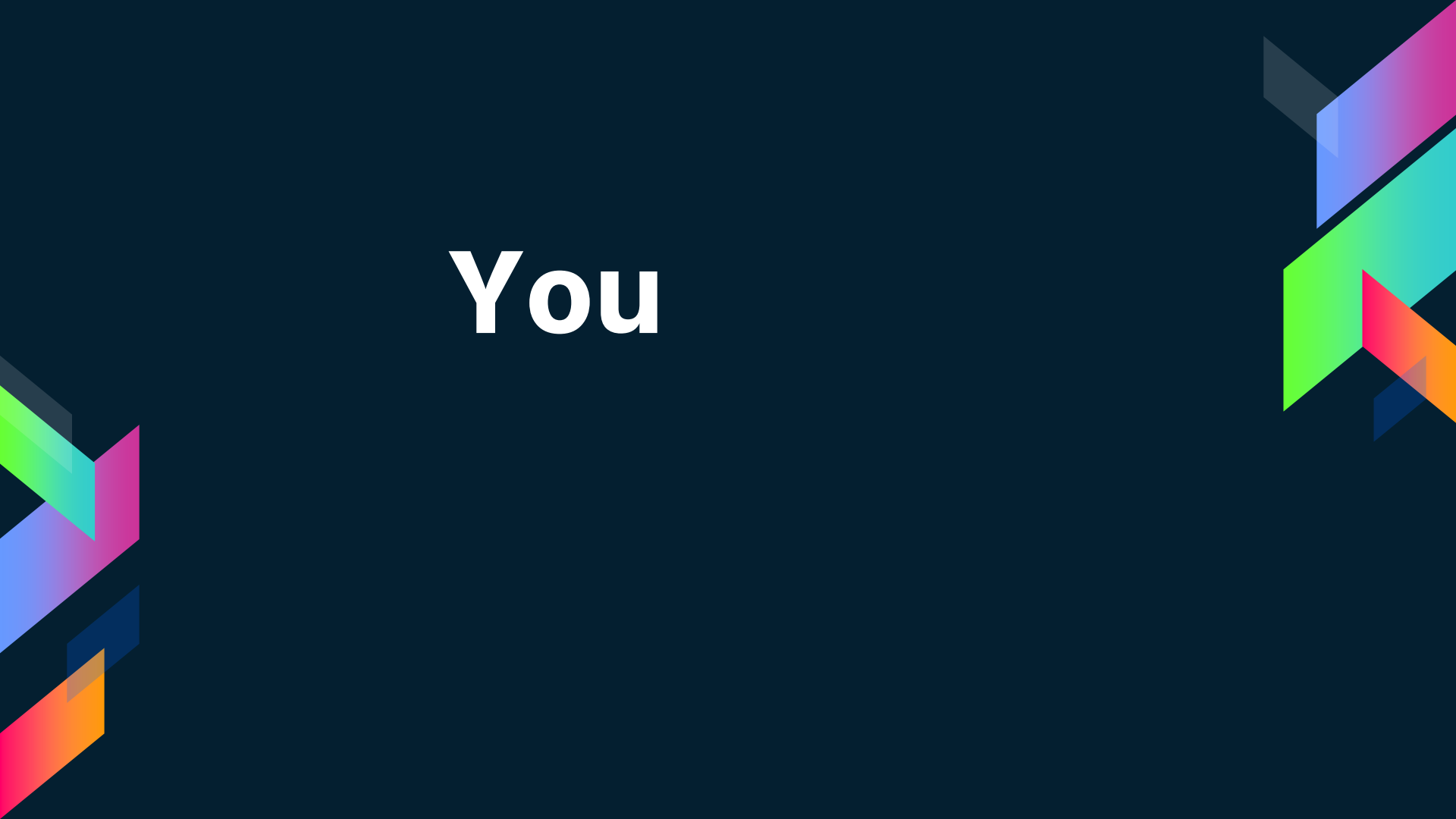
City, state, zip, or country

Search

USAJOBS.GOV

Search for 2210 || 1550


You



Abstract geometric shapes in the bottom-left corner, including a green triangle, a cyan triangle, a pink triangle, a blue triangle, and an orange triangle, all pointing towards the center.

You

It's okay to answer
more than once

Abstract geometric shapes in the bottom-right corner, including a pink triangle, a cyan triangle, a green triangle, a red triangle, and an orange triangle, all pointing towards the center.

Abstract geometric shapes in the top-left corner, including a green triangle, a blue parallelogram, and a pink parallelogram, all pointing towards the center.

You

It's okay to answer
more than once

Front-End

Abstract geometric shapes in the bottom-right corner, including a green triangle, a blue parallelogram, and a pink parallelogram, all pointing towards the center.

Abstract geometric shapes in the bottom-left corner, including a green triangle, a cyan triangle, a pink triangle, a blue triangle, and an orange triangle, all pointing towards the center.

You

It's okay to answer
more than once

Back-End

Abstract geometric shapes in the bottom-right corner, including a green triangle, a cyan triangle, a pink triangle, a blue triangle, and an orange triangle, all pointing towards the center.

Abstract geometric shapes in the top-left corner, including a large cyan triangle, a smaller magenta triangle, and a small blue triangle, all pointing towards the center.

You

It's okay to answer
more than once

DBA

Abstract geometric shapes in the bottom-left corner, including a large cyan triangle, a smaller magenta triangle, and a small blue triangle, all pointing towards the center.

Abstract geometric shapes in the top-left corner, including a large cyan triangle, a smaller magenta triangle, and a small blue triangle, all pointing towards the center.

You

It's okay to answer
more than once

DBA

Abstract geometric shapes in the bottom-left corner, including a large cyan triangle, a smaller magenta triangle, and a small blue triangle, all pointing towards the center.

Abstract geometric shapes in the top-left corner, including a large cyan triangle, a smaller magenta triangle, and a small blue triangle, all pointing towards the center.

You

It's okay to answer
more than once

Environment

Abstract geometric shapes in the bottom-left corner, including a large cyan triangle, a smaller magenta triangle, and a small blue triangle, all pointing towards the center.

The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract, overlapping geometric shapes in shades of green, cyan, magenta, and blue. Similarly, in the top-right and bottom-right corners, there are abstract shapes in shades of magenta, cyan, red, and orange. The text "Good News" is centered in the middle of the image in a white, bold, sans-serif font.

Good News

Bad News



The background is a dark navy blue. In the top-left and bottom-left corners, there are abstract geometric shapes made of overlapping translucent polygons in shades of green, cyan, magenta, and blue. Similar shapes are in the top-right and bottom-right corners, featuring shades of magenta, cyan, red, and orange.

Bad News

I was lying

About the OWASP Top 10

OWASP Top 10 is an Awareness Document

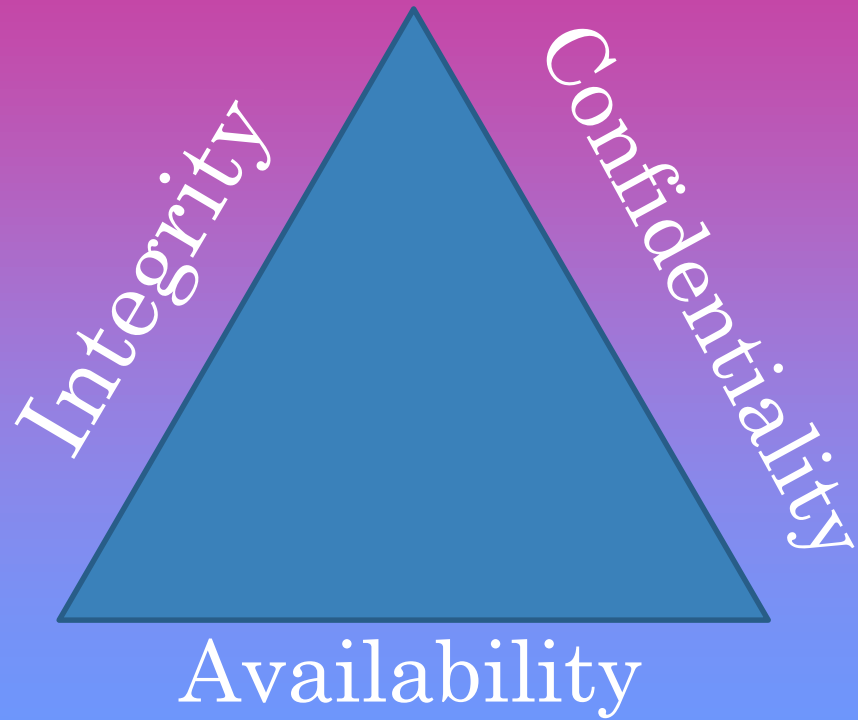
- **Not a standard...**

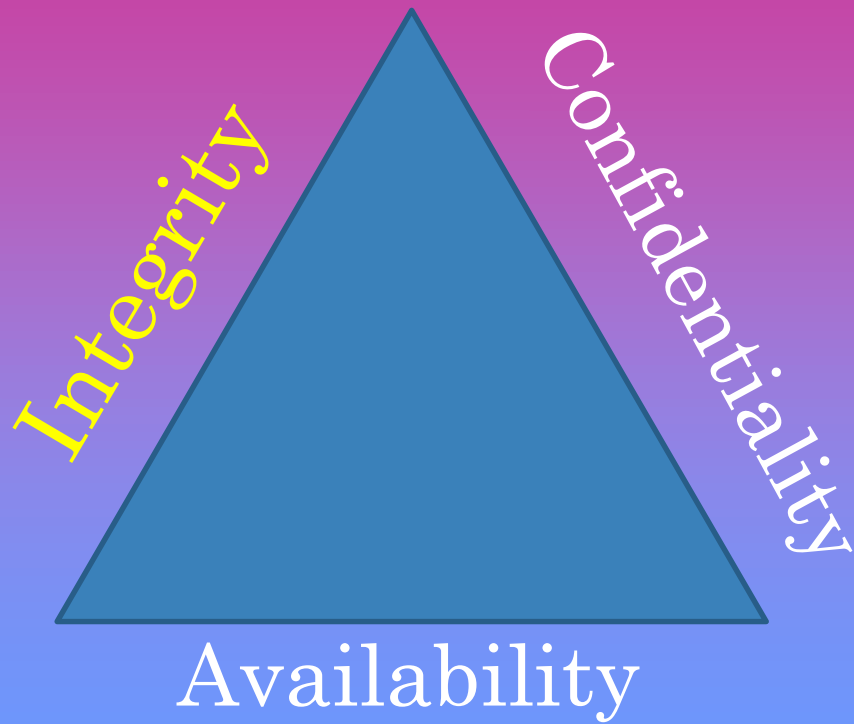
First developed in 2003

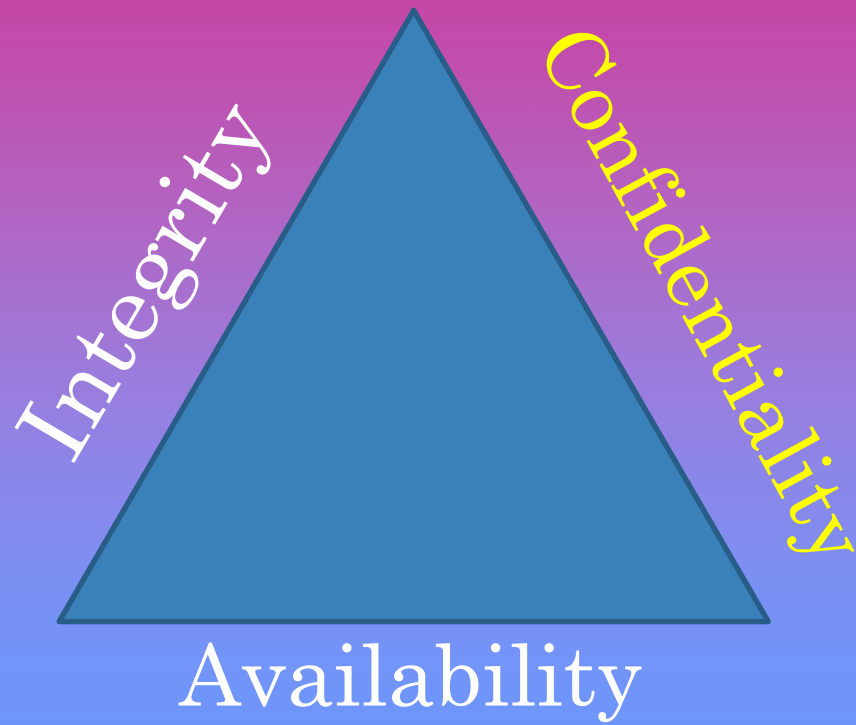
- **Was probably 3rd or 4th OWASP project, after**
 - **Developers Guide**
 - **WebGoat**
 - **Maybe WebScarab ??**

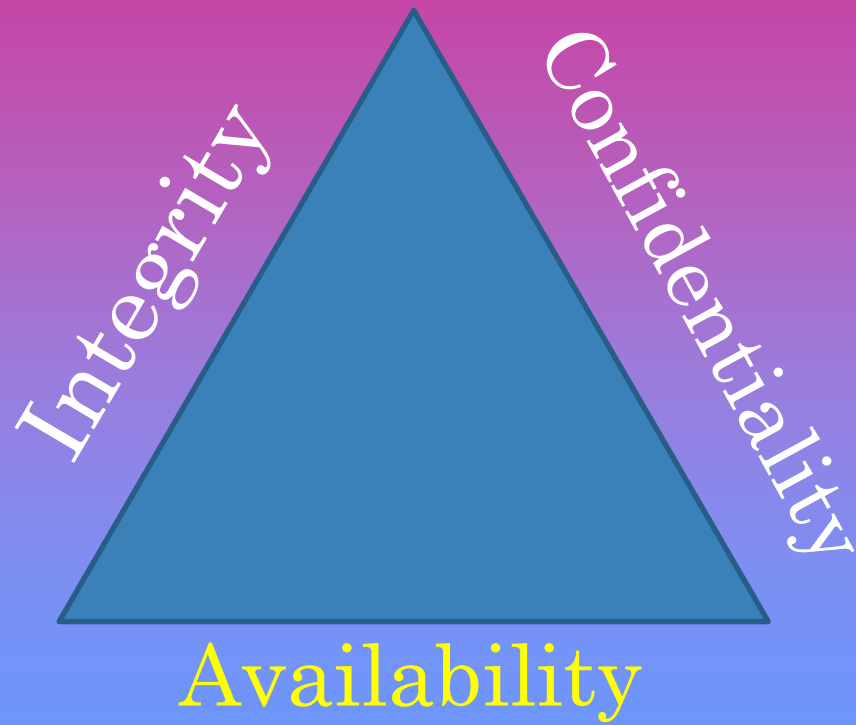
Released

- **2003, 2004, 2007, 2010, 2013, 2017**

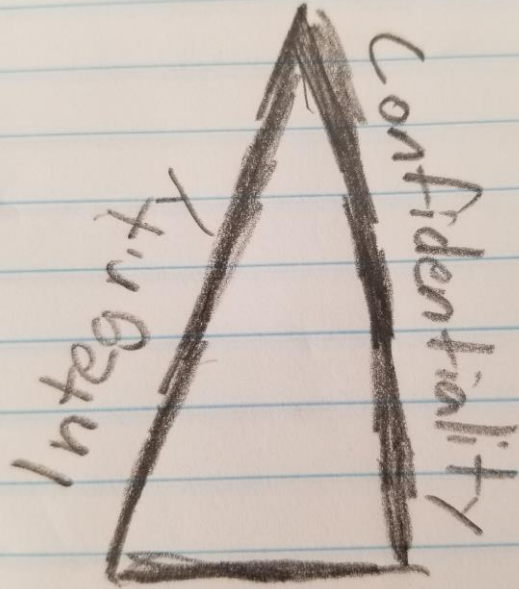




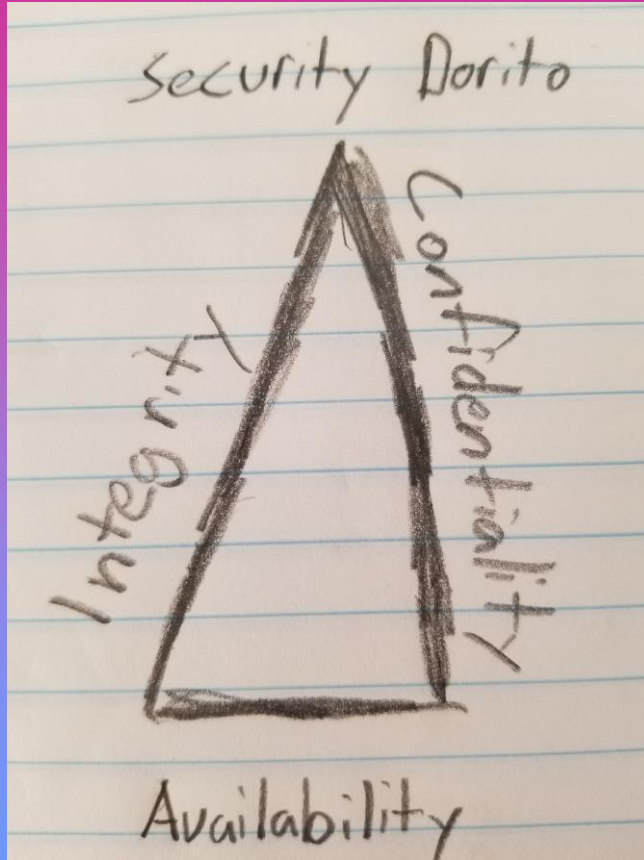




Security Dorito



Availability



Delicious!



Top Ten Security Vulnerabilities

Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping translucent shapes in shades of red, orange, and yellow. The top-right corner displays a group of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-right corner shows a series of overlapping translucent shapes in shades of red, orange, and yellow.

10

10 – CSRF

**Makes users
do bad things**



The image features a dark blue background with abstract, colorful geometric shapes in the corners. These shapes are composed of overlapping triangles and polygons in shades of green, blue, pink, and orange, creating a modern, digital aesthetic. The main text is centered and reads:

**Makes users
do bad things**

..or annoying things

```
<body>
  <h1>We're not hacking you</h1>
  <script>
    //hehe... we're using CSRF
    fetch('https://your-dumb-bank.com/transfer/', {
      method: 'POST',
      body: JSON.stringify({
        to_account: 'attacker_account',
        amount: 1000
      })
    })
  </script>
</body>
```

```
<system.webServer>
  <httpProtocol>
    <customHeaders>
      <add name="Access-Control-Allow-Origin" value="*" />
      <add name="Access-Control-Allow-Methods" value="*" />
      <add name="Access-Control-Allow-Credentials" value="true"/>
      <add name="Access-Control-Allow-Headers" value="*" />
    </customHeaders>
  </httpProtocol>
</system.webServer>
```





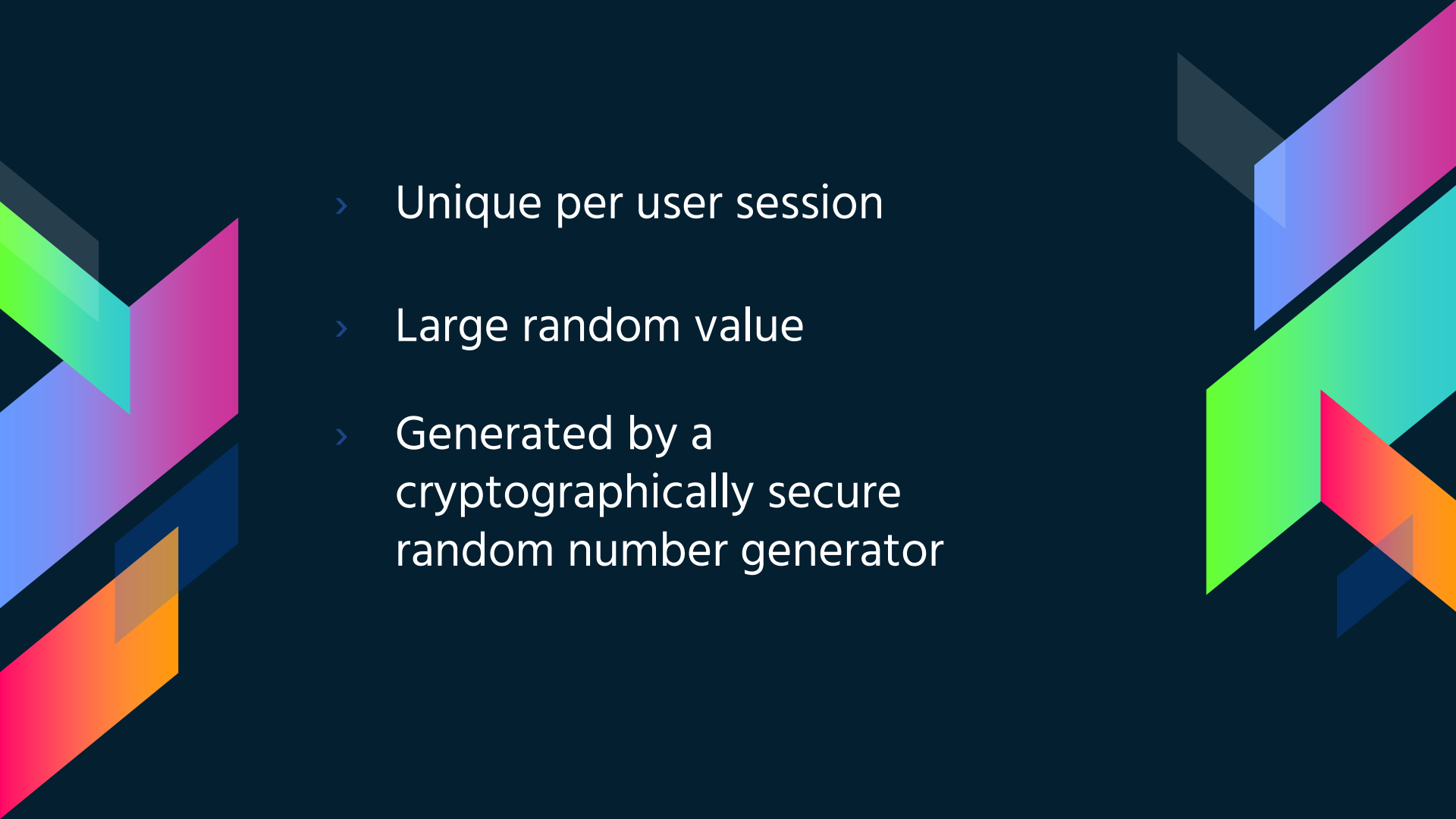
The background is a dark navy blue. In the top-left and bottom-left corners, there are overlapping geometric shapes in shades of cyan, magenta, and orange. In the top-right and bottom-right corners, there are overlapping geometric shapes in shades of magenta, cyan, and orange. The text "Disallow CORS" is centered in the middle of the image.

Disallow CORS



- 
- Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping shapes in shades of blue, green, and yellow. The top-right corner has a cluster of shapes in shades of orange, red, and yellow. The bottom-left corner contains a cluster of shapes in shades of blue, green, and yellow. The bottom-right corner features a cluster of shapes in shades of orange, red, and yellow.
- › Unique per user session

- 
- Abstract geometric shapes in the top-left corner, including a green triangle, a cyan trapezoid, a pink parallelogram, a blue parallelogram, and an orange parallelogram, all overlapping and pointing towards the center.
- › Unique per user session
 - › Large random value
- 
- Abstract geometric shapes in the top-right corner, including a pink parallelogram, a cyan parallelogram, a green parallelogram, a red parallelogram, and an orange parallelogram, all overlapping and pointing towards the center.

- 
- The slide features a dark blue background with abstract, colorful geometric shapes in the corners. On the left, there are overlapping shapes in shades of green, cyan, magenta, and orange. On the right, there are shapes in shades of magenta, cyan, green, and orange. The central text is white and consists of a bulleted list.
- › Unique per user session
 - › Large random value
 - › Generated by a cryptographically secure random number generator

```
<form class="_w0d _w0d"
  action="https://www.facebook.com/login/device-based/regular/logout/?button_name=logout"
  data-nocookies="1" id="u_e_3" method="post"
  onsubmit="return window.Event &&& Event.__inlineSubmit &&& Event.__inlineSubmit(this,event)">
  <input type="hidden" name="fb_dtsg" value="AQElSu6f0iHB:AQFeG3yGZTL4" autocomplete="off">
  <input type="hidden" autocomplete="off" name="ref" value="mb">
  <input type="hidden" autocomplete="off" name="h" value="Afd4CKBf94IkFDQx">
</form>
```

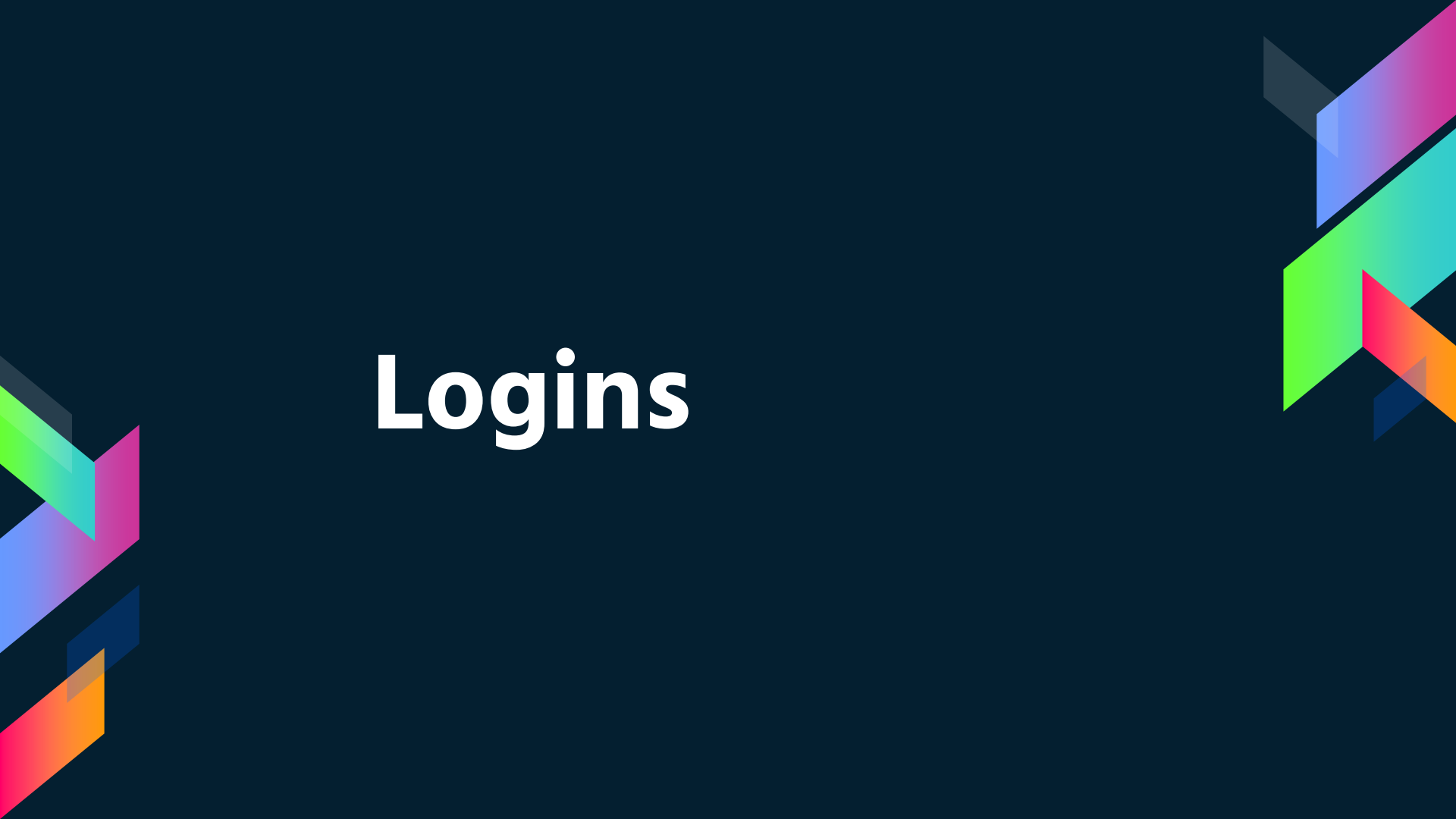
9

The slide features a dark blue background with decorative geometric shapes in the corners. On the left, there are overlapping translucent shapes in shades of green, cyan, magenta, and blue. On the right, there are similar overlapping shapes in shades of magenta, cyan, green, and orange. The main text is centered and reads:

9 – Insufficient Logging and Monitoring



Logins



The background is a dark navy blue. In the top-left and bottom-left corners, there are overlapping, semi-transparent geometric shapes in shades of green, cyan, magenta, and blue. In the top-right and bottom-right corners, there are similar overlapping shapes in shades of magenta, cyan, red, and orange.

Logins

It's called a login for a reason

Transactions



Access Control Failures





The image features a dark navy blue background. In the top-left and bottom-left corners, there are overlapping geometric shapes in shades of cyan, magenta, and orange. Similarly, in the top-right and bottom-right corners, there are overlapping geometric shapes in shades of magenta, cyan, and orange. The central text is white and italicized.

If you don't log, you're in a fog

Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping triangles in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping rectangles in shades of blue, green, and yellow. The top-right corner displays a collection of overlapping triangles in shades of blue, green, and yellow. The bottom-right corner shows a series of overlapping rectangles in shades of blue, green, and yellow.

8

The background is a dark navy blue. In the top-left and bottom-left corners, there are overlapping, semi-transparent geometric shapes in shades of green, cyan, magenta, and blue. In the top-right and bottom-right corners, there are similar overlapping shapes in shades of magenta, cyan, green, and orange. The text is centered in the middle of the slide.

8 – Using Components with Known Vulnerabilities

Abstract geometric shapes in the corners. The top-right corner features a cluster of overlapping triangles in shades of pink, purple, blue, green, and orange. The bottom-left corner features a similar cluster of overlapping triangles in shades of green, blue, orange, and pink. The background is a solid dark blue.

143,000,000

People

Equifax



The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract, overlapping geometric shapes in shades of green, cyan, magenta, and blue. Similarly, in the top-right and bottom-right corners, there are abstract shapes in shades of magenta, cyan, red, and orange. The central text is white and bold.

Throw it away

The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract geometric shapes composed of overlapping translucent polygons in shades of green, cyan, magenta, and blue. Similar shapes are located in the top-right and bottom-right corners, featuring a color gradient from purple to pink to orange. The text "Routinely check" is centered in the middle of the image in a white, bold, sans-serif font.

Routinely check

Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping translucent shapes in shades of red, orange, and yellow. The top-right corner displays a cluster of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-right corner features a series of overlapping translucent shapes in shades of red, orange, and yellow.

7

The slide features a dark blue background with decorative geometric shapes in the corners. These shapes are composed of overlapping triangles and polygons in various colors including green, cyan, magenta, blue, and orange, creating a modern, abstract look.

7 – Insecure Deserialization

```
console.log(document.cookie); // '{"role':'user'}"  
  
document.cookie = '{"role':'admin'}";
```



**Cookies are a
sometimes tool**

Integrity Checks

Logging

Avoidance



Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping triangles in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping rectangles in shades of red, orange, and yellow. The top-right corner displays a group of overlapping triangles in shades of blue, green, and yellow. The bottom-right corner shows a series of overlapping rectangles in shades of red, orange, and yellow.

6

6 — XSS

```
const name = document.location.hash.substr(1);
let greeting;
if(name){
  greeting = 'Greetings, ' + decodeURI(document.location.hash.substring(1));
}else{
  greeting = 'Greetings!'
}
document.write(greeting);
```

```
const name = document.location.hash.substr(1);  
let greeting;  
if(name){  
  greeting = 'Greetings, ' + decodeURI(document.location.hash.substring(1));  
}else{  
  greeting = 'Greetings!'  
}  
document.write(greeting); // why were we even using .textContent? --junior dev
```



📄 your-dumb-bank.com/example.html#George%20Costanza

Your Dumb Bank

Greetings, George Costanza



 `your-dumb-bank.com/example.html#<script>alert('evil');</script>`



This page isn't working

Chrome detected unusual code on this page and blocked it to protect your personal information (for example, passwords, phone numbers, and credit cards).

Try [visiting the site's homepage](#).

ERR_BLOCKED_BY_XSS_AUDITOR

Chrome

Your Dumb Bank

Greetings,

evil

OK

Firefox

Your Dumb Bank

Greetings,

This site says...

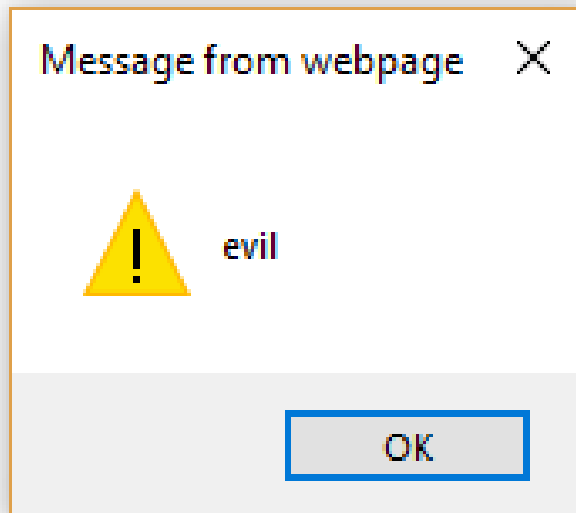
evil

OK

Edge

Your Dumb Bank

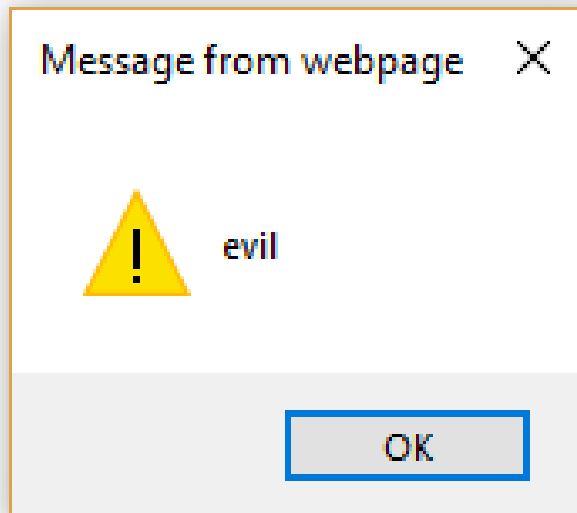
Greetings,



IE

Your Dumb Bank

Greetings,



IE ***Shocking***

**B***I*

I totally agree with OP.

```
<script>
```

```
  alert('evil');
```

```
</script>
```



Reply

cancel

saved

**XSS DOESN'T EVER HAPPEN
IN THE REAL WORLD**

**DAMMIT, ROBIN.
EVERY CODE REVIEW...**



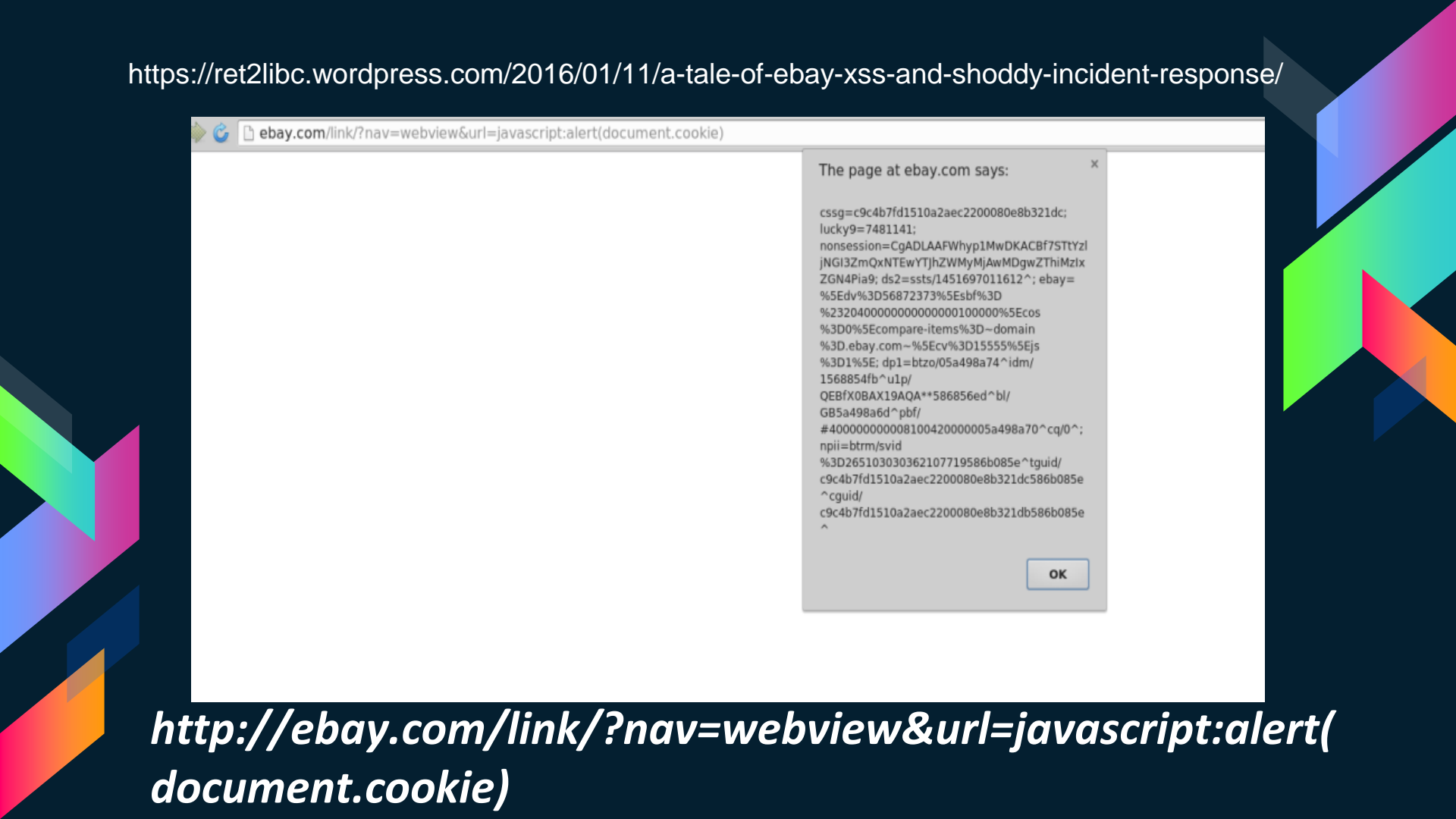
<https://ret2libc.wordpress.com/2016/01/11/a-tale-of-ebay-xss-and-shoddy-incident-response/>

The screenshot shows a web browser window with the address bar containing the URL `http://ret2libc.wordpress.com/2016/01/11/a-tale-of-ebay-xss-and-shoddy-incident-response/`. The main content area displays a message from ebay.com stating:

```
cssg=c9c4b7fd1510a2aec2200080e8b321dc; lucky9=7481141; nonsession=CgADLAAFWhyp1MwDKACBf7STTYzl jNGI3ZmQxNTEwYTJhZWMyMjAwMDgwZThiMzlx ZGN4Pia9; ds2=ssts/l451697011612^; ebay=%5Edv%3D56872373%5Esb%3D %2320400000000000000000000000000000 %3D0%5Ecompare-items%3D~domain %3D.ebay.com~-%5Ecvt%3D15555%5Ejs %3D1%5E; dp1=btzo/O5a498a74^idm/ 1568854fb^u1p/ QEB/XOBAX19AQA**586856ed^bl/ GB5a498a6d^pbfl #400000000008100420000005a498a70^cq/0^; npii=btrim/svid %3D265103030362107719586b085e^tguid/c9c4b7fd1510a2aec2200080e8b321dc586b085e ^cguid/c9c4b7fd1510a2aec2200080e8b321db586b085e ^
```

An "OK" button is visible at the bottom right of the alert box.

[`http://ebay.com/link/?nav=webview&:url=javascript:alert\(document.cookie\)`](http://ebay.com/link/?nav=webview&:url=javascript>alert(document.cookie))

[illegible]

Trusted Frameworks



Escape Strings



HIGH FIVE



INTERMISSION



Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping translucent shapes in shades of red, orange, and yellow. The top-right corner displays a group of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-right corner shows a series of overlapping translucent shapes in shades of red, orange, and yellow.

5

The slide features a dark blue background with decorative geometric shapes in the corners. These shapes are composed of overlapping triangles and polygons in various colors including green, cyan, magenta, blue, and orange, creating a modern, abstract look.

5 – Security Misconfiguration

Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping triangles in shades of green, blue, and purple. The top-right corner has a similar cluster with pink, blue, and green triangles. The bottom-left corner contains a cluster with orange, red, and blue triangles. The bottom-right corner has a cluster with green, yellow, and orange triangles. All shapes are semi-transparent and overlap each other.

**Turn off unnecessary
features**

**Remove
unnecessary
software**



The image features a dark blue background with abstract, colorful geometric shapes in the corners. These shapes are composed of overlapping triangles and polygons in shades of green, cyan, magenta, blue, and orange, creating a modern, digital aesthetic.

Turn off detailed errors

Server Error in '/' Application.

Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)

May 26 2009 14:24:20

Copyright (c) 1988-2005 Microsoft Corporation

Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)

' to data type int.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Data.SqlClient.SqlException: Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)

May 26 2009 14:24:20

Copyright (c) 1988-2005 Microsoft Corporation

Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)

' to data type int.

Source Error:

```
Line 46:         catch (Exception ex)
Line 47:         {
Line 48:             throw ex;
Line 49:         }
Line 50:     finally
```

Source File: c:\webroot\Sock_Puppets\App_Code\Generic DataAccess.cs **Line:** 48

Stack Trace:

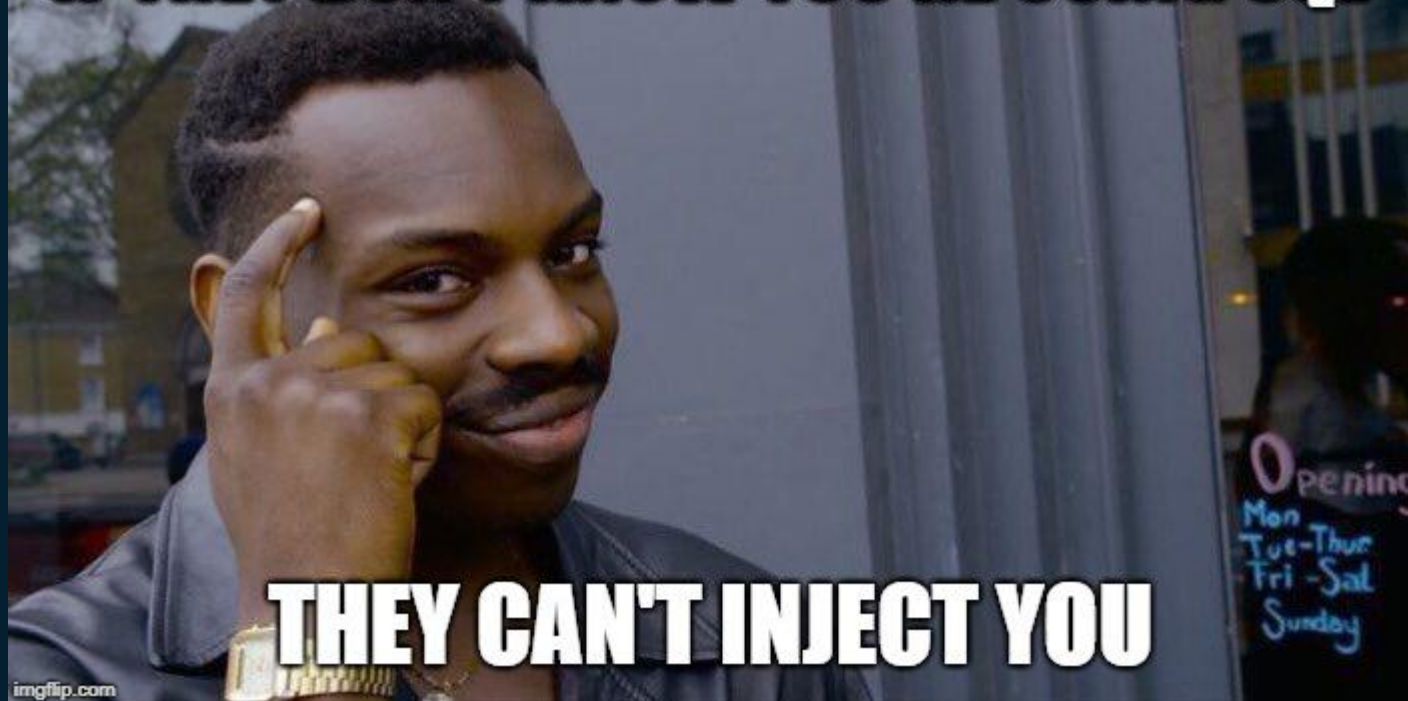
```
[SqlException (0x80131904): Conversion failed when converting the nvarchar value 'Microsoft SQL Server 2005 - 9.00.4053.00 (Intel X86)
May 26 2009 14:24:20
Copyright (c) 1988-2005 Microsoft Corporation
Standard Edition on Windows NT 5.0 (Build 2195: Service Pack 4)
' to data type int.]
GenericDatabaseAccess.ExecutesSqlCommandScalar(DbCommand command) in c:\webroot\Sock_Puppets\App_Code\Generic DataAccess.cs:48
SSC.Web.Controls.UserControls.DisciplineSelect.TriggerCodeValid(String triggerCode) in c:\webroot\Sock_Puppets\UserControls\DisciplineSelect.ascx.cs:305
SSC.Web.Controls.UserControls.DisciplineSelect.IbSelect_Click(Object sender, ImageClickEventArgs e) in c:\webroot\Sock_Puppets\UserControls\DisciplineSelect.ascx.cs:296
System.Web.UI.WebControls.ImageButton.OnClick(ImageClickEventArgs e) +108
System.Web.UI.WebControls.ImageButton.RaisePostBackEvent(String eventArgument) +118
System.Web.UI.WebControls.ImageButton.System.Web.UI.IPostBackEventHandler.RaisePostBackEvent(String eventArgument) +10
System.Web.UI.Page.RaisePostBackEvent(IPostBackEventHandler sourceControl, String eventArgument) +13
System.Web.UI.Page.RaisePostBackEvent(NameValueCollection postData) +36
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1565
```

Version Information: Microsoft .NET Framework Version:2.0.50727.4223; ASP.NET Version:2.0.50727.4223

The background is a dark navy blue. In the top-left and bottom-left corners, there are overlapping geometric shapes in shades of green, cyan, magenta, and blue. In the top-right and bottom-right corners, there are overlapping geometric shapes in shades of magenta, cyan, green, and orange. The text is centered in the middle of the image.

***Security through Obscurity is
NOT Security***

IF THEY DON'T KNOW YOU'RE USING SQL



THEY CAN'T INJECT YOU

imgflip.com

Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping translucent shapes in shades of red, orange, and yellow. The top-right corner displays a group of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-right corner shows a series of overlapping translucent shapes in shades of red, orange, and yellow.

4

The slide features a dark blue background. In the top-left and bottom-left corners, there are overlapping, semi-transparent geometric shapes in shades of green, blue, and orange. Similarly, in the top-right and bottom-right corners, there are overlapping, semi-transparent geometric shapes in shades of pink, blue, and orange. The main text is centered and reads:

4 – Broken Access Control

Prevent Caching



The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract, overlapping geometric shapes in shades of green, cyan, magenta, and blue. Similarly, in the top-right and bottom-right corners, there are abstract shapes in shades of magenta, cyan, red, and orange. The central text is white and reads "Deny by default".


Deny by default

Prevent Path Traversal



3



The slide features a dark blue background with decorative geometric shapes in the corners. These shapes are composed of overlapping triangles and polygons in various colors including green, cyan, magenta, blue, and orange, creating a modern, abstract look.

3 – Sensitive Data Exposure

The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract geometric shapes composed of overlapping translucent polygons in shades of cyan, magenta, and orange. Similar shapes are located in the top-right and bottom-right corners, featuring a gradient from blue to green to yellow. The word "HTTPS" is centered in the middle of the image in a large, white, sans-serif font.

HTTPS



HASH

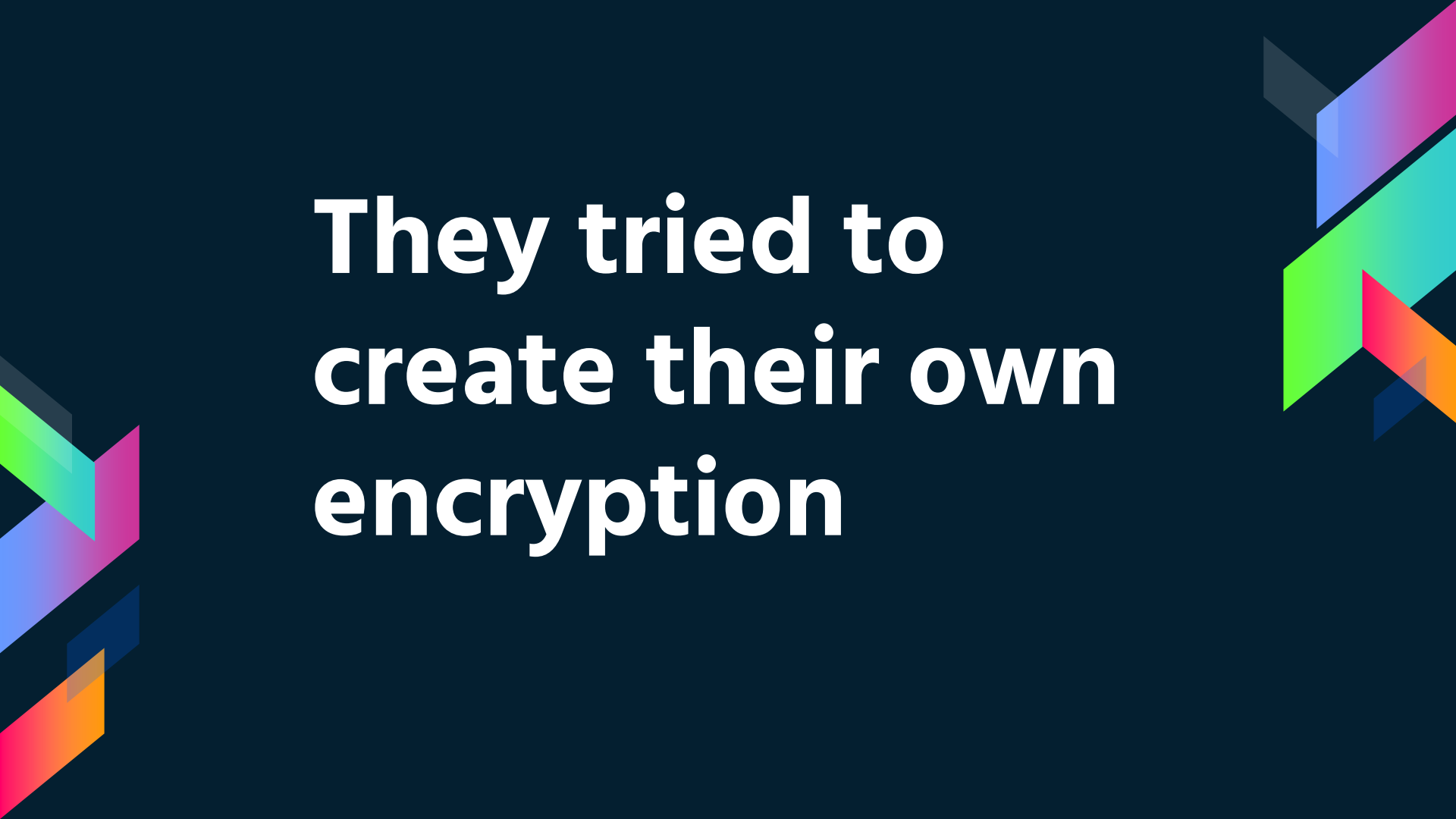
Username	Salt value	String to be hashed	Hashed value = SHA256 (Password + Salt value)
user1	E1F53135FAE559C253	password123+E1F53135E559C253	72AE25495A7981C40622D49F9A52E4F1565C90F048F59027BD9C8C8900D5C3D8
user2	F84B03D034B409D4E	password123+84B03D034B409D4E	B4B6603ABC670967E99C7E7F1389E40CD16E78AD38EB1468EC2AA1E62B8BED3A



The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract, overlapping geometric shapes in shades of green, cyan, magenta, and blue. Similarly, in the top-right and bottom-right corners, there are abstract shapes in shades of magenta, cyan, green, and orange. The central text is white and reads:

**Why did the
dinosaurs die?**

**They tried to
create their own
encryption**



Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping triangles in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping rectangles in shades of blue, green, and yellow. The top-right corner displays a collection of overlapping triangles in shades of blue, green, and yellow. The bottom-right corner shows a series of overlapping rectangles in shades of blue, green, and yellow.

2

The slide features a dark blue background with decorative geometric shapes in the corners. These shapes are composed of overlapping triangles and polygons in various colors including green, cyan, magenta, blue, and orange, creating a modern, abstract look.

2 – Broken Authentication

MF Authentication

The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract, overlapping geometric shapes in shades of green, cyan, magenta, and blue. Similarly, in the top-right and bottom-right corners, there are abstract shapes in shades of magenta, cyan, red, and orange. The central text 'No Defaults' is rendered in a clean, white, sans-serif font.

No Defaults

Limit failures



The image features a dark blue background with abstract, colorful geometric shapes in the corners. These shapes are composed of overlapping triangles and polygons in shades of green, blue, pink, and orange, creating a modern, digital aesthetic. The main text is centered in a large, white, sans-serif font.

**Same message for
login failures**



Sign in

That Microsoft account doesn't exist. Enter a different account or [get a new one](#).

Next

No account? [Create one!](#)

Abstract geometric shapes in the corners. The top-left corner features a cluster of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-left corner contains a series of overlapping translucent shapes in shades of red, orange, and yellow. The top-right corner displays a group of overlapping translucent shapes in shades of blue, green, and yellow. The bottom-right corner shows a series of overlapping translucent shapes in shades of red, orange, and yellow.

1

1 - Injection


```
string age = Request.parameters["age"];  
cmd.CommandText = "SELECT * FROM Customers WHERE age > " + age;  
  
sqlConnection.Open();  
reader = cmd.ExecuteReader();  
sqlConnection.Close();
```

Query Customers Older Than:

Age:

Submit

```
string UserName = Request.parameters["user_name"];
string Password = Request.parameters["password"];
string sql = "SELECT * FROM Customers";
||| sql += "WHERE UserName = " + UserName + " AND PASSWORD = " + Password;
cmd.CommandText = sql;
```

Name:

admin

Password:

admin OR 1 = 1;

Submit

The image features a dark navy blue background. In the top-left and bottom-left corners, there are abstract, overlapping geometric shapes in shades of green, cyan, magenta, and blue. Similarly, in the top-right and bottom-right corners, there are abstract shapes in shades of magenta, cyan, red, and orange. The text 'NoSQL?' is centered in the middle of the image.

NoSQL?

```
db.myCollection.find( {  
  $where: "this.userName == $userName && this.password == $password"  
} } );
```

Server-side validation



Parameterized Queries



**Let's check
back in with
Dave**





Managing Risks

In Secure Web Applications

Any questions?

You can find me at:

@dennythecoder · denny.headrick@gmail.com