city:1].mv-page .mv-x:hover{-webkit-transition:none}.mv-domain{bottom:24px;color:#777;margin:0 7px;position:absolute;text-align:center;width:90%}.mv-fav{bane-height:16px}#mv-noti-lks span,#mv-noti-error-lks span{-webkit-margin-start:6px;color:#11{bottom:0;display:inline-block;font-inone;padding:0 4px}#mv-noti-tion:relative;vertical-align:top}#mv-noti.mv-noti-hide,#mv-noti-error.mv-noti-hide,#mv-noti.mv-link-hide(display:none)form{height:39px}#fkbx{background-color fkbx:hover{border:1px solid #a9a9a9;border-top-color:#909090}.fkbxfcs #fkbx{border:1px solid #4d90fe}#fkbx>input{background:transparent;border:none;bottor position:absolute;right:9px;text-align:initial;text-overflow:ellipsis;top:0;visibility:hidden;white-space:nowrap}html[dir=rtl] #fkbx-text{left:auto;right:9px}#fkbx_cibx_crt{visibility:inherit;-webkit-animation:block@ackground:ellipsis;top:0;visibility:hidden;white-space:nowrap}html[dir=rtl] #fkbx-text{left:auto;right:9px}#fkbx_cibx_crt{visibility:inherit;-webkit-animation:block@ackground:ellipsis;top:0;visibility:hidden;white-space:nowrap}html[dir=rtl] #fkbx-text{left:auto;right:9px}#fkbx_cibx_crt{visibility:hidden;white-space;nowrap}html[dir=rtl] #fkbx-text{left:auto;right:9px}#fkbx_cibx_crt{visibility:hidden;white-space;nowrap}html[dir=rtl] #fkbx-text{left:auto;right:9px}#fkbx_cibx_crt{visibility:hidden;white-space;nowrap;width:0, and cibx_crt{visibility:hidden;white-space;nowrap;width:0, and cibx_crt{visibility:hidden

sub{color:#4285f4;font-size:16px;left:79px;postux:relative;top:-20px;white-space:nowrap;width:0}#mngb{position:absolute;top:15px;-webkit-transition:opacity
ly:'Roboto'}body.hide ._rzc{display:none}.des-cla{}.des-cla #most-visited{margin-top:50px}.des-cla #mv-tiles{height:276px;line-height:138px}.des-cla .mv-tile{backgrounds}.default-th
cla .mv-mask{border-radius:3px;b\\\EAK\\SESION\\\ border-style:solid}.default-th
.des-cla .mv-page .mv-focused~.mv-mask.des-cla .mv-page:rocus .mv-mask{-webkit-transition:background-color .u0ms ease-in-out:background:linear-gradient()

eight: 85px;top: 1px;width: 138px;.des-cla .mv-title{bottom:-27px;height: 18px;left:0;width: 140px;.des-cla .mv-locialiback .mv-domain{bottom:24px;margin:07p)%{opacity:1}}body{font:small arial,sans-serif;margin:0;min-height:616px;text-align:-webkit-center}body.hide,body.hide-sf #fkbx,body.hide-sf #lga{visibility:h user-select:none;z-index:1}#mv-tiles{margin:0;overflow:hidden;position:relative;text-align:start}#mv-single{border:none;height:100%;width:100%}.mv-tile{-w

og.mv-page{cursor:pointer;outline:none}._kte{neight:100%;visibility:nidden;width:100%}.mv-page ._kte{visibility:visible}.mv-mask,.mv-thumb,.mv-locthumb,.n er-radius:3px;pointer-events:none}.mv-locgradient{background:-webkit-linear-gradient(left,rgba(35,35,35,1) 0%,rgba(35,35,35,1) 40%,rgba(35,35,35,0.3) 60% g:content-box:overflow:bidden:position:absolute:text-align:center:text-overflow:ellinsis:white-space:nowrap} my-locfallback.img{beight:auto:left:0:pointer-ey

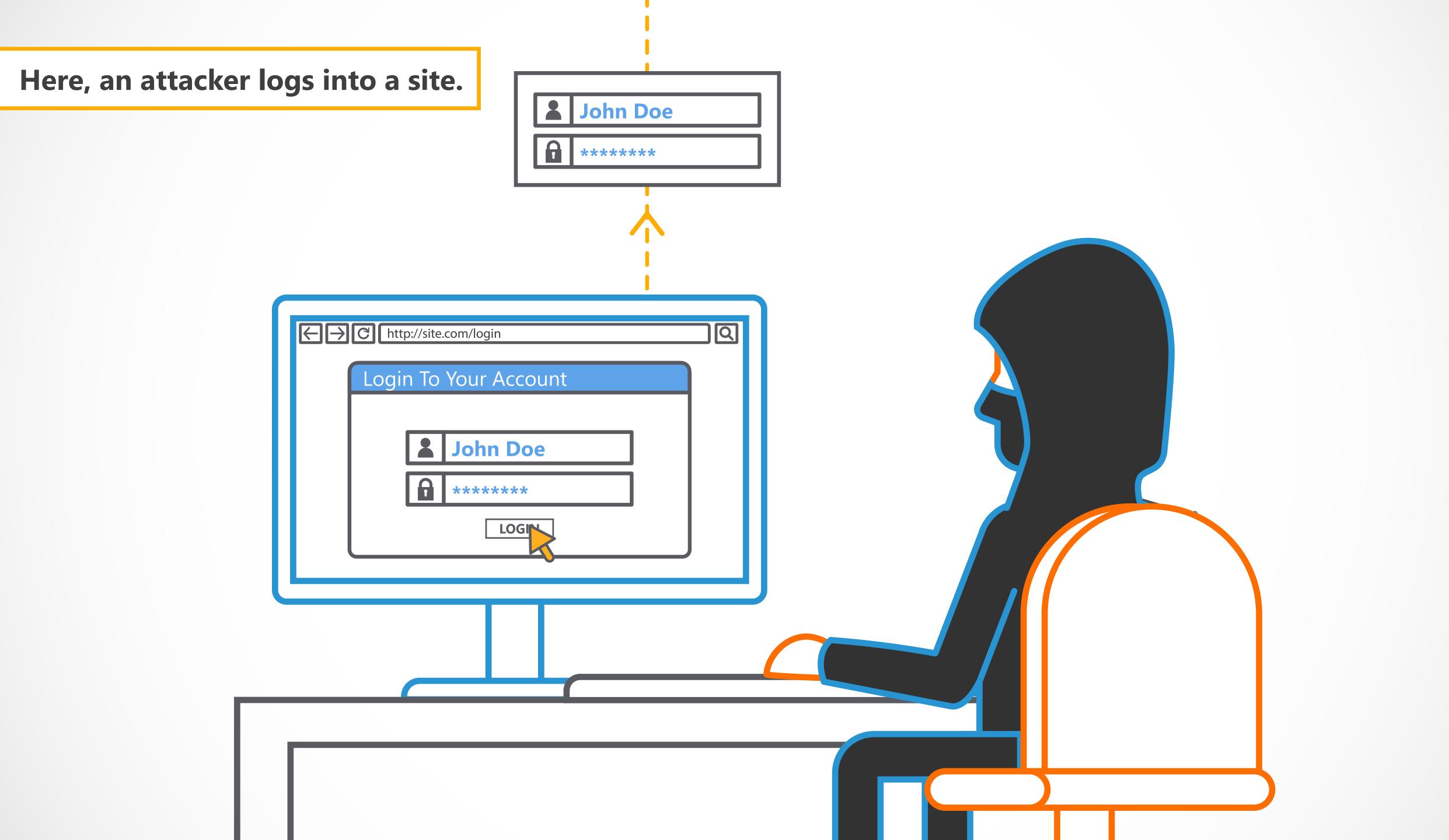
ng:content-box;overflow:nidden;position:absolute;text-align:center;text-overflow:ellipsis;white-space:nowrap}.mv-loctaliback img{height:auto;left:0;pointer-events.none;position:absolute;text-overflow:ellipsis;text-shadow:1px 1px #232323;top:0;white-space:normal;width:79px}.mv-x-hide .m

relative; vertical-a VOCzvjmbRz3j3xUjn6CfeYreUJ2wQkGD75INPX1mFfsEFrrcIYCvdhC4paWQakxajpJMr0C9YFg54i7AsC 4i7AsC ht:39px}#fkbx{background-who were the content of the content

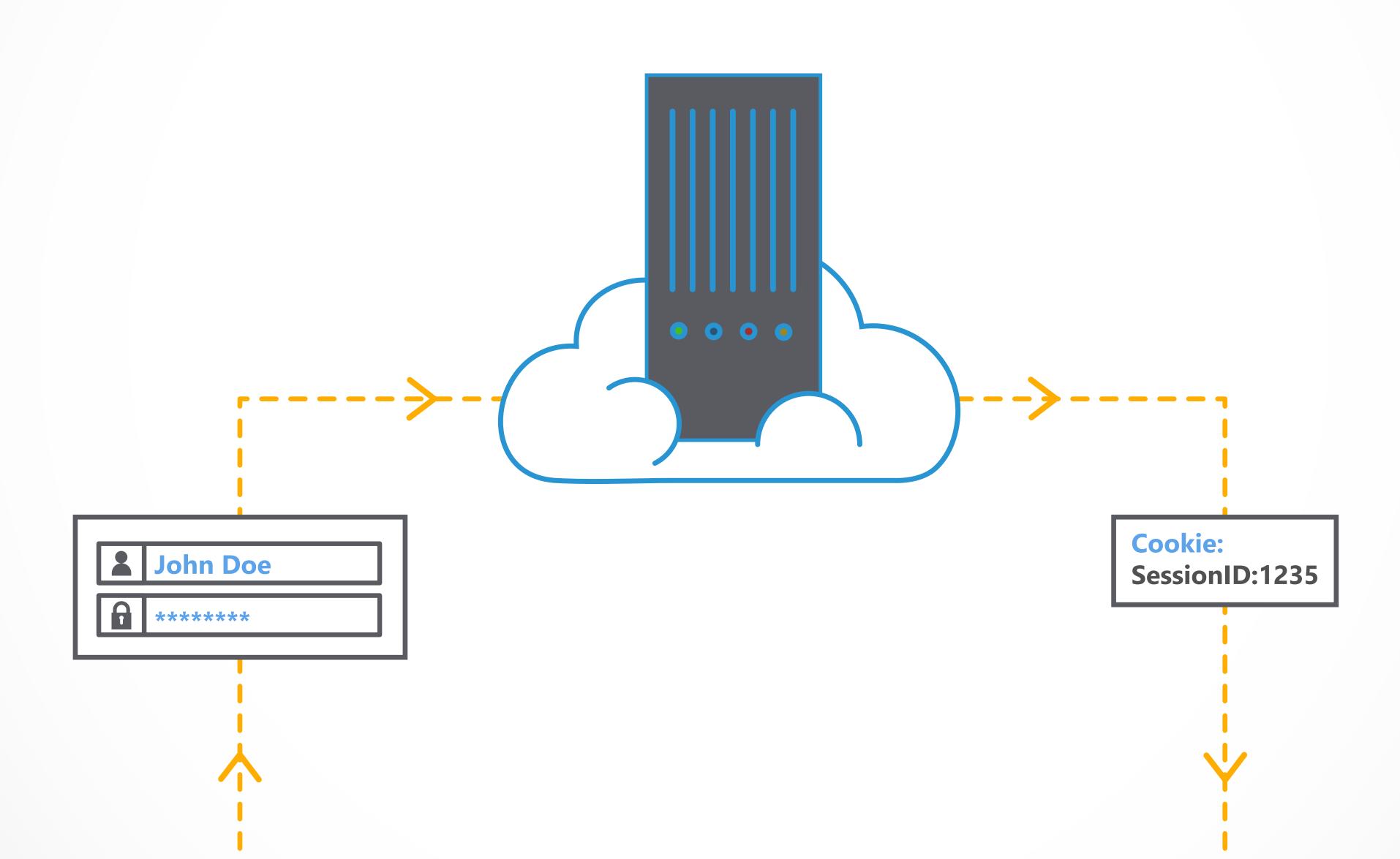
oosition:absolute:right:9px:text-align:initial:text-overflow:ellipsis:top:0:visibility:hidden:white-space:nowrap}html[dir=rtl] #fkbx-text{left:auto:right:9px}#fkbx

We'll go through

some preventions steps for vulnerabilities in this category



The site uses a simple increment to generate session IDs.



The site uses a simple increment to generate session IDs. Cookie: SessionID:1235 ← → C http://site.com/sessionID=1235 Q Logout Welcome 'User'!

The attacker, noticing the predictability of the ID generation,



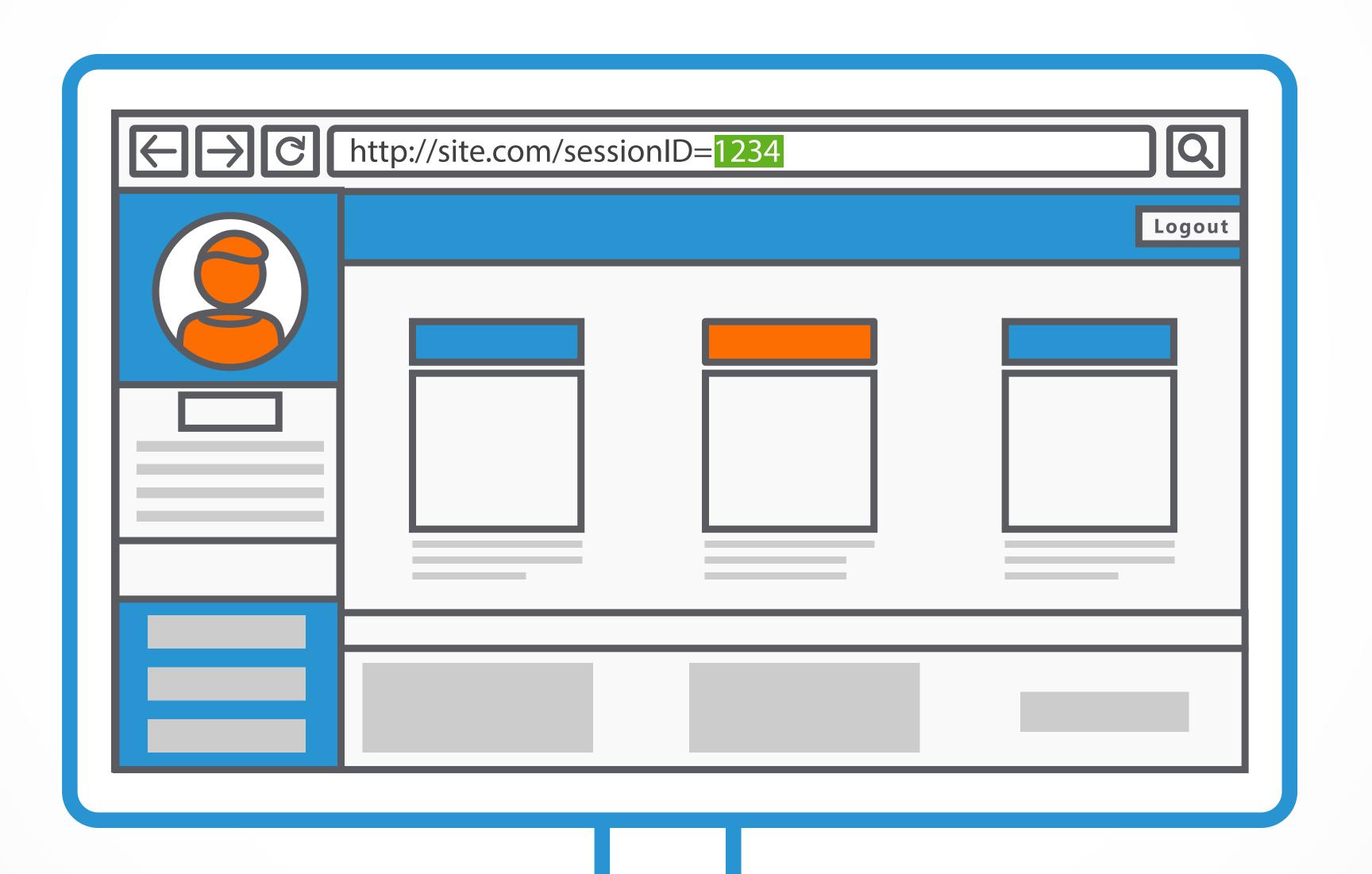
deduces new IDs, which he uses to browse back to the site.



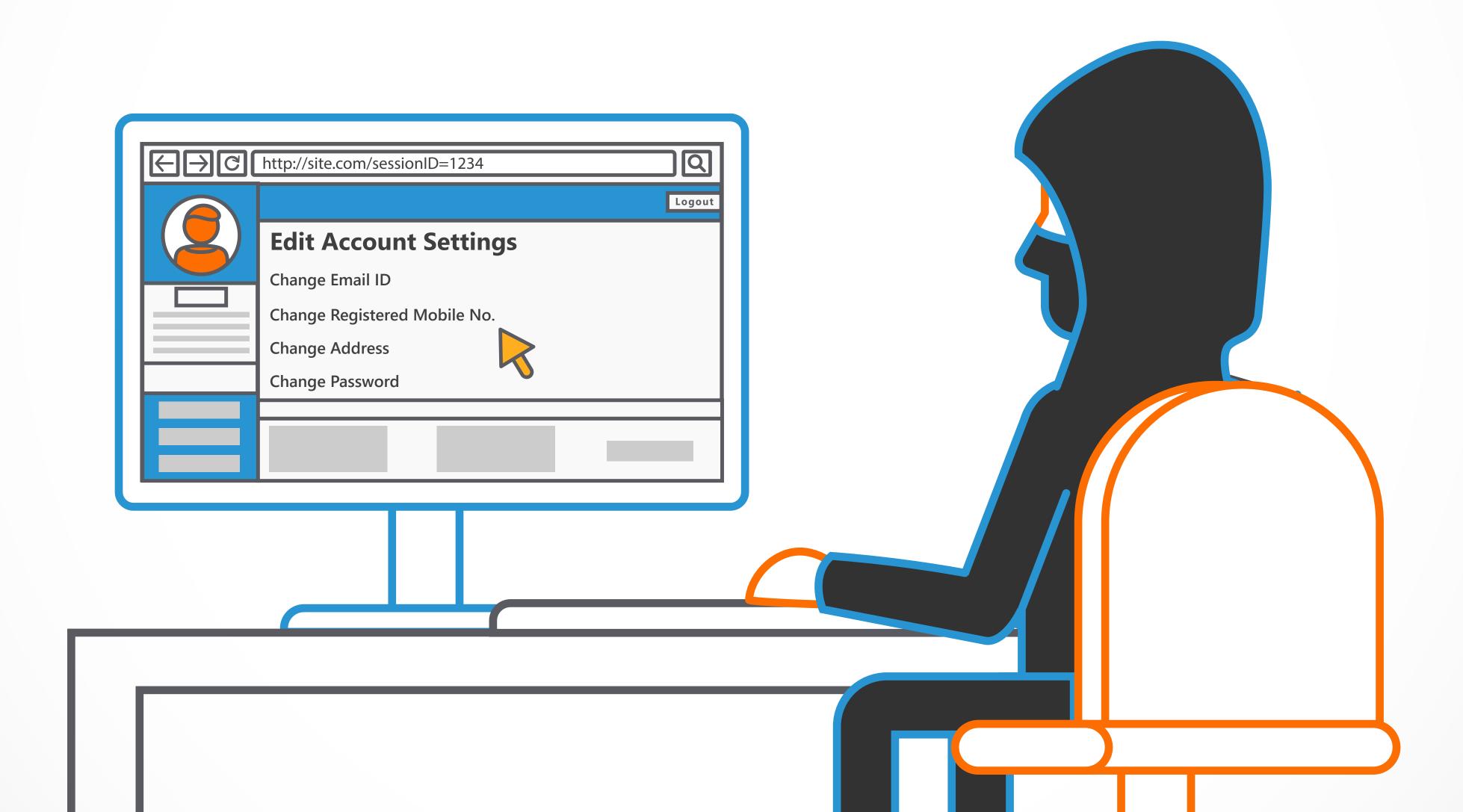
After a few attempts, the attacker finds a session ID that is associated with another authenticated user.



After a few attempts, the attacker finds a session ID that is associated with another authenticated user.



By being able to predict session IDs he is able to impersonate the authenticated user and is allowed full access to the user's account.

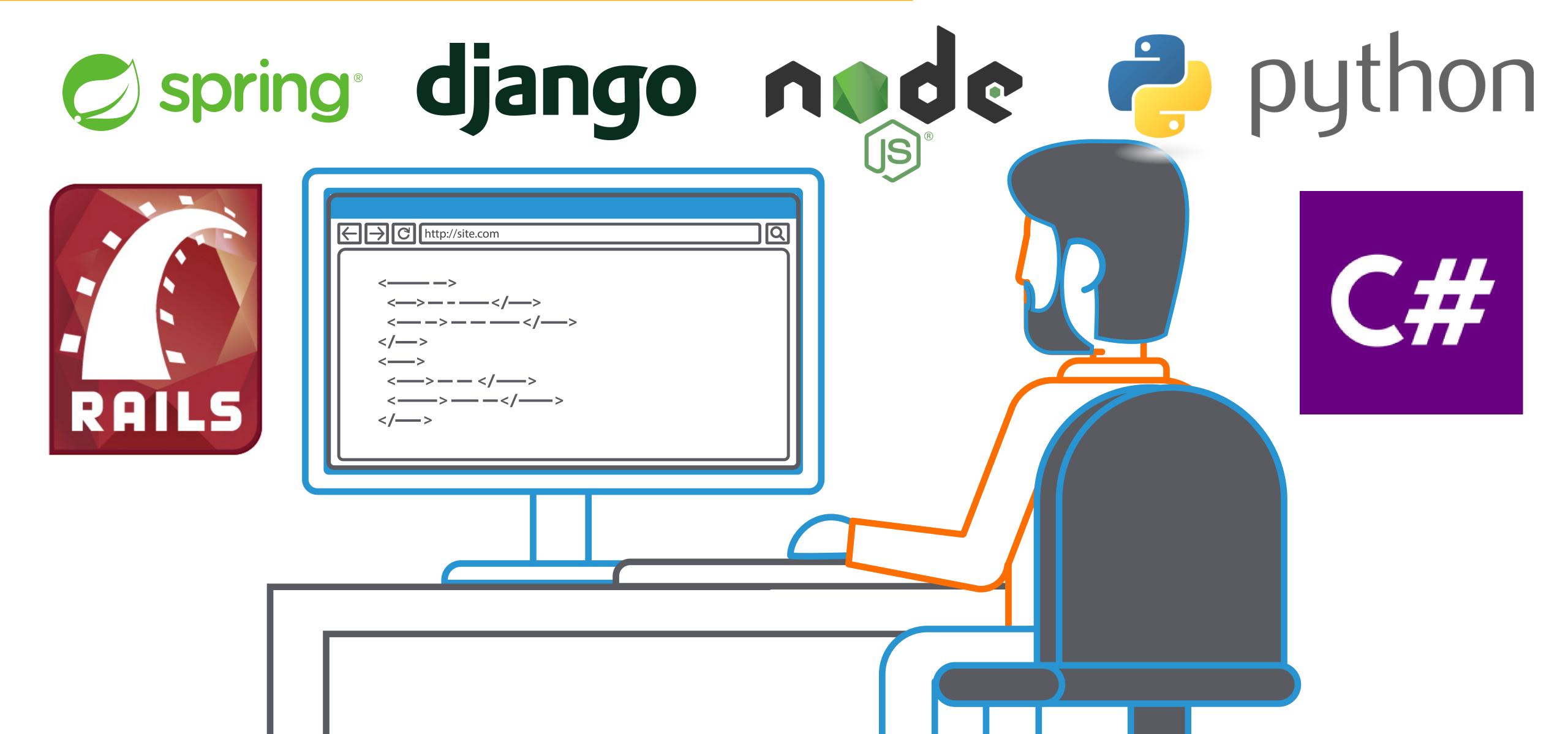


By being able to predict session IDs he is able to impersonate the authenticated user and is allowed full access to the user's account.



POOR SESSION MANAGEMENT CAN BE PREVENTED

using built-in session management functionality provided by your development framework, instead of inventing your own.

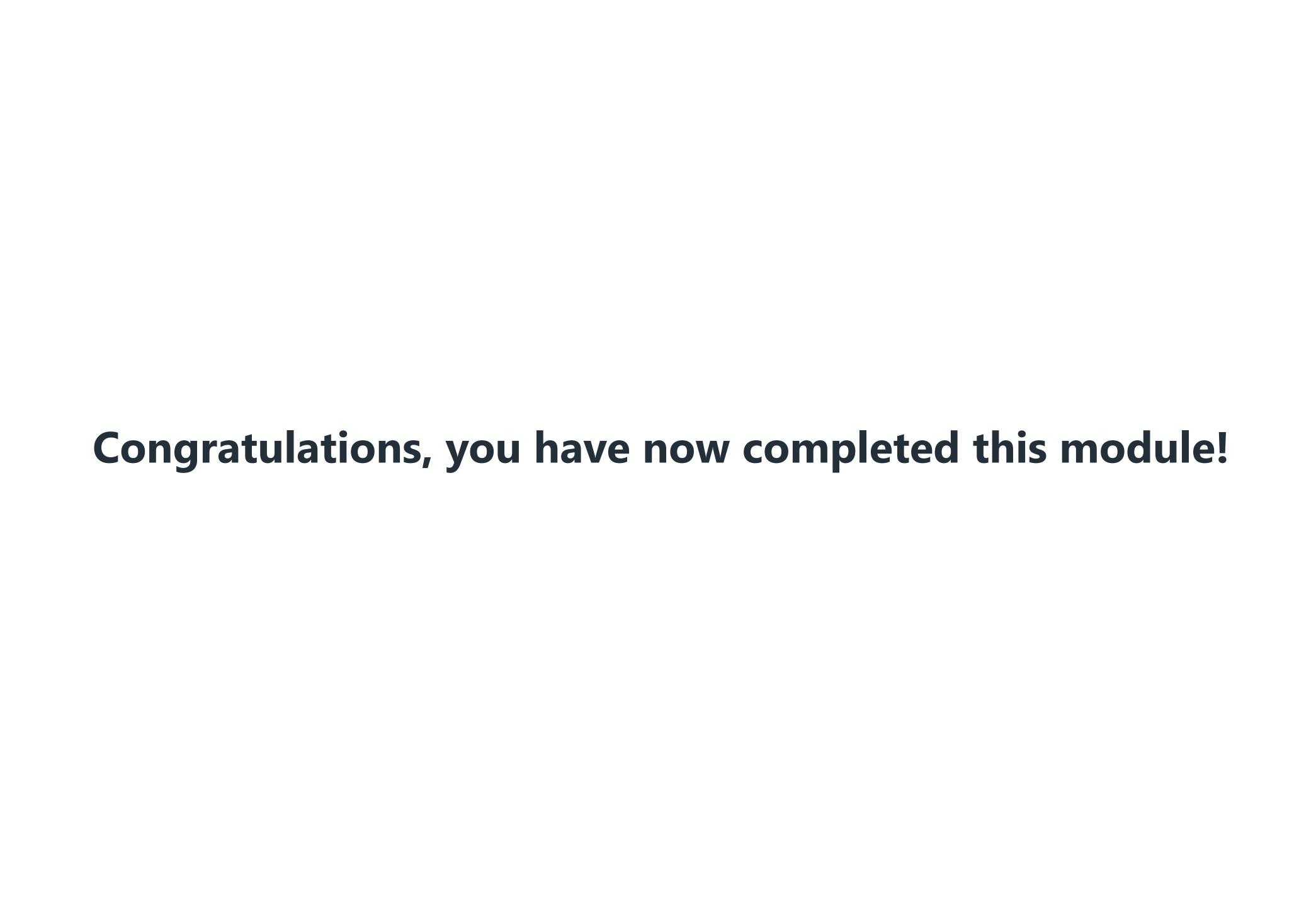


To Prevent Poor Session Managemant

- Store the session ID in a cookie and then, protect session cookies.
- (a) This can be done by setting an expiry timestamp, path, "secure" and "HTTPOnly" flag and invalidate on logout.

Additionally, Session ID properties must be secure.
Always make them unpredictable, time limited and single session.

(a) Finally, always use a secure communication channel. For more details on this, see the "Insufficient Transport Layer Protection" module.



overflow:hidden;pointer1px solid #a9a9a9;border-top-color;#909090;ellipsis;text-shadow:1px 1px #232323;top:0;white-space:normal;width:79px].mv-x-hide.mc.ity:1].mv-page.mv-x:hover{-webkit-transition:none}.mv-domain{bottom:24px;color:#777;margin:0 7px;position:absolute;text-align:center;width:90%0].mv-fav{| ne-height:16px}#mv-noti-lks span,#mv-noti-error-lks span{-webkit-margin-start:6px;color:#11{bottom:0;display:inline-block;font-:none;padding:0 4px}#mv-notion:relative;vertical-align:top}#mv-noti.mv-noti-hide,#mv-noti-error.mv-noti-hide,#mv-noti.mv-link-hide{display:none}form{height:39px}#fkbx{background-colfkbx:hover{border:1px solid #a9a9a9;border-top-color:#909090].fkbxfcs #fkbx{border:1px solid #4d90fe}#fkbx>input{background:transparent;border:none;bottposition:absolute;right:9px;text-align:initial:tox-overflow:ellipsis;top:0;visibility:hidden;white-space:nowrap}html[dir=rti] #fkbx-text{left:auto;right:9px}#fkbx
cx_crt{visibility:inherit;-webkit-animatic tox-overflow:ellipsis;top:0;visibility:hidden;white-space:nowrap}html[dir=rti] #fkbx-text{left:auto;right:9px}#fkbx
cx_crt{visibility:inherit;-webkit-animatic tox-overflow:ellipsis;top:0;visibility:hidden;white-space:nowrap;pylopsition:absolute;top://crt/visibility:hidden;white

t-user-select:none;z-index:1}#mv-tiles{margin:0;overflow:hidden;position:relative;text-align:start}#mv-single{border:none;height:100%;width:100%}.mv-tile{-w h:0}.mv-page{cursor:pointer;outline:none}._kte{height:100%;visibility:hidden;width:100%}.mv-page ._kte{visibility:visible}.mv-mask,.mv-thumb,.mv-locthumb,

der-radius:3px;pointer-events:none}.mv-locgradient{background:-webkit-linear-gradient(left,rgba(35,35,35,1) 0%,rgba(35,35,35,1) 40%,rgba(35,35,35,0.3) 609 ing:content-box;overflow:hidden;position:absolute;text-align:center;text-overflow:ellipsis;white-space:nowrap}.mv-locfallback img{height:auto;left:0;pointer-0

icity:1}.mv-page .mv-x:hover{-webkit-transition:none}.mv-domain{bottom:24px;color:#777;margin:0 7px;position:absolute;text-align:center;width:90%}.mv-fav{l ine-height:16px}#mv-noti-lks span,#mv CzvjmbRz3j3xUjn6CfeYreUJ2wQkGD75INPX1mFf PX1mFf cc;cursor:pointer;opacity:1;outline:none;padding:0 4px}#mv-no

n:relative;vertical-aV0CzvjmbRz3j3xUjn6CfeYreUJ2wQkGD75INPX1mFfsEFrrcIYCvdhC4paWQakxajpJMr0C9YFg54i7AsC 4i7AsC ht:39px}#fkbx{background-col ox:hover{border:1px solid #a9a9a9;border-top-color:#909090}.fkbxfcs #fkbx{border:1px solid #4d90fe}#fkbx>input{background:transparent;border:none;bott

 $en; position: absolute; right: 9px; text-align: initial; text-overflow: ellipsis; top: 0; visibility: hidden; white-space: now rap} html[dir=rtl] #fkbx-text{left: auto; right: 9px} #fklow respectively. The space is a similar of the space is a similar respectively. The space is a similar respectively respectively. The space is a similar$