Just Give me a Trial, Please

Sam Curry, Justin Rhinehart

zlz

- Full time bug bounty hunter (on-and-off for about ~4 years)
- Run security blog @ samcurry.net

sshell

- Senior Analyst @ Bishop Fox
- Doesn’t run security blog @ samcurry.net

*.target.com

axway.target.com

cms.target.com

tableau.target.com

jamf.target.com

jira.target.com

jenkins.target.com

vpn.target.com

www.bugbounty.com

dns.vendor.com

www.bugbounty.com

dns.bugbounty.com

(probably OK)

vendor-product.bugbounty.com

↓

IP owned by bugbounty.com

↓

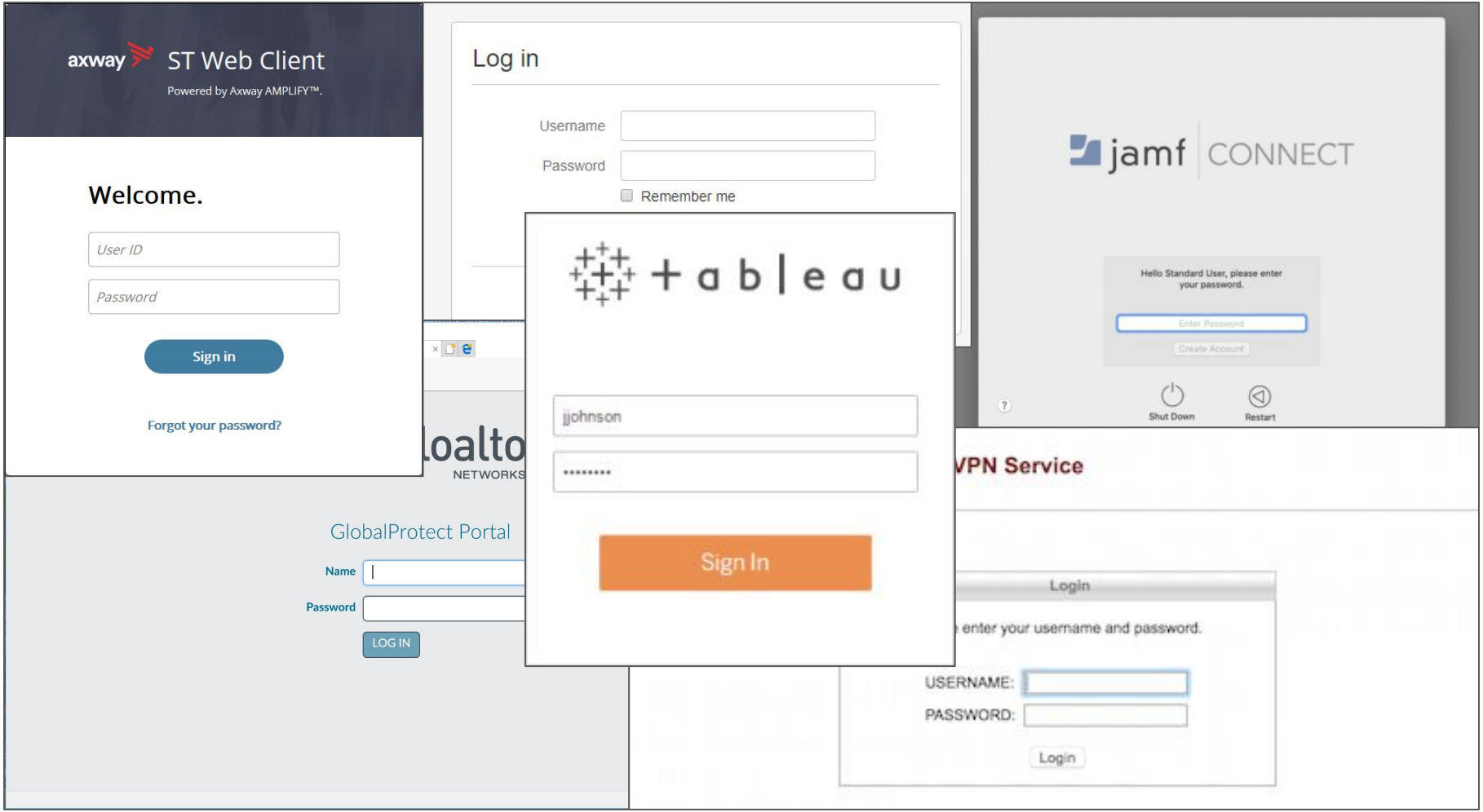
↓

super secret bug bounty internal network

Vendors

“I’d like to hack your product”

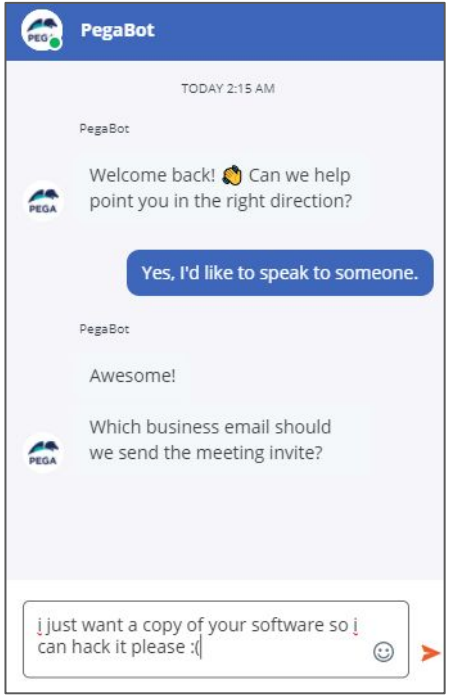
“I’d like to buy your product”


axway ST Web Client
Powered by Axway AMPLIFY™.
Welcome.
User ID
Password
Sign in
Forgot your password?
Log in
Username
Password
Remember me
jamf CONNECT
Hello Standard User, please enter your password.
Enter Password
Create Account
Shut Down
Restart
tableau
jjohnson
Sign In
NETWORKS
GlobalProtect Portal
Name
Password
LOG IN
VPN Service
Login
enter your username and password.
USERNAME:
PASSWORD:
Login

How do I hack a login page?

Option A

Option B

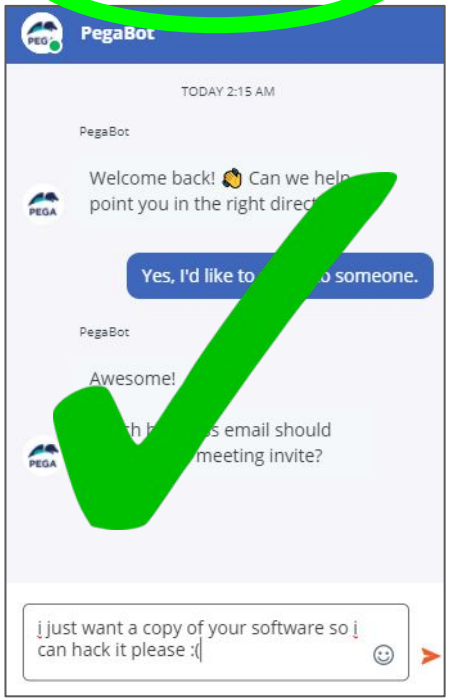


How do I hack a login page?

Option A

(Sadly, we are not Orange Tsai)

Option B



“I have absolutely *no idea* what you’re talking about…

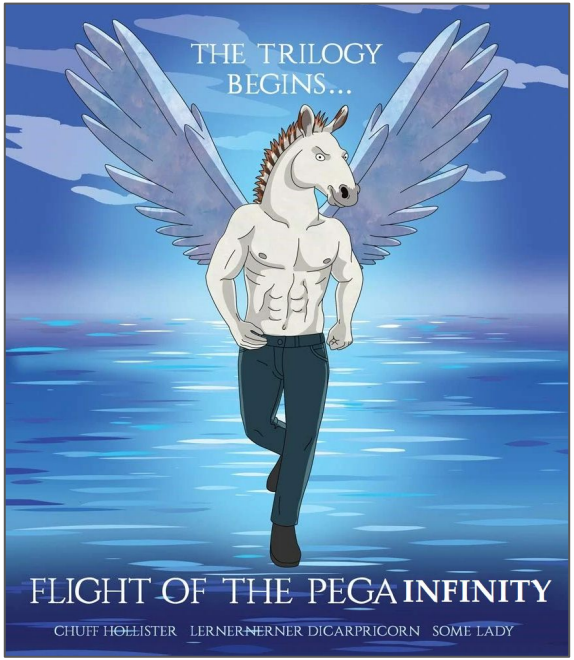
… but I’ve added your email to our spam list and will cold call you for the next 3 years”

Issues hacking vendors

- Hackers don’t own billion dollar companies
  - … at least not us ...
  - We’re not very good sales targets, why waste time on a demo?
- Who do I ask for permission?
  - From an outside perspective, how can I tell who I’m connected to?
- They don’t want to be hacked
  - Afraid of CVEs
  - Software too distributed

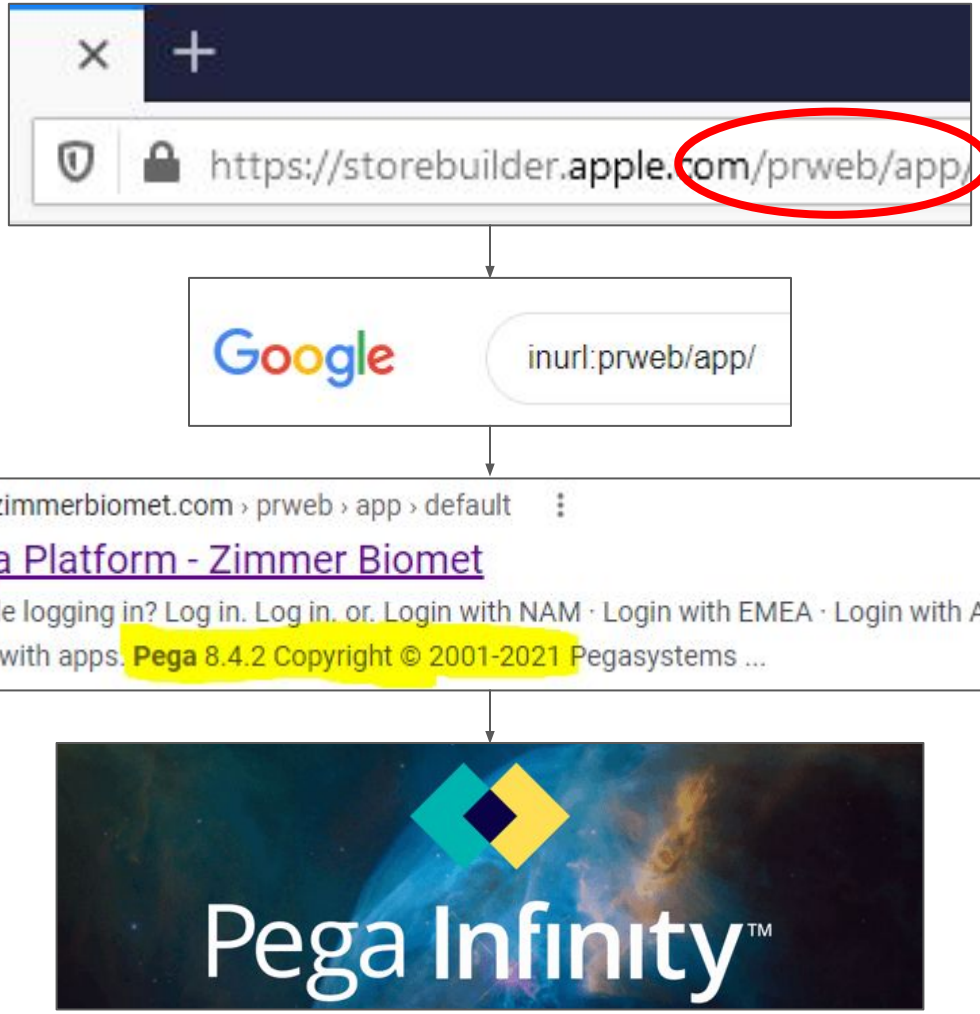
Vendor Methodology

Hacking Pega Infinity



d0nut zlz ziot xehle sshell

hmm….


https://storebuilder.apple.com/prweb/app/
Google
inurl:prweb/app/
drive.zimmerbiomet.com › prweb › app › default
Pega Platform - Zimmer Biomet
Trouble logging in? Log in. Log in. or. Login with NAM · Login with EMEA · Login with APAC · Login with apps. Pega 8.4.2 Copyright © 2001-2021 Pegasystems ...
Pega Infinity™

Pega Infinity™

Revolutionary software that unifies customer engagement and intelligent automation

Pega Customer Decision Hub™

Pega Customer Service™

Pega Sales Automation™

CUSTOMER ENGAGEMENT

INTELLIGENT AUTOMATION

Pega Platform™

- Case Management
- Low-code App Dev
- Mobile

Pega RPA™

REAL-TIME, OMNI-CHANNEL AI

END-TO-END AUTOMATION & ROBOTICS

MICROJOURNEY -CENTRIC RAPID DELIVERY

SITUATIONAL LAYER CAKE™

SOFTWARE THAT WRITES YOUR SOFTWARE™

CLOUD CHOICE

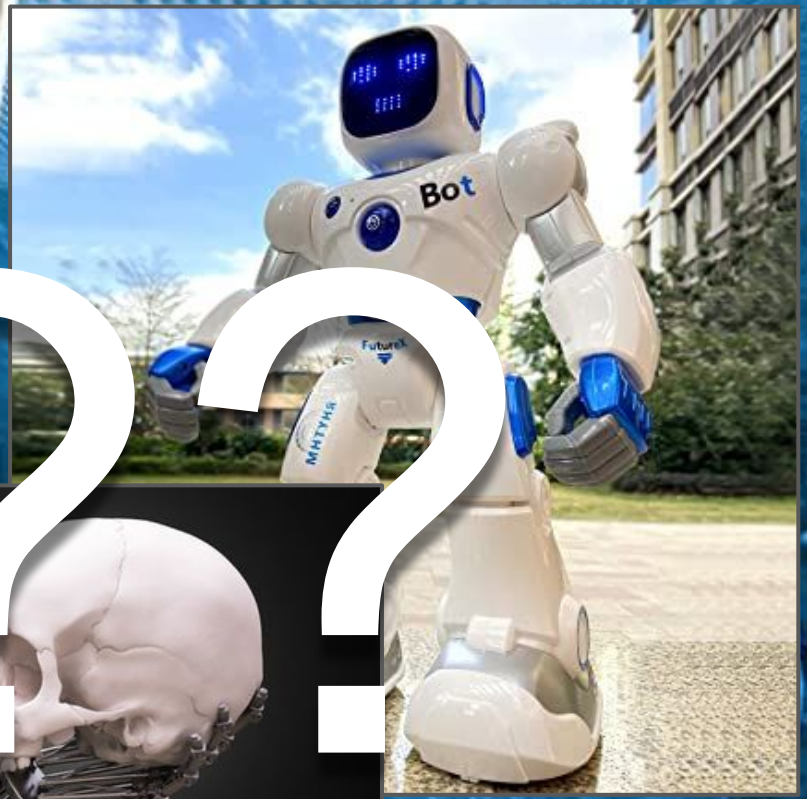
Industry-leading technology

Start fast and scale

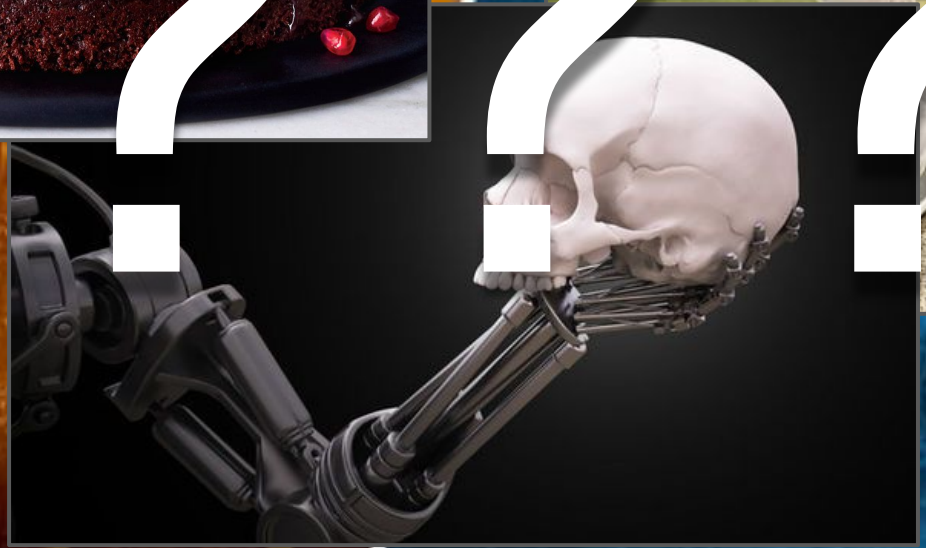
Future proof your investment

PEGA DX ARCHITECTURE™

PEGA


Bot

???



A servlet is a Java program supporting a Web server or Web application server. Internally, PRPC server code consists of several servlets, including these:

Servlet	Description
DiagnosticData	Supports downloading logs and report files from the System Management application, and downloading log files with the DesignerStudio > System > Tools > Logs > Log Files menu item.
HeapDisplay	Diagnostics
PRHTTPService	Supports Service HTTP rules (*Rule-Service-HTTP* rule type)
PRImpExpServlet	Exports or imports rules, data, and other objects. Reserved for installation and support issues.
PRPortletService	Supports access from portlets.
PRServlet	Supports interactive users using HTTP and a web browser; presents dynamic content such as the portal displays and forms. PRServlet is no longer required in a Pega 7 URL as of Pega 7.1.6.
PRServletContainerAuth	Supports interactive users using HTTP and a web browser, when using Java EE context authentication, where users are authenticated by the application server.
PRServletProtected	Supports HTTP Basic Authentication over Secure Sockets Layer (SSL).
PRServletProtectedAuth	Supports HTTP Basic Authentication over SSL.
PRSOAPServlet	Responds to service requests from SOAP clients, uses packages of Service SOAP rules. By default, uses the same TCP/IP port as PRServlet.
PRSOAPServletContainerAuth	Responds to service requests from SOAP clients, uses packages of Service SOAP rules, when Java EE context authentication is in use. By default, uses the same TCP/IP port as PRServlet.
PRSOAPSimulator	Helps in testing a SOAP connector. See *Testing Services and Connectors*, a document on the Integration area of the PDN.
PRStartup	Used briefly during system startup and to start agents and listeners.
PRTraceServlet	Implements the Tracer debugging tool.
RuleFileServlet	Serves static content through HTTP protocol messages, such as images, Cascading Style Sheets and JavaScript files. These are extracted to the file system from *Rule-File-** rules upon first request.
SecManServlet	Diagnostics

“**PRServlet**:Supports interactive users using HTTP and a web browser; presents dynamic content such as the portal displays and forms.”

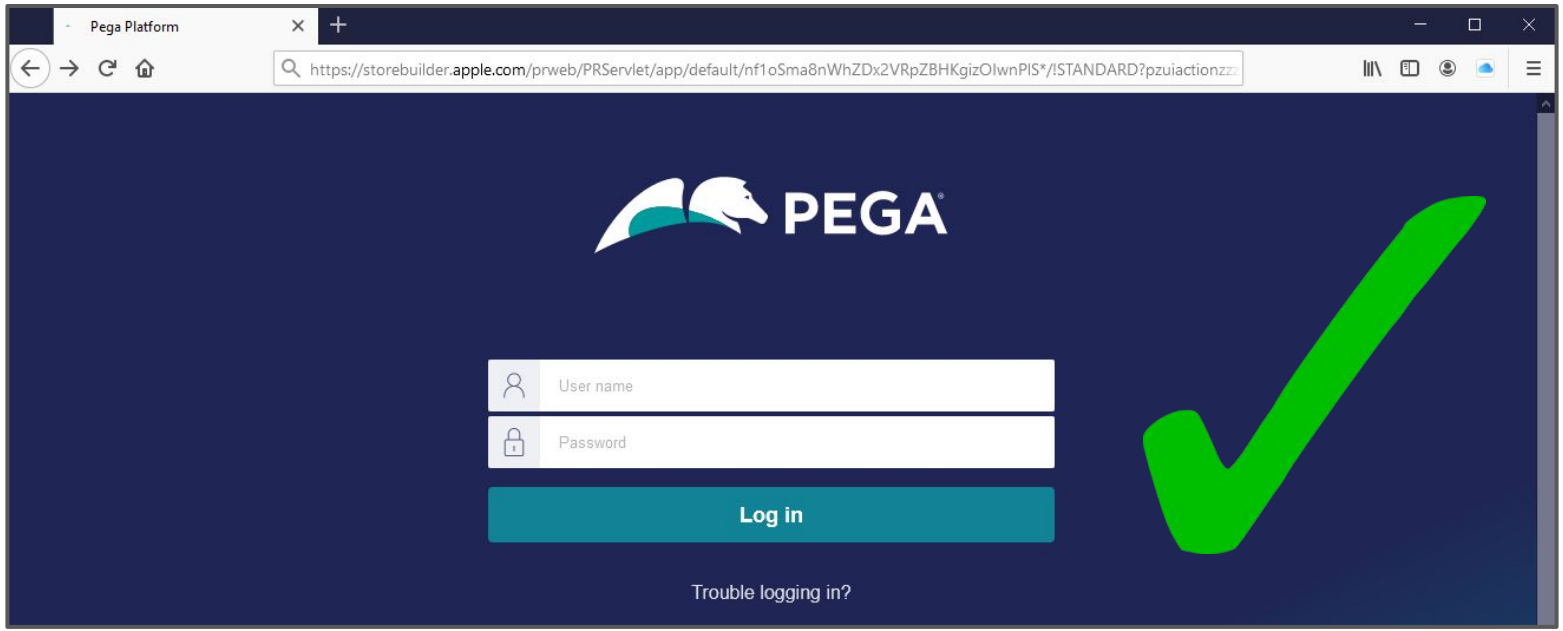
https://community.pega.com/sites/default/files/help_v717/definitions/s/servlet.htm

Defeating Apple's WAF using an Aliased Endpoint

`https://storebuilder.apple.com/prweb/PRServlet/`

=

`200 OK`



Notes for Testing Methodology on Unauthenticated Apps

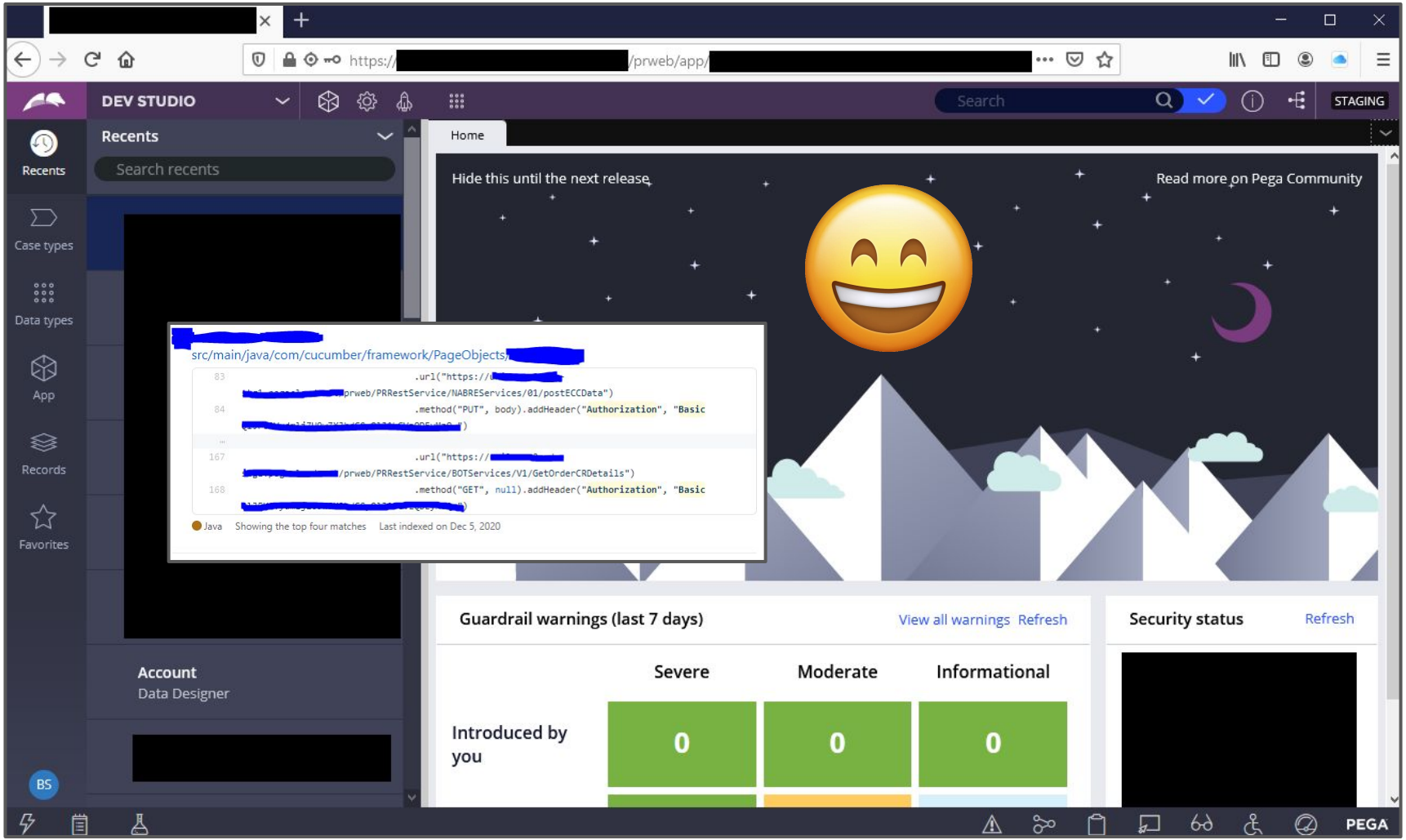
- How is it restricting our access?
  - Is it the HTTP server itself? A deployed application? Some sort of WAF?
- What functionality is available?
  - Functionality as in *all* functionality
    - How does the server handle URIs? Any directory traversal?
    - Are there any headers the service will process?
    - Is there an API, and if so, is anything publicly accessible? (Github!)
- Is a copy of the source obtainable?
  - Did any of their customers leak it somewhere (they'll be happy for you to report it!)
- Can you authenticate (with permission) to *any* version of the app?
  - Does your company run a version of the software?
  - Are there trials available (make sure to say "please" when asking)?
  - Default credentials, broken SSO, or any leaked employee credentials that will work?

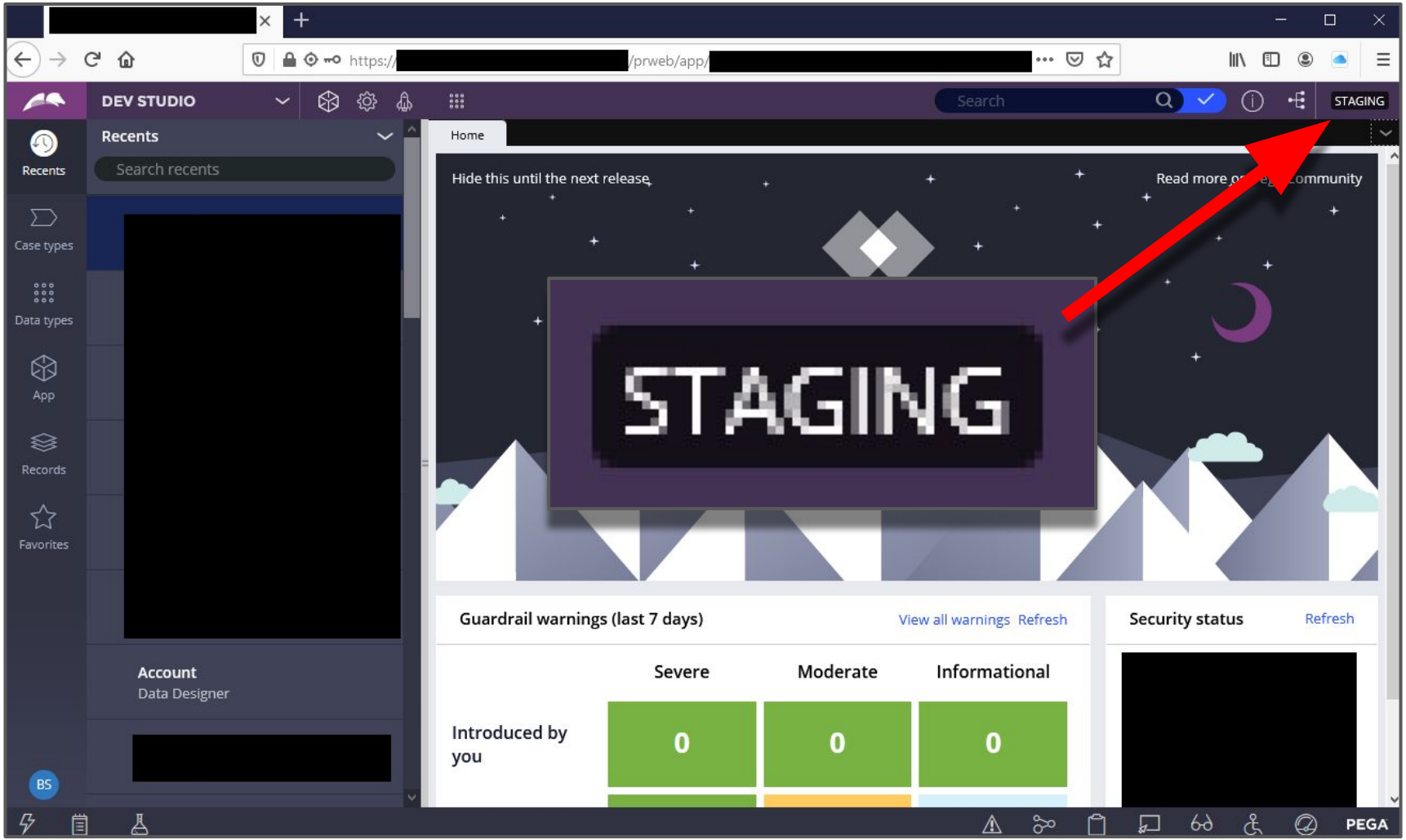
[redacted]

src/main/java/com/cucumber/framework/PageObjects/[redacted]

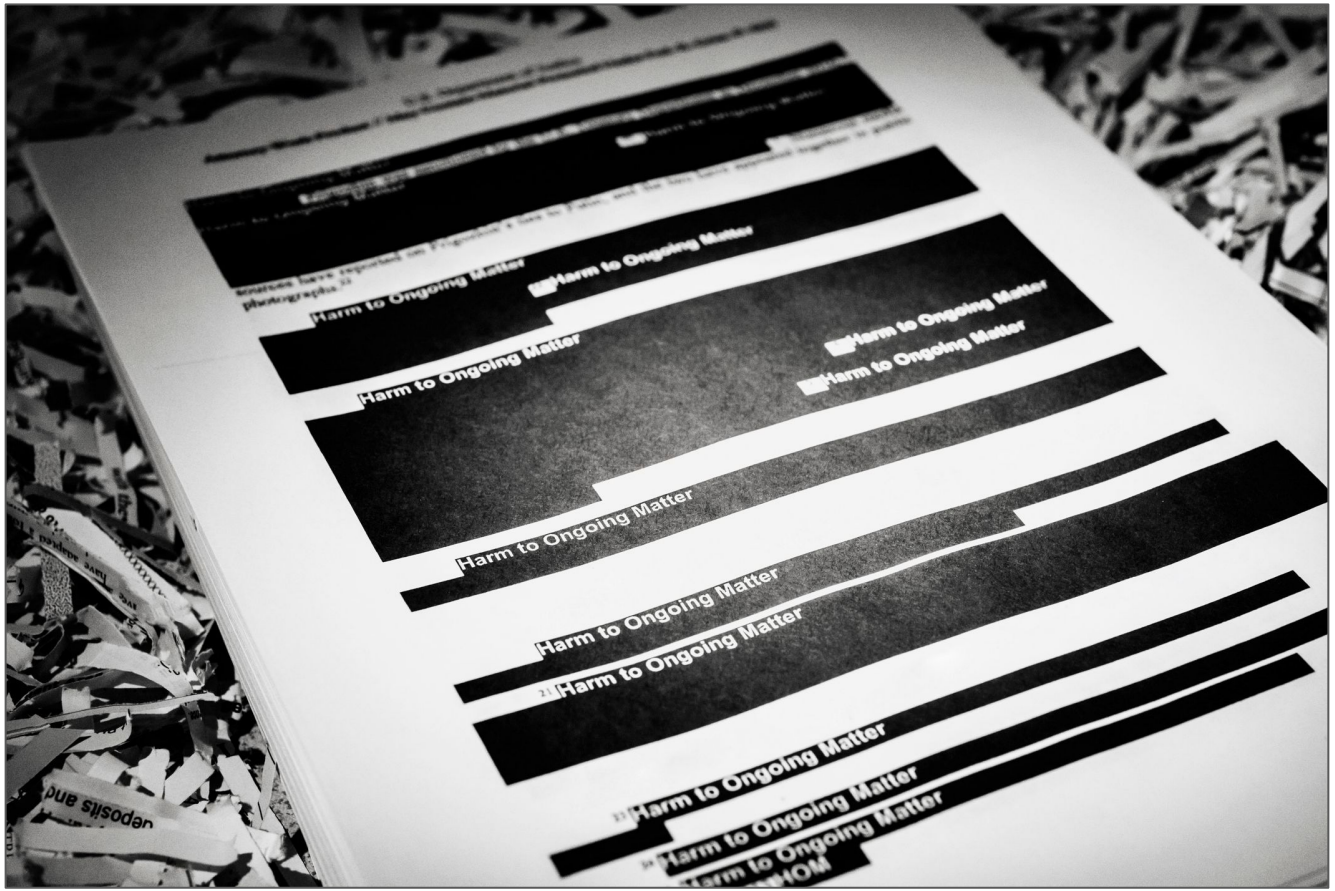
```
83                                  .url("https://[redacted]
                                    prweb/PRRestService/NABREServices/01/postECCData")
84                                  .method("PUT", body).addHeader("Authorization", "Basic
                                    [redacted])
...
167                                 .url("https://[redacted]
                                    /prweb/PRRestService/BOTServices/V1/GetOrderCRDetails")
168                                 .method("GET", null).addHeader("Authorization", "Basic
                                    [redacted])
```

Java Showing the top four matches Last indexed on Dec 5, 2020


https://[redacted]/prweb/app/[redacted]
DEV STUDIO
Search
STAGING
Recents
Search recents
Case types
Data types
App
Records
Favorites
Home
Hide this until the next release
Read more on Pega Community
src/main/java/com/cucumber/framework/PageObjects/[redacted]
83 .url("https://[redacted]prweb/PRRestService/NABREServices/01/postECCData")
84 .method("PUT", body).addHeader("Authorization", "Basic [redacted]
167 .url("https://[redacted]/prweb/PRRestService/BOTServices/V1/GetOrderCRDetails")
168 .method("GET", null).addHeader("Authorization", "Basic [redacted]
Java Showing the top four matches Last indexed on Dec 5, 2020
Account
Data Designer
BS
Guardrail warnings (last 7 days)
View all warnings Refresh
Severe
Moderate
Informational
Introduced by you
0
0
0
Security status
Refresh
PEGA


DEV STUDIO
Search
STAGING
Recents
Search recents
Case types
Data types
App
Records
Favorites
Account
Data Designer
BS
Home
Hide this until the next release
STAGING
Guardrail warnings (last 7 days)
View all warnings
Refresh
Severe
Moderate
Informational
Introduced by you
0
0
0
Security status
Refresh
PEGA

… and then ...


Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter
Harm to Ongoing Matter

- Actively hacking an application you're not supposed to have access to
- Trying any functionality which is state changing
- Storing or distributing anything sensitive you logged

- While confirming access, passively logging the post-authentication functionality
- Clearly communicating to the affected customer exactly what you saw or clicked on
- Using common sense

Notes for Post-Auth Hacking on a Pre-Auth Target

- Is there any “preview” functionality or widgets?
  - Huge number of possible issues, often an easy way to find XSS or SSRF
- How does authentication work post auth?
  - Forgot password rate limit bypass, session mishandling, cryptographic issues, etc.
  - Privilege escalation issues for any low level users
  - Functionality to send invitations to new users, force reset passwords, etc.
  - Is there a guest user, can you enable it, how does it work?
- Have you completely tested to see if authentication is honored on everything?
  - There are typically so many different areas of the app and sometimes something slips by
  - Many tools available to automatically replay requests without cookies

Thank you Nahamcon!

- Questions? Just kidding. It’s pre-recorded.

Sam Curry
@samwcyo

Justin Rhinehart
@sshell_