Dakota State University

Offensive Security Club

ACTIONS

Competition Information

Finals

Team: 3

Team Information Has Been Locked

Overall Score

echnical (35%)	4.4	Injects (30%)	18.6	Report (15%)	8.0	Presentation (20%)	9.0	Compliance	0.0

Final Score 40.0

Compliance and Rules Modifications

No compliance events were noted for this competition.

Inject Response Feedback

nject	Feedback
inals verall	Great question team. Good job making the client feel better about the issue in the opening of your email, identifying the ransomware, and a decryption tool. Good job making the client feel better about the issue in the opening of your email, identifying the ransomware, and a decryption tool. Lacking information about how to prevent the issue, as well as details about why this may have happened. Didn't provide information about why ransomware insurance would only be useful short-term, which seemed a bit strange. Good detailed content focused on the client. Answer was too high level and then went too technical, response was disjointed. Primary point of contact was organized and was well informed, but very technical for an audience with the CEO. Comparison to vertical. Excellent responses to initial question and follow ups. Use caution when offering personal opinions (there are places where this is appropriate and ways to soften your approach depending on your rapport with the client).

Technical Feedback

For the "customer data exposure through jawbreaker api" -- the write up and title talk at length about how "sensitive" customer data can be obtained through the API, but the remediation talks about needing to authenticate the API. The remediation is correct, but the finding you presented isn't that the API is unauthenticated. The findings need to match the remediation, and clearly explain the risk. In this case, the risk isn't that the API returns customer data, that's expected and intended functionality; the risk is that the API does not require authentication. Additionally there is a separate risk (and therefore a second finding) because the API also lacks authorization controls to restrict data returned to only that which belongs to the customer that is logged in.

Report Feedback

I like that you included both short and long term recommendations.
Ideally the report should indicate it's confidential. Executive summary does not really address overall risk to the organization. Scope should be in the executive summary.

The remediation section from old vulnerabilities is nice. The Strategic Recommendations is a good section.
A compliance section would be helpful to the client to summarize the issues at the top. A tools used section in the appendix would be helpful to the client.

Good style.
You mentioned potential violations but did not elaborate further, good start. Wording was fairly informal.

Awesome report style/format. Excellent exec. summary section...almost fun to read (what is wrong with us...). One of the few teams to point out OSINT. Good use of croissants. Visuals/graphics best out of all teams imo.
Would love to see more in your appendix- perhaps all of the references relisted there for example, as well as any additional info. Also, an extra section on executive compliance is needed...GDPR didn't make it into your report, but I was glad to see your reference to PCI-DSS! GDPR can result in massive fines for a company, and is a bear of a regulation for a company to follow, so would have been good to include remediation steps/analysis in this regard.

appendix B is great and I love how you have organized the report. Also excellent job on the technical findings and ordering them according to impact.
Appendix A should go into the executive summary so we know what scale you are using.

Very clean style, information mostly very clear
Steps to reproduce were not very well separated or clear on how to perform, while this is a report, some care should be done to ensure the receiving organization can reproduce findings to mitigate them .

Presentation Feedback

- Very confident presentation, you seemed at ease the entire time
- "Although our relationship with you was only this weekends engagement, we hope your relationship with security lasts a lifetime" that was a real zinger, good work I might steal that.
- Your presentation was a bit too technical - this was supposed to be a presentation for an executive audience. Execs probably don't know the difference between postgres and mysql.
- Good job explaining overall business impact of the findings as a whole, I would like to have seen the impacts tied a bit to the compliance frameworks
- In the business comparisons section, having the two bullet points drew the audience attention away from the main thing

that you were attempting to convey there which was that LBC had better then average security
  - Good security strengths section
  - Good job of reading your customer throughout the competition and including the comparison section

Great job of focusing the narrative on a senior executive level from the outset. Nice job addressing the relative security posture up front, only team to do so. Needed to get to material recommendations earlier (started with only 45s left), to leave appropriate time for Q/A.

Team 3

Good engaging intro
Team intro good, would like to see roles in writing but all good.
Scoping slide was strong, good detail.
Good recap of remediated vulns
Risk categories are good. You could have found a less wordy way to present that however. Its always good to link to or reference the standards like NIST you are using, in order to build credibility.
Findings slides were well designed with progressive iteration of detail. The immediate tie to business impact was very good. You should have also tied it immediately to compliance impact however, before switching gears to the next finding. You do address it somewhat but not integrated with the individual findings.
Try not to read off phones / papers when presenting.
Time management was a bit weak.
Recommendations were a bit too positive.

If you read from a script, don't make it sound like you are reading from a script.

if you can focus on time management better. The tldr up front could have been stronger.

Initial start was strong, and getting the audience to laugh/smile at the beginning is a good way to humanize the presentation

Some of the slides had too much text, try to dilute this down to individual bullet points

Try to avoid reading text, and speak from bullets

Time management could be better - didn't finish or leave time for questions, barely covered recommendations

- Suggest adding severity to each findings in key findings slide
- Keep eye contact
- Like the business comparisons slide as this is what executive want to know
- Need better time management

You had findings criticality rubric on each slide - which I liked - but you didn’t use it then on those slides when you showed the findings. You started strong but then didn’t leave enough time for recommendations and questions.

-inlcude your name and contact info in the slide, you want the people in this room looking you up.
-I like your emphasis on risk categories. impactful but moved through quickly to get to content
-I like the content you are including and how you lay it out, but I am not sure how I feel about it being in outline format (2a) instead of bullet points but no big deal.
-I don't know I would have your # of findings on every slide, if that was your guide so we could reference it as you rate each finding it would be very effective.
-better than average security posture - I disagree, but appreciate you included
-i like that next steps are broken down into critical, short term, and long term.
-incident response strong word - I would soften to investigate to ensure there isn't an incident