SaaS Security Basics on a Shoestring Budget

Presented by Jade Null

GLITCHSECURE

GLITCHSECURE

whoami

GlitchWitch (they/them)

Founder & Hacker

→ aka **Jade Null**

→ Hacking since I was a pre-teen

→ Experienced penetration tester

→ Semi-recent founder

Previously worked for...

BISHOPFOX

Independently helped protect...

vistaprint textnow

Shaw) MIDAS

GLITCHSECURE

I've been there...

As a hacker turned SaaS Founder I know security is HARD.

Especially without a huge budget or team

GLITCHSECURE

What to expect from this talk

General Info & Quick Wins

→ Basic security concepts and information

Risk and Impact

→ Should you care? When?

Actionable Advice

→ Free and low-cost tools, vendors & best practice

GLITCHSECURE

Who this talk is for... and how you can help

SaaS and Software Companies

→ Smaller companies and solo tech founders

Not For Hackers & Security Pros

→ This talk isn't for you, but you can help

Feedback Wanted

→ You can help shape this talk!

GLITCHSECURE

hunter2

What's your P@sSw0rd?

Password security for you and your customers

GLITCHSECURE

Authentication - Info

Level of effort 💀💀⚪⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

Password Managers

→ Securely store and manage all your passwords in one place.
→ Ensure strong, unique passwords for each account.

Multi-factor

→ Requires users to provide more than one form of identification.
→ Protects against account compromise.

Leaked Passwords

→ Evaluate whether a password has been exposed in a data breach.
→ Can reduce the risk of account compromise and password stuffing.

GLITCHSECURE

Authentication - Actionable Advice

Level of effort 💀💀⚪⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

Password Managers

→ Use a password manager like Bitwarden.
→ Limit account sharing.

Multi-factor

→ Enable by default, email → TOTP → WebAuthN.
→ Require for sensitive actions.

Leaked Passwords

→ Enable through HIBP / K-anonymity API.
→ Some providers and frameworks have built in support.

GLITCHSECURE

reply-all

Email security, monitoring, and deliverability

Forward this to 10 people by midnight... or else

GLITCHSECURE

Email Security - Info

Level of effort 💀💀💀⚪⚪

Financial Cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️⚪⚪

SPF (Sender Policy Framework)

→ Helps prevent email phishing and spoofing attacks.
→ Allows domain owners to define which servers are authorized to send emails on your domains behalf.

DKIM (DomainKeys Identified Mail)

→ Provides an additional layer of security for email communication.
→ Ensures the integrity of the message and its source.

DMARC (Domain-based Message Authentication, Reporting and Conformance)

→ Provides reporting and insights about emails sent from a domain.
→ Can help with identifying spoofing and deliverability issues.

GLITCHSECURE

Email Security - Actionable Advice

Level of effort 💀💀💀⚪⚪

Financial Cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️⚪⚪

SPF (Sender Policy Framework)

→ Set SPF records for both transactional and marketing

→ Start with Softfail `~all` and monitor before using Hardfail `-all`

DKIM (DomainKeys Identified Mail)

→ Set DKIM records for all your email providers that offer it

→ These are generated by the sending server (Google, Microsoft, AWS SES, etc). Configuration will vary.

DMARC (Domain-based Message Authentication, Reporting and Conformance)

→ Use a free service like DMARC Digest to get weekly reports

GLITCHSECURE

whoami

Limiting attack surface

Because you can’t secure it
if you forgot it existed

GLITCHSECURE

Attack Surface - Info

Level of effort 💀💀💀⚪⚪

Financial cost 🤑🤑⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

Subdomain Identification

→ A process of finding all subdomains associated with a domain.
→ Helps in identifying third-party and shadow IT subdomains that may pose a risk.

Port Scanning

→ A technique to identify open ports on a computer or network device.
→ Helps in determining which services are exposed.

Web Application Firewalls

→ Filters and monitors traffic between a web application and the internet.
→ An extra layer of protection, helps mitigate some types of attacks.

GLITCHSECURE

Attack Surface - Actionable Advice

Level of effort 💀💀💀⚪⚪

Financial cost 🤑🤑⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

Subdomain Enumeration

→ Monitor your DNS providers for changes.
→ Utilise certificate transparency monitoring tools like CloudFlare.
→ Open source tools like subfinder can help when access is limited.

Port Scanning

→ nmap -p 1-65565 -Pn -vvv

Web Application Firewalls

→ Use a service like CloudFlare, take time to configure
→ Protect Origin IP with cloud provider firewall
→ Cloudflare Access, Tailscale Tunnel, etc for internal apps

GLITCHSECURE

git commit -m “fix security”

Source Code Security

404 witty subtitle not found

GLITCHSECURE

Source Code Security - Info

Level of effort 💀💀⚪⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️⚪⚪

Branch Protection

→ Restrictions that can be applied to branches in a repository.
→ Enforces code quality, prevents accidental changes.

Commit Signing

→ Provides assurance that the commit was made by a trusted individual.

Dependencies

→ Effective dependency management can help minimize attack surface.
→ Early detection of vulnerabilities through continuous monitoring.

GLITCHSECURE

Source Code - Actionable Advice

Level of effort 💀⚪⚪⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️⚪⚪

Branch Protection

→ Ensure `main/staging/dev` branches are locked down.
→ Require PRs, Test passing, Linting, etc before merge.

Commit Signing

→ Follow Github's commit signature verification documentation.
→ Keep private key backed up and use a secure password.

Dependencies

→ A free tool like Snyk or Dependabot can get you quite far
→ Snyk free can be configured to dial back usage, still get daily results
→ Set yourself a weekly or monthly reminder to run npm update

GLITCHSECURE

DevOps - Info

Level of effort 💀💀⚪⚪⚪

Financial cost 🤑🤑⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

SAST (Static Application Security Testing)

→ A type of security testing that examines the application's source code, without executing the application.

→ Helps identify and fix potential flaws before the application is deployed

Logging & Error Monitoring

→ Provides a record of system activities and events.

→ Enables detection of breaches, intrusions, or unauthorized access.

GLITCHSECURE

DevOps - Actionable Advice

Level of effort 💀💀💀⚪⚪

Financial cost 🤑🤑⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

SAST (Static Application Security Testing)

→ Free tools like SonarCube, Semgrep Code, and Github Code Scanning.
→ Can be integrated into CI/CD and combined with branch protection.

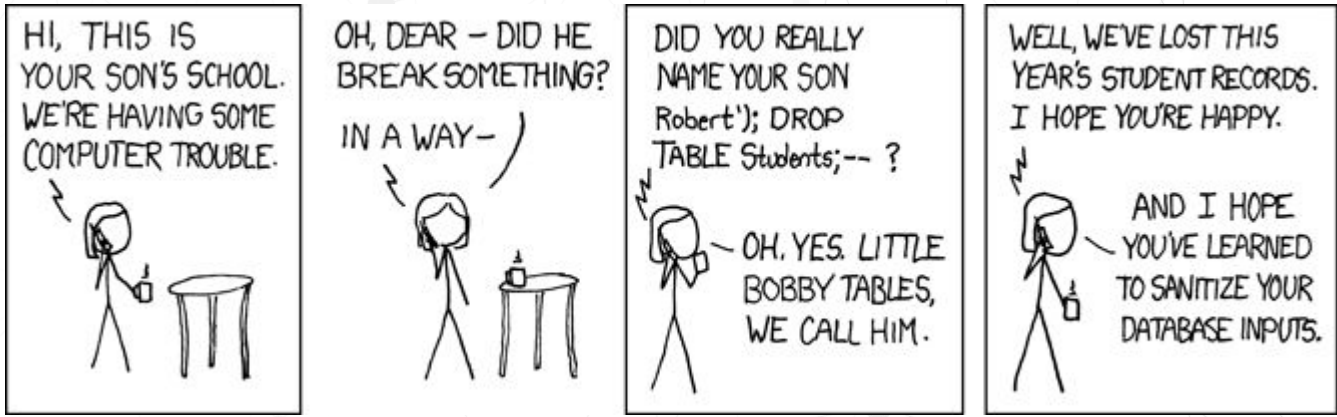
Logging & Error Monitoring

→ Implement error monitoring for both backend and frontend.
→ Free tools like Sentry.io can go a long way.
→ Platform specific tools like flareapp.io can take you even further.
→ A surprising number of vulnerabilities can be identified this way.

GLITCHSECURE

Application'); DROP TABLE Security;--

Web & Application Security



GLITCHSECURE

Web Security - Info

Level of effort 💀💀⚪⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

HSTS & SSL

→ Helps prevent data interception on untrusted networks.
→ HSTS can enforce the use of secured HTTPS connections.

Cookies

→ Used to store session information and preferences.
→ Measures can be taken to protect the information contained within cookies and prevent unauthorised access or tampering.

Session Management

→ Process of securely managing and maintaining user sessions on a web application or system to prevent unauthorised access.

GLITCHSECURE

Web Security - Actionable Advice

Level of effort 💀💀⚪⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️❤️⚪

HSTS & SSL

→ Modern day SSL is free. Let's Encrypt + Google Trust Services
→ Enforcing HSTS is an easy win
→ `strict-transport-security: max-age=31536000; includeSubDomains; preload`

Cookies

→ Ensure flags such as `Secure`, `HttpOnly`, `Path`, `Domain`, and expiry.
→ OWASP Session Management Cheat Sheet → Cookie Section

Session Management

→ Ensure session timeout and logout actually works... yes really.
→ Provide users notification and control of new sessions.

GLITCHSECURE

AppSec - Info

Level of effort 💀💀💀⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️❤️❤️

Rate Limiting

→ A technique used to control the amount of traffic or requests that can be sent or received within a specific time period.

IDOR (Insecure Direct Object Reference)

→ A vulnerability class that allows an attacker to access or manipulate sensitive data by directly referencing a resources without authorisation.
→ Can lead to exposure of sensitive information.

Injection Flaws (XSS, SQLi, SSRF, etc)

→ A vulnerability class that allows an attacker to manipulate input data to execute arbitrary commands or inject malicious code.

GLITCHSECURE

AppSec - Actionable Advice

Level of effort 💀💀💀⚪⚪

Financial cost 🤑⚪⚪⚪⚪

Impact ❤️❤️❤️❤️❤️

Rate Limiting

→ Implement on sensitive and resource triggering end-points.
→ Test this using a free tool like Burp Community's *Repeater.*

IDOR (Insecure Direct Object Reference)

→ Free tools like Burp Community can help you here again.
→ Navigate your app as an end user, watch for requests with unique IDs and repeat those with known valid IDs for other users/resources.

Injection Flaws (XSS, SQLi, SSRF, etc)

→ Test for blind XSS with a tool like ezXSS or a simple `"/><script>alert(1)</script>`
→ Test for SQLi with a free tool like SQLMap.
→ Review the Server-Side Request Forgery Prevention Cheat Sheet

GLITCHSECURE

hacker voice: i'm in

External Security Testing

Rabbit? Flu shot? Someone talk to me!

GLITCHSECURE

Security Testing - Info

Level of effort 💀💀💀⚪⚪

Financial cost 🤑🤑🤑⚪⚪

Impact ❤️❤️❤️❤️❤️

Vulnerability Scanning

→ Automated tooling to identify known vulnerabilities
→ Best for misconfigurations, outdated software, and networks.

DAST (Dynamic Application Security Testing)

→ Identifies vulnerabilities in real-time during the application's runtime.
→ Can find more complex injection and business logic flaws.

Penetration Testing

→ Performed by trained professionals.
→ Simulating real-world attacks to identify vulnerabilities.

GLITCHSECURE

Security Testing - Actionable Advice

Level of effort 💀💀💀⚪⚪

Financial cost 🤑🤑🤑⚪⚪

Impact ❤️❤️❤️❤️❤️

Vulnerability Scanning

→ Tons of free tools exist
→ OpenVAS, Nuclei, and OWASP ZAP provide coverage

DAST (Dynamic Application Security Testing)

→ Implement a free tool in CI/CD like Dasterdly
→ Consider spending $$$$ for piece of mind and enterprise deals

Penetration Testing

→ DIY first by following the OWASP ASVS.
→ You won't be happy if you cheap out. Sorry not sorry.

GLITCHSECURE

Vuln Reports - Info

Level of effort 💀💀💀⚪⚪

Financial cost 🤑🤑🤑⚪⚪

Impact ❤️❤️❤️⚪⚪

Vulnerability Disclosure Policies

→ A documented set of guidelines for reporting security vulnerabilities.
→ Defined by your organization, encourages responsible reporting.

Bug Bounty

→ Takes a VDP one step further by incentivizing reports.
→ Provides an opportunity for researchers to earn rewards.

Beg Bounty

→ “scaremongering for profit”, typically low quality or flat out fake.
→ Demand payment before disclosing flaws, typically targeting non VDP.

GLITCHSECURE

Vuln Reports - Actionable Advice

Level of effort 💀💀💀⚪⚪

Financial cost 🤑🤑🤑⚪⚪

Impact ❤️❤️❤️⚪⚪

Vulnerability Disclosure Policies

→ Create with Disclose.io Policy Maker + 2 hours of a vCISO's time

→ Work to define what you consider valid and in scope, set clear expectations for communication and timelines.

Bug Bounty

→ Requires budget and well defined VDP and process.

→ Check out the OpenCage blog post "Running a security bounty program as a bootstrapped business: lessons learned".

Beg Bounty

→ Refer them to your VDP or BB, publicly shame if they try to extort.

GLITCHSECURE

Internal “secur-a-thon” day

Low cost high impact

→ Setup a password manager & require MFA for all staff
→ Upgrade your email security
→ Enable branch protection rules
→ Setup dependency monitoring, or at minimum an upgrade schedule
→ Setup error tracking
→ Configure HTTP Security Headers & Cookie flags
→ Make sure your WAF is configured
→ Start hacking and securing yourself, OWASP Cheat Sheet & ASVS
→ Contact GlitchSecure ;-)

GLITCHSECURE

Minimum Viable Secure Product

Low cost high impact - mvsp.dev

→ Provides a checklist and criteria for secure products.
→ Easy to understand application security focused controls.

Homework for next week

→ Stop procrastinating on password managers
→ Review your email security
→ Ensure your WAF is actually configured
→ Setup branch protection and dependency management
→ Start logging
→ Setup a free vulnerability scanning or DAST tool
→ Contact GlitchSecure ;)

GLITCHSECURE

Get in touch

Jade Null
Founder & Hacker

jade@glitchsecure.com
glitchsecure.com