
Hvernig maður finnur EKKI veikleika
SYNDIS
Creative[in]Security

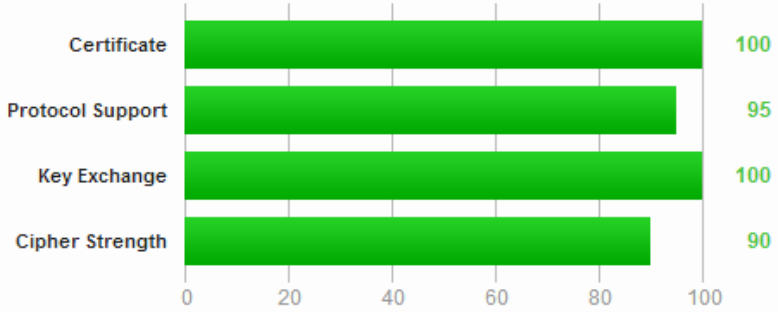

OLD WAYS
WON'T OPEN
NEW
DOORS


KEEP
CALM
this requires a
PARADIGM
SHIFT

Summary

Overall Rating

A+



Documentation: SSL/TLS Deployment Best Practices, SSL Server Rating Guide, and OpenSSL Cookbook.

This server is not vulnerable to the Heartbleed attack. (Experimental)

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

Veikleikagreining/Vulnerability scanners

ERPScan
QUALYS Continuous Security
Nessus vulnerability scanner
MAXPATROL
CORE SECURITY
BeyondTrust
nexpose
Сканер-ВС
BEYOND security
DIGITAL DEFENSE INCORPORATED
OpenVAS
SAINT
F-Secure.
tripwire
secpod Expose the Unknown

Penetration testing is a mandatory component of regulations such as PCI DSS and also considered essential practice for any business with a high degree of dependence on online operations. Testing empowers companies to identify and remediate security issues in their running web applications before hackers can exploit them. Using CHECK, CREST, SANS and OWASP trained resource, we provide:

FROM: £150

- Web application penetration testing, across .net, Java and PHP platforms.
- Legacy application penetration testing of legacy client/server applications, AS/400 and mainframes.
- Standalone application testing, of compiled executables.
- External network penetration testing
- Internal network penetration testing
- Remote access and two-factor authentication testing
- Physical penetration testing
- Wireless penetration testing
- PCI DSS penetration testing
- Social engineering
- Phishing simulations
- Reputational analysis

http://www.algartmedia.com/index.cfm/service/software-penetration-testing

Anti virus

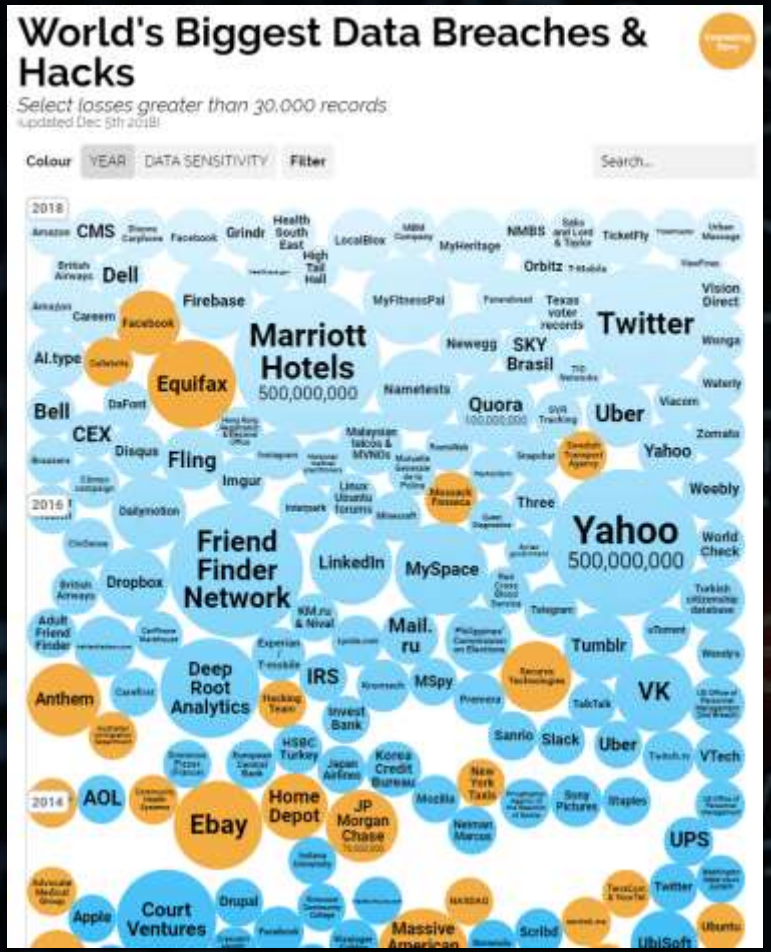
=

?

Penetration testing is a mandatory component of regulations such as PCI DSS and also considered essential practice for any business with a high degree of dependence on online operations. Testing empowers companies to identify and remediate security issues in their running web applications before hackers can exploit them. Using CHECK, CREST, SANS and OWASP trained resource, we provide:

FROM: £150

- Web application penetration testing, across .net, Java and PHP platforms.
- Legacy application penetration testing of legacy client/server applications, AS/400 and mainframes.
- Standalone application testing, of compiled executables.
- External network penetration testing
- Internal network penetration testing
- Remote access and two-factor authentication testing
- Physical penetration testing
- Wireless penetration testing
- PCI DSS penetration testing
- Social engineering
- Phishing simulations
- Reputational analysis



https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

https://www.ibm.com/security/data-breach/?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&cy=US

Reynslusaga dagsins

Regarding a vulnerability report

“Hello team, This is Utsav an Independent security researcher and pentester, would you Guys let me know whether you are running any bug bounty program for official WEBSITE ? I want to report security vulnerability, I found some Vulnerability. Please ask your Officials.”

Re: Regarding a vulnerability report

“**Hello Utsav.**
No we do not have a bug bounty program. If you have found some vulnerability in our system I would really like to know about it so I can investigate.
Kind regards,
KaraConnect”

Re: Regarding a vulnerability report

“Hie, if i report valid issues will it be considered for rewards according to severity of issues?

Utsav”

Clickjacking veikleiki

Hello ,

here i am reporting an issue related to clickjacking **Profile, Update, password change, settings etc**

while i was going through your site i found your website is vulnerable to clickjacking..

here some description about click jacking..

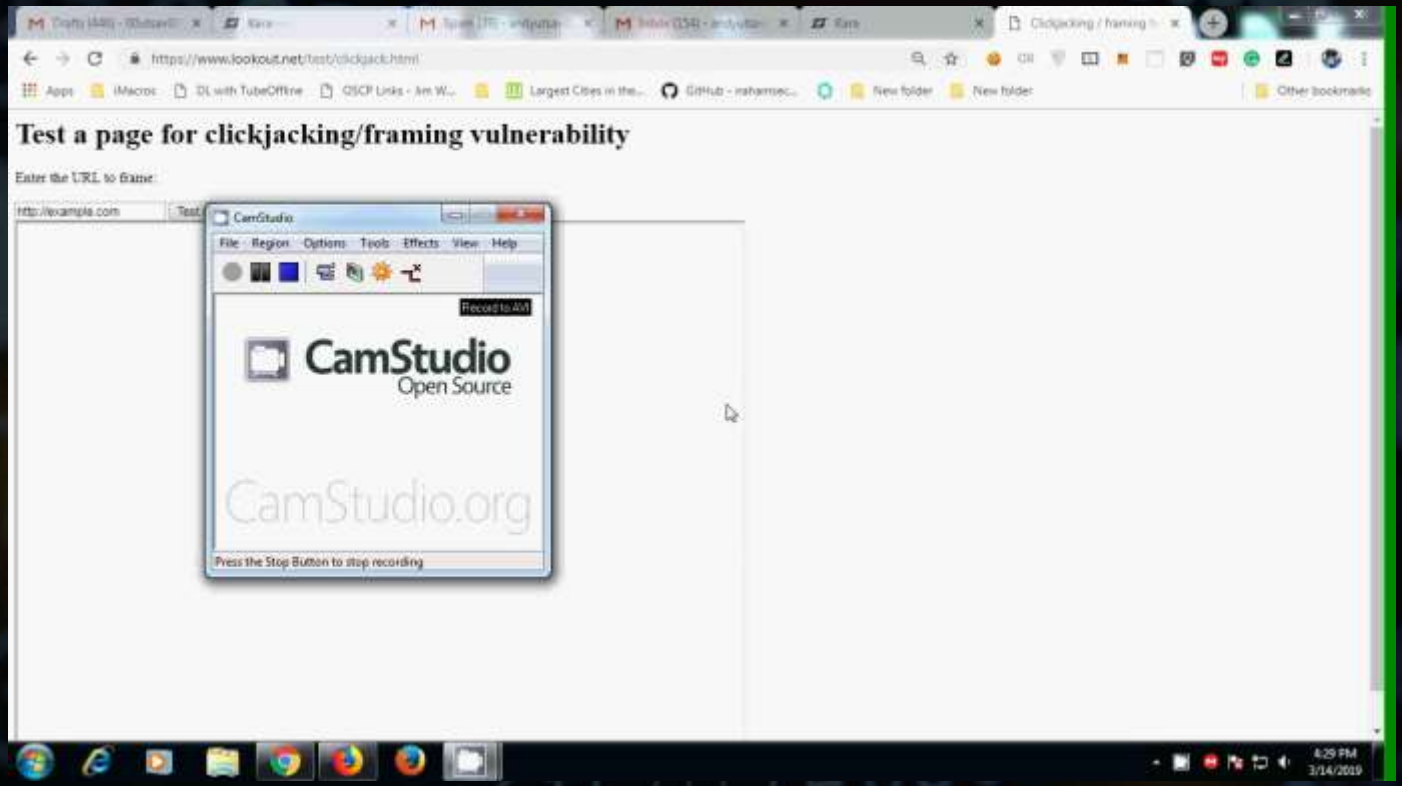
Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

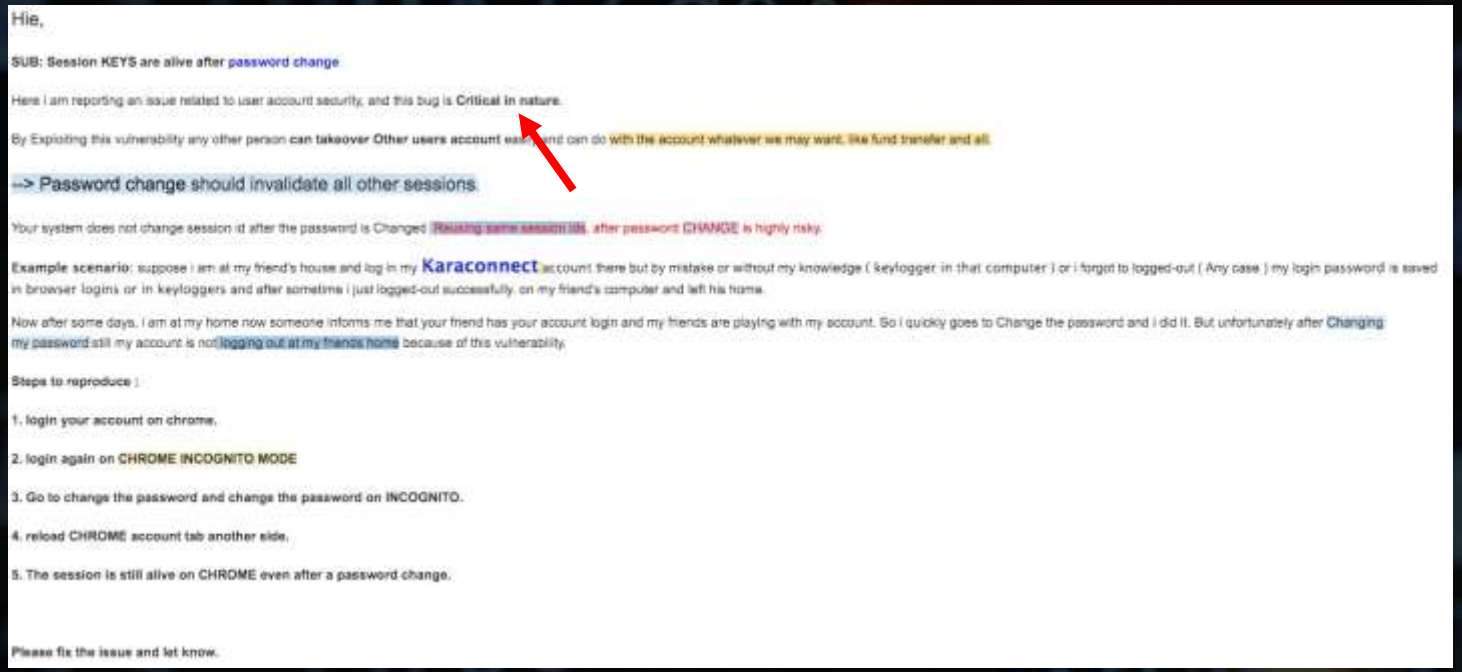
Solution : http://blog.kotowicz.net/2009/12/5-ways-to-prevent-clickjacking-on-your.html

please watch the video poc for steps to reproduce--

Clickjacking veikleiki



Lota úreldist ekki við breytingu á lykilorði



Hie,

SUB: Session KEYS are alive after password change

Here I am reporting an issue related to user account security, and this bug is **Critical in nature**.

By Exploiting this vulnerability any other person **can takeover Other users account** easily and can do with the account whatever we may want, like fund transfer and all.

--> Password change should invalidate all other sessions.

Your system does not change session id after the password is Changed. Reusing same session ids, after password CHANGE is highly risky.

Example scenario: suppose i am at my friend's house and log in my **Karaconnect** account there but by mistake or without my knowledge (keylogger in that computer) or i forgot to logged-out (Any case) my login password is saved in browser logins or in keyloggers and after sometime i just logged-out successfully. on my friend's computer and left his home.

Now after some days, I am at my home now someone informs me that your friend has your account login and my friends are playing with my account. So i quickly goes to Change the password and i did it. But unfortunately after Changing my password still my account is not logging out at my friends home because of this vulnerability.

Steps to reproduce :

1. login your account on chrome.

2. login again on CHROME INCOGNITO MODE

3. Go to change the password and change the password on INCOGNITO.

4. reload CHROME account tab another side.

5. The session is still alive on CHROME even after a password change.

Please fix the issue and let know.

Mjög alvarlegir öryggisveikleikar?

Hello ,

here i am reporting an issue related to clickjacking **Profile, Update, password change, settings etc**

while i was going through your site i found your website is vulnerable to clickjacking..

here some description about click jacking..

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> or <iframe>. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Solution : http://blog.kotowicz.net/2009/12/5-ways-to-prevent-clickjacking-on-your.html

please watch the video poc for steps to reproduce--

Hie,

SUB: Session KEYS are alive after password change

Here i am reporting an issue related to user account security, and this bug is **Critical in nature.**

By Exploiting this vulnerability any other person **can takeover Other users account** easily and can do with the account whatever we may want, like fund transfer and all.

--> Password change should invalidate all other sessions

Your system does not change session id after the password is Changed (Reusing same session ids), after password CHANGE is highly risky.

Example scenario: suppose i am at my friend's house and log in my **Karaconnect** account there but by mistake or without my knowledge (keylogger in that computer) or i forgot to logged-out (Any case) my login password is saved in browser logins or in keyloggers and after sometime i just logged-out successfully on my friend's computer and left his home.

Now after some days, i am at my home now someone informs me that your friend has your account login and my friends are playing with my account. So i quickly goes to Change the password and i did it. But unfortunately after Changing my password still my account is not logging out at my friends home because of this vulnerability.

Steps to reproduce :

1. login your account on chrome.

2. login again on CHROME INCOGNITO MODE

3. Go to change the password and change the password on INCOGNITO.

4. reload CHROME account tab another side.

5. The session is still alive on CHROME even after a password change.

Please fix the issue and let know.

Mentor öryggisveikleikinn

FRÉTTABLAÐIÐ

Fréttir | Markaðurinn | Sport | Lífið | Skoðun | Glamour

Innlent

Komst yfir upplýsingar um 422 börn í Mentor

Fimmtudaginn síðastliðinn komst það upp að óprúttnum aðila tókst að safna kennitölum og forsíðumyndum 422 nemenda í 96 skólum í sveitarfélögum um allt land á Íslandi.

Daníel Freyr Birkisson
danielfreyr@frettabladid.is
Mánudagur 18. febrúar 2019
18.54 GMT

Deila

Viðkomandi tókst að safna kennitölum og myndum af á fimmta hundrað nemendum. Mentor ihugar réttarstöðu sína. Fréttablaðið/Ernir

Fimmtudaginn síðastliðinn komst það upp að óprúttnum aðila tókst að safna kennitölum og forsíðumyndum 422 nemenda í 96 skólum í sveitarfélögum um allt land á Íslandi. Notandinn var skráður inn á skólaupplýsingakerfið Mentor og gat hann sótt upplýsingarnar vegna veikleika í kerfinu.

Innlent

Foreldri safnaði saman upplýsingum í Mentor

Óprúttinn aðili, sem safnaði saman upplýsingum um á fimmta hundrað nemenda í gegnum Mentor, var með aðgang að kerfinu. Mentor hefur haft samband við Persónuvernd.

Bryndís Silja Pálmadóttir
Þriðjudagur 19. febrúar 2019
12.30 GMT

Deila

Foreldrar séu haft samband við skóla og fengið upplýsingar um það hvort upplýsingum um börn þeirra hafi verið stolið. Fréttablaðið/Ernir

Óprúttinn aðili, sem tókst að safna saman kennitölum og forsíðumyndum á fimmta hundrað nemenda í gegnum Mentor, er foreldri eða forráðamaður barns og hafði því aðgang að kerfinu. Niclas Walter, forsjóri Mentor, staðfestir þetta í samtali við Fréttablaðið en ekki er talið að upplýsingunum hafi verið safnað í annarlegum tilgangi.

How to Earn Money as a Bug Bounty Hunter

Patrick Allan

8/17/17 4:30pm • Filed to: PROGRAMMING

125.5K 13 4

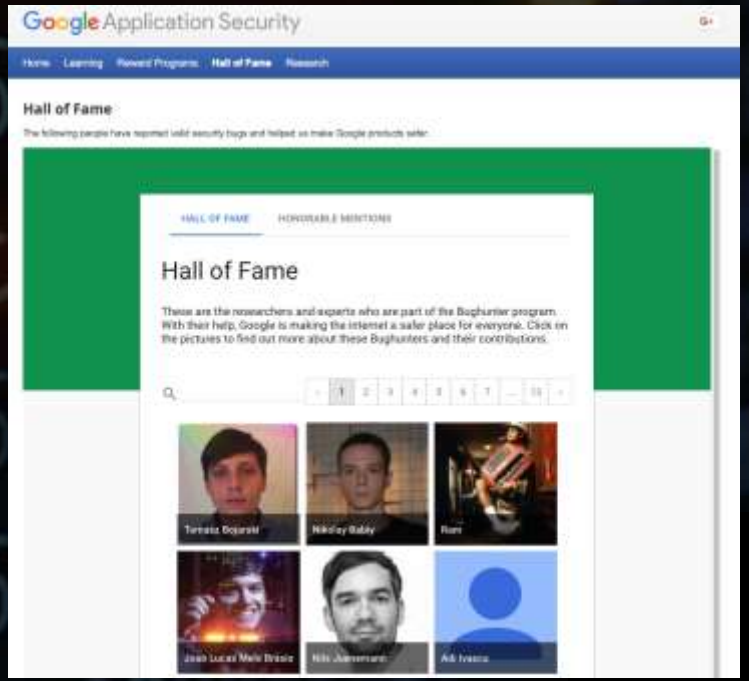
https://lifehacker.com/how-to-earn-money-as-a-bug-bounty-hunter-1797946520

Hvernig á að takast á við þetta?

Responsible disclosure

Vulnerability Disclosure Policy (VDP)

Bug Bounty Program (BBP)



Vulnerability Disclosure Policy (VDP)

WHAT IS A VULNERABILITY DISCLOSURE POLICY?

A VDP is the digital equivalent of "if you see something, say something." It's intended to give anyone — ethical hackers (aka "researchers" or "finders"), anyone who stumbles across something amiss — clear guidelines for reporting potentially unknown or harmful security vulnerabilities to the proper person or team responsible.

Think of this real-life analogy: you walk past a neighbor's house and see their back door was left wide open. What would you do? You'd probably knock on their door, holler for them, or maybe even call them.

Bug Bounty Program (BBP)

- Þúsundir einstaklinga með fjölbreytta þekkingu sem leitar að öryggisvillum
- Hvati er að finna alvarlegri öryggisveikleika sem gefa meir af sér annað hvort í peningum eða virðingu
- Hægt að gera mun ítarlegri prófanir sem tekur tillit til tilgangs hugbúnaðar og felur oft í sér að nýir veikleikar finnast í sérsmíðuðum kerfum
- Mikil samkeppni þar sem sá fyrsti til að finna veikleika er sá sem fær hrós eða pening fyrir vikið. Veikleikar eru líka lagaðir hratt.
- Greiðsla er fyrir veikleika en ekki verkefni **Pay Per Bug** (PPB)
- Eflir öryggiskúltúr innandyra þar sem öryggishættur og veikleikar eru ekki tabú og hvetur alla til að taka þátt í að efla öryggi

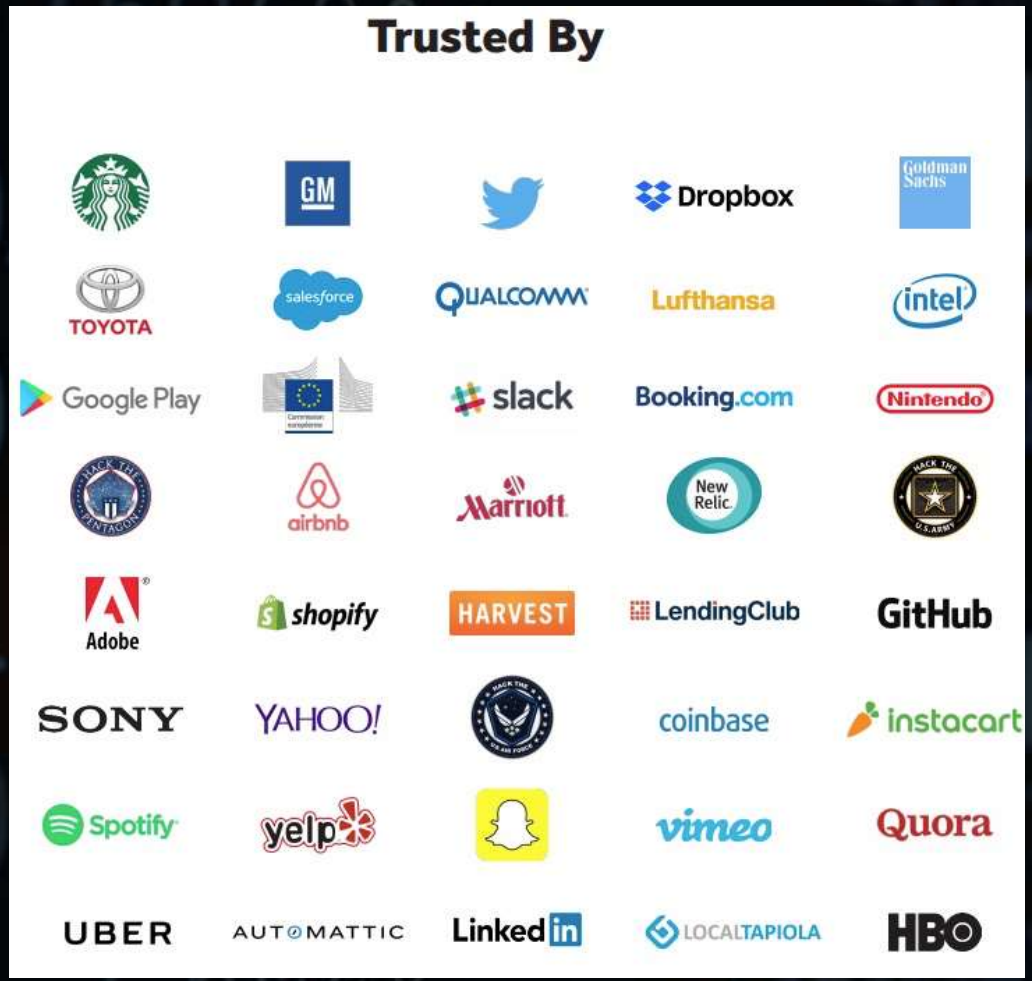
Veikleikaskönnun/ hefðbundnar árásarþjónustur

- Fámennur hópur einstaklinga sem vinna verkefnin og veikleikaskönnun treystir eingöngu á þekkta veikleika
- Hvati er oftast á fjölda veikleika frekar en áhersla á að sanna veikleika og áhrif þeirra
- Tól og þjónustur nýta sér að mestu eingöngu þekkta öryggisveikleika þar sem það borgar sig ekki að leita að nýjum veikleikum
- Lítil samkeppni sem felst fyrst þar sem forskot felst í öflun verkefnis frekar en gæði vinnunnar
- Kúnni greiðir fyrir skýrslu þar sem fókus er oft á fjölda veikleika frekar en sönnun og/eða alvarleika veikleika og þeirra áhrif
- Getur búið til kúltúr af ótta þar sem hvatinn er oft eingöngu hlíting við staðla frekar en eins örugg kerfi og gögn og kostur er

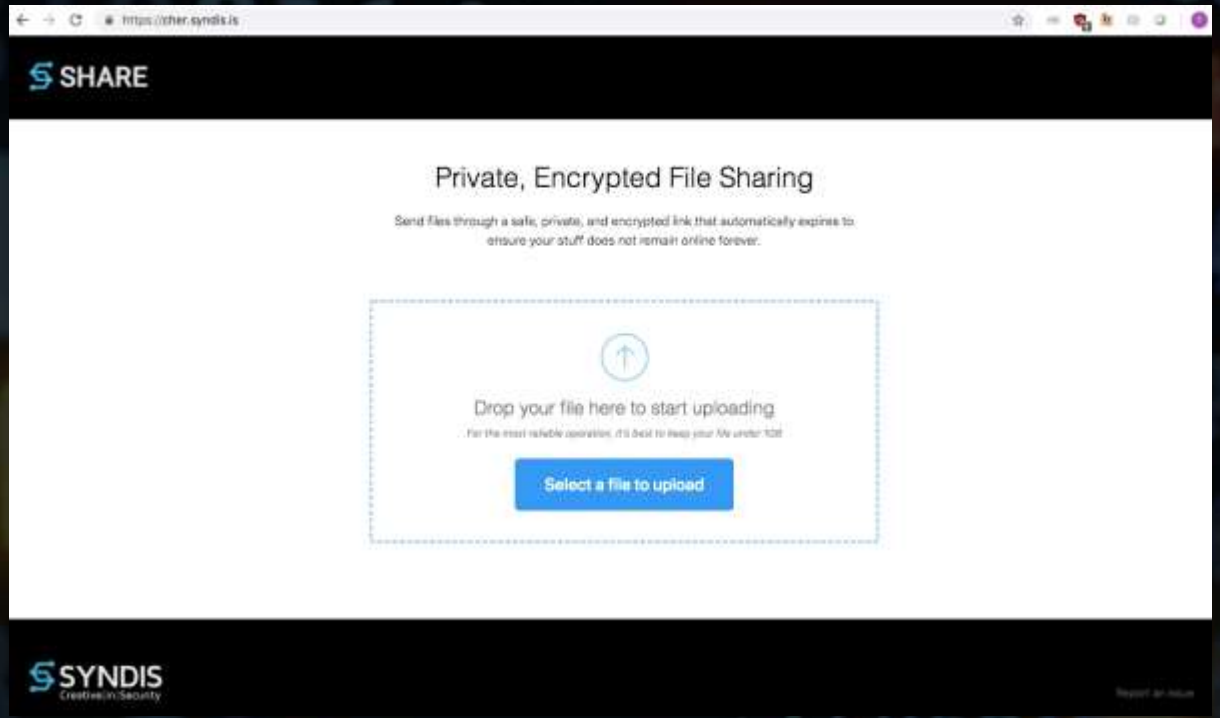
Virkar þetta?

https://www.wired.com/story/hack-the-pentagon-bug-bounty-results/

Trusted By

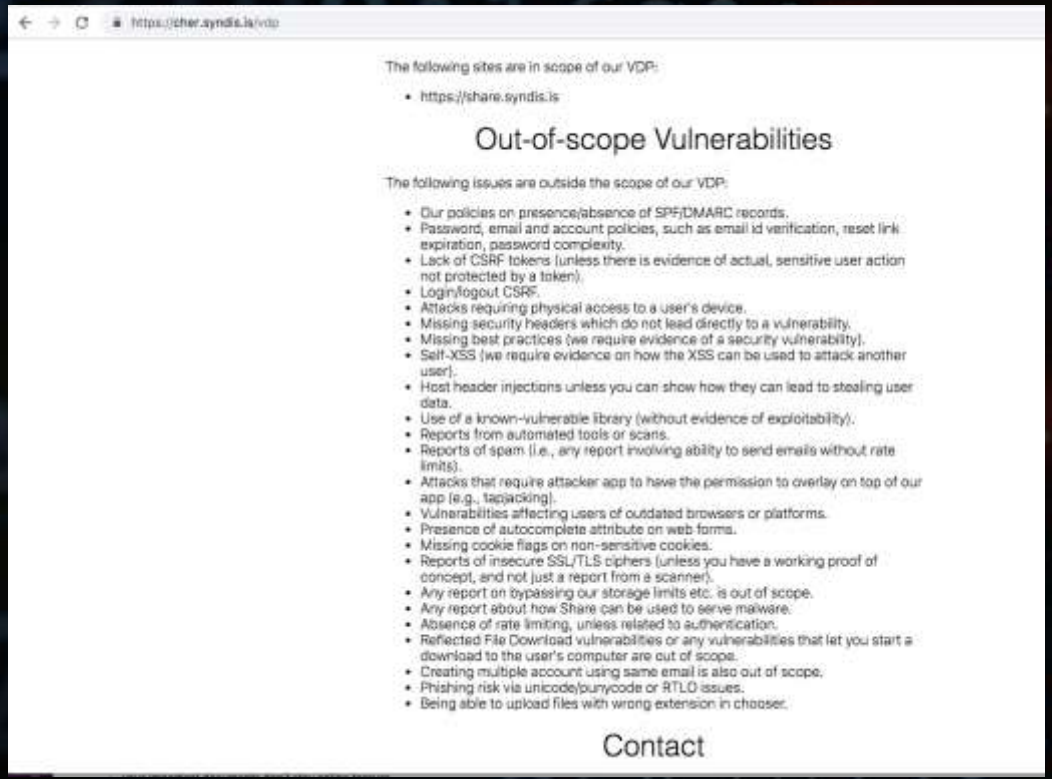

GM
Dropbox
Goldman Sachs
TOYOTA
salesforce
QUALCOMM
Lufthansa
intel
Google Play
slack
Booking.com
Nintendo
airbnb
Marriott
New Relic
Adobe
shopify
HARVEST
LendingClub
GitHub
SONY
YAHOO!
coinbase
instacart
Spotify
yelp
vimeo
Quora
UBER
AUTOMATTIC
LinkedIn
LOCALTAPIOLA
HBO

Súpa eigið meðal



https://cher.syndis.is/vdp

Súpa eigið meðal



The following sites are in scope of our VDP:

- https://share.syndis.is

Out-of-scope Vulnerabilities

The following issues are outside the scope of our VDP:

- Our policies on presence/absence of SPF/DMARC records.
- Password, email and account policies, such as email id verification, reset link expiration, password complexity.
- Lack of CSRF tokens (unless there is evidence of actual, sensitive user action not protected by a token).
- Login/logout CSRF.
- Attacks requiring physical access to a user's device.
- Missing security headers which do not lead directly to a vulnerability.
- Missing best practices (we require evidence of a security vulnerability).
- Self-XSS (we require evidence on how the XSS can be used to attack another user).
- Host header injections unless you can show how they can lead to stealing user data.
- Use of a known-vulnerable library (without evidence of exploitability).
- Reports from automated tools or scans.
- Reports of spam (i.e., any report involving ability to send emails without rate limits).
- Attacks that require attacker app to have the permission to overlay on top of our app (e.g., tapjacking).
- Vulnerabilities affecting users of outdated browsers or platforms.
- Presence of autocomplete attribute on web forms.
- Missing cookie flags on non-sensitive cookies.
- Reports of insecure SSL/TLS ciphers (unless you have a working proof of concept, and not just a report from a scanner).
- Any report on bypassing our storage limits etc. is out of scope.
- Any report about how Share can be used to serve malware.
- Absence of rate limiting, unless related to authentication.
- Reflected File Download vulnerabilities or any vulnerabilities that let you start a download to the user's computer are out of scope.
- Creating multiple account using same email is also out of scope.
- Phishing risk via unicode/punycode or RTLO issues.
- Being able to upload files with wrong extension in chooser.

Contact

https://cher.syndis.is/vdp

Hvernig finnur maður EKKI veikleika

Með því að hunsa þá leið sem veikleikar finnast!

Takk fyrir

@theorg1