從設計的思維出發
建立與開發安全的 Web 應用程式系統

陳偉雄 Wilson Chen

Who am I ?

- Works at Trend Micro in 10 years
- Focus on
  - Front-end development
  - Server-client architecture
  - Web Security
- Products
  - OfficeScan
  - Advanced Threat Assessment Service

Web Applications

Web Applications

Events

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會 社群 搜尋

新聞

ibon售票系統遭爆有漏洞，專家：曝露網站設計不嚴謹的老問題

統一超商的ibon售票系統旅遊專區遭發現有漏洞，利用瀏覽器檢視程式碼就能竄改票價、結算金額，就能以1元買到8張票。資安專家認為這曝露出國內常見的不夠嚴謹問題，系統設計上忽視對回傳數值的驗證，才會導致這樣離譜的問題發生。

文/ 蘇文彬 | 2015-09-17 發表

讚 4.7 萬 按讚加入iThome粉絲團 讚 1 分享 G+

Events

即時 | 娛樂 | 影音 | 社會 | 政治 | 生活 | 國際 | 新奇 | 運動 | 財經 | 寵物 | 名家

批台網頁資安爛　駭高鐵嫌犯酸：銅牆鐵壁卻沒關門

2015/08/20 09:04:00　友善列印　加入好友　讚 2　G+　A-　A　A+

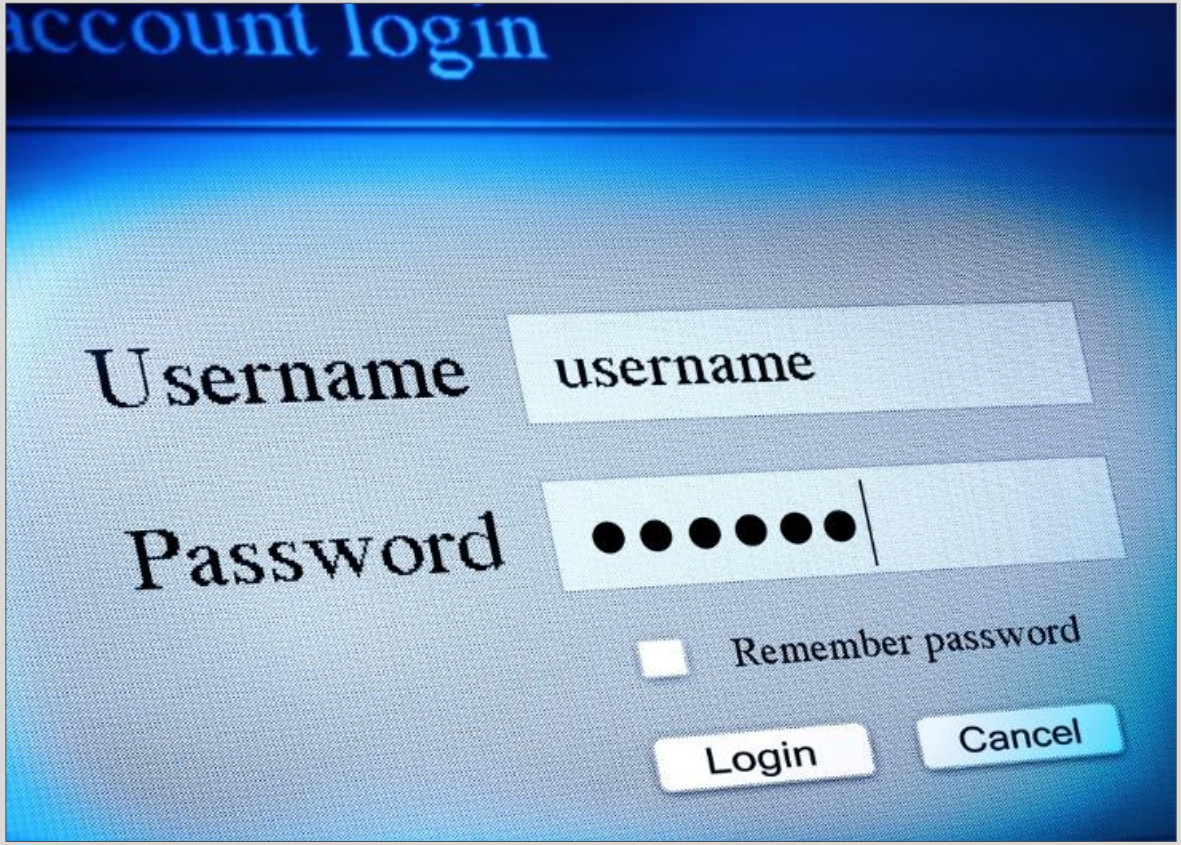
社會中心 / 綜合報導

警方最近破獲一起智慧型犯罪，嫌犯為北市「數位基因公司」董座許迺赫與其公司股東洪維昇，他們在今（2015）年3月至4月間數度入侵高鐵網站，利用網站設計漏洞來竄改票價、升等包廂，但落網後許嫌竟稱犯案「只是為了挑戰自己」，不是為了錢。許嫌犯案後還在個人臉書上發文酸民間企業的資安，說他們是「銅牆鐵壁卻忘了關門」。

Events


ibon 售票系統
107/1/1-107/12/31止，持單張ibon票券存根聯
星巴克 2杯相同飲料第二杯享半價優惠或美式好友分享
登入 | 註冊
APP下載
合作提案
退票查詢
訂單查詢
限時搶購
運動
交通
旅遊
電影
演唱會
音樂
展覽
親子
講座
舞蹈
戲劇
詳細搜尋
HOT
2018臺中世界花卉博覽會
傳藝園區門票退票
刷卡回饋春春飲搶最優13%
2018台灣國際兒童影展
MONKEY MAJIK IN TAIPEI 2018
凱蒂·佩芮 見證巡演 2018 台北站
刷卡回饋春春飲搶最優13%
Back to office！ibon mart咖啡買1送1up
2018
台灣國際兒童影展
TICFF
3/30(五)>4/7(六)
台北信義威秀影城
早鳥好康票
50元
3/9－3/15
單場享樂票
80元
3/16－4/7
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Audits
EditThisCookie
Styles
Computed
Event Listeners
DOM Breakpoints
凱蒂·佩芮 見證巡演 2018 台北站

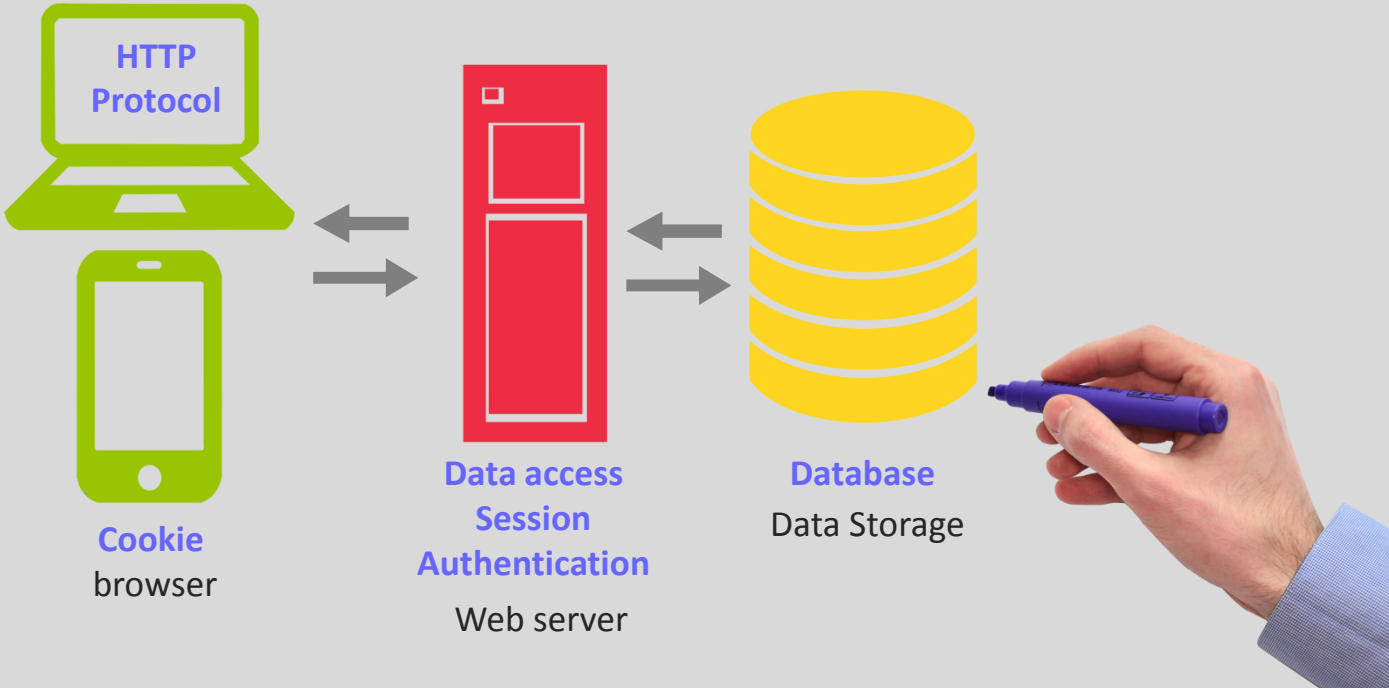
Events


account login
Username
username
Password
Remember password
Login
Cancel


Self-defense

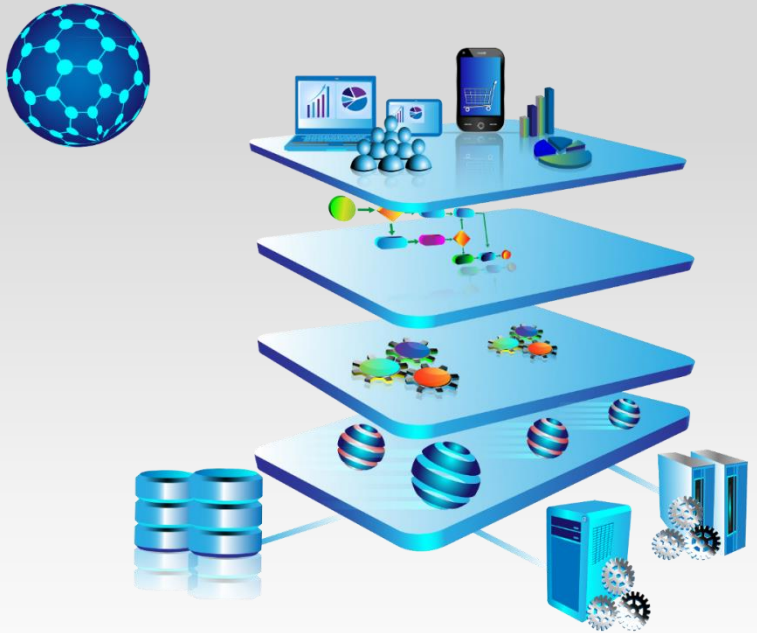
Web Application

- A client-server computer program
- Access over internet



Web Application Security Points

- Data access
- HTTP Protocol
- Database
- Session
- Cookie
- Authentication



Events

NETCRAFT

Contact Us | Subscribe

Search Netcraft Search

Home | News | Anti-Phishing | Security Testing | Internet Data Mining | Performance | About Netcraft

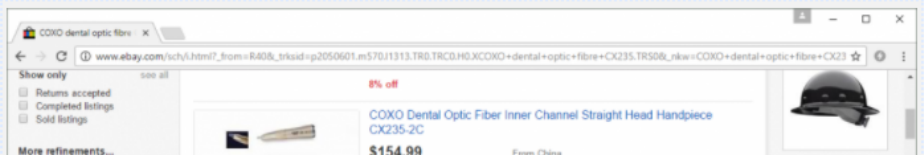
Hackers still exploiting eBay's stored XSS vulnerabilities in 2017

Fraudsters are still exploiting eBay's persistent cross-site scripting vulnerabilities to steal account credentials, years after a series of similar attacks took place. Worse still, many of the listings that exploited these vulnerabilities remained on eBay's website for more than a month before they were eventually removed.

All of the attacks stem from the fact that eBay allowed fraudsters to include malicious JavaScript in auction descriptions. Previous attacks exploited this vulnerability to place malicious redirect code on high-value vehicle listings, with the intention of stealing login credentials from other eBay members, whose accounts could then be used to list even more fraudulent vehicle listings.

But fraudsters are now using malicious scripts on a wide variety of lower-value items, including legitimate listings that had already been posted from reputable eBay accounts. Fraudsters have seemingly compromised these accounts and appended additional information to many of the members' existing listings – and this is where the malicious JavaScript is placed.

As can be seen below, the cybercriminals even used listings of dental tools to extract credentials from their victims, bypassing eBay's toothless listing policies in a similar way to the attacks that took place a few years ago.



Most Popular

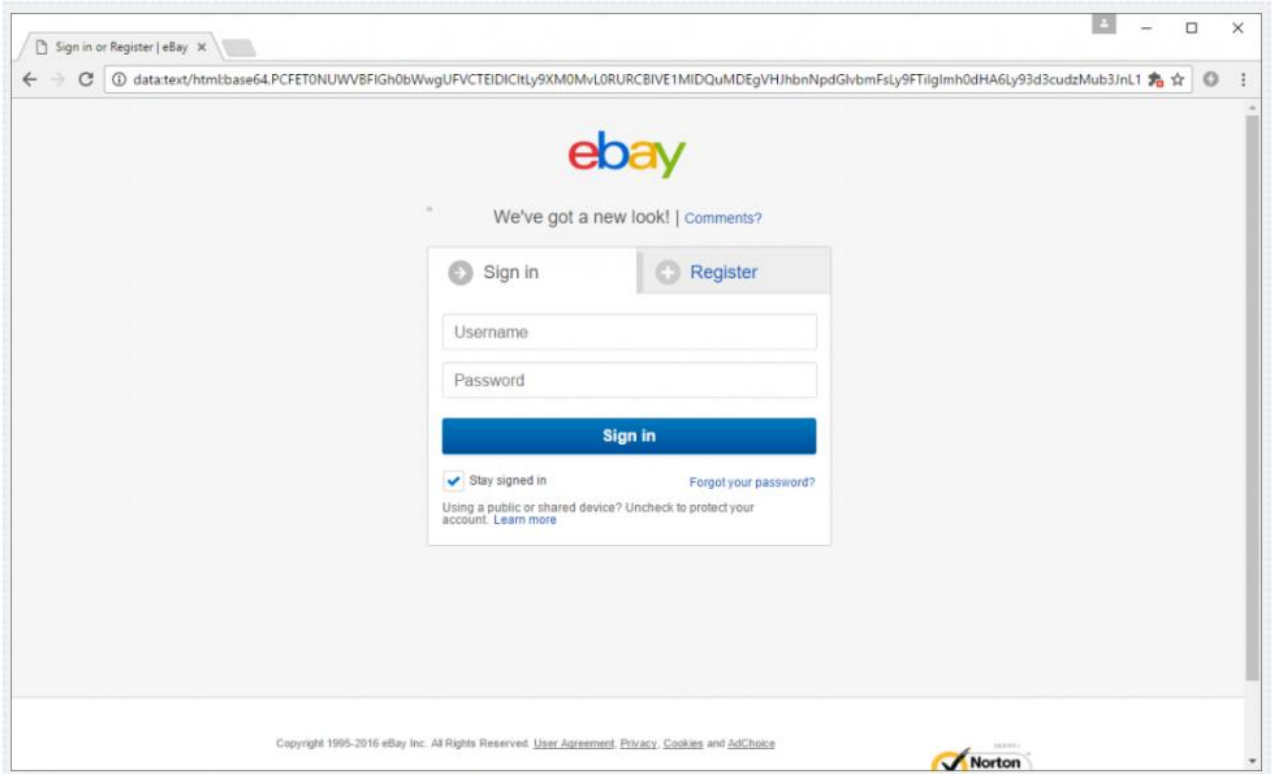
1. 95% of HTTPS servers vulnerable to trivial MITM attacks
2. January 2018 Web Server Survey
3. The hidden "well-known" phishing sites
4. December 2017 Web Server Survey
5. Google's POODLE affects oodles
6. HTTP Public Key Pinning: You're doing it wrong!
7. February 2018 Web Server Survey
8. Hackers still exploiting eBay's stored XSS vulnerabilities in 2017
9. Let's Encrypt and Comodo issue thousands of certificates for phishing
10. Cloud Wars: Alibaba becomes 2nd largest hosting company

Get in Touch

+44 (0) 1225 447500
info@netcraft.com

Events

But the malicious code in this listing executes as soon as the page has loaded, which causes it to be displayed for only a split second. In the blink of an eye — and without any further interaction — the victim is redirected to a spoofed login form:



Data access

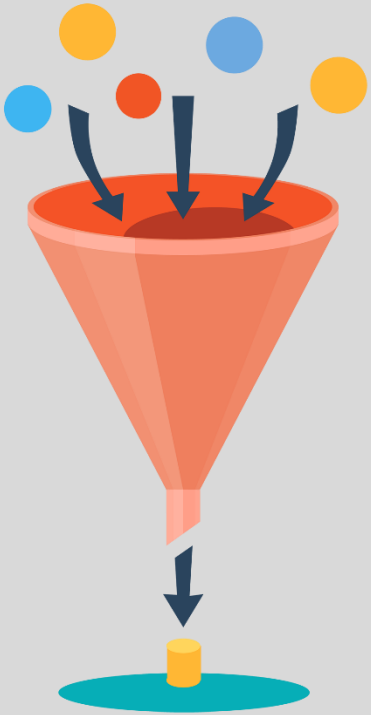
- Don’t trust input from client

Data access

- Don’t trust input from client
- Validation on server
  - ✓ Whitelist
  - ✓ Blacklist if you can’t whitelist

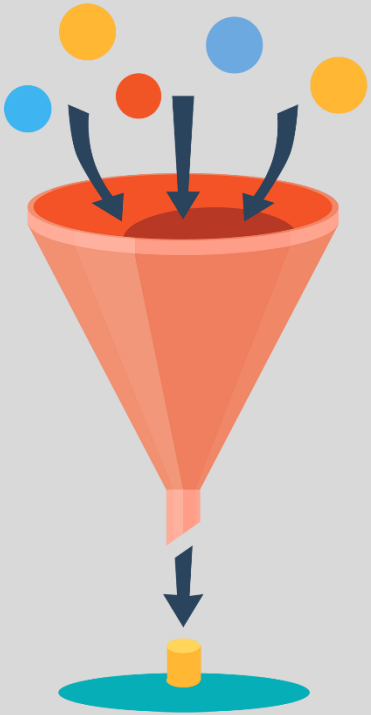
Data access

- Don’t trust input from client
- Validation on server
  - ✓ Whitelist
  - ✓ Blacklist if you can’t whitelist
- Sanitization



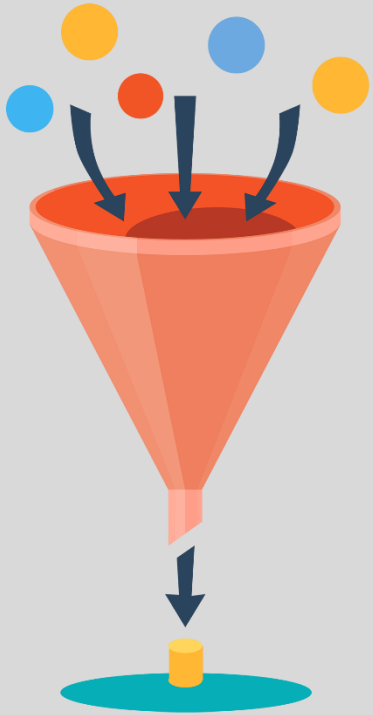
Data access

- Don’t trust input from client
- Validation on server
  - ✓ Whitelist
  - ✓ Blacklist if you can’t whitelist
- Sanitization
- Avoid reflecting input back to a user



Data access

- Don’t trust input from client
- Validation on server
  - ✓ Whitelist
  - ✓ Blacklist if you can’t whitelist
- Sanitization
- Avoid reflecting input back to a user
- Encode all application data output



HTTP Protocol

TechNews 3C新報 財經新報 讚 你和其他 45 萬人都說讚。 在粉絲團上追蹤我們

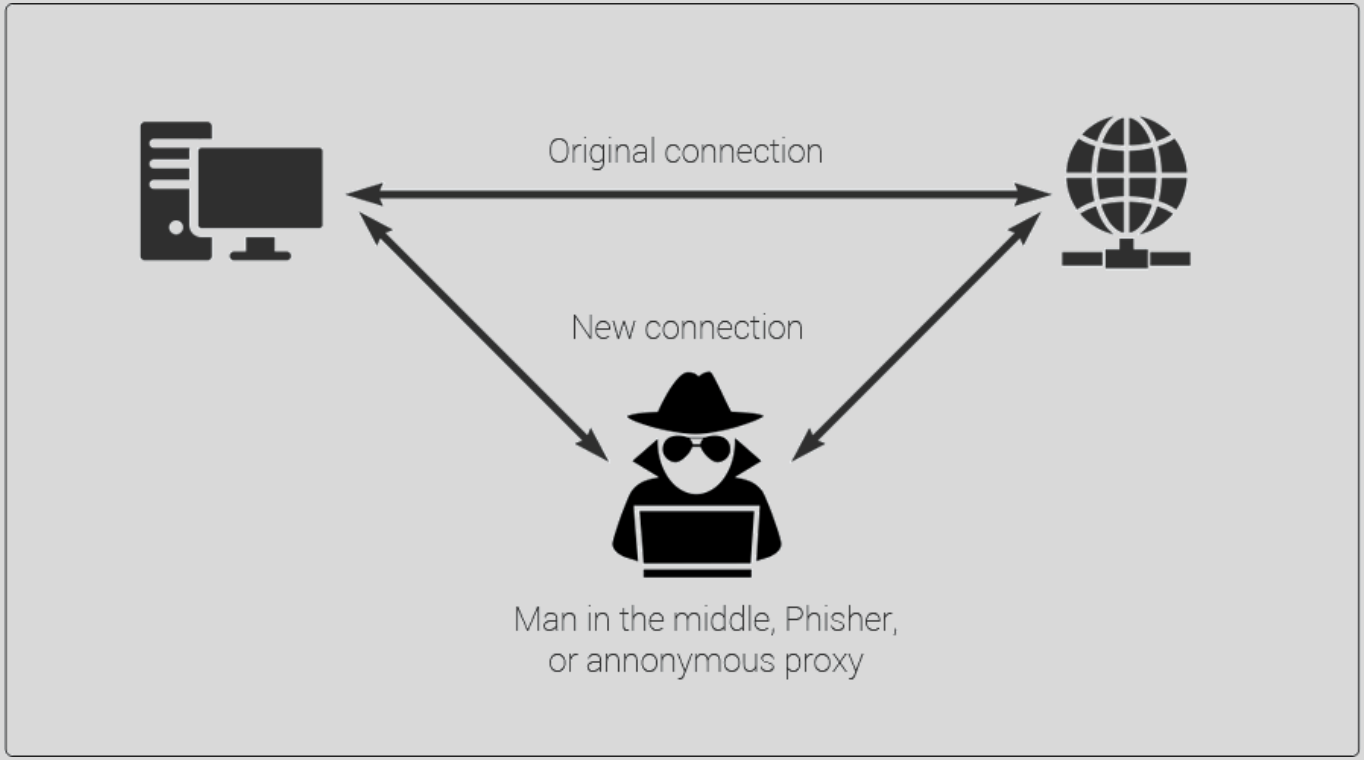
TechNews 科技新報

行動裝置 網路 名人堂 零組件 AI 人工智慧 尖端科技 生物科技 能源科技 人力資源 市場動態 企業部落格 精選 關於我們 廣告合作

政府網站使用 https 比率僅 11.2%，恐危及整體國家資安環境

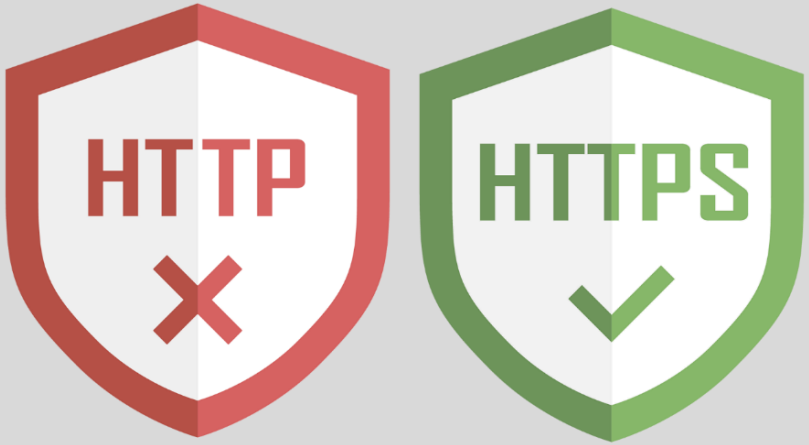
作者 Atkinson | 發布日期 2017 年 10 月 05 日 18:45 | 分類 網路, 資訊安全 Follow G+ 讚 32 分享

Man in the middle attack



HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS



HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security

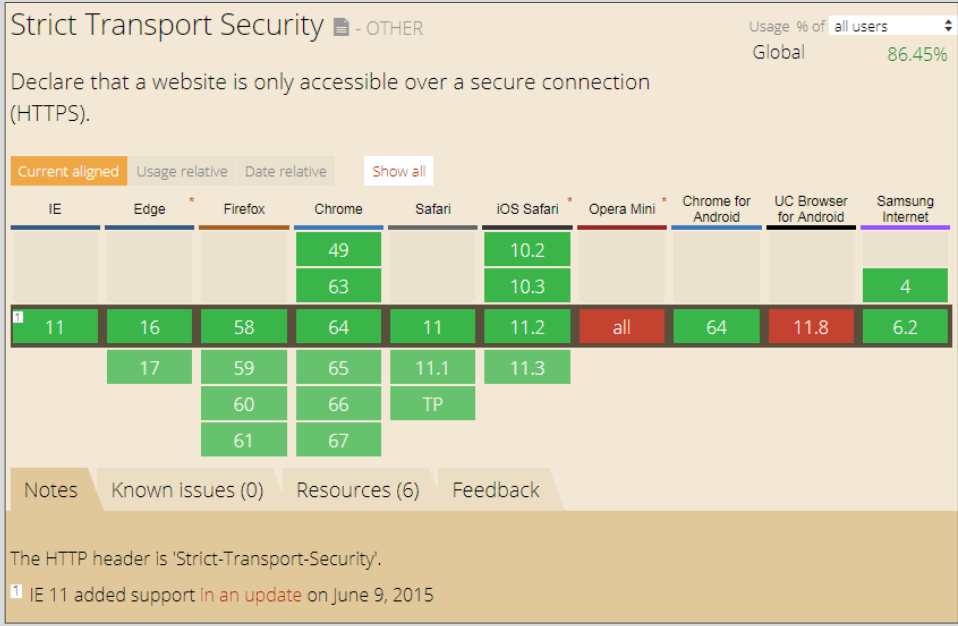
HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security



HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security
- HTTP Header

HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security
- HTTP Header
  - ✓ Content-Security-Policy

```
Content-Security-Policy: <policy-directive>; <policy-directive>
```

```
Content-Security-Policy: default-src https: 'unsafe-eval' 'unsafe-inline';
```

HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security
- HTTP Header
  - ✓ Content-Security-Policy
  - ✓ X-XSS-Protection

```
X-XSS-Protection: 0
X-XSS-Protection: 1
X-XSS-Protection: 1; mode=block
X-XSS-Protection: 1; report=<reporting-uri>
```

HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security
- HTTP Header
  - ✓ Content-Security-Policy
  - ✓ X-XSS-Protection
  - ✓ X-Frame-Options

```
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Frame-Options: ALLOW-FROM https://example.com/
```

HTTP Protocol

- HTTPS for all
  - ✓ SSL
  - ✓ TLS
- HSTS
  - ✓ Strict-Transport-Security
- HTTP Header
  - ✓ Content-Security-Policy
  - ✓ X-XSS-Protection
  - ✓ X-Frame-Options
  - ✓ X-Content-Type-Options

```
X-Content-Type-Options: nosniff
```

Database


Home
Hacking
Tech
Deals
Cyber Attacks
Malware
Spying
The Hacker News
Security in a serious way
+1,699,900
455,000
2,095,600
shutterstock
WordPress Plugin Used by 300,000+ Sites Found Vulnerable to SQL Injection Attack
Friday, June 30, 2017
Wang Wei
Share
1
Share
Tweet
Share
WordPress Hacking
SQL Injection Attack
ALIEN VAULT
GDPR Checklist:
A 9-Step Guide
GET YOUR FREE COPY TODAY
shutterstock

Database

- Sanitization

Database

- Sanitization
- Avoid building Query strings from user input

Database

- Sanitization
- Avoid building Query strings from user input
- Bind parameters for queries, not concatenate

Session

Welcome > Blog Home > Privacy > Session Hijacking Bug Exposed GitLab Users Private Tokens

by Chris Brook

August 31, 2017 , 5:00 pm

GitLab, the popular web-based Git repository manager, fixed a vulnerability recently that could have exposed its users to session hijacking attacks.

Top Stories

Ad Network Circumvents Ad-Blocking Tools To Run In-Browser Cryptojacker Scripts

March 1, 2018 , 12:40 pm

Supporters of Net Neutrality Vow to Fight Rule Changes

February 23, 2018 , 8:31 am

Session

Uncovering the GitLab Vulnerability

My first indication that there might be an issue with the GitLab service came when I saw that my session token was fully visible in my URL.

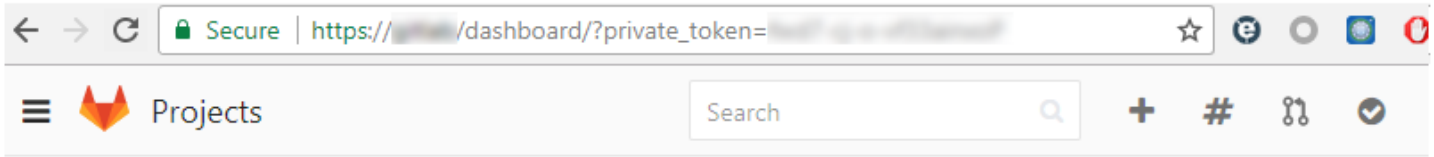


Fig. 1: Token is visible in URL.

A simple copy/paste of the token granted me access to every actionable item on the GitLab platform, e.g., user dashboards, account information, individual projects and website code. To make sure this wasn't a simple glitch, I used the same token on different browsers and machines—all with the same result.

Session

- Never expose session identifier

Session

- Never expose session identifier
- Protect session cookie with attribute

Session

- Never expose session identifier
- Protect session cookie with attribute
- Set proper expiration date

Session

- Never expose session identifier
- Protect session cookie with attribute
- Set proper expiration date
- Create a new session
  - ✓ after authenticating
  - ✓ when a user change privilege

Cookie

- Secure
- HttpOnly
- Expires
- Domain/Path

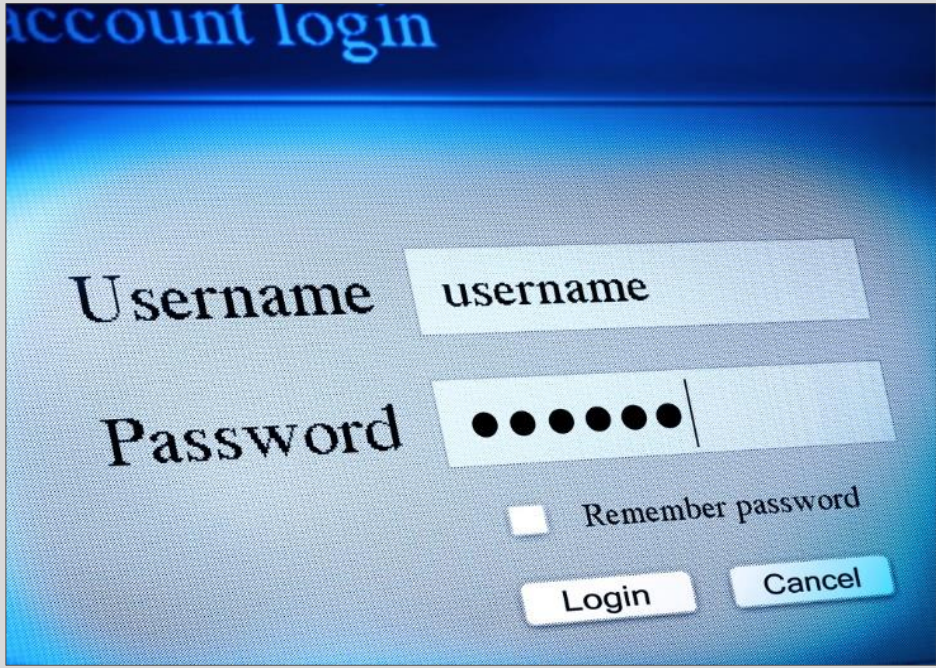
Cookie

- Secure
- HttpOnly
- Expires
- Domain/Path

```
Set-Cookie: id=a3fWa; Expires=Wed, 21 Oct 2015 07:28:00 GMT; Secure; HttpOnly
```

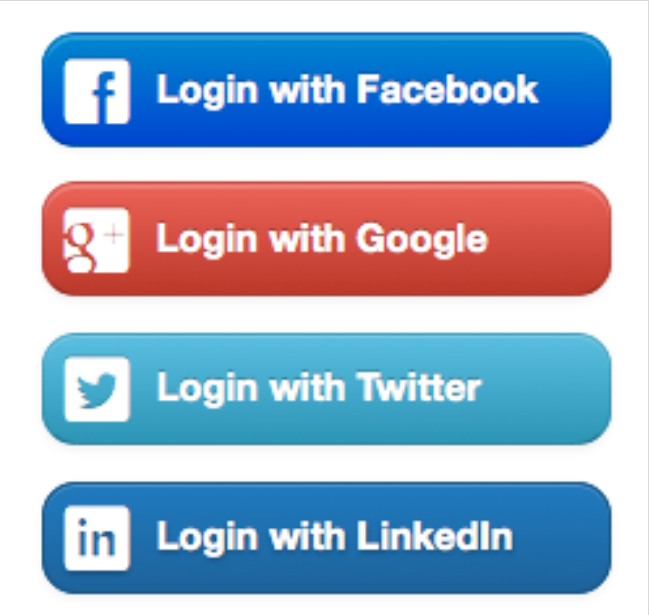
Authentication

- Password
  - ✓ Length
  - ✓ Hash and Salt
  - ✓ Avoid storing passwords for external services



Authentication

- Password
  - ✓ Length
  - ✓ Hash and Salt
  - ✓ Avoid storing passwords for external services
- SSO



Authentication

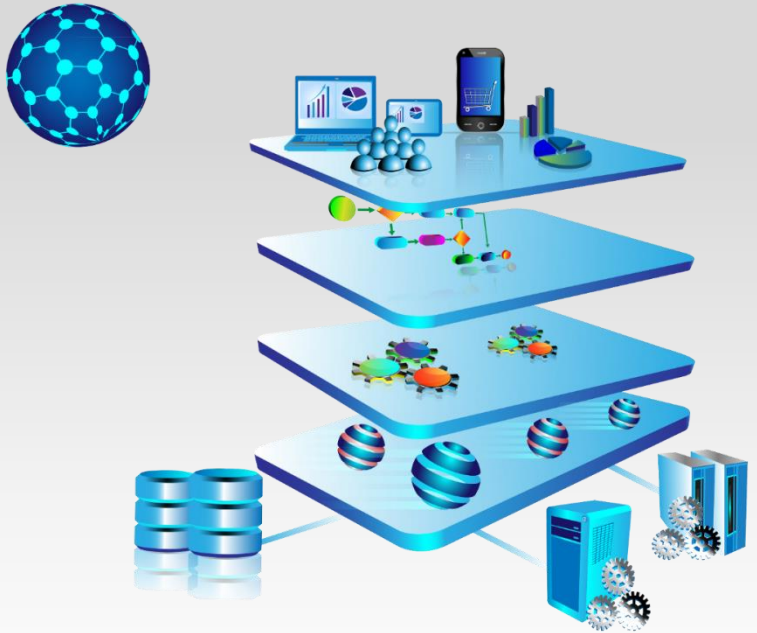
- Password
  - ✓ Length
  - ✓ Hash and Salt
  - ✓ Avoid storing passwords for external services
- SSO
- 2FA

Authentication

- Password
  - ✓ Length
  - ✓ Hash and Salt
  - ✓ Avoid storing passwords for external services
- SSO
- 2FA
- Conceal if users exist

Recap

- Data access
- HTTP Protocol
- Database
- Session
- Cookie
- Authentication



Q & A

Thank you.